Mark* VleS Functional Safety Systems for General Market
Volume I: System 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: July 2019


* 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>Rev</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td><em>Intrinsic Variables and Totalizers</em></td>
<td>Updated totalizer support by ControlST version</td>
</tr>
<tr>
<td></td>
<td><em>Signal Reference Structure</em></td>
<td>Updated the grounding recommendations for single control cabinet paragraph for clarification</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
<td>Acronym</td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>AWG</td>
<td>American Wire Gauge</td>
<td>PDM</td>
</tr>
<tr>
<td>BoP</td>
<td>Balance of Plant</td>
<td>PE</td>
</tr>
<tr>
<td>CDH</td>
<td>Control Data Highway</td>
<td>PLC</td>
</tr>
<tr>
<td>CMOS</td>
<td>Complementary Metal-Oxide ...</td>
<td>RLD</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Code/Check</td>
<td>RTD</td>
</tr>
<tr>
<td>DAC</td>
<td>Digital-to-Analog Converter</td>
<td>RTU</td>
</tr>
<tr>
<td>DCE</td>
<td>Data Communication Equipment</td>
<td>SDI</td>
</tr>
<tr>
<td>DCS</td>
<td>Distributed Control System</td>
<td>SIFT</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
<td>TMR</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
<td>TTL</td>
</tr>
<tr>
<td>EGD</td>
<td>Ethernet Global Data</td>
<td>UDH</td>
</tr>
<tr>
<td>EMC</td>
<td>Electromagnetic Capability</td>
<td>UDP</td>
</tr>
<tr>
<td>EMI</td>
<td>Electromagnetic Interference</td>
<td>UTC</td>
</tr>
<tr>
<td>ERA</td>
<td>Electrical Riser Angle</td>
<td>UTP</td>
</tr>
<tr>
<td>FE</td>
<td>Functional Earth</td>
<td>VLAN</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Position System</td>
<td>WAN</td>
</tr>
<tr>
<td>GTS</td>
<td>Global Time Source</td>
<td></td>
</tr>
<tr>
<td>HMI</td>
<td>Human-machine Interface</td>
<td></td>
</tr>
<tr>
<td>HRSG</td>
<td>Heat Recovery Steam Generator</td>
<td></td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical ...</td>
<td></td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and ...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Electronics Engineers</td>
<td></td>
</tr>
<tr>
<td>KP</td>
<td>Keyphasor*</td>
<td></td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
<td></td>
</tr>
<tr>
<td>MPU</td>
<td>Magnetic Pickup</td>
<td></td>
</tr>
<tr>
<td>MDH</td>
<td>Monitoring Data Highway</td>
<td></td>
</tr>
<tr>
<td>MTBF</td>
<td>Mean Time Between Failures</td>
<td></td>
</tr>
<tr>
<td>MTBFO</td>
<td>Mean Time Between Forced Outage</td>
<td></td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time To Repair</td>
<td></td>
</tr>
<tr>
<td>NEMA®</td>
<td>National Electrical Manufacturer’s Association</td>
<td></td>
</tr>
<tr>
<td>NFPA</td>
<td>National Fire Protection ...</td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
<td></td>
</tr>
<tr>
<td>PDH</td>
<td>Plant Data Highway</td>
<td></td>
</tr>
</tbody>
</table>
### Related Documents

<table>
<thead>
<tr>
<th>Document Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GEH-6860</td>
<td>Mark VIeS Control General Market Functional Safety Manual</td>
</tr>
<tr>
<td>GEH-6861</td>
<td>Mark VIeS Functional Safety System Equipment in Hazardous Locations (HazLoc) Instruction Guide</td>
</tr>
<tr>
<td>GEH-6862</td>
<td>ToolboxST User Guide for Mark VIeS Functional Safety Systems</td>
</tr>
<tr>
<td>GEI-100861</td>
<td>Mark VIeS Functional Safety Control Systems PDM Application Guide for General Market</td>
</tr>
<tr>
<td>GEI-100862</td>
<td>Mark VIeS Functional Safety Contact Input Module Summary Sheet</td>
</tr>
<tr>
<td>GEI-100863</td>
<td>Mark VIeS Functional Safety Relay Contact Output Module Summary Sheet</td>
</tr>
<tr>
<td>GEI-100864</td>
<td>Mark VIeS Functional Safety Vibration Input Module Summary Sheet</td>
</tr>
<tr>
<td>GEI-100865</td>
<td>Mark VIeS Functional Safety Universal Analog I/O Module Summary Sheet</td>
</tr>
<tr>
<td>GEI-100866</td>
<td>Mark VIeS Functional Safety Analog I/O Module Summary Sheet</td>
</tr>
<tr>
<td>GEI-100867</td>
<td>Mark VI and Mark VIeS Functional Safety UCSC Controller Summary Sheet</td>
</tr>
<tr>
<td>GEI-100868</td>
<td>Mark VI Modbus Master Communication Module Summary Sheet</td>
</tr>
<tr>
<td>GEI-100869</td>
<td>Mark VI Industrial Ethernet / IONet Switches Summary Sheet</td>
</tr>
<tr>
<td>GEI-100870</td>
<td>Mark VI Power Distribution Module Summary Sheet</td>
</tr>
<tr>
<td>GEH-6742</td>
<td>Mark VI and Mark VIeS Virtual Controller User Guide</td>
</tr>
<tr>
<td>GEI-100795</td>
<td>Trender Instruction Guide</td>
</tr>
<tr>
<td>GEI-100620</td>
<td>WorkstationST Alarm Viewer Instruction Guide</td>
</tr>
</tbody>
</table>
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 Control System Overview

1.1 Introduction ......................................................................................................................................... 11
1.2 Controllers ......................................................................................................................................... 13
1.3 IONet Switches .................................................................................................................................... 13
1.4 Distributed I/O Modules ..................................................................................................................... 14
1.5 Power Distribution .............................................................................................................................. 20
1.6 Redundancy Options ........................................................................................................................... 20
1.7 Reliability and Availability .................................................................................................................. 32
1.8 Component Part Numbers and Serial Numbers/Barcodes ................................................................. 39

## 2 Functional Safety

2.1 Safety Instrumented System (SIF) ......................................................................................................... 48
2.2 Risk Reduction ...................................................................................................................................... 49
2.3 Safety System Redundancy Options .................................................................................................... 50

## 3 Ethernet Networks

3.1 Overview ............................................................................................................................................... 55
3.2 IONet Layer ........................................................................................................................................ 59
3.3 Unit Control Layer .............................................................................................................................. 65
3.4 Supervisory Layer ............................................................................................................................... 69
3.5 Monitoring Layer ............................................................................................................................... 70
3.6 Enterprise Layer ................................................................................................................................ 70
3.7 Ethernet Cabling for Monitoring, Supervisory, and Unit Control Layers ........................................ 71
3.8 Third-party Communication Links ..................................................................................................... 75

## 4 Communication Protocols

4.1 OPC Protocols ..................................................................................................................................... 79
4.2 Modbus Protocol ................................................................................................................................. 82
4.3 Ethernet Global Data (EGD) ............................................................................................................... 84
4.4 System Data Interface (SDI) Protocol ................................................................................................. 86
4.5 Network Time Protocol (NTP) ............................................................................................................ 87
4.6 Fieldbus Communications .................................................................................................................. 89

## 5 Technical Regulations, Standards, and Environment

5.1 Safety Standards ................................................................................................................................ 91
5.2 Conditions for Compliance ................................................................................................................ 92
5.3 Electrical ............................................................................................................................................ 93
5.4 Environment ..................................................................................................................................... 95

## 6 Installation Guidelines

6.1 Installation Support .............................................................................................................................. 101
6.2 Equipment Receiving and Handling ................................................................................................. 104
6.3 Power Requirements .......................................................................................................................... 106
6.4 Grounding ........................................................................................................................................... 107
6.5 Cable Separation and Routing .......................................................................................................... 115
6.6 Power and I/O Field Wiring ............................................................................................................... 121
6.7 Connecting Power to the System ...................................................................................................... 124
6.8 Startup Checks .................................................................................................................................. 125
1 Control System Overview

1.1 Introduction

The Mark* VIeS Functional Safety System is used for safety-critical applications in the general market that conform to IEC® 61508. Its architecture enables unique engineered solutions for a variety of large industrial applications. It is used in a wide variety of control and protection applications, including steam, gas, and wind turbines, power generation balance of plant (BoP), deep sea drilling, desalinization, gas compression, and other facility-wide equipment management systems. The control system primarily consists of three hardware components: controllers, I/O modules, and I/O network (IONet) switches. It provides more options for redundancy, better maintainability, and greater capability for locating I/O modules closer to the controlled equipment. It features high-speed, network input/output (I/O) for Simplex, Dual, and Triple Modular Redundant (TMR) systems. Industry-standard Ethernet communications are used for I/O, controllers, and supervisory interface to operator and maintenance stations, as well as third-party systems. It also provides quality, time-coherent data at controller and plant level for effectively managing control system equipment.

The ControlST* Software Suite, which contains the ToolboxST* and WorkstationST* applications, is used for programming, configuration, trending, and analyzing diagnostics.

The Mark VIeS Safety controller and I/O can operate independently or integrated with the rest of the Mark VIe controllers for safety-critical applications that conform to IEC® 61508. It also uses ControlST to simplify maintenance while retaining a unique set of certified hardware and software blocks. ToolboxST provides a means to lock or unlock the Mark VIeS Safety controller for configuration and safety instrumented function (SIF) programming.

The information in this document applies to the overall Mark* VIe control system or Mark VIeS Functional Safety System control products; however, your application may not be licensed to access full system capability and I/O packs as described in this document. For example, the Mark VIeS Functional Safety System for General Markets only utilizes the following I/O packs:

- Analog I/O (YAIC)
- Universal Analog (YUAA)
- Vibration Input Monitor (YVIB)
- Relay Output (YDOA)
- Discrete Contact Input (YDIA)
- Power Distribution System Diagnostics (PPDA)
- Serial Modbus Communication (PSCA)
- Mark VIeS Safety Controller (UCCS2x)
- Mark VIe Controller for Gateway (UCSCH1x)
Typical Architecture for Large Industrial Functional Safety Systems
1.2 Controllers

In Functional Safety Systems, the Mark VIe controller serves as a gateway to the Mark VIeS Safety controller. The controller is a stand-alone, single-board controller with scalable processing power. It includes built-in power supplies and requires no batteries or jumper settings. Controllers run the ControlST Software Suite, providing a common software environment for turbine and generator excitation controls in the power island and balance of plant equipment to simplify operations and maintenance. The Mark VIeS Safety controller is IEC 61508 certified to Safety Integrity Level (SIL) 3. Refer to Mark VIeS Control General Market Functional Safety Manual (GEH-6860) for more information.

The controller is loaded with software specific to its application, for example steam, gas, land-marine (LM), BoP, offshore drilling, desalination, DCS, wind power conversion, and so forth. It can run Relay Ladder Diagrams (RLD) or blocks. The IEEE® 1588 protocol is used through the R, S, and T I/O networks (IONet) to synchronize the clock of the I/O modules and controllers to within ±100 microseconds. Data is transferred to and from the control system database in the controller over the I/O networks (IONet). IONet data includes process inputs/outputs to the I/O packs.

In a dual system, IONet data also includes:

- Internal state values and initialization information from the designated controller
- Status and synchronization information from both controllers

In a triple module redundant (TMR) system, IONet data also includes:

- Internal state values for voting and status and synchronization information from all three controllers
- Initialization information from the designated controller

For more information on the Mark VIeS Safety controller, refer to Mark VIeS Functional Safety Systems for General Market Volume II: System Guide for General-purpose Applications (GEH-6855_Vol_II), the chapter Controllers.

1.3 IONet Switches

GE’s Industrial Ethernet 10/100 switches (ESWA and ESWB) provide the performance and features needed in today’s real-time industrial control systems. Use 8-port ESWA or 16-port ESWB Ethernet switches in all control system I/O networks to maintain the reliability needed for I/O module reception of controller outputs.

For more information on the IONet switches, refer to Mark VIeS Functional Safety Systems for General Market Volume II: System Guide for General-purpose Applications (GEH-6855_Vol_II), the chapter Unmanaged Ethernet Switches.
1.4 **Distributed I/O Modules**

The I/O modules contain three basic parts: terminal board, terminal block, and I/O pack. The terminal board mounts to the cabinet and comes in two basic types: S and T. The I/O pack mounts to the terminal board J-port connector. Both terminal board types provide the following features:

- Terminal blocks for I/O wiring
- Mounting hardware
- Input isolation and protection
- I/O pack connectors
- Unique electronic ID

### 1.4.1 I/O Packs

I/O packs in the Mark VIeS Functional Safety System have a common processor board and a data acquisition board that is unique to the type of connected device. I/O packs on each terminal board digitize the I/O variables, perform algorithms, and communicate with the Mark VIeS Safety controller.

The I/O pack provides fault detection through a combination of special circuitry in the data acquisition board and software running in the Central Processing Unit (CPU) board. The fault status is transmitted to and used by the controllers. The I/O pack transmits inputs and receives outputs on both network interfaces if connected.

Each I/O pack also sends an identification message (ID packet) to the main controller when requested. The packet contains, the hardware catalog number of the I/O board, the hardware revision, the board barcode serial number, the firmware catalog number, and the firmware version. The I/O packs have a temperature sensor that is accurate to within ±2°C (±3.6 °F). Every I/O pack temperature is available in the database and can be used to generate an alarm.
1.4.2 Terminal Boards

Signal flow begins with a sensor connected to a terminal block on a board. Wide and narrow terminal boards are arranged in vertical columns of high and low-level wiring. An example of a wide board is a board that contains magnetic relays with fused circuits for solenoid drivers. A shield strip is provided to the left of each terminal block. It can be connected to a metal base for immediate grounding or floated to allow individual ground wires from each board to be wired to a centralized, cabinet ground strip.
1.4.2.1 T-type

T-type terminal boards typically fan the sensor inputs to three separate I/O packs. Usually, the TMR board hardware votes the outputs from the three I/O packs. T-type boards contain two, 24-point, barrier-type, removable, terminal blocks. Each point can accept two 3.0 mm (0.12 in) (#12AWG) wires with 300 V insulation per point with either spade or ring-type lugs. In addition, captive clamps are provided for terminating bare wires. Screw spacing is 9.53 mm (0.375 in) minimum and center-to-center.

**Note** Some application-specific TMR terminal boards do not fan inputs or vote the outputs.

These terminal blocks have the following features:

- Black in color with white number labels
- Terminal rating is 300 V, 10 A
- UL recognized
- Recommended screw tightening torque is 7 lb-in (0.8 Nm).
1.4.2.2 S-type

S-type boards provide a single set of screws for each I/O point and allow a single I/O pack to condition and digitize the I/O. They are half the size of T-type boards and are standard base mounted but can also be DIN-rail mounted. These boards can be used for simplex, dual, or dedicated triple redundant sensors by using one, two, or three modules.

S-type boards have Euro-style, box type terminal blocks. Some boards are available as either removable or fixed terminal block versions. S-type board terminal blocks accept one 2.05 mm (0.08 in) (#12 AWG) wire or two 1.63 mm (0.06 in) (#14 AWG) wires, each with 300 V insulation per point. Screw spacing is 5.08 mm (0.2 in) minimum and center-to-center.

These terminal blocks have the following features:

- Green in color with number labels.
- Terminal rating is 300 V, 10 A
- UL and CSA recognized
- Recommended screw tightening torque is 5 lb-in (0.5 - 0.6 Nm)
### 1.4.3 I/O Module Types

#### Mark VIeS Functional Safety System I/O Types

<table>
<thead>
<tr>
<th>I/O Pack</th>
<th># of Packs</th>
<th>Terminal Board</th>
<th>Mark VIeS Safety I/O Types</th>
<th>Connector Type</th>
<th>Removable</th>
</tr>
</thead>
<tbody>
<tr>
<td>YAI51B</td>
<td>1, 3</td>
<td>TBAIS1C</td>
<td>10 analog inputs (voltage, 0-20 mA)</td>
<td>Box</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>STAIS2A</td>
<td>2 analog outputs (0-20 mA)</td>
<td>Box</td>
<td>Yes</td>
</tr>
<tr>
<td>YDI51B</td>
<td>1, 2, 3</td>
<td>TBCIS2C</td>
<td>24 discrete inputs w/ group isolation (24 V dc, 48 V dc, or 125 V dc)</td>
<td>Box</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>1, 2, 3</td>
<td>TBCIS3C</td>
<td></td>
<td>Box</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>STCIS2A</td>
<td></td>
<td>Box</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>STCIS4A</td>
<td></td>
<td>Box</td>
<td>Yes</td>
</tr>
<tr>
<td>YVI51B</td>
<td>1, 3</td>
<td>TVBAS2B</td>
<td>Refer to GEH-6855_Vol_II for a complete list of supported inputs. TVBAS2B includes buffered outputs and BNC connectors.</td>
<td>Box</td>
<td>Yes</td>
</tr>
<tr>
<td>YDO51B</td>
<td>1, 3</td>
<td>TRLYS1B</td>
<td>12 type C mechanical relays with 6 solenoids, coil diagnostics (115/230 V ac, 24/48/125 V dc), and SOE for relay outputs</td>
<td>Barrier</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>1, 3</td>
<td>TRLYS1D</td>
<td>6 type A mechanical relays for solenoids, solenoid impedance diagnostics (24/125 V dc), and SOE for relay outputs</td>
<td>Barrier</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>TRLYS1F</td>
<td>36 mechanical relays, 12 voted type A normally open (NO) outputs (115 V ac, 24/48/125 V dc)</td>
<td>Barrier</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>TRLYS2F</td>
<td>36 mechanical relays, 12 voted type B normally closed (NC) outputs (115 V ac, 24/48/125 V dc)</td>
<td>Barrier</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>SRLYS2A</td>
<td>12 type C mechanical relays (115/230 V ac, 24/48/125 V dc) (refer to the table Optional Daughter Boards), and SOE for relay outputs</td>
<td>Box</td>
<td>Yes</td>
</tr>
<tr>
<td>YUA51A</td>
<td>1</td>
<td>SUAAS1A</td>
<td>16 Simplex Analog I/O channels can be configured as: Thermocouple (TC), Resistance Temperature Device (RTD), voltage input (± 5 V or ± 10 V), 4 to 20 mA current input, 0 to 20 mA current output, pulse accumulator, digital input (DI), or digital output (DO)</td>
<td>Box</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Optional Daughter Boards

<table>
<thead>
<tr>
<th>Daughter Board</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>WROBH1A</td>
<td>Adds solenoid interface to first 6 relay circuits</td>
</tr>
<tr>
<td>WROF1H1A</td>
<td>Adds fuse in COM leg of all 12 relay circuits</td>
</tr>
<tr>
<td>WROGH1A</td>
<td>Adds fuse power distribution in COM leg of all 12 relay circuits</td>
</tr>
</tbody>
</table>

#### Fieldbus I/O Types

<table>
<thead>
<tr>
<th>I/O Pack</th>
<th>Qty per Board</th>
<th>Board</th>
<th>Communications Types</th>
<th>Connector Type</th>
<th>Removable</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSCAH1B</td>
<td>1</td>
<td>SCAH1A</td>
<td>6 Modbus Master serial or 1 Modbus Ethernet</td>
<td>Box</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>SCAH2A</td>
<td>6 Modbus Master serial or 1 Modbus Ethernet</td>
<td>Box</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### 1.4.4 Terminal Board Fuse Details

The following tables are provided for the customer to assist in inventory management of the replaceable fuses used on some terminal boards.

#### Discrete I/O Terminal Board Fuses

<table>
<thead>
<tr>
<th>Board</th>
<th>Fuse Designator</th>
<th>GE Part #</th>
<th>Fuse Rating</th>
<th>MFR #</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS400TRLYS1B</td>
<td>FU1, FU2, FU3, FU4, FU5, FU6, FU7, FU8, FU9, FU10, FU11, FU12</td>
<td>64G5005-011+RFU7</td>
<td>FUSE, 3.15A, 500VAC/400VDC</td>
<td>LITTELFUSE 04773.15MXP</td>
</tr>
<tr>
<td>IS400TRLYS1D</td>
<td>FU1, FU2, FU3, FU4, FU5, FU6, FU7, FU8, FU9, FU10, FU11, FU12</td>
<td>64G5005-011+RFU7</td>
<td>FUSE, 3.15A, 500VAC/400VDC</td>
<td>LITTELFUSE 04773.15MXP</td>
</tr>
<tr>
<td>IS400WROBH1A</td>
<td>FU1, FU2, FU3, FU4, FU5, FU6, FU7, FU8, FU9, FU10, FU11, FU12</td>
<td>64G5005-011+RFU7</td>
<td>FUSE, 3.15A, 500VAC/400VDC</td>
<td>LITTELFUSE 04773.15MXP</td>
</tr>
<tr>
<td>IS400WROFH1A</td>
<td>FU1, FU2, FU3, FU4, FU5, FU6, FU7, FU8, FU9, FU10, FU11, FU12</td>
<td>64G5005-011+RFU7</td>
<td>FUSE, 3.15A, 500VAC/400VDC</td>
<td>LITTELFUSE 04773.15MXP</td>
</tr>
<tr>
<td>IS400WROGH1A</td>
<td>FU1, FU2, FU3, FU4, FU5, FU6, FU7, FU8, FU9, FU10, FU11, FU12</td>
<td>64G5005-011+RFU7</td>
<td>FUSE, 3.15A, 500VAC/400VDC</td>
<td>LITTELFUSE 04773.15MXP</td>
</tr>
</tbody>
</table>

#### Power Distribution Terminal Board Fuses

<table>
<thead>
<tr>
<th>Board</th>
<th>Fuse Designator</th>
<th>GE Part #</th>
<th>Fuse Rating</th>
<th>MFR #</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS400JPDDG1A</td>
<td>FU1N, FU1P, FU2N, FU2P, FU3N, FU3P, FU4N, FU4P, FU5N, FU5P, FU6N, FU6P</td>
<td>323A2396P96+FU6</td>
<td>FUSE 15A</td>
<td>LITTELFUSE 314015P</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>COOPER BUSSMANN ABC-15</td>
</tr>
<tr>
<td>IS400JPDDG2A</td>
<td>FU1N, FU1P, FU2N, FU2P, FU3N, FU3P, FU4N, FU4P, FU5N, FU5P, FU6N, FU6P</td>
<td>323A2396P96+FU6</td>
<td>Empty fuse holders with black caps accepting 5 X 20 mm (0.20 X 0.79 in) fuses</td>
<td>LITTELFUSE 314015P</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>COOPER BUSSMANN ABC-15</td>
</tr>
<tr>
<td>IS400JPDDG3A</td>
<td>FU1N, FU1P, FU2N, FU2P, FU3N, FU3P, FU4N, FU4P, FU5N, FU5P, FU6N, FU6P</td>
<td>323A2396P96+FU6</td>
<td>Empty fuse holders with grey caps accepting 31.75 X 6.35 mm (1.25 X 0.25 in) fuses</td>
<td>LITTELFUSE 314015P</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>COOPER BUSSMANN ABC-15</td>
</tr>
<tr>
<td>IS400JPDEG1A</td>
<td>FU11, FU12, FU21, FU22, FU31, FU32</td>
<td>323A2396P20+FU6</td>
<td>FUSE 7 A</td>
<td>LITTELFUSE 312007P</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>COOPER BUSSMANN AGC-7</td>
</tr>
<tr>
<td></td>
<td>FA1, FA2, FUB1, FUB2, FUC1, FUC2</td>
<td>323A2396P96+FU6</td>
<td>FUSE 15A</td>
<td>LITTELFUSE 314015P</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>COOPER BUSSMANN ABC-15</td>
</tr>
<tr>
<td>IS400JPDGH1A</td>
<td>FU1, FU2, FU3, FU4, FU5, FU6, FU7, FU8</td>
<td>323A2396P250+FU6</td>
<td>FUSE 10A 250V SLOW BLOW</td>
<td>LITTELFUSE 326010</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>COOPER BUSSMANN MDA-10</td>
</tr>
<tr>
<td>IS400JPDGH1A</td>
<td>FU10, FU11, FU12, FU13, FU14, FU15, FU16, FU17, FU18, FU19, FU20, FU21, FU22, FU23</td>
<td>323A2396P96+FU6</td>
<td>FUSE 15A 3AB ABC FAST ACTING</td>
<td>LITTELFUSE 314015P</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>COOPER BUSSMANN ABC-15</td>
</tr>
<tr>
<td>IS400JPDGH2A</td>
<td>FU1, FU2, FU3, FU4, FU5, FU6, FU7, FU8</td>
<td>323A2396P250+FU6</td>
<td>FUSE 10A 250V SLOW BLOW</td>
<td>LITTELFUSE 326010</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>COOPER BUSSMANN MDA-10</td>
</tr>
<tr>
<td>IS400JPDGH2A</td>
<td>FU10, FU11, FU12, FU13, FU14, FU15, FU16, FU17, FU18, FU19, FU20, FU21, FU22, FU23</td>
<td>323A2396P96+FU6</td>
<td>FUSE 15A 3AB ABC FAST ACTING</td>
<td>LITTELFUSE 314015P</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>COOPER BUSSMANN ABC-15</td>
</tr>
</tbody>
</table>
1.5 Power Distribution

The Mark VIeS Functional Safety System are designed to operate on a flexible, modular selection of power sources. The power distribution modules (PDM) support 115/230 V ac, 24 and 125 V dc power sources in many redundant combinations. The power applied is converted to 28 V dc for operation of the I/O packs, controllers, and switches.

Note Refer to Mark VIe and Mark VIeS Safety Systems Power Distribution Modules (PDM) Application Guide (GEI-100861). The JPDS or JPDG core power distribution board allows for the optional attachment of a PPDA I/O pack for system feedback.

The PDM can be divided into two substantially different categories, the core distribution system, and the branch circuit elements. They serve as the primary power management for a cabinet or series of cabinets. The branch circuit elements take the core output and fan it into individual circuits for consumption in the cabinets. Branch circuits provide their own feedback mechanisms, which are not part of the feedback provided by the PPDA I/O pack. The wide variety of power distribution components available for use with the Mark VIeS Functional Safety System allow for a flexible and scalable power distribution solution.

1.6 Redundancy Options

The Mark VIeS Functional Safety System provides scalable levels of redundancy. The basic system is a single (simplex) controller with simplex I/O and one network. The Dual system has two controllers, singular or fanned TMR I/O and dual networks, which provides added reliability and online repair options. The TMR system has three controllers, singular or fanned TMR I/O, three networks, and state voting between controllers providing the maximum fault detection and availability.

1.6.1 Controller Redundancy

Controller redundancy consists of the following:

- Simplex controller
- Dual controllers
- Triple Modular Redundant (TMR) controllers
1.6.1.1 Simplex Controller

The simplex control architecture contains one controller connected to an Ethernet interface through the Ethernet network (IONet). No redundancy is provided and no online repair of critical functions is available. Online replacement of non-critical I/O (that where the loss of the I/O does not stop the process) is possible.

Each I/O pack delivers an input packet at the beginning of the frame on its primary network. The controller sees the inputs from the I/O modules, performs application code, and then delivers an output packet(s) for all I/O modules. The following diagram displays typical simplex controller architecture.
1.6.1.2 Dual Controllers

The dual control architecture contains two controllers, two IONets, and singular or fanned TMR I/O modules.

The dual control architecture reliability can be significantly better than the single controller. The network and controller components are redundant and can be repaired online. The I/O reliability can be mixed and matched to meet varying requirements.

In a dual control system, both controllers receive inputs from the I/O modules on both networks and transmit outputs on their respective IONet continuously. When a controller or network component fails, the system continues operating. I/O packs receive inputs from both controllers, but prefer the designated controller. If the only packet received is from a non-designated controller, then the I/O pack will use that packet.

**Note** With dual controllers, the level of I/O reliability can be varied to meet the application needs because not all I/O has to be dual redundant.

The Mark VIeS Safety controllers listen for the data on both networks at power on. The channel that delivers the first valid packet becomes the preferred network. As long as the data arrives on that channel the controller uses this data. When the preferred channel does not deliver the data in a frame, the other channel becomes the preferred channel as long as valid data is supplied. This prevents a given controller from bouncing back and forth between two sources of data. This does mean that different controllers may have separate preferred sources of data but this can also happen if any component fails.

The I/O modules listen for the data on both networks at power on. If the packet from the designated controller is received, that one is the preferred network. When the designated controller packet does not arrive in a given frame, the other channel is used as long as valid data is supplied.

In a dual control system, the application logic in each controller tries to produce the same results. After many iterations of running the application, it is possible for the internal data values to differ due to mathematical round off, and different past history (power-up). To converge this data, the internal data (state) variables are taken from the designated controller and transmitted to the non-designated controller for its use. This is known as state exchange.

State variables are any internal variables not immediately derived from input or control constants. Any variable that is used prior to being re-calculated is an internal state variable.
This principle can be displayed in the following two equations:

\[ A = B + C \]
\[ C = 3 \times D \]

Assume B and D are inputs and A and C are intermediate values. Since C is used prior to being calculated, the value of C during the previous scan retains some state information. Therefore, C is a state variable that must be updated in the non-designated controller if both controllers are to remain synchronized.

In the Mark VIeS Safety controller, Boolean state variables are updated on every control frame. The analog state variable updates are multiplexed. A subset of analog state variables is updated every control frame. The controller rolls through each subset until all state variables are transmitted.

### 1.6.1.3 Triple Modular Redundant (TMR) Controllers

The TMR control architecture contains three controllers, three IONets, and singular or fanned TMR I/O Modules. **Reliability and availability** are much better with TMR controllers than with dual controllers due to increased fault detection capability. In addition to all of the dual redundant features, the TMR controller provides three independent outputs to all TMR I/O modules and the state variables between controllers are voted.

In a TMR control system, all three controllers receive inputs from the I/O modules on all networks and transmit outputs on their respective IONet continuously. If a controller or network component fails, the system does not require fault detection or failover time to continue operating. All controllers transmit their copy of the state variables after the output packet has been transmitted. Each controller takes the three sets of state variables and votes the data to get the values for the next run cycle.

**Note** The level of I/O reliability can be varied to meet the application needs because I/O redundancy can be simplex, dual, or TMR.
1.6.2  I/O Redundancy

There are various options available for single and multiple packs and single and dual networks for I/O redundancy. The following are options for TMR I/O modules:

- Single Pack Dual Network I/O Module (SPDN)
- Two Single Pack, Single Network (2SPSN) I/O Modules
- Dual Pack, Dual Network (DPDN) I/O Module
- Triple Pack, Dual Network (TPDN) I/O Module
- Hot Backup I/O Module
- Triple Pack, Triple Network (TPTN) I/O Module

1.6.2.1 Single Pack Dual Network I/O Module (SPDN)

This configuration is typically used for non-critical single sensor I/O. A single sensor connects to a single set of acquisition electronics which is then connected to two networks.

- Single data acquisition
- Redundant network

The I/O pack delivers input data on both networks at the beginning of the frame and receives output data from both controllers at the end of the frame.

1.6.2.2 Two Single Pack, Single Network (2SPSN) I/O Modules

This configuration is typically used for inputs where there are multiple sensors monitoring the same process points. Two sensors are connected to two independent I/O modules.

- Redundant sensors
- Redundant data acquisition
- Redundant network
- Online repair

Each I/O pack delivers input data on a separate network at the beginning of the frame and receives output data from separate controllers at the end of the frame.

1.6.2.3 Dual Pack, Dual Network (DPDN) I/O Module

This is a special case for inputs only, using a dual pack, dual network module. A fanned input terminal board can be populated with two packs providing redundant data acquisition for a set of inputs.

- Redundant data acquisition
- Redundant network
- Online repair

Each I/O pack delivers input data on a separate network at the beginning of the frame.
1.6.2.4 Triple Pack, Dual Network (TPDN) I/O Module

This is a special case mainly intended for outputs, but also applies to inputs. The special output voting/driving features of the TMR I/O modules can be used in a dual control system. The inputs from these modules are voted in the controller.

- Redundant data acquisition
- Output voting in hardware
- Redundant network
- Online repair

Two of the I/O packs are connected to separate networks delivering input data and receiving output data from separate controllers. The third I/O pack is connected to both networks. This pack delivers inputs on both networks and receives outputs from both controllers.

1.6.2.5 Hot Backup I/O Module

This is a special case mainly intended for a small set of I/O packs used as a gateway to another network. In this configuration, there are dual I/O packs, dual network but only one I/O pack is communicating to the gateway network at one time, the other I/O pack operates in a backup mode. The inputs from active module are used in the controller.

- Redundant data acquisition
- Redundant network
- Online repair

The two I/O packs are both connected to both networks, but only communicates to the controller and the gateway network. If a failure occurs on the active I/O pack, the backup I/O pack becomes the active I/O pack, thus maintaining communication with the connected devices.

1.6.2.6 Triple Pack, Triple Network (TPTN) I/O Module

For medium integrity applications with medium to high reliability sensors, one sensor can be fanned to three I/O packs. The special output voting/driving features of the TMR I/O modules can be used in a TMR control system. The inputs from these modules are voted in the controllers. A fanned input terminal board can be populated with three packs providing redundant data acquisition for a set of inputs.

- Redundant data acquisition
- Output voting in hardware
- Redundant networks, packs, and controllers
- Online repair

Each of the I/O packs are connected to separate networks delivering input data and receiving output data from separate controllers.
1.6.3 Input Processing

All inputs are available to all three controllers, but there are several ways that the input data is handled. For inputs existing in only one I/O module, all three controllers use the same value as common input without voting, as displayed in the table below. Inputs that appear in all three I/O channels may be voted to create a single input value. The triple inputs may come from three independent sensors. They can also be created from a single sensor by hardware fanning at the terminal board.

<table>
<thead>
<tr>
<th>Redundancy</th>
<th>Available IONet Topology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplex</td>
<td>One I/O pack with one IONet</td>
</tr>
<tr>
<td></td>
<td>The number of IONets in a system equals the number of controllers.</td>
</tr>
<tr>
<td>Dual</td>
<td>One I/O pack with two IONets</td>
</tr>
<tr>
<td></td>
<td>Two I/O packs with one IONet per pack</td>
</tr>
<tr>
<td></td>
<td>Three I/O packs with &lt;R&gt; one IONet to controller &lt;R&gt;, &lt;S&gt; one IONet to controller &lt;S&gt;, and &lt;T&gt; two IONets with one to controller &lt;R&gt; and one to controller &lt;S&gt;</td>
</tr>
<tr>
<td>TMR</td>
<td>Fanned – three packs, one IONet/pack with one terminal board</td>
</tr>
<tr>
<td></td>
<td>Dedicated – three packs, one IONet/pack with three separate S-type terminal boards</td>
</tr>
</tbody>
</table>

![Simplex – One I/O pack, One IONet](image1)

![Dual – One I/O pack, Two IONets](image2)

![Dual – Two I/O Packs, One IONet](image3)

![Dual – Three I/O Packs with 1, 1, 2 IONets](image4)
For any of the above input configurations, multiple inputs can be used to provide application redundancy. For example, three Simplex inputs can be used and selected in application code to provide sensor redundancy.

The Mark VIeS Functional Safety System provides configuration capability for input selection and voting using a simple, highly reliable and efficient selection/voting/fault detection algorithm to reduce application configuration effort. This maximizes the reliability options for a given set of sensor inputs and provides output voting hardware compatibility. All applicable subsets of reliability options are available on a per terminal board basis for any given Mark VIeS topology. For example, in a TMR controller, all simplex and dual option capabilities are also provided.

While each IONet is associated with a specific controller that is responsible for transmitting outputs, all controllers see all IONets. The result is that for a simplex input the data is not only seen by the output owner of the IONet, it is seen in parallel by any other controllers. The benefit of this is that loss of a controller associated with a simplex input does NOT result in the loss of that data. The simplex data continues to arrive at other controllers in the system.

A single input can be brought to the three controllers without any voting. This is used for non-critical, generic I/O, such as monitoring 0-20 mA inputs, contacts, thermocouples, and resistance temperature devices (RTD).

One sensor can be fanned to three I/O boards as above for medium-integrity applications. This is used for sensors with medium-to-high reliability. Three such circuits are needed for three sensors. Typical inputs are 0-20 mA inputs, contacts, thermocouples, and RTDs.
Three independent sensors can be brought into the controllers without voting to provide the individual sensor values to the application. Median values can be selected in the controller if required. This configuration, displayed in the following figure, is used for special applications only.
The following figure displays three sensors, each one fanned and then software implemented fault tolerance (SIFT) voted. This provides a high reliability system for current and contact inputs, and temperature sensors.

Three Sensors, Each One Fanned and Voted, for Medium-to-High Reliability Applications

Highly reliable speed input applications are brought in as dedicated inputs and SIFT voted. The following figure displays this configuration. Inputs such as speed control and overspeed are not fanned so there is a complete separation of inputs with no hardware cross coupling which could propagate a failure. RTDs, thermocouples, contact inputs, and 0-20 mA inputs can also be configured this way.

Three Sensors with Dedicated Inputs, Software Voted for High Reliability Applications
1.6.4 Output Processing

The system outputs are the portion of the calculated data transferred to the external hardware interfaces and then to the various actuators controlling the process. TMR outputs are voted in the output voting hardware. Any system can output individual data through simplex hardware.

The three voting controllers calculate TMR system outputs independently. Each controller sends the output to its associated I/O hardware (for example, the R controller sends output to the R I/O). The three independent outputs are then combined into a single output by a voting mechanism. Different data types require different methods of establishing the voted value.

The outputs from the three controllers fall into three groups:

- Outputs are driven as single ended non-redundant outputs from individual I/O networks
- Outputs exist on all three I/O networks and are merged into a single output by the hardware
- Outputs exist on all three I/O networks and are output separately to the controlled process. This process may contain external voting hardware.

For normal relays, the three outputs feed a voting relay driver, which operates a single relay per channel. For critical protective signals, the three outputs drive three independent relays, with the relay contacts connected in the typical six-contact voting configuration.

For servo outputs, the three independent currents drive a three-coil servo actuator, which adds them by magnetic flux summation, as displayed in the following figure. Failure of a servo driver is sensed and a deactivating relay contact is closed to short the servo coil.
The following figure displays 0-20 mA outputs combined through a 2/3 current sharing circuit that allows the three outputs to be voted to one. Failure of a 0-20 mA output is sensed and a deactivating relay contact is opened.
1.7 Reliability and Availability

1.7.1 Mean Time Between Failure (MTBF)

MTBF is a basic measurement of reliability for systems. It is the average failure-free operating time during a particular measurement period under defined conditions. A failure may or may not result in a problem with the overall system depending on any redundancy employed. MTBF is usually specified for each replaceable system component.

MTBF roll-up of system components gives the equipment owner the knowledge needed to determine how long the equipment can be expected to operate without failure under given conditions. If it is essential that the equipment does not fail during operation, the owner can use this data to schedule maintenance or replacement of the equipment prior to failure. Alternately, redundant applications could be used to prevent system problems when a failure occurs.

MTBF data is also used to determine the weak links in a system. The system engineer provides contingency options for those weak links to obtain higher reliability.

1.7.2 Mean Time Between Forced Outage (MTBFO)

MTBFO is a measurement of system availability, which includes the effects of any fault tolerance that may exist. This average time between failures causes the loss of system functions.

The engineer must be very aware of MTBF and MTBFO when designing a reliable continuous system. To maximize the MTBFO, Mark VleS Safety control systems undergo evaluation of all system component MTBF values. The effects of failures and contingency operation are then analyzed to maximizing MTBFO.

To continue operation after a critical system component has failed, a control must have one or more backups in place (redundancy) to improve the MTBFO significantly above that of a Simplex control. The simplest method is adding a second component that takes over the critical function when a fault is detected.

The redundancy in the system can be either active or standby. The Mark VleS Safety control uses active redundancy and has all components operating simultaneously. Standby redundancy activates backup systems after a failure is detected.

Realizing the full benefits of redundancy, a system failure must be detectable for the control to bypass it. In a dual control, gross failures are readily detectable while subtle failures are more difficult to detect. TMR controls, using two out of three voting, are always able to select a valid value when presented with any single failure.

Depending on the equipment, the time required to detect the fault and switch to the new component may be hours/minutes/seconds/milliseconds. In the case of fuel-flow control to a turbine, this is required to be done in milliseconds.

When a redundant control bypasses a failure, it is required that the system annunciate the presence of the failure and that repairs be completed in a timely fashion. The term Mean Time to Repair (MTTR) refers to the time it takes to identify and repair a given failure. The Mark VleS Safety control system is designed to support a MTTR of four hours. This preserves the MTBFO benefits of redundancy resulting in unequaled system reliability. A control is used to run the system as well as detect system failures. In a Dual control, configured for one out of two to run, it is often necessary to add dedicated tripping controls for each critical trip system. This is done to yield running reliability while maintaining required tripping reliability.

A TMR control normally configures the control for two out of three selection. This yields high running and tripping reliability from the primary control. Additional dedicated tripping controls can be used to achieve even higher tripping reliability, but they must also be TMR to preserve running reliability.
1.7.3 Fault Detection

A system offering redundancy can be less reliable than a non-redundant system. The system must be able to detect and announce faults so it can be repaired before a forced outage occurs. Fault detection is needed to ensure a component or group of components are operating properly. Fault detection is achieved through one or more of the following methods.

- Operator inspection of the process
- Operator inspection of the equipment.
- Special hardware circuits to monitor operation
- Hardware and software watchdogs
- Software logic
- Software heartbeats

Complex control systems have many potential failure points. This can be very costly and time consuming to create foolproof fault detection. Failure to control the outputs of a system is the most damaging. Fault detection must be determined as close to the output as possible to achieve the highest level of reliability. With the Mark VIeS Functional Safety System configured using triple redundant controllers and I/O modules, a high level of detection and fault masking is provided by voting the outputs of all three controllers and monitoring discrepancies.

All Mark VIeS Functional Safety Systems benefit from the fault detection design of the I/O packs. Every pack includes function-specific fault detection methods attempting to confirm correct operation. This is made possible by the powerful local processing that is present in each input and output pack. Some examples of this include:

- Analog to digital (A/D) converters are compared to a reference standard each conversion cycle. If the converted calibration input falls outside of acceptable ranges, the pack declares bad health.
- Analog output 0-20 mA use a small current-sense resistor on the output terminal board. This output is read back through a separate A/D converter and compared to the commanded value. A difference between the commanded and actual value exceeding an acceptable level results in the output being declared in bad health.
- Discrete input opto-isolators are periodically forced to an on condition, then forced off. This is done independently of the actual input and is fast enough not to interfere with the sequence of events (SOE) time capture. If any signal path is stuck and does not respond to the test command, the signal is declared in bad health.

1.7.4 Online Repair

When a component failure is detected and healed in the control system on a critical path, a potential failure has been avoided. Subsequent actions can include:

Option 1 - Continue running until the backup component fails. However, this option is not recommended. A redundant system, where the MTTR is infinite can have a lower total reliability than a simplex system.

Option 2 - Continue running until the system is brought down in a controlled manner to replace the failed component. This option is a valid procedure for some processes needing predictable mission times. Many controlled processes cannot be easily scheduled for a shut down.

Option 3 - Replace the component online.

**Note** As MTTR increases from the expected four hours to infinite, the system reliability can decline from significantly greater down to less than a simplex system reliability. Repair should be accomplished as soon as possible.

Option 3 is required to get the maximum benefit from redundant systems with long mission times. In Dual or TMR Mark VIeS Safety controller applications, the controllers and redundant I/O packs can be replaced online.
To ensure online repair capability, control systems must have their redundancy tested after installation and after any system modifications. Refer to the requisition specific system application documentation/control specification (if available) for redundancy testing procedures.

**Forced Outage Probability versus Time (Conventional TMR)**

**Forced Outage Probability versus Time (TMR)**
1.7.5 Designated Controller

Although three controllers, R, S, and T, contain identical hardware and software, some of the functions performed are unique. A single designated controller can perform the following functions:

- Supply initialization data to the other two controllers at start-up
- Keep the master time clock
- Supply variable state information to the other controllers if one fails

For the purposes of deciding which controller is to be the designated controller, each controller nominates itself on a weighting algorithm. The nominating values are voted among the controllers and the majority value is used. If there is a tie, or no majority, the priority is R, then S, and then T. If a designated controller is powered down and later powered up, the designated controller will move and not come back if all controllers are equal. This ensures that a toggling designated controller is not automatically re-selected.

Designated controller selection is based on:

- Control state
- UDH connectivity
- IONet connectivity
- NVRAM health

1.7.6 Communication Loss

Each output pack monitors the IONet for valid commands from one or two controllers. In the event that a valid command is not received within an expected time the pack declares the communication as being lost. Upon loss of communication the pack action is configurable. The pack can continue to hold the last commanded value indefinitely or it can be commanded to go to a specified output state. The default action is to go to a power-down state, the same as if the power were removed from the pack.


For critical loops, the default action is the only acceptable choice. The other options are provided for non-critical loops, where running liability may be enhanced by an alternate output.

1.7.7 State Exchange

To keep multiple controllers in synchronization, the Mark VIeS Safety control efficiently exchanges the necessary state information through the IONet. State information includes calculated values such as timers, counters, integrators, and logic signals such as bi-stable relays, momentary logic with seal-in, and cross-linked relay circuits. State information is voted in TMR controllers and follows the designated controller in dual or faulted TMR systems.

1.7.8 Voting

Voting in the Mark VIeS Functional Safety System is separated into analog and logic voting. Additionally, fault detection mechanisms directly choose owned inputs and designated states.
1.7.8.1 **Median Value Analog Voting**

The analog signals are converted to a floating-point format by the I/O pack. The voting operation occurs in each of the three controller modules (R, S, and T). Each controller receives a copy of the data from the other two channels. For each voted data point, the controller has three values including its own. The median value voter selects the middle value of the three as the voter output. This is the most likely of the three values to be closest to the true value.

### Median Value Voting Examples

<table>
<thead>
<tr>
<th>Sensor Inputs</th>
<th>Sensor Input Value</th>
<th>Median Selected Value</th>
<th>Sensor Input Value</th>
<th>Median Selected Value</th>
<th>Sensor Input Value</th>
<th>Median Selected Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor 1</td>
<td>981</td>
<td>910</td>
<td>1020</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sensor 2</td>
<td>985</td>
<td>981</td>
<td>985</td>
<td>978</td>
<td>985</td>
<td>985</td>
</tr>
<tr>
<td>Sensor 3</td>
<td>978</td>
<td>978</td>
<td>978</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Median Value Voting Examples with Normal and Bad Inputs**

1.7.8.2 **Two Out of Three Logic Voter**

Each of the controllers has three copies of the data for the logic voter. Voting is a simple logic process, inputting the three values and finding the two values that agree.

1.7.8.3 **Disagreement Detector**

A disagreement detector continuously scans the input prevote input data sets and produces an alarm bit if a disagreement is detected between the three values. Any disagreement between the prevote logical signals generates an alarm. Failure of one of the three voted input circuits has no effect on the controlled process since the fault is masked by SIFT. Without a disagreement detector, a failure could go unnoticed until a second failure occurs.

For analog signals, comparisons are made between the voted value and each of the three prevote values. The delta for each value is compared with a user programmable limit value. The limit can be set as required to avoid nuisance alarms, but give indication that one of the prevote values has moved out of normal range. Each controller is required to compare only its prevote value with the voted value; for example, R compares only the R prevote value with the voted value. Nominal, analog voting limits are set at a 5% adjustment range, but can be configured to any number for each analog input.

1.7.9 **UDH Fault Tolerance — Command Action**

Using IONet connectivity, the controller copies command traffic from the UDH across all controllers. This provides fault tolerance for dual UDH networks.
1.7.10  Forced Variables

The controller has a feature called Forced Variables. This allows the maintenance technician using application software to set analog or logical variables to forced values. Variables remain at the forced value until unforced. Both compute and input processing respect forcing. Any applied forcing is preserved through power down or restart of the controller.

---

**Warning**

Logic Forcing is for offline software checkout and troubleshooting and should only be used in conjunction with proper lockout/tag out procedures. Forcing of protective functions is never permissible for an operating unit.

---

1.7.11  Peer I/O

In addition to the data from the I/O modules, there is a class of data coming from other controllers in other cabinets connected through the UDH network. For integrated systems, this network provides a data path between multiple turbine controllers and possibly the controls for the generator, the exciter, or the HRSG/boiler.

Selected signals from the controller database can be mapped into pages of peer outputs that are broadcast periodically on the UDH I/O to peer controllers. For TMR systems, the UDH communicator performs this action using the data from its internal database. In the event of a redundant UDH network failure, the controller will request data over the remaining network, the IONet.
1.7.12 Rate of Response

Mark VIeS Safety controllers can run at a variety of frame rates to meet the application needs of the industrial control solution. Control systems are tuned accordingly, based on a variety of factors including: complexity of controller application logic, processor type, and number of I/O and other interfaces used. The following diagram provides an example of typical processes that occur during a single controller frame in sequence.

Notes
Assumes a Triple Moduar Redundant (TMR) configuration, versus dual, or simplex

- Subsystem activities identified with a gray rectangle
- Activities that span multiple subsystems identified with a dashed brown rectangle
1.8 Component Part Numbers and Serial Numbers/Barcodes

1.8.1 Common Terminology

The following terms are used to identify Mark controls components:

**Backward Compatible** A part is backward compatible when it can directly replace an earlier version of the part in all specified end-use applications without requiring any changes to the host system.

**Base Part Number** The part number that is used to uniquely identify a part as a component in a higher-level assembly or to order a backward compatible replacement part. The base part number remains unchanged for all backward-compatible versions of the part. An example of a base part number is IS400YDIAS1B.

**Hardware Form** The three characters following the module or board type in the part number that together with the Type uniquely defines a module or board in the ToolboxST configuration tool. An example hardware form is H1B.

**Module or Board Type** The four letter mnemonic taken from characters 6 – 9 of the full part number that is used to identify the function of the part. An example of a board type is Pack Discrete Input A (YDIA).

**Part Number** The Part Number is the ANSI/EIA-649-A National Consensus Standard for Configuration Management, Product Identifier, that represents a specific version of a printed wiring assembly (PWA) and consists of all applicable fields specified in the table **Product Identifier Fields Example**. The Part Number identifies the baseline design of a product and is changed each time the design is changed. An example part number is IS420YDIAS1B.

**Printed Circuit Board Assembly (PCBA)** Indicates a single board.

**Printed Wiring Assembly (PWA)** The ANSI/EIA-649-A National Consensus Standard for Configuration Management, Product Identifier, that indicates one or more PCBAs.

**Printed Wiring Board (PWB)** The PC-T-50 Terms and Definitions for Interconnecting and Packaging Electronic Circuits that indicates a circuit board without any parts added.

**Serial Number/Barcode** A unique number assigned to a component that indicates the date of manufacture and the supply vendor.
### 1.8.2 Part Number Convention

A part number consists of up to nine fields of information defined in the following tables.

#### Product Identifier Fields Example

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Part Number Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS200ABCDG1AAA</td>
<td>IS 2 00 ABCD G 1 A A A</td>
</tr>
</tbody>
</table>

#### Part Number Field Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Field Name</th>
<th>Code</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Issuing organization code</td>
<td>IS</td>
<td>GE Power, Salem, Virginia, USA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DS</td>
<td>GE Power, Salem, Virginia, USA</td>
</tr>
<tr>
<td>II</td>
<td>Hazardous substance code</td>
<td>2</td>
<td>Not RoHS [3] compliant</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>RoHS [3] Compliant</td>
</tr>
<tr>
<td>III</td>
<td>Assembly level code [4]</td>
<td>00</td>
<td>PCBA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>01</td>
<td>Coated PCBA [5]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>05</td>
<td>PCBA designed as a component to be soldered into another PCBA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10</td>
<td>PCBA with an added manufacturing or assembly process step [6]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11</td>
<td>Coated PCBA with an added manufacturing or assembly process step [6]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>15</td>
<td>PCBA with added application firmware and/or daughter-board(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>20</td>
<td>1 or more PCBAs in an enclosure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>21</td>
<td>1 or more PCBAs in an enclosure and all PCBAs are coated [5]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>30</td>
<td>One or more PWAs on a base</td>
</tr>
<tr>
<td></td>
<td></td>
<td>31</td>
<td>One or more PWAs on a base and all PCBAs are coated [5]</td>
</tr>
<tr>
<td>IV</td>
<td>Board or Module Type</td>
<td>4</td>
<td>4 letter mnemonic that describes the function of the PWA</td>
</tr>
<tr>
<td>V</td>
<td>Technology code</td>
<td>G</td>
<td>Lead-through hole components only, no surface-mount technology</td>
</tr>
<tr>
<td></td>
<td></td>
<td>H</td>
<td>Contains surface-mount technology components</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S</td>
<td>Functional safety system component [7]</td>
</tr>
<tr>
<td>VI</td>
<td>Assembly variant</td>
<td>1</td>
<td>1 numeric character, excluding 0</td>
</tr>
<tr>
<td>VII</td>
<td>Backward compatibility version</td>
<td>1</td>
<td>1 alpha character, excluding: I, O, Q</td>
</tr>
<tr>
<td>VIII</td>
<td>PWA version</td>
<td>Breadboard: BR + 1 numeric character, excluding 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prototype: PR + 1 numeric character, excluding 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Production: 1 alpha character, excluding: I, O, Q</td>
<td></td>
</tr>
<tr>
<td>IX</td>
<td>Optional character</td>
<td>Breadboard: Not used</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prototype: Not used</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Production</td>
<td>PWB version (assembly levels 00, 05 only): 1 alpha character, excluding: I, O, Q</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Marked for use in hazardous (classified) locations [9]: X</td>
</tr>
</tbody>
</table>
### Part Number Field Definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Field Name</th>
<th>Code</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[4] There are some legacy part numbers with assembly level code “020”. These identify assemblies of one or more PCBAs, and may not follow the current versioning rules.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[5] Coated PWAs with assembly level codes 01, 21, and 31 are approved for use in environments where the overall corrosion potential due to airborne contaminants does not exceed severity level G3, as defined in ANSI/ISA-71.04-2013 Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[6] Certain legacy boards: IS210AEAAH<em>B, IS210AEABH</em>A, IS210AEACH1A, IS210AEBH<em>B, IS210AEDBH</em>A, IS210AEPSG1A, IS210AEPSG*B were originally released as un-coated IS200 and coated IS210 parts, but the un-coated parts were never used in the host product. As these designs evolve, the IS200 level parts are being abandoned and the IS210 level parts are being maintained using the level 00 rules.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[7] Each functional safety system PWA is certified to meet IEC 61508 and is equivalent in form, fit, and function to any PWA with a part number that differs only in the Technology Code (field 5). For example: IS400UCSBS1ABB is equivalent in form, fit, and function to IS400UCSBH1ABB, but is also certified to meet IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[8] NFPA 70 National Electrical Code, Article 500 Hazardous (Classified) Locations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes:

- The following figures are examples of component labels identifying the part number.
Example Controller Label

On the replacement, the revision letter will be the same or a higher letter.

Example I/O Pack Label

12-character alphanumeric part number

On the replacement part number received, the revision letter will be the same or a higher letter.
Internal GE employees and certain third-party parts suppliers can use the ENOVIA PLM tool to search for parts. The following Power Generation PLM web portal is available to assist with account registration and training on how to use the tool to search for parts: http://colab.ge.com/dashboard/canvas/v/518d03b3bf1d408e570001c9/home

1.8.3 Serial Number/Barcode Convention

The serial number/barcode consists of seven characters composed from the following 31 permitted characters:
0 1 2 3 4 5 6 7 9 A C D E F G H J K L M N P R S T U V W X Y Z.

It is composed of five coded groups that represent the component’s supply vendor, date of manufacture, and component count in the following format: VYMDSs1s0. The following table describes what these group codes represent.

<table>
<thead>
<tr>
<th>Group Code</th>
<th>Description</th>
</tr>
</thead>
</table>
| V          | Vendor code (one-character)  
Contact your GE representative or GE Technical Support for further information on vendors and manufacturing locations. |
| Y          | Year code (one character)  
Refer to the table Year Codes for permitted values. |
| M          | Month code (one character)  
Refer to the table Month Codes for permitted values. |
| D          | Day-of-month code (one character)  
Refer to the table Day-of-Month Codes for permitted values. |
| S1S0       | Serial number count code (three characters)  
The total count of unique serial numbers generated for a component is reset to zero each day at 12:00 AM, and then incremented by one for each unique serial number generated thereafter. This code limits the number of unique serial numbers to 313 (29,791) per day. Contact your GE representative or GE Technical Support for more information on this code. |
The following tables define the groups and characters in a serial number/barcode.

<table>
<thead>
<tr>
<th>Year</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>0</td>
</tr>
<tr>
<td>2006</td>
<td>1</td>
</tr>
<tr>
<td>2007</td>
<td>2</td>
</tr>
<tr>
<td>2008</td>
<td>3</td>
</tr>
<tr>
<td>2009</td>
<td>4</td>
</tr>
<tr>
<td>2010</td>
<td>5</td>
</tr>
<tr>
<td>2011</td>
<td>6</td>
</tr>
<tr>
<td>2012</td>
<td>7</td>
</tr>
<tr>
<td>2013</td>
<td>9</td>
</tr>
<tr>
<td>2014</td>
<td>A</td>
</tr>
<tr>
<td>2015</td>
<td>C</td>
</tr>
<tr>
<td>2016</td>
<td>D</td>
</tr>
<tr>
<td>2017</td>
<td>E</td>
</tr>
<tr>
<td>2018</td>
<td>F</td>
</tr>
<tr>
<td>2019</td>
<td>G</td>
</tr>
<tr>
<td>2020</td>
<td>H</td>
</tr>
<tr>
<td>2021</td>
<td>J</td>
</tr>
<tr>
<td>2022</td>
<td>K</td>
</tr>
<tr>
<td>2023</td>
<td>L</td>
</tr>
<tr>
<td>2024</td>
<td>M</td>
</tr>
<tr>
<td>2025</td>
<td>N</td>
</tr>
<tr>
<td>2026</td>
<td>P</td>
</tr>
<tr>
<td>2027</td>
<td>R</td>
</tr>
<tr>
<td>2028</td>
<td>S</td>
</tr>
<tr>
<td>2029</td>
<td>T</td>
</tr>
<tr>
<td>2030</td>
<td>U</td>
</tr>
<tr>
<td>2031</td>
<td>V</td>
</tr>
<tr>
<td>2032</td>
<td>W</td>
</tr>
<tr>
<td>2033</td>
<td>X</td>
</tr>
<tr>
<td>2034</td>
<td>Y</td>
</tr>
<tr>
<td>2035</td>
<td>Z</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Month</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>January</td>
<td>0</td>
</tr>
<tr>
<td>February</td>
<td>1</td>
</tr>
<tr>
<td>March</td>
<td>2</td>
</tr>
<tr>
<td>April</td>
<td>3</td>
</tr>
<tr>
<td>May</td>
<td>4</td>
</tr>
<tr>
<td>June</td>
<td>5</td>
</tr>
<tr>
<td>July</td>
<td>6</td>
</tr>
<tr>
<td>August</td>
<td>7</td>
</tr>
<tr>
<td>September</td>
<td>9</td>
</tr>
<tr>
<td>October</td>
<td>A</td>
</tr>
<tr>
<td>November</td>
<td>C</td>
</tr>
<tr>
<td>December</td>
<td>D</td>
</tr>
</tbody>
</table>
### Day-of-Month Codes

<table>
<thead>
<tr>
<th>Day-of-Month</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>7</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>A</td>
</tr>
<tr>
<td>11</td>
<td>C</td>
</tr>
<tr>
<td>12</td>
<td>D</td>
</tr>
<tr>
<td>13</td>
<td>E</td>
</tr>
<tr>
<td>14</td>
<td>F</td>
</tr>
<tr>
<td>15</td>
<td>G</td>
</tr>
<tr>
<td>16</td>
<td>H</td>
</tr>
<tr>
<td>17</td>
<td>J</td>
</tr>
<tr>
<td>18</td>
<td>K</td>
</tr>
<tr>
<td>19</td>
<td>L</td>
</tr>
<tr>
<td>20</td>
<td>M</td>
</tr>
<tr>
<td>21</td>
<td>N</td>
</tr>
<tr>
<td>22</td>
<td>P</td>
</tr>
<tr>
<td>23</td>
<td>R</td>
</tr>
<tr>
<td>24</td>
<td>S</td>
</tr>
<tr>
<td>25</td>
<td>T</td>
</tr>
<tr>
<td>26</td>
<td>U</td>
</tr>
<tr>
<td>27</td>
<td>V</td>
</tr>
<tr>
<td>28</td>
<td>W</td>
</tr>
<tr>
<td>29</td>
<td>X</td>
</tr>
<tr>
<td>30</td>
<td>Y</td>
</tr>
<tr>
<td>31</td>
<td>Z</td>
</tr>
</tbody>
</table>
2 Functional Safety

This chapter provides an introduction to the Mark VIeS Functional Safety System, which is used for functional safety loops to achieve SIL 2 and 3 capabilities. The Mark VIeS Functional Safety System is used by operators knowledgeable in Safety-instrumented System (SIS) applications to reduce risk in critical safety functions. Safety controllers and distributed I/O modules are programmed specifically for safety control use, and this specific control hardware has been IEC 61508 certified.

Functional safety is concerned about the speed of the control system’s reaction to trip the system (energize to trip) or to provide an emergency shut-down (de-energize to trip) when a safety-critical event occurs. With this in mind, safety equipment is rated to meet Safety Integrity Levels (SIL), which are achieved by analyzing probability of failure on demand.

The Mark VIeS Functional Safety System is differentiated in the general market because of its significant flexibility, easy of control logic development, and redundancy capabilities. Its safety I/O is very flexible in application, for example both analog inputs and outputs are available. The Mark VIeS Safety control is an engineered solution designed for the customers that work on our systems to help simplify and reduce maintenance costs.

The Mark VIeS Functional Safety System is available for integration into other safety-critical applications outside of GE, for example emergency shutdown, burner management, and fire and gas-critical control applications. This solution reflects the experience of three plus decades, four generations, and over 10,000 installed triple-redundant digital turbine controls.
2.1 Safety Instrumented System (SIF)

While the Safety controller performs the logic solving tasks for the system, it also interfaces with the ToolboxST application for configuration, diagnostics, and changes to controller application logic (blocks). The ToolboxST application provides a means to lock or unlock the Safety controller for configuration and safety-instrumented function (SIF) programming. This allows the user to install a safety function, test it, and place the controller in *Locked* mode to perform safety control.

Interfaces to Mark VIeS Safety controller must be strictly regulated to avoid interference with the operation of the system. Data exchange to the safety control must be restricted and only used when validated by the SIL application logic.

The Mark VIeS Safety control was designed and certified to meet functional safety standards according to *IEC 61508* Parts 1 through 3. It is certified for use in both high-and low-demand applications, uses redundant architecture configurations, and a hardware fault tolerance (HFT) of 1 to achieve safety integrity level (SIL) 3. The highest achievable SIL with an HFT of 0 is SIL 2.

IEC 61508-4 definitions are as follows:

- **Safety**
  Freedom from unacceptable risk.

- **Risk**
  Combination of the probability of occurrence of harm and the severity of that harm.

- **Functional Safety**
  Part of the overall safety relating to the equipment under control (EUC) and the EUC control system that depends on the correct functioning of the Electrical/electronic/programmable electronic (E/E/PE) safety-related systems, other technology safety-related systems, and external risk reduction facilities.
2.2 Risk Reduction

Functional safety relates to proper equipment operation, as well as other risk reduction facilities. Layers of protection (LOP) concepts are illustrated in the following figure.

The LOP around a process can be used to introduce risk reduction. Failure to carefully analyze the available LOP and the likelihood-consequence relationship of the risks involved with process control failure can lead to an expensive over-design of the system. The goal is to reduce the risk to a level that is as low as reasonably practicable (ALARP).

To achieve functional safety, it is necessary to analyze the potential hazards to personnel and property, including any environmental impact, that could occur when the control of equipment is lost.

Requirements for safety function and integrity must be met to achieve functional safety. Safety function requirements describe what the safety function does and is derived from the hazard analysis. The safety integrity requirement is a quantitative measure of the likelihood that a safety function will perform its assigned task adequately. For safety functions to be effectively identified and implemented, the system as a whole must be considered.

A primary parameter used in determining the risk reduction in a safety controller is the Average Probability of Failure on Demand (PFD_{avg}). The inverse of the PFD_{avg} is the Risk Reduction Factor (RRF).
2.2.1 Modes of Operation

A demand mode is a mode of operation in which the safety function is called upon only on demand. IEC 61508-4 clause 3.5.12 defines two demand modes of operation:

- Low demand mode
- High demand or continuous mode

Low demand describes the mode in which safety function demand occurs no greater than once per year. In high demand mode, the frequency of demand is greater than once per year. Continuous mode is regarded as very high demand and is associated with the safety function operating to keep the EUC within its normal safe state.

The mode of operation is relevant when determining the target failure measure of a safety function. Low demand mode relates to the Probability of Failure on Demand (PFD)\textsubscript{avg}, whereas high demand or continuous demand mode relates to measuring the Probability of Failure per Hour (PFH) (there are approximately $10^4$ hours in a year). IEC 61508 defines a scale of four distinct levels of risk reduction referred to as the Safety Integrity Level (SIL).

<table>
<thead>
<tr>
<th>SIL</th>
<th>PFD\textsubscript{avg} Low Demand Mode</th>
<th>PFH High Demand Mode</th>
<th>RRF</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\geq 10^{-2}$ to $&lt; 10^{-1}$</td>
<td>$\geq 10^{-6}$ to $&lt; 10^{-5}$</td>
<td>$&gt; 10$ to $\leq 100$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-3}$ to $&lt; 10^{-2}$</td>
<td>$\geq 10^{-7}$ to $&lt; 10^{-6}$</td>
<td>$&gt; 100$ to $\leq 1,000$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-4}$ to $&lt; 10^{-3}$</td>
<td>$\geq 10^{-8}$ to $&lt; 10^{-7}$</td>
<td>$&gt; 1,000$ to $\leq 10,000$</td>
</tr>
</tbody>
</table>

The SIL applies to all elements in the safety loop (sensors, logic solver, and final element) and their architecture. The loop must be considered in its entirety.

2.3 Safety System Redundancy Options

Redundancy is a key feature in safety control system design that can enable on-line repair without interrupting the process. The unique Ethernet back-bone of the Mark VIeS Safety system enables several options for redundancy to achieve required SIL. This provides the safety control engineer unparalleled flexibility to meet the safety SIL requirements for each application in the most cost effective manner.

\[
RRF = \frac{1}{PFD_{avg}}
\]
2.3.1 **Triple Modular Redundant (TMR) Redundancy**

The Triple Modular Redundant (TMR) control modes can provide:

- Two out of three (2oo3) voting
  - SIL 3 high/low demand for de-energize-to-trip
  - or
  - SIL 2 low demand for energize-to-trip
- Hardware fault tolerance (HFT): 1
- Degradation sequence: [2oo3] > [1oo2] > [Fail Safe]

**TMR Controllers**

Three Mark VIeS controllers work as a set synchronizing data every frame (sweep). Each controller receives inputs on all 3 I/O networks, and sends output commands on designated I/O network.

**TMR I/O Network**

Ethernet based TMR I/O network supports both centralized and distributed I/O modules.

**PC Based Gateway**

PC based communication interface, options:
- OPC-DA server
- OPC-UA server
- Modbus master

**Embedded Controller Gateway**

Embedded controller for communication interface, options:
- OPC-UA server
- Modbus slave

**TMR Fanned Input**

Single discrete/ analog sensor is fanned through a common terminal board to three independent input packs, 2oo3 voting is done in the controller set.

**TMR Dedicated Input**

Three redundant discrete/analog sensors are wired to three independent input modules, 2oo3 voting is done in the controller set.

**TMR Outputs Voted on Terminal Board**

The three packs receive output commands from their associated controller, the common terminal board then performs 2oo3 voting on the outputs and controls the discrete actuator.

**TMR Outputs Voted in Actuator**

Three independent output modules receive the output command from their associated controller, then command the actuator, 2oo3 voting performed in the actuator.
2.3.2 **Dual Redundancy**

The Dual control modes can provide:

- One-out-of-two (1oo2) voting, SIL 3 high/low demand for de-energize-to-trip
- Two-out-of-two (2oo2) voting, SIL 2 low demand for energize and de-energize-to-trip
- Hardware Fault Tolerance (HFT): 1

**Dual Controllers**
Dual Mark VleS controllers work as a controller set synchronizing data every frame (sweep). Each controller receives inputs on both I/O networks, and sends output commands on designated I/O network.

**PC Based Gateway**
PC based communication interface, options:
- OPC-DA server
- OPC-UA server
- Modbus master

**Dual I/O Network**
Ethernet based dual I/O network supports both centralized and distributed I/O modules.

**Embedded Controller Gateway**
Embedded controller for communication interface, options:
- OPC-UA server
- Modbus slave

**Single Sensor**
Single sensor wired to a single input module with dual I/O network to controller set.

**Dual Sensor**
Dual sensors wired to independent input modules with independent I/O networks to controller set.

**TMR Fanned Input**
Single sensor is fanned through a common terminal board to three independent input packs, 2oo3 voting done in the controller set.

**TMR Outputs Voted on Terminal Board**
The three output packs receive an output command from designated controller, the common terminal board then performs 2oo3 voting and controls the actuator.

**1oo2 De-energize to Trip in Output Modules**
Two independent output modules receive the output command from designated controller, combination of two creates 1oo2 de-energize to trip function across the two modules.
2.3.3 Simplex Redundancy

The Simplex control mode is used for one-out-of-one (1oo1), SIL 2 low demand for de-energize-to-trip applications.

**Simplex Controller**
Simplex Mark VleS controller receives inputs and sends outputs on the one I/O network.

**I/O Network**
Ethernet based I/O network supports both centralized and distributed I/O modules.

**Single Sensor**
Single sensor wired to a single input module with a simplex I/O network to controller.

**Dual Sensor**
Dual sensors wired to independent input modules with a simplex I/O network to controller.

**Simplex Output**
One output pack receives an output command from the controller.

**Sensor A**

**Sensor A1**

**Sensor A2**

**Actuator**

**PC Based Gateway**
PC based communication interface, options:
- OPC-DA server
- OPC-UA server
- Modbus master

**Embedded Controller Gateway**
Embedded controller for communication interface, options:
- OPC-UA server
- Modbus slave

**Third Party Control System**
3 Ethernet Networks

3.1 Overview

The integrated control system is based on a hierarchy of Ethernet networks, used to interconnect individual nodes or zones. These networks separate the different communication traffic into layers according to their individual functions. This hierarchy extends from the I/O modules and controllers (providing real-time control of the process) to the HMIs, and out to facility-wide monitoring and external networks (industrial internet).

Each network layer uses industry standard components and protocols to simplify integration between different platforms and improve overall reliability and maintenance. These layers are designated as IONet, Unit Control, Supervisory, and Enterprise in the following figure, which displays a simplified network hierarchy and is not representative of any specific installation.
Simplified Network Hierarchy (Switches Not Shown)
3.1.1 GE Large Industrial Plant Network Architecture

The current networking architecture for GE large industrial plants uses a mesh architecture design (also known as hub and spoke) with redundant network switches. This design enables flexibility for implementation of cyber security offerings, allowing secure access to unit control data from external customer and monitoring networks. Trunks from the root or hub switches to the edge or spoke switches shall be single-mode fiber for all new site installations. These trunks are configured to provide the UDH, PDH, Monitoring Data Highway (MDH), and can also provide other optional networks to further partition network access to specified unit control equipment and data.

Network security can be implemented by adding an additional layer 3 security hardware infrastructure. Network traffic is then regulated by an additional series of routers, switches, and firewalls. The Baseline Security Center appliance can be installed to allow for tighter network security with or without the additional layer 3 security hardware by providing white listing and restricted access to network devices. Various options for existing sites are available to improve network security without having to relocate equipment or cable runs.

In the following figure, both cyber security offerings (the layer 3 hardware and the Baseline Security Center server) are displayed as a simplified example that is not representative of any specific installation. This industrial plant network architecture provides flexibility to cost for sites with various security compliance requirements. A qualified GE networking engineer can determine best fit options for particular customer facilities.
Note Considerations for network upgrades are provided in the section *Network Retrofit Guidelines.*
3.2 IONet Layer

IONet communication is internal between the controller(s) and the I/O modules through an unmanaged IONet switch. IONet redundancy can be one, two, or three networks, and is equal to the controller redundancy.

**Note** Refer to the section *Controller Redundancy* for more information.

The IONet provides direct communication between controllers and I/O modules. IONet EGD protocol (which is different than UDH EDG protocol) is used. The I/O modules send their inputs to the controllers and the controllers send their outputs to the I/O modules each frame, as displayed in the section *Rate of Response*. Examples of IONet traffic are as follows:

- Status of control system input data from the I/O packs to the controller set
- Status of control system output data from the controller set to the I/O packs
- I/O pack configuration data from the ToolboxST application to the controller to the I/O packs
- I/O pack health status data from the packs to the controller
- Field device input data from the I/O pack to the controller

**Note** The ESWx switch is used for IONet communication.

The sharing of input data between two control sets (*Shared IONet*) on a single IONet is available for the following controllers:

- One Mark VIeS Safety controller set and one Mark VIe controller set
- Two Mark VIe controller sets

**Note** A control set is the group of controllers (based on redundancy) with the set of owned I/O modules. From the ToolboxST System Editor Summary View, a control set displays as a single controller.
3.2.1 IONet Specifications

IONets are IEEE 802.3 100 Megabits full duplex Ethernet networks. All traffic on each IONet is deterministic UDP/IP based packets. Each network (red, blue, black) is an independent IP subnet. The IEEE 1588 standard for precision clock synchronization protocol is used to synchronize frame and time between the controllers, and the I/O modules on the IONet. This synchronization provides a high level of traffic flow control on the networks.

The following figure display maximum IONet cable lengths.

<table>
<thead>
<tr>
<th>Item</th>
<th>IONet Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE specification</td>
<td>802.3u</td>
</tr>
<tr>
<td>Wire speed</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>Cable types</td>
<td>100Base-TX: UTP Cat 5e  &lt;br&gt; 100Base-FX: MMF or SMF</td>
</tr>
<tr>
<td>Maximum taps per segment</td>
<td>2</td>
</tr>
<tr>
<td>Maximum packets per network</td>
<td>199</td>
</tr>
<tr>
<td>Maximum number of switches</td>
<td>5</td>
</tr>
<tr>
<td>Topology</td>
<td>Star</td>
</tr>
</tbody>
</table>

For the control system IONet topologies, the following rules apply for deploying SMF systems:

- No more than five switches can be placed in series between controller and remote I/O module.
- The topology should be kept as flat and balanced as possible (star topology).
- Use the GE ESWA or ESWB switch with additional IR SFP single-mode transceiver for SFP1 and SFP2.
  - GE part # 65G2100-009 for single-mode fiber distances up to 2 km
  - GE part # 65G2100-008 for single-mode fiber distances up to 15 km

---

Use of any other switch in this application may cause miss operation and/or damage to the associated equipment.
3.2.2  **IONet Switches**

IONet switches are unmanaged, fully switched, and full-duplex to prevent collisions. They provide data buffering and flow control during the critical input scan. Only industrial grade switches that meet the codes, standards, performance, and environmental criteria for industrial applications are used for the IONet. GE industrial Ethernet 10/100 IONet switches (ESWA and ESWB) have an operating temperature of -40 to 70°C (-40 to 158 °F), have provisions for redundant 18 to 36 V dc power sources (200/400 mA), and can be DIN-rail mounted. The switches also provide LEDs to indicate the status of the IONet link, speed, activity, and duplex.

![16-port ESWB IONet Switch](image)

### 3.2.2.1 Approved IONet Switches

**Caution**

Use only GE-approved Ethernet switches in all control system I/O networks. Unsupported switches can prevent I/O modules from receiving controller outputs.

<table>
<thead>
<tr>
<th>Part #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS420ESWAH1A</td>
<td>8 ports 10/100BASE-TX + 1 port 100BASE-FX LC-type connection</td>
</tr>
<tr>
<td>IS420ESWAH2A</td>
<td>8 ports 10/100BASE-TX + 2 ports 100BASE-FX LC-type connection</td>
</tr>
<tr>
<td>IS420ESWAH3A</td>
<td>8 ports 10/100BASE-TX</td>
</tr>
<tr>
<td>IS420ESWAH4A</td>
<td>8 ports 10/100BASE-TX + 1 port 100BASE-LX10 LC-type connection</td>
</tr>
<tr>
<td>IS420ESWAH5A</td>
<td>8 ports 10/100BASE-TX + 2 ports 100BASE-LX10 LC-type connection</td>
</tr>
<tr>
<td>IS420ESWBH1A</td>
<td>16 ports 10/100BASE-TX + 1 port 100BASE-FX LC-type connection</td>
</tr>
<tr>
<td>IS420ESWBH2A</td>
<td>16 ports 10/100BASE-TX + 2 ports 100BASE-FX LC-type connection</td>
</tr>
<tr>
<td>IS420ESWBH3A</td>
<td>16 ports 10/100BASE-TX</td>
</tr>
<tr>
<td>IS420ESWBH4A</td>
<td>16 ports 10/100BASE-TX + 1 port 100BASE-LX10 LC-type connection</td>
</tr>
<tr>
<td>IS420ESWBH5A</td>
<td>16 ports 10/100BASE-TX + 2 ports 100BASE-LX10 LC-type connection</td>
</tr>
</tbody>
</table>
3.2.3 IONet Switch Guidelines

IONet is presently recommended to pass through a maximum of five switches in series when traveling from an I/O pack to a main controller for the following reasons:

- IONet switches are not managed switches.
- Every Ethernet switch introduces latency into the transmission of Ethernet packets.
- Each controller frame allocates a period of time to service I/O data.

---

**Note:** Maximum of 5 IONet switches that Ethernet packets pass through between I/O pack and controller

---

*Five Maximum IONet Switches in Series Between Controller and I/O Pack*
3.2.4 I/O Pack Ethernet Addressing

On the IONet, I/O packs are assigned IP addresses through the DHCP servers in the controllers. The Host ID presented to the DHCP server is based on the board type and serial number information stored on a serial EEPROM located on the terminal board. Since the Host ID is part of the terminal board, the I/O pack can be replaced without having to update the ToolboxST application or controller communication IDs.

**Note** When a terminal board is replaced, the user must associate the new Host ID to the configured device. The ToolboxST application presents a list of unrecognized devices that have requested IP addresses to simplify this process.

IONets are Class C networks. Each is an independent network with different subnet addresses. The IONet IP host addresses for the controllers are fixed. The IP addresses of the I/O packs are assigned by the ToolboxST application, and the controller automatically distributes the addresses to the I/O packs through a standard Dynamic Host Configuration Protocol (DHCP) server in the controllers.
3.2.5 Shared IONet

Beginning with ControlST V04.06, the Shared IONet feature allows the sharing of Mark VleS Safety inputs with another basic process Mark Vle controller set, saving the cost of redundant sensors and I/O. Specific configurations supported include:

- One Mark VleS Safety controller and one Mark Vle controller
- Two Mark Vle controllers

**Shared IONet Example**

The owner controller allows for the configuration of the owned I/O modules, writes outputs, reads SOEs, and provides diagnostic information. Owned I/O modules are attached to their owner controller that can configure and write to them, and obtain their IP addresses from their owner controller. Outputs from controllers are received by their owned I/O modules (not shared I/O modules).

A shared I/O module sends field device inputs to both its owner controller and to the consumer controller. The consumer controller receives the field device inputs from the shared I/O modules that are owned by the other owner controller. Configuration of the control sets is managed with the ToolboxST application. The computer with the ToolboxST application communicates with the I/O devices through a software gateway function residing in the controllers.

**Note** Refer to the *Mark Controllers Shared IONet User Guide* (GEH-6812) for more information.
3.3 Unit Control Layer

The Unit Control layer or Unit Data Highway (UDH) provides the network connections that support continuous operation of the process equipment, including controller sets (general-purpose, safety loops, turbine-specific, static starter, exciter) and HMIs. The UDH is an Ethernet-based network that provides direct or broadcast peer-to-peer communications between a controller set and an operator/maintenance interface. The controllers operate at a fundamental rate called the frame rate, which is configurable, and is dependant on the controller processor type, the amount of application code being run, and other loads.

Controllers and HMIs use the EGD protocol to exchange real-time data, which on the UDH is based on UDP/IP (for data exchange) and HTTP (for configuration of pages). In addition, SDI protocol is used by the ToolboxST application to download to the controller over the UDH. Alarms and capture buffer uploads (that feed trip logs) are also through the SDI protocol.

**Note** Current controls systems network architecture has UDH, PDH, and MDH connections on a common set of network switches and media trunks.

The UDH connections to the controllers and HMIs are unshielded-twisted pair (UTP) Cat 5e from edge switches. This redundant mesh architecture allows network connectivity even if one cable or switch is faulty. Redundant networks still comprise one logical network.

The following figure displays the UDH network with connections to the controllers and HMIs.
3.3.1 **UDH Communicator in Redundant Controller Set**

In dual or TMR controller sets, a single controller is designated to transmit real-time and alarm data for the set; this is the UDH Communicator. This data includes both control signals (EGD) and alarms (SDI). Since each controller has an independent, physical connection to the UDH, if a UDH network fault occurs where one controller becomes isolated from its companion controllers, the isolated controllers assumes the role of UDH communicator for that network fragment. For this reason, a controller set has only one designated controller, while there could be multiple UDH communicators. The designated controller is always a UDH communicator.

*Note* UDH command data is replicated to redundant controllers by the UDH Communicator, allowing for synchronization across the redundant controller set.

When a controller does not receive external EGD data from its UDH connection, it may request that the data be forwarded across the IONet from another UDH communicator. One or more communicators supply the data, and the requesting controller uses the last data set received. Only the external EGD data used in sequencing by the controllers is forwarded in this manner.

### 3.3.2 UDH Network Specifications

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Network</td>
<td>Ethernet, full duplex, in a single or redundant star configuration</td>
</tr>
<tr>
<td>Media and Distance</td>
<td>Ethernet 100Base-TX for switch to controller/device connections. The cable is 22 to 26 AWG unsheilded twisted pair; category 5e EIA/TIA 568 A/B. Distance is up to 100 m. Ethernet 100Base-FX with fiber-optic cable optional for distances up to 2 km (1.24 mi).</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>At least 25 nodes, given a 25 Hz data rate. Other configurations may be available.</td>
</tr>
<tr>
<td>Type of Nodes Supported</td>
<td>Controllers, PLCs, operator interfaces, and engineering workstations</td>
</tr>
<tr>
<td>Protocol</td>
<td>EGD, based on UDP/IP</td>
</tr>
<tr>
<td>Message Integrity</td>
<td>32-bit CRC appended to each Ethernet packet plus integrity checks built into UDP and EGD</td>
</tr>
<tr>
<td>Time Sync Methods</td>
<td>Network time protocol (NTP), accuracy ±1 ms</td>
</tr>
</tbody>
</table>

### 3.3.3 Control System Devices on UDH

#### 3.3.3.1 Mark VIeS Safety Controller

The Mark VIeS Safety controller is used for safety-critical SIL applications. ToolboxST is used for configuration of the Mark VIeS Safety controllers. For more information, refer to *Mark VIeS Functional Safety Systems for General Market Volume II: System Guide for General-purpose Applications* (GEH-6855_Vol_II), the chapter Controllers.

#### 3.3.3.2 Human-machine Interface

The Human-machine Interface (HMI) is the main operator interface to the Mark VIeS Functional Safety System. HMIs are desktop computers running a Windows® 7 or Windows 10 operating system with multiple communication drivers for the redundant data highways, WorkstationST and ToolboxST applications, and the CIMPLICITY Advanced Viewer for the Graphical User Interface (GUI). The operator initiates commands from the real-time graphic displays, and views real-time process data and alarms. Detailed I/O diagnostics and system configuration is accomplished from the ToolboxST applications.

*Note* HMIs typically connect to both PDH and UDH networks.
The WorkstationST server is the hub of the system, channeling data between the UDH and the PDH, and providing data support and system management. The server also has the responsibility for device communication for both internal and external data interchanges. WorkstationST servers collect data on the UDH, and use the PDH to communicate with HMI viewers. Configuration servers, Historian servers, and Alarm servers are used for large system scaling. Multiple servers can be used to provide redundancy so that communication with the viewers continues even if one server fails.

**Note** The HMI can be configured as a server or viewer, containing tools and utility programs.

### 3.3.3.3 Historian

The Historian computer runs ControlST software including Historian reports, the WorkstationST application, and Trender, and can be configured for PI or Proficy data exchange to an external database server. The Historian is a data archival system based on client-server technology, used for data collection, storage, and display of process data. Flexible tools enable the operator to quickly generate custom trends and reports from the archived process data. The Historian combines high-resolution digital event data from the Mark VIeS Safety controllers with process analog data, creating a sophisticated tool for investigating cause-effect relationships.

The Historian receives data from the controllers over the UDH. The HMIs and other operator interface devices communicate to the Historian through the PDH. Network technology provided by the Windows operating system allows interaction from network computers, including query and view capabilities, using the Historian Client Tool Set. The interface options include the ability to export data into spreadsheet applications.

### 3.3.4 Control Data Highway (CDH)

A second UDH or redundant Ethernet Communication known as the Control Data Highway (CDH) allows two separate controllers to communicate with each other. The second CDH Ethernet can be added to a control system currently using the other UDH Ethernet port. The following table displays requirements for hardware setup.

**Note** To configure a CDH, refer to the ToolboxST User Guide for Mark VIeS Functional Safety Systems (GEH-6862), the section Networks.

#### CDH Hardware Setup

<table>
<thead>
<tr>
<th>First Controller</th>
<th>Second Controller</th>
<th>Ethernet Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplex</td>
<td>Simplex</td>
<td>Each controller connects through the second Ethernet port using a single cross-over category 5 network cable.</td>
</tr>
<tr>
<td>Simplex</td>
<td>Dual</td>
<td>The simplex controller connects to the second Ethernet ports of both the &lt;R&gt; and &lt;S&gt; controllers of the dual system using a category 5 network cable through a network switch.</td>
</tr>
<tr>
<td>Simplex</td>
<td>TMR</td>
<td>The simplex controller connects to the second Ethernet ports of &lt;R&gt;, &lt;S&gt;, and &lt;T&gt; controllers of the TMR system using a category 5 network cable through a network switch.</td>
</tr>
<tr>
<td>Dual</td>
<td>Dual</td>
<td>The &lt;R&gt; and &lt;S&gt; controllers of each system connect using a category 5 network cable through a network switch.</td>
</tr>
<tr>
<td>Dual</td>
<td>TMR</td>
<td>The &lt;R&gt; and &lt;S&gt; controllers of the dual system connect to the &lt;R&gt;, &lt;S&gt;, and &lt;T&gt; controllers of the TMR system using a category 5 network cable through a network switch.</td>
</tr>
<tr>
<td>TMR</td>
<td>TMR</td>
<td>The &lt;R&gt;, &lt;S&gt;, and &lt;T&gt; controllers of each system connect using a category 5 network cable through a network switch. With the TMR and TMR configuration, the customer does not have to use the network if all EGD exchanges run at frame rate.</td>
</tr>
</tbody>
</table>
CDH Application Example
3.4 Supervisory Layer

The Supervisory layer contains the Plant Data Highway (PDH), which connects to WorkstationST servers, Alarm Viewers, printers, historians, and other HMIs. Additional cyber security management equipment can also reside on the PDH. The PDH has no direct connection to the Mark VIeS Safety controllers, which communicate over the UDH.

The PDH network is used to further partition equipment and to restrict access or prevent disruptions to the Mark VIeS Safety controllers (which are busy broadcasting data across the UDH). The PDH should be used to copy or transfer large files from HMI to HMI (for example, CIMPPLICITY projects).

PDH uses redundant cables to form one single logical network, and the mesh architecture is identical to the UDH. The hardware consists of edge Ethernet switches with single-mode fiber-optic trunks connected to root switches, then standard Cat 5e outputs to HMIs and other devices. Redundant Ethernet switches and cables prevent complete network failure if a single component fails. The PDH and the UDH are physically the same network of switches, but use different ports for the particular data highway.

**Supervisory Layer Example**

**PDH Network Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Network</td>
<td>IEEE 802.3 Ethernet in a mesh topology</td>
</tr>
<tr>
<td>Speed</td>
<td>100 megabit per second or with 1000 megabit per second trunks interconnecting switches</td>
</tr>
<tr>
<td>Media and Distance</td>
<td>Ethernet 100Base-TX is used for switch to controller/device connections. Cable is CAT 5e compliant. Distance is up to 100 m (328 ft). Fiber-optic connections, Ethernet 100FX, 1000SX, 1000 LX are used for distances of 2 km (1.24 mi), 550 m (1804.46 ft), and 5 km (3.11 mi), respectively. Fiber-optic cable provides the best signal quality, completely free of electromagnetic interference (EMI) and radio frequency interference (RFI). Large point-to-point distances are possible, and since the cable does not carry electrical charges, ground potential problems are eliminated.</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>Up to 1024 nodes supported</td>
</tr>
<tr>
<td>Protocols</td>
<td>Ethernet-compatible protocol, typically TCP/IP-based. Use OPC UA or Modbus over Ethernet for external communications.</td>
</tr>
<tr>
<td>Message Integrity</td>
<td>32-bit cyclic redundancy code (CRC) appended to each Ethernet packet plus additional checks in protocol used.</td>
</tr>
<tr>
<td>External Interfaces</td>
<td>Various third-party interfaces are available; OPC UA and Modbus are the most common.</td>
</tr>
</tbody>
</table>
3.5 Monitoring Layer

The monitoring data highway (MDH) is used to further partition the flow of data to individual assets, and can include connection to GE Monitoring and Diagnostic (M&D) equipment: the On-Site Monitor (OSM) or Remote Services Gateway (RSG). The data that is allowed to travel over the MDH is managed by two specially configured Cisco 2901 routers. The same mesh architecture and trunks provide the MDH from the root to edge switches, then from special configured ports on the edge switches to the OSM or RSG. Other devices may also be included on the MDH to meet customer requirements. Connectivity to the RSG and OSM is designed during the plant requisition phase, so the MDH is not the only available implementation of GE M&D equipment.

Note Refer to the figure Simplified Network Hierarchy.

3.6 Enterprise Layer

The Enterprise layer allows access to specific control system data or communication sources for facility-wide or group asset management systems. The Enterprise layer can include the following features:

- Additional firewalls, routers, and security features
- Interface to customer network
- GE Demilitarized Zone (DMZ) for hosting GE assets to be accessed external from customer site facility

The Industrial Internet Gateway (IIG) option consists of a firewall appliance that is inserted as a barrier between the ICS VLAN and any other external devices. The firewall establishes security regions, or zones, as defined in the IEC standard 62443 or ISA 99. Equipment is allocated to each zone based on their function and relative security risk to the Mark VIeS Functional Safety System. For diagnostic or analysis purposes, access to specifically tagged control system data or communications can be allowed from outside the plant. Since any outside communications represent a significant risk to the integrity and security of the control system, establishing a DMZ that terminates the outside networks and then only allows specific authenticated traffic to flow from the DMZ to specific hosts behind the DMZ is recommended.

Enterprise Layer Example (does not represent an actual installation)

The IIG establishes four interfaces to connect from the firewall: Customer, DMZ, and ICS VLAN. The Customer interface typically connects to an additional upstream router or firewall provided by the customer. The DMZ has a rule set or policy that is implemented by GE to enable remote access to key resources. These resources are able to collect specifically configured control system data or perform specifically configured control system functions. The ICS VLAN connects from the IIG firewall to a switch that terminates at two routers and then into the root switch and on to the edge switch.
3.7 Ethernet Cabling for Monitoring, Supervisory, and Unit Control Layers

3.7.1 Single-mode Fiber

For new sites, single-mode fiber-optic (SMF) cables are installed for all trunks. Trunks tie edge switches to the root switch. The main advantages of fiber-optic transmission are as follows:

- Fiber segments can be longer than copper because the signal attenuation per foot is less.
- In high-lightning areas, copper cable can pick up currents, which can damage the communications electronics. Since the glass fiber does not conduct electricity, the use of fiber-optic segments avoids pickup and reduces lightning-caused outages.
- Grounding problems are avoided with optical cable. The ground potential can rise when there is a ground fault on transmission lines, caused by currents coming back to the generator neutral point, or lightning.
- Optical cable can be routed through a switchyard or other electrically noisy area and not pick up any interference. This can shorten the required runs and simplify the installation.
- Fiber-optic connections normally have higher signal levels and decreased chances of packet discard from noise corruption. Typical differences in error rate is 10000 lower for fiber-optic cables.
- The cost per connection for fiber may now be less than copper cables. Large, multifiber trunk cables contain many fibers, so cost per foot for each connection may actually cost less than multiple copper cables.
- Fiber-optic cable with proper jacket materials can be run buried in trays or in conduit.
- High-quality fiber-cable is light, tough, and easily pulled. With careful installation, it can last the life of the plant.

Note Refer to Fiber-optic Cable and Patch Panel Selection (GHT-200001) for more information.

3.7.1.1 SMF Specifications

- Single-mode fiber-optic cables are connected from the root switch group to the edge switch group, providing redundancy.
- SMF cable lengths are less than or equal to 15 km (9.32 mi).
- SMF cables must be terminated and/or spliced by a certified fiber-optic cable installer. SMF cables cannot be terminated and/or spliced by requisition or field engineers.
- SMF cables are 8.3/125 µm Core/Cladding diameter with a numeric aperture of 0.13.
### 3.7.1.2 SMF and Trunks

Use the following rules for installing SMF cables:

- SMF cable lengths cannot exceed 15 km (9.32 mi).
- SMF cables must be terminated and/or spliced by a certified fiber-optic cable installer, not by installation engineers.
- SMF is used for new unit installations because the new network switches used have Gbit speeds. SMF has greater distance capability than multi-mode fiber (MMF) in Gbit applications.

The small form-factor pluggable (SFP) or Mini-GBIC is a compact, hot-pluggable transceiver used in network switch applications. It interfaces the network switch to a fiber optic or copper networking cable. It is a popular industry format supported by many network component vendors.

The switches used in the system network design use SFPs with LC Connectors to connect to single mode fiber-optic cable for new installations.
3.7.1.3 **SMF Component Sources**

The following are typical sources for single-mode fiber-optic cables and connectors.

**Fiber-optic Cable:**

Optical Cable Corporation  
5290 Concourse Drive  
Roanoke, VA 24019  
Phone: +1-540-265-0690

Part Numbers (from OCC)

Each of these cables are SMF 8.3/125 um Core/Cladding diameter with a numeric aperture of 0.13.

OC041214-01 4 Fiber Zero Halogen Riser Rated Cable.  
OC041214-02 4 Fiber Zero Halogen with CST Armor.  
OC041214-03 4 Fiber with Flame Retardant Polyurethane.  
OC041214-04 4 Fiber with Flame Retardant Polyurethane with CST Armor

Corning Cable Systems  
PO Box 489  
Hickory, NC 28603-0489  
Phone: +1-800-743-2671

**Fiber-optic Connectors:**

3M® - Connectors and Installation kit  
Thomas and Betts - Connectors and Assembly polishing kit  
Amphenol - Connectors and Termination kit

3.7.2 **Unshielded Twisted Pair (UTP) Copper Cables**

3.7.2.1 **Cat 5e Cables for PDH, UDH, MDH**

These copper cables are used for data highways connections from edge switches to HMIs and controllers.

- High-quality, category 5e UTP cable, for 10/100Base-TX Ethernet  
- Four pairs of twisted 22 AWG or 24 AWG wire  
- Protective plastic jacket  
- Impedance: 75 – 165 Ω  
- Connector: RJ-45 UTP connector for solid wire

3.7.2.2 **Cat 6 Cables for Layer 3 Security Hardware**

These copper cables are used for the additional layer 3 security offering, and provide connections from root switches to an additional series of routers, switches, and firewalls.

- High-quality, category 6 UTP cable, for 10/100Base-TX Ethernet  
- Four pairs of twisted 22 AWG or 24 AWG wire  
- More stringent specifications for crosstalk and system noise  
- Protective plastic jacket  
- Connector: RJ-45 UTP connector for solid wire  
- Backward compatible with the Category 5/5e cable standards
3.7.3 Installing Ethernet

The data highways use a number of 100Base-TX segments and some fiber-optic segments. These guidelines comply with IEEE 802.3 standards for Ethernet. For details on installing individual Ethernet LAN components, refer to the instructions supplied by the manufacturer of that equipment.

**Note** Refer to the section Cable Separation and Routing.

If the connection within a building and the sites share a common ground, it is acceptable to use 100Base-TX connections. If connecting between buildings, or there are differences in ground potential within a building, or distances exceed 100 m (328 ft), then 100Base-FX fiber is required.

3.7.4 Network Retrofit Guidelines

Existing sites should upgrade from Allied Telesis to Cisco switches, and use single-mode fiber (SMF) for all ICS VLAN trunks. These required Cisco network switches can use SFPs with LC connectors to connect to multi-mode fiber (MMF), however this is not recommended because it downgrades them to only 100 Mb speed (with SMF, the switches function at Gb speeds).

**Note** GE recommends replacing MMF with SMF. If not, the network is downgraded to only run at 100 MB speed.

The GE requisition engineer needs to understand the ramifications if existing sites have MMF runs and the options for retermination of Ethernet cables, changes to junction boxes, and so forth. Only a certified cable installer (not the GE field engineer) can do any changes to MMF sites. Also, it is not recommended to use a converter from MMF SC connector to single SMF LC connector as this can cause network latency or introduce an additional failure point.

**Note** Refer to the figure in the section SMF and Trunks that displays the LC connector and SFP.

The options for supporting the new network switch architecture are as follows:

- Re-terminate existing MMF with LC connectors to connect to the SFPs. This downgrades to 100 Mb speed, and requires a certified cable technician.
- Use SC to LC conversion part (323A4747CSP1G). This is not recommended as it can introduce network latency and another possible point of failure. In addition, it still downgrades network to 100 Mb speed.
- Run new SMF cables and use new Cisco switches to full capabilities of Gbit speeds (preferred solution).
3.7.4.1 MMF Cable, Outdoor Use (Data Highways)

Note The following sub-sections provide more details on existing site MMF cabling specifications.

- Multi-mode fiber, 62.5/125 µ core/cladding, 850 nm infrared light
- Four sub-cables with elastomeric jackets and aramid strength members, and plastic outer jacket
- Cable construction: flame retardant pressure extruded polyurethane. Cable diameter: 8.0 mm (0.31 in). Cable weight: 65 Kg/km
- Optical Cable Corporation part number: RK920929-A

![Warning]

Never look directly into a fiber because some longer links use lasers, which can cause permanent eye damage. Most fiber links use LEDs, which cannot damage the eyes.

3.7.4.2 MMF Cable, Heavy Duty Outdoor Use

- Multi-mode fiber, 62.5/125 µ core/cladding, 850 nm infrared light
- Four sub-cables with elastomeric jackets and aramid strength members, and armored outer jacket
- Cable construction: flame retardant pressure extruded polyurethane. Armored with 0.155 mm (0.01 in) steel tape, wound with 2 mm (0.08 in) overlap, and covered with polyethylene outer jacket, 1 to 1.5 mm (0.04 to 0.06 in) thick. Cable diameter: 13 mm (0.51 in). Cable weight: 174 Kg/km
- Optical Cable Corporation part number: RK920929-A-CST

3.7.4.3 MMF Cable, Indoor Use (Data Highways)

- Multi-mode fiber, 62.5/125 µ core/cladding, 850 nm infrared light
- Twin plastic jacketed cables (Zipcord) for indoor use
- Cable construction: tight-buffered fibers surrounded by aramid strength members with a flexible flame retardant jacket. Cable dimensions: 2.9 mm (0.11 in) diameter x 5.8 mm (0.23 in) width. Cable weight: 15 Kg/km
- Corning Cable Systems part number: 002K58-31141–24

3.8 Third-party Communication Links

External communication links are available to interface with third-party plant controls or devices. This allows operators to have access to real-time data, and provides for discrete and analog commands to be passed to the Mark VIeS Safety controller. The Mark VIeS Functional Safety System can be linked to third-parties in several different ways:

- OPC UA direct from the controller (UCSC)
- OPC UA, DA, AE from the WorkstationST server
- Serial or Ethernet Modbus® Slave link from the WorkstationST server
- Ethernet Modbus Slave direct from the Mark VIe controller to the third-party device (Ethernet to serial converter device may be used)

When connecting to third-party devices, the security of the networks and the overall network architecture need to be considered and engineered accordingly. Third-party links are best connected through a firewall where one is available. Consideration must be given to redundancy and availability of communication paths.
4 Communication Protocols

The Mark VIeS Functional Safety System uses a variety of communication protocols to interface both internally between control system equipment and out to specialized field devices and other third-party equipment. This allows some protocols to be sent directly to the Mark VIeS Safety controllers, while others must first communicate with the I/O module that then interfaces with the controller. Other protocols use an HMI with WorkstationST application as a gateway.

External Interface Protocols:
- OPC DA and AE Servers
- OPC UA Server
- Modbus TCP and RTU
- Third-party interface for other protocols

Equipment Control and Configuration Protocols:
- Ethernet Global Data (EGD)
- Network Time Protocol (NTP)
- System Data Interface (SDI)
- OPC UA Server

Equipment Control and Configuration Protocols:
- Ethernet Global Data (EGD)
- Precision Time Protocol IEEE 1588
- System Data Interface (SDI)

Fieldbus Network Protocols:
- Modbus Master RS-232, RS-422, RS-485
- Modbus Master Ethernet
External Interface Protocols

External interface protocols support transmitting and receiving data with third-party control, monitoring, and supervisory systems through the Plant Data Highway (PDH). Communication is important but normally not critical to control and equipment protection. The protocol types include:

- Variable feedback and commands to and from a third-party Distributed Control System (DCS)
- Alarm annunciation and management interface with third-party systems
- Interface with third-party industrial protocol gateways

Equipment Control and Configuration Protocols

The Unit Data Highway (UDH) and IONet networks use several different protocols for equipment control and configuration, as described in the following table.

<table>
<thead>
<tr>
<th>Equipment Control and Configuration Protocols</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Global Data (EGD)</td>
<td>• Feedback and commands between HMI and Mark VIeS Safety controllers on UDH</td>
</tr>
<tr>
<td></td>
<td>• Control data between Mark VIeS Safety controllers on UDH</td>
</tr>
<tr>
<td></td>
<td>• Real time data between I/O modules and Mark VIeS Safety controllers on</td>
</tr>
<tr>
<td></td>
<td>IONet</td>
</tr>
<tr>
<td></td>
<td>• Redundant controller data synchronization</td>
</tr>
<tr>
<td>Network Time Protocol (NTP)</td>
<td>Clock synchronization between Mark VIeS Safety controllers, I/O packs,</td>
</tr>
<tr>
<td></td>
<td>WorkstationST PCs, and a master time source. NTP operates on both the UDH</td>
</tr>
<tr>
<td></td>
<td>and IONet networks.</td>
</tr>
<tr>
<td>System Data Interface (SDI)</td>
<td>• ToolboxST configuration and monitoring with controllers, I/O packs, and</td>
</tr>
<tr>
<td></td>
<td>WorkstationST PCs</td>
</tr>
<tr>
<td></td>
<td>• Real time alarm annunciation and management between controllers and</td>
</tr>
<tr>
<td></td>
<td>WorkstationST Alarm Server</td>
</tr>
<tr>
<td></td>
<td>• Transmission of trip log data from controllers to WorkstationST Alarm</td>
</tr>
<tr>
<td></td>
<td>Server</td>
</tr>
<tr>
<td>OPC-UA Server</td>
<td>Mark VIeS Safety controller interfaces with OPC-UA client functions on UDH</td>
</tr>
<tr>
<td></td>
<td>network</td>
</tr>
<tr>
<td>Precision Time Protocol IEEE 1588</td>
<td>IEEE 1588 is designed for local systems requiring high precision that cannot</td>
</tr>
<tr>
<td></td>
<td>afford the a GPS receiver at each node. The standards describe a</td>
</tr>
<tr>
<td></td>
<td>hierarchical master-slave architecture for clock distribution.</td>
</tr>
</tbody>
</table>

Fieldbus Network Protocols

The Mark VIeS Functional Safety System has limited support of Fieldbus protocols from the gateway controller. Fieldbus protocols network field devices (sensor and actuators) with the control system, enabling diagnostic and configuration functions along with traditional real time control. The Mark VIe gateway controller within the functional safety system supports the following protocols:

- Modbus Master RS-232, RS-422, and RS-485
- Modbus Master Ethernet
4.1 **OPC Protocols**

The Object Linking and Embedding for Process Control (OPC) protocols are widely-adopted standards for communication between vendors across different industries. The OPC Foundation provides the specification for the standards, as well as programming proxy stubs. Supported OPC protocols include:

- OPC Data Access (DA) communicates real-time data
- OPC Alarms and Events (AE) for alarm and event messaging and management
- OPC Unified Architecture (UA) that integrates OPC-DA and OPC-AE into a common framework

Refer to the following documents for additional information:

- *WorkstationST OPC DA Server Instruction Guide* (GEI-100621)
- *WorkstationST OPC AE Server Instruction Guide* (GEI-100624)
- *WorkstationST OPC UA Server Instruction Guide* (GEI-100828)
- *ToolboxST User Guide for Mark VIeS Functional Safety Systems* (GEH-6862) for OPC UA configuration from the Mark VIeS Safety controller and Mark VIeS for OPC DA, AE, HDA, and UA configuration from the WorkstationST server

### 4.1.1 WorkstationST OPC DA Server

OPC Data Access (DA) is designed for real-time data flow between industrial controllers and supervisory functions, such as HMIs and data historians. The WorkstationST-based OPC DA server includes an EGD server and SDI interface for non-EGD variables. In Mark controls applications, the OPC DA server is commonly used to interface with the CIMPLICITY Advanced Viewer and Proficy historian.
4.1.2 Mark VIeS Safety Controller OPC UA Server

An OPC UA server enables the real-time exchange of variables with an OPC UA client. Beginning with ControlST V05.01, it is available in the UCSB/UCSC controller (not available in UCSCS2A Mark VIeS Safety controllers).

4.1.3 WorkstationST OPC AE

OPC Alarm and Event (AE) protocol enables third-party OPC AE clients to obtain live alarm and event notifications. The server complies with the OPC AE 1.1 specification and has an internal client that can be configured to receive external alarm and event data from external OPC AE servers. The following figure illustrates the data flow for a common application.
4.1.4 WorkstationST OPC UA Server

The OPC UA specification combines OPC Data Access (DA), OPC Alarms and Events (AE), and OPC Historical Data Access (HDA), into one interface. The WorkstationST OPC UA server supports:

- OPC Data Access (DA)
- Historical Alarm and Event access (HDA)

In large systems, there are multiple historians that are logging the same variable at different frequencies. And depending on the situation, an OPC HDA client will prefer one historian versus another. The HDA server-client is designed to support this scenario.

The following figure illustrates the data flow for an example system around the WorkstationST OPC UA supported functions.
### 4.2 Modbus Protocol

Modbus is a Request-Response protocol typically used for Supervisory Control and Data Acquisition (SCADA) interface, either as the **Master** for data acquisition by the SCADA or a **Slave** to transmit data to the SCADA. The application data unit (ADU) layer offers three methods of implementation:

- TCP/IP
- RTU
- ASCII

The Request-Response protocol is straightforward to implement; however, it has an inherent latency in the Request-Response cycle between the two computers instead of the Event Driven messages (exception reporting) available with OPC. Additionally, it does not support individual high-resolution time stamps for each alarm and event, but rather a single time stamp for a set of data transmitted from the Slave to the Master upon request.

In the Mark control systems, Modbus is supported in both the controllers and WorkstationST. For the Mark VleS Safety controller, only Ethernet Modbus and the Modbus Read command from the Modbus Master is supported (Serial Modbus and the Write command is not supported).

**Note** Modbus protocol does not provide security against unauthorized commands or interception of data. A separate Modbus gateway should be considered rather than a shared resource.

### 4.2.1 WorkstationST Modbus

Modbus in the WorkstationST has full support, as follows:

- One or multiple Modbus masters running simultaneously
- One or multiple Modbus slaves running simultaneously
- Ethernet or serial communication running simultaneously
- Each Modbus page is configured with ToolboxST, enabling virtually any variable in the system to be mapped to a page
4.2.2 Controller Modbus

The Mark VIeS Safety controllers directly support the Ethernet Modbus Slave interface. The Ethernet Modbus protocol is layered on top of the TCP/IP stream sockets.

Note A subset of the Modbus function codes are supported.
4.3 Ethernet Global Data (EGD)

The EGD protocol on the UDH is used for Mark VIeS Safety controller to Mark VIe HMI (running WorkstationST application), or for Controller to Controller communications, and is configured using the ToolboxST application for the Mark VIeS Safety controller and the WorkstationST application. Controller data configured for transmission over EGD is separated into groups called **exchanges**. Multiple exchanges make up **pages**. Pages can be configured either to a specific address (unicast), if supported, or to multiple consumers at the same time (broadcast or multicast), if supported.

**Note** IONet EGD transmissions occur between controller and I/O packs. IONet EGD communication is transparent to the user, requiring no specific configuration by the user. An IONet EGD report can be generated in ToolboxST to provide network status values for all IONet communication displayed in the current component and reflects totals of the controller exchange. For further details, refer to the **ToolboxST User Guide for Mark VIeS Functional Safety Systems** (GEH-6862), the section **IONet EGD Report**.

Each page is identified by the combination of a Producer ID and an Exchange ID. The consumer recognizes the data and knows where to store it. EGD allows one controller component, referred to as the producer of the data, to simultaneously send information at a fixed periodic rate (frame rate) to any number of peer controller components, known as the consumers. This network supports a large number of controller components capable of both producing and consuming information.

The exchange contains a configuration signature, which displays the revision number of the exchange configuration. If the consumer receives data with an unknown configuration signature, it makes that data unhealthy. If a transmission is interrupted, the receiver waits three periods for the EGD message, after which it times out and the data is considered unhealthy.

**EGD Communications Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example types of</td>
<td>Supervisory data is transmitted periodically at either 480 or 960 ms. Controller data is transmitted to the HMI at frame rate. Controller to</td>
</tr>
<tr>
<td>communication</td>
<td>Controller data is transmitted at 40 ms.</td>
</tr>
<tr>
<td>Message Type</td>
<td>Broadcast – a message sent to all stations on a subnet Unicast – a directed message to one station Multicast – a message sent to a group of</td>
</tr>
<tr>
<td></td>
<td>destinations simultaneously in a single transmission</td>
</tr>
<tr>
<td>Redundancy</td>
<td>Refer to the section <strong>Controller Redundancy to Prevent Loss of Communication.</strong></td>
</tr>
<tr>
<td>Sizes</td>
<td>Each exchange can contain a maximum of 1400 bytes of data (or payload). Pages can contain multiple exchanges. The number of exchanges within a</td>
</tr>
<tr>
<td></td>
<td>page and the number of pages within an EGD node are limited by each EGD device type. The controller does not limit the number of, exchanges, or</td>
</tr>
<tr>
<td></td>
<td>pages.</td>
</tr>
<tr>
<td>Message Integrity</td>
<td>Ethernet supports a 32-bit CRC appended to each Ethernet packet. Reception timeout is determined by EGD device type. The exchange times out after</td>
</tr>
<tr>
<td></td>
<td>an exchange update had not occurred within four times the exchange period, using Sequence ID. Missing/out of order packet detection UDP and IP</td>
</tr>
<tr>
<td></td>
<td>header checksums Configuration signature (data layout revision control) Exchange size validation</td>
</tr>
<tr>
<td>Function Codes</td>
<td>EGD allows each controller to send a block of information to, or receive a block from, other controllers in the system.</td>
</tr>
</tbody>
</table>
4.3.1 Controller Redundancy to Prevent Loss of Communication

In a TMR controller set, each controller receives UDH EGD data independently from a direct Ethernet connection. If the connection is broken, a controller can request the missing data from the second or third controller through the IONet. One controller in a TMR configuration is automatically selected to transmit the EGD data onto the UDH. If the UDH fractures, causing the controllers to be isolated from each other onto different physical network segments, multiple controllers are enabled for transmission. These controllers provide data to each of the segments. These features add a level of Ethernet fault tolerance to the control system.

**Note** There are many features that make the Mark VIeS Safety control system fault tolerant, including the network configuration.

Similarly, with dual redundant controllers, each controller receives UDH EGD data independently from a direct Ethernet connection. If the connection is broken, a controller may request the missing data from the second through the IONet. One controller in a dual controller set is automatically selected to transmit the EGD data onto the UDH. If the UDH fractures causing the controllers to be isolated from each other onto different physical network segments, each controller is enabled for transmission, providing data to both segments.
4.4 System Data Interface (SDI) Protocol

The SDI protocol is a configuration protocol layered upon TCP/IP. SDI is used primarily between the ToolboxST application and the other control system devices on the UDH (controllers, HMIWs, and Historians). SDI commands support configuration downloads, file transfers, debugging, live data access, and a variety of other activities. The SDI connection between the ToolboxST application and the controllers is secured when the Baseline Security Center server is deployed. SDI is also used by the WorkstationST application to monitor controller status, upload trip logs, transport alarms from the devices to the WorkstationST Alarm Server, and to transmit alarm commands to the controllers.

**Note** The Mark VIeS Functional Safety System can support up to a maximum of 10 supervisory computers with individual alarm server connections to a unit controller (not including OSM and Historian).

The total number of SDI connections to any particular controller must be limited to prevent overburdening controller resources, so attention must be paid to the overall system architecture during the application engineering design phase. For example, supporting a large number of WorkstationST Alarm Viewers is best accomplished by deploying a centralized alarm server with a single SDI connection to the controller rather than having each HMI run its own alarm server and therefore a separate SDI connection from the controller to each HMI. In addition, sites with multiple HMIs should limit requests for controller trip logs to be made from only a few HMIs as to not overburden the Mark VIeS Safety controller.

Because EGD does not create a connection per HMI, EGD is typically used for live data transfer and to fan data out from controllers to a large number of HMIs. SDI is used for live data in cases such as ExperTune® support, where a large number of variables must be made available but only a few variables will be accessed at any one time.

An SDI server runs on the Mark VIeS Safety controller to provides a communication mechanism between the controller and the HMI. The server on the controller waits for the ToolboxST and WorkstationST applications to establish connections. It allows the HMI to retrieve data from the controller and for the ToolboxST and WorkstationST applications to run commands in the controller.

SDI is a communication scheme that is built on top of TCP/IP, which provides a reliable delivery mechanism between two communicating parties. Data that is sent from one to the other is guaranteed to be delivered, and delivered in the correct order. When a segment of data is sent by TCP/IP, the sender will wait for an acknowledgement of the segment. If the acknowledgment is not received, the data will be resent. Also, if data is not delivered in the correct order, TCP/IP will reorganize it in the correct order. TCP/IP will also discard any duplicate packets.
4.5 **Network Time Protocol (NTP)**

4.5.1 **Control System Time Synchronization**

The control time synchronization option synchronizes all controllers and HMIs on the UDH to a Global Time Source (GTS) or master time source. Typical GTS systems are Global Positioning Satellite (GPS) receivers such as the StarTime GPS Clock or similar time processing hardware.

**Note** Refer to GEH-6808, the section How to Configure Time Synchronization in the ToolboxST Application.

GE recommends using a dedicated NTP box that is not part of the HMI, but a time/frequency processor board can be placed in the HMI as an alternative. This NTP box or board acquires time from the master time source with a high degree of accuracy. When the HMI receives the time signal, it makes the time information available to the turbine and generator controls on the network by way of NTP. The HMI server provides time to client devices either by broadcasting time, or by responding to NTP time queries, or both methods.

Supplying a time/frequency processor board in another HMI server as a backup can provide redundant time synchronization. Normally, the primary HMI server on the UDH is the time master for the UDH, and other computers without the time/frequency board are time slaves. The time slave computes the difference between the returned time and the recorded time of request and adjusts its internal time. Each time slave can be configured to respond to a time master through unicast mode or broadcast mode.

Local time is used for display of real time data by adding a local time correction to UTC. A node’s internal time clock is normally UTC rather than local. This is done because UTC time steadily increases at a constant rate while corrections are allowed to local time. Historical data is stored with global time to minimize discontinuities.

4.5.2 **Clock Stratum**

**Note** This stratum is different from the clock strata used in telecommunication systems.

The term *Stratum* defines the levels in the hierarchy of clocks that makeup NTP. Each level is assigned a layer number starting with zero at the top. The stratum level defines its distance from the reference clock and prevents cyclical dependencies in the hierarchy.

**Note** Stratum is not an indication of the quality or reliability, it is common to fine Stratum 3 time sources that are higher quality than other Stratum 2 time sources.

**Stratum 0** are devices such as atomic (cesium, rubidium) clocks, GPS clocks, or other radio clocks. Stratum 0 devices are usually not attached to the network. Instead, they are locally connected to computers (for example, through an RS-232 connection using a pulse per second signal).

**Stratum 1** are computers attached to Stratum 0 devices. Normally they act as servers for timing requests from Stratum 2 servers through NTP. These computers are also referred to as time servers.

**Stratum 2** are computers that send NTP requests to Stratum 1 servers. Normally a Stratum 2 computer will reference a number of Stratum 1 servers and use the NTP algorithm to gather the best data sample, dropping any Stratum 1 servers that are wrong. Stratum 2 computers are grouped with other Stratum 2 computers to provide more stable and robust time for all devices in the peer group. Stratum 2 computers normally operate as servers for Stratum 3 NTP requests.

**Stratum 3** are computers that use exactly the same NTP functions of peering and data sampling as Stratum 2, and can be used as servers for lower strata. NTP support up to 256 strata, depending on the version of NTP protocol in use.
4.5.3 **NTP Timestamps**

The 64-bit timestamps used by NTP consist of a 32-bit seconds part and a 32-bit fractional second part, giving NTP a time scale of $2^{32}$ seconds (136 years) and a theoretical resolution of $2^{-32}$ seconds (233 picoseconds). The timescale wraps around every $2^{32}$ seconds (136 years). NTP uses an epoch of January 1, 1900. The first rollover will occur in 2036.

**Note** The current NTPv4 format supports Era Number and Era Offset, which corrects date rollover issues.

Implementations should disambiguate NTP time using a knowledge of the approximate time from other sources. Since NTP only works with the differences between timestamps and never their absolute values, the wraparound is invisible as long as the timestamps are within 68 years of each other. This means that the rollover will be invisible for most running systems, since they will have the correct time to within a very small tolerance. However, systems that are starting up need to know the date within no more than 68 years. The Mark VIeS Functional Safety System uses a battery powered hardware clock to avoid this problem.

4.5.4 **Clock Synchronization Algorithm**

To synchronize its clock with a remote server, the NTP client must compute the round-trip delay time. The round-trip delay $= (t_3 - t_0) - (t_2 - t_1)$.

The time of the request packet transmission is $t_0$, the time of the packet reception is $t_1$, the time of the response packet transmission is $t_2$, and the time of the response packet reception is $t_3$. The elapsed time on the client side between the emission of the request packet and the reception of the response packet is $t_3 - t_0$. The time the server waited before sending the answer is $t_2 - t_1$.

The offset $= ((t_1 - t_0) + (t_2 - t_3)) / 2$.

The NTP synchronization is correct when both the incoming and outgoing routes between the client and the server have a symmetrical nominal delay. If the routes do not have a common nominal delay, the synchronization has a systematic bias of half the difference between the forward and backward travel time.

4.5.5 **Clients and Servers**

The relationship between NTP servers and clients can be configured to operate in several ways. Computers using NTP can operate in different modes with respect to different machines. For example, a single machine could be a client of a machine with a lower stratum number, while being a peer to a machine on the same stratum, and a broadcast server to a number of clients at higher stratum numbers.

**Servers** provide time to clients. Clients send requests to the server and the server sends back a time stamped response, along with information such as accuracy and stratum.

**Clients** get time responses from a NTP server or servers, and uses the information to calibrate its clock. This consists of the client determining how far its clock is off and adjusting its time to match that of the server. The maximum error is determined based on the round-trip delay time for the packet to be received.

**Peers** are members of a group of NTP servers that are tightly coupled. In a group of two peers, at any given time, the most accurate peer is acting as a server and the other peers are acting as clients. The result is that peer groups will have closely synchronized times without requiring a single server to be specified.

**Broadcast or Multicast Mode**

The NTP server can operate in either broadcast or multicast mode. Broadcast servers send periodic time updates to a broadcast address, while multicast servers send periodic updates to a multicast address. Using broadcast packets can greatly reduce the NTP traffic on a network, especially for a network with many NTP clients.
The NTP broadcast or multicast client listens for NTP packets on a broadcast or multicast address. When the first packet is received, it attempts to quantify the delay to the server to better quantify the correct time from later broadcasts. This is accomplished by a series of brief interchanges where the client and server function as a regular (non-broadcast) NTP client and server. Once these interchanges occur, the client has an idea of the network delay and can estimate the time based only on broadcast packets. If this interchange is not desirable, it can be disabled using NTP’s access control features.

4.5.6 Accuracy and Resolution

NTP may take several minutes or even hours to adjust a system's time to the ultimate degree of accuracy. There are several reasons for this. NTP averages the results of several time exchanges to reduce the effects of variable latency, so it may take several minutes for NTP to even reach consensus on what the average latency is. Generally this happens in about five minutes. In addition, it often takes several adjustments for NTP to reach synchronization. Users should not expect NTP to immediately synchronize two clocks.

To allow clocks to quickly achieve high accuracy, yet avoid overshooting the time with large time adjustments, NTP uses a system where large adjustments occur quickly and small adjustments occur over time. For small time differences (less than 128 ms), NTP uses a gradual adjustment. This is called slewing. For larger time differences, the adjustment is immediate. This is called stepping. If the accuracy of the clock becomes too insufficient (off by more than 17 minutes), NTP aborts the NTP daemon, with the assumption that something is wrong with either the server or client. To accurately synchronize with a server, the client needs to avoid step adjustments.

The degree of synchronization to a server is dependent primarily on network latency. Because NTP uses UDP packets, traffic congestion could temporarily prevent synchronization, but the client can still self-adjust, based on its historic drift. Under good conditions on a LAN without too many routers or other sources of network delay, synchronization to within a few milliseconds is normal. Anything that adds latency, such as hubs, switches, routers, or network traffic, will reduce this accuracy.

If even more synchronization accuracy is required, use the following options:

- Connecting directly to a reference clock. Then, accuracy is limited only by the accuracy of the reference clock and the hardware and software latencies involved in these connections.
- Clocks can use pulse per second (PPS) radio receivers, which receive on-the-second radio pulses from a national standards organization. If the time is within a fraction of a second, the PPS pulses can be used to precisely synchronize to the tick of the second. The method achieves accuracies in the tens of microsecond range.

4.6 Fieldbus Communications

Refer to the following table for the available Fieldbus communications types, and refer to the listed documentation for further information.

<table>
<thead>
<tr>
<th>Fieldbus</th>
<th>Hazardous Location Approval?</th>
<th>Safety Version Available?</th>
<th>Related Documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>HART Enabled Analog I/O</td>
<td>Yes</td>
<td>Yes</td>
<td>GEH-6855_VOL_II, Mark VIeS HART Enabled Analog Input/Output (YUAA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GEI-100662, HART Message Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GEH-6821, Device Manager User Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GEI-100757, WorkstationST Device Manager Gateway Instruction Guide</td>
</tr>
<tr>
<td>Serial Communications:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Modbus master serial</td>
<td>Yes</td>
<td>No</td>
<td>GEH-6855_VOL_II, Mark VIe Control Serial Communication (PSCA)</td>
</tr>
</tbody>
</table>
5  Technical Regulations, Standards, and Environment

This chapter describes the technical regulations, standards, and environmental guidelines used for the design of all printed circuit boards, modules, core components, panels, and cabinet line-ups in the control system.

5.1 Safety Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN/CSA® 22.2 No. 61010-1-12</td>
<td>Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use, Part 1: General Requirements</td>
</tr>
<tr>
<td>IEC® 60529</td>
<td>Intrusion Protection Codes IP20 minimum (NEMA 1)</td>
</tr>
</tbody>
</table>
5.2 Conditions for Compliance

If the following conditions for compliance are not met or if unapproved third-party equipment is included in the control panel, then the user is responsible for obtaining the appropriate Low Voltage Safety and EMC certifications for the assembled Mark VIeS Functional Safety System and I/O-based panels.

- Control equipment must be mounted inside a grounded steel enclosure, with doors that require a tool or key to open, and 0.86 mm minimum steel thickness. The enclosure must provide a minimum Intrusion Protection of IP 20 and an internal micro-environment of not more than Pollution Degree 2.

- PE and FE connections must be clearly marked. Customer must connect PE/FE to suitable building ground system through minimum 120 mm² (4/0 AWG) gauge wire. Refer to the chapter Installation Guidelines, the section Grounding for more information.

- Use only Mark VIeS product line controllers, I/O, switches, and power supplies.

- Customer power supply mains connection terminal boards must be clearly marked with L (Line) and N (Neutral) for each AC supply feed connection and Hi (+) and Lo (-) for each DC supply feed connection.

- A Power Requirements nameplate with supply source designations, voltage, and rated current shall be located on the front door of the cabinet with the customer supply mains connections. Refer to the chapter Installation Guidelines, the section Power Requirements for details and nameplate examples.

- The customer shall provide an easily accessible external disconnect device for each of the mains supplies near the control panel. The customer shall provide external 30 A two-pole circuit breaker protection for each 120 V ac and 125 V dc mains and 15 A two-pole circuit breaker protection for each 240 V ac and 220 V dc mains. Circuit breaker can serve as the Disconnect Device if mounted accessible to the control panel.

- Any accessory outlet / socket must be labeled near the outlet with the max rated current.

- All AC and DC power supply mains must connect through a Mark VIeS Overvoltage Transient Protection and EMI Filter circuit. These OV and EMI filter circuits are built-in to the JPDB and JPDF Power Distribution Modules. If JPDB/JPDF are not used to distribute AC and DC power supply mains to the Mark VIeS Safety control, then a separate GE Filter Module 246B8279Gx should be used to filter the mains. Refer to Mark VIe and Mark VIeS Safety Systems Power Distribution Modules (PDM) Application Guide (GEI-100861) for more information.

- Elevation shall not exceed 2000 m for compliance to 61010-1.

- Appropriate Warning nameplates shall be applied to the front door of each panel cabinet and shall include appropriate warning symbols per IEC 61010-1 per Table 1. Refer to the following examples. Warning nameplates shall highlight the presence of electrical circuits that must be disconnected before opening the enclosure for servicing, electrical shock or burn hazard, Qualified Personnel Only, and include symbols 12 and 14 from IEC 61010-1 Table 1.
5.3 Electrical

5.3.1 Electromagnetic Compatibility Directive (EMC) 2014/30/EU

Equipment is not approved for use in a residential, commercial or light industrial environment and should not be connected to a residential electric power network. For EMC Directive compliance, Mark VIeS components shipped loose from the factory must be installed in an enclosure with a minimum steel thickness of 0.86 mm and have a minimum Intrusion Protection (IP) of 20.

The Mark VIeS Safety control system fulfills the requirements listed in the following table.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN 55011:2009 + A1:2010</td>
<td>ISM equipment - Electromagnetic disturbance characteristics</td>
</tr>
<tr>
<td>EN 61000-6-2: 2005</td>
<td>Generic Immunity Industrial Environment</td>
</tr>
<tr>
<td>EN/IEC 61326-1</td>
<td>Electrical equipment for measurement, control and laboratory use – EMC requirements</td>
</tr>
<tr>
<td>IEC 61000-4-2</td>
<td>Electrostatic Discharge Susceptibility</td>
</tr>
<tr>
<td>IEC 61000-4-3</td>
<td>Radiated RF Immunity</td>
</tr>
<tr>
<td>IEC 61000-4-4</td>
<td>Electrical Fast Transient Susceptibility</td>
</tr>
<tr>
<td>IEC 61000-4-5</td>
<td>Surge Immunity</td>
</tr>
<tr>
<td>IEC 61000-4-6</td>
<td>Conducted RF Immunity</td>
</tr>
<tr>
<td>IEC 61000-4-11</td>
<td>Voltage Variation, Dips and Interruptions</td>
</tr>
</tbody>
</table>

5.3.2 Low Voltage Directive 2014/35/EU

Under the conditions specified in this document, the Mark VIeS Functional Safety control fulfills the requirements of CAN/CSA-C22.2 No. 61010-1-12, UL Standard. No. 61010-1 (3rd Edition), and EN 61010-1 (3rd edition) Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use, Part 1: General Requirements.

The protection provided by this equipment may be impaired if it is used in a manner that is not specified by the manufacturer.
5.3.3 **Supply Voltage**

### 5.3.3.1 Line Variations
Control equipment meets the requirements for Overvoltage Category II equipment (IEC 60664-1:2007) under the Conditions for Compliance specified in this document.

**Ac Supplies** – Operating line variations of ±10%


**Dc Supplies** – Operating line variations of -30%, 10% or 140 V dc. This meets IEC 60204-1 2005.

### 5.3.3.2 Voltage Unbalance
Less than 2% of positive sequence component for negative sequence component
Less than 2% of positive sequence component for zero sequence components


### 5.3.3.3 Harmonic Distortion Voltage Unbalance

**Voltage:** Less than 10% of total rms voltages between live conductors for 2nd through 5th harmonic
Additional 2% of total rms voltages between live conductors for sum of 6th through 30th harmonic

This meets IEC 60204-1 2005.

**Current:** The system specification is not per individual equipment
Less than 15% of maximum demand load current for harmonics less than 11
Less than 7% of maximum demand load current for harmonics between 11 and 17
Less than 6% of maximum demand load current for harmonics between 17 and 23
Less than 2.5% of maximum demand load current for harmonics between 23 and 35


### 5.3.3.4 Frequency Variations
Frequency variation of ±5% when operating from ac supplies (20 Hz/sec slew rate)
This exceeds IEC 60204-1 2005.

### 5.3.3.5 Surge
Withstand 2 kV common mode, 1 kV differential mode
This meets IEC 61000-4-5 (ENV50142), and ANSI C62.41 (combination wave).
5.4 Environment

5.4.1 Temperature Considerations

Control electronics can be packaged in a variety of different configurations and designed for different environmental conditions. Proper thermal considerations for active electronics with heat sensitive components must be considered for electronics packaging.

For internal enclosure design considerations, components have an ambient temperature rating. The allowable temperature change without condensation is ±15°C (59 °F) per hour. It is recommended that the environment be maintained at levels less than the maximum rating of the equipment to maximize life expectancy. Packaging the equipment and selecting an appropriate enclosure to maintain the desired temperature is a function of the following:

- Internal heat dissipation from the assemblies
- Outside ambient temperature
- Cooling system (if used)

5.4.2 Enclosures

It is recommended that enclosures not be placed in direct sunlight, and locations near heat generating equipment need to be evaluated. Since the internal temperature increases from the bottom to the top of the enclosure, limiting the temperature at the top is a key design objective.

When selecting an enclosure system for control system hardware, it is the responsibility of the system designer to select an enclosure which will ensure reliable operation of the enclosed equipment. The designer must ensure that the local temperatures inside the enclosure do not exceed the rating of the equipment. For solid door and vented free convection cooling designs, enclosure level analyses which predict overall temperature rises are typically insufficient. It is instead necessary to consider the localized hot spots generated by the distributed heat sources inside the enclosure and verify that those heated zones do not exceed the temperature rating of equipment located in the hot spot.

For all types of enclosure systems, it is important to highlight the potential effect of changes from the original design. GE designed enclosure systems are engineered to maintain the control system components within their specified temperature ratings. Modifying the enclosure or adding additional equipment to the enclosure could potentially compromise the thermal design.
While effective enclosure cooling can be accomplished in many ways, including active cooling like air conditioners, thermoelectric coolers, or vortex coolers, most enclosures are air cooled using one of the following cooling systems. The following are key points to consider when selecting one of these systems and are not intended to take the place of proper enclosure thermal analyses.

5.4.2.1 Solid Door

Solid door enclosures are an occasional necessity where environmental conditions outside the enclosure are potentially harmful to the enclosed equipment. Great care should be used in applying fully enclosed cabinets without supplemental cooling, however, as relatively low power can result in significant internal temperature rises. For this reason, and because the enclosure can also be susceptible to temperature rise due to unanticipated heat sources outside the enclosure, this type of architecture is only recommended where additional analysis validates that thermal design requirements are met.

5.4.2.2 Free Convection Cooled

Free convection cooled ventilated enclosures are commonly used for control equipment and are suitable in many cases for providing sufficient cooling air to internal equipment. The application of filters to the air vents is also a common practice and can provide similar Ingress Protection (IP) rating to a solid door. It should be noted, however, that a filtered cabinet with clogged filters will function like a solid door enclosure and can result in over-temperature conditions. For this reason, it is recommended that the use of filters be limited to cases where the additional IP rating is required. In those cases, the filters must be regularly maintained to ensure proper operation of the cooling system.

5.4.2.3 Fan Cooled

Fan cooled ventilated enclosures are typically used on enclosures where greater thermal margin is desired or where the ambient temperature outside the enclosure is close to the operating temperature of the internal equipment. The fan cooled enclosures can also be provided with filters to improve the IP rating of the enclosure. Again the filters should be regularly maintained to ensure that the cooled system operates to its required capability. While fan cooled systems can ideally maintain internal enclosure temperatures within a few degrees of the external temperature, care must still be used when applying these systems to ensure that all components receive adequate cooling air. It is possible in forced cooling systems to have components which experience greater temperature rises than they would in free convection if the component is located in an area of poor circulation or recirculation.
5.4.3 Temperature of Components

The equipment can be applied as a distributed system, with multiple enclosures mounted in remote locations. Temperature sensors and diagnostics are built into the equipment for continuous monitoring. Each I/O pack’s local processor board contains a temperature sensor. This sensor is located in close proximity to the main processor on the I/O pack processor board and is thus positioned to report the approximate temperature of the main processor itself.

Because this sensor is detecting the internal component temperature, reported temperatures (which are above the ambient temperature rating of the component for the enclosure design) are normal and should not be cause for concern. These temperatures are continuously available in the database and from the ToolboxST application. Detection of an excessive temperature generates a diagnostic alarm, so if there are no temperature alarms, then the equipment is within acceptable range for normal operations. Even if alarms are present, the components themselves should continue to operate well above the alarm limit. Excessive temperatures can however, limit the life of the equipment. With the latest version of BPPC-based processor firmware, the diagnostic alarm for excessive heating is set at 90 °C.

The equipment should be arranged by following normal wiring practices for separation of high and low levels, but in a few cases, heat should be considered. Some components dissipate more heat than others. If there is a significant temperature rise from the bottom of the enclosure to the top, then electronics with significant heat dissipation should be mounted lower in the enclosure.

For internal enclosure design considerations, many Mark VIeS Functional Safety System components have an ambient temperature rating of -40 to 70°C (-40 to 158 °F).

All ATEX applications remain rated for -30 to 65°C (-22 to 149 °F).
5.4.4 Shipping and Storage Temperature

Temperature range during equipment shipping and storage is listed in the following table.

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Temperature Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O pack, modules, and controllers</td>
<td>-40 to 85°C (-40 to 185 °F)</td>
</tr>
<tr>
<td>Control Server</td>
<td>-40 to 65°C (-40 to 149 °F)</td>
</tr>
<tr>
<td>Cisco network switches</td>
<td>-40 to 85°C (-40 to 185 °F)</td>
</tr>
</tbody>
</table>

Refer to [www.Cisco.com](http://www.Cisco.com) for more detailed product information.

5.4.5 Control Room Operating Environment

To ensure proper performance and normal operational life, the control room environment should be maintained as follows:

**Note** Higher ambient temperature decreases the life expectancy of any electronic component. Keeping ambient air in the preferred (cooler) range should extend component life.

Ambient temperature (preferred): 20 to 30°C (68 to 86 °F)
Relative humidity: 5 to 95%, non-condensing

Environments that include excessive amounts of any of the following elements reduce cabinet performance and life:

- Dust, dirt, or foreign matter
- Vibration or shock
- Moisture or vapors
- Rapid temperature changes
- Acid or caustic fumes
- Power line fluctuations
- EMI or noise introduced by:
  - Radio frequency signals, typically from nearby portable transmitters
  - Stray high voltage or high-frequency signals, typically produced by arc welders, unsuppressed relays, contactors, or brake coils operating near control circuits

**Note** Enclosures can be custom engineered for other locations if desired.

The preferred location for the control system cabinet would be in an environmentally controlled room or in the control room itself. The cabinet should be mounted where the floor surface allows for attachment in one plane (a flat, level, and continuous surface). The customer provides the mounting hardware. Lifting lugs are provided and if used, the lifting cables must not exceed 45° from the vertical plane. Finally, the cabinet is equipped with a door handle, which can be locked for security.

Interconnecting cables can be brought into the cabinet through removable access plates. Convection cooling of the cabinet requires that conduits be sealed to the access plates. In addition, air passing through the conduit must be within the acceptable temperature range as listed previously.

5.4.6 Humidity

The ambient humidity range is 5 to 95% non-condensing. This exceeds EN50178.
5.4.7 Elevation

Note † Elevation shall not exceed 2000 m for compliance to 61010-1.

Equipment elevation is related to the equivalent ambient air pressure:

- Normal operation: 0 to 1000 m (0 to 3280.8 ft) at 101.3 to 89.8 kPa
- Extended operation: 1000 to 3000 m† (3280.8 to 6561.7 ft) at 89.8 to 69.7 kPa
  The extended operation and shipping specifications exceed EN50178.
- Shipping: 4600 m (15091.8 ft) at 57.2 kPa max

Note For extended altitude operation, the maximum ambient temperature rating of the equipment should be reduced by 1°C (3.4 °F) for each additional 410 m (1345 ft) above 1000 m (3280.83 ft). Therefore, an I/O pack rated for 65°C (149 °F) at 1000 m (3280.8 ft) will be rated for 62.6°C (144.7 °F) at 2000 m (6562 ft).

5.4.8 Contaminants

The control equipment withstands the following concentrations of corrosive gases at 50% relative humidity and 40°C (104 °F):

Note This meets EN50178 Section A.6.1.4 Table A.2 (m).

<table>
<thead>
<tr>
<th>Corrosive Gas</th>
<th>Concentration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sulfur dioxide (SO2)</td>
<td>30 ppb</td>
</tr>
<tr>
<td>Hydrogen sulfide (H2S)</td>
<td>10 ppb</td>
</tr>
<tr>
<td>Nitrous fumes (NO)</td>
<td>30 ppb</td>
</tr>
<tr>
<td>Chlorine (Cl2)</td>
<td>10 ppb</td>
</tr>
<tr>
<td>Hydrogen fluoride (HF)</td>
<td>10 ppb</td>
</tr>
<tr>
<td>Ammonia (NH3)</td>
<td>500 ppb</td>
</tr>
<tr>
<td>Ozone (O3)</td>
<td>5 ppb</td>
</tr>
</tbody>
</table>

5.4.9 Vibration

5.4.9.1 Seismic

Universal Building Code (UBC) - Seismic Code section 2312 Zone 4 (Optional)

5.4.9.2 Operating/Installed at Site

Vibration of 1.0 G Horizontal, 0.5 G Vertical at 15 to 120 Hz

Refer to Seismic UBC for frequencies lower than 15 Hz.
5.4.10 Applications in Hazardous Locations (HazLoc)

Certain controllers, I/O packs, terminal boards, option boards, trip boards, power distribution boards, and IONet switches are designed to operate in hazardous locations (Class 1, Division 2, Groups A, B, C, and D; Class I, Zone 2; and ATEX II 3 G). Refer to the *Mark VleS Functional Safety System Equipment in Hazardous Locations (HazLoc) Instruction Guide* (GEH-6861) for more information.

**Note**  ATEX applications are rated only for operation within an enclosure with ambient temperatures from -30 to 65 °C (-22 to 158 °F). With the latest version of firmware, the excessive heat diagnostic alarm for BPPC-based I/O packs is set at 90 °C.

5.4.11 Applications in Harsh Environments


**Note**  For Mark VleS Functional Safety System products, G3 compatibility does not depend on conformal coating; however, conformal coating is available for certain Mark VleS products.
6 Installation Guidelines

This chapter defines installation requirements for the control system. Specific topics include GE installation support, wiring practices, grounding, typical equipment weights and dimensions, and power dissipation and heat loss.

Warning

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

6.1 Installation Support

GE’s system warranty provisions require both quality installation and that a qualified service engineer be present at the initial equipment startup. To assist the customer, GE offers both standard and optional installation support. Standard support consists of documents that define and detail installation requirements. Optional support is typically the advisory services that the customer may purchase.

6.1.1 Early Planning

To help ensure a fast and accurate exchange of data, a planning meeting with the customer is recommended early in the project. This meeting should include the customer’s project management and construction engineering representatives. It should accomplish the following:

• Familiarize the customer and construction engineers with the equipment
• Set up a direct communication path between GE and the party making the customer’s installation drawings
• Determine a drawing distribution schedule that meets construction and installation needs
• Establish working procedures and lines of communication for drawing distribution
6.1.2 **GE Installation Documents**

Installation documents consist of both general and requisition-specific information. The cycle time and the project size determine the quantity and level of documentation provided to the customer.

General information, such as this document, provides product-specific guidelines for the equipment. They are intended as supplements to the requisition-specific information.

Requisition documents, such as outline drawings and elementary diagrams provide data specific to a custom application. Therefore, they reflect the customer’s specific installation needs and should be used as the primary data source.

*As-Shipped* drawings consist primarily of elementary diagrams revised to incorporate any revisions or changes made during manufacture and test. These are issued when the equipment is ready to ship. Revisions made after the equipment ships, but before start of installation, are sent as *Field Changes*, with the changes circled and dated.

6.1.3 **Technical Advisory Options**

To assist the customer, GE offers the optional technical advisory services of field engineers for:

- Review of customer’s installation plan
- Installation support

These services are not normally included as installation support or in basic startup and commissioning services displayed below. GE presents installation support options to the customer during the contract negotiation phase.
6.1.4 **Installation Plan and Support**

It is recommended that a GE field representative review all installation/construction drawings and the cable and conduit schedule when completed. This optional review service ensures that the drawings meet installation requirements and are complete.

Optional installation support is offered: planning, practices, equipment placement, and onsite interpretation of construction and equipment drawings. Engineering services are also offered to develop transition and implementation plans to install and commission new equipment in both new and existing (revamp) facilities.

6.1.5 **Customer's Conduit and Cable Schedule**

The customer’s finished conduit and cable schedule should include:

- Interconnection wire list (optional)
- Level definitions
- Shield terminations

The cable and conduit schedule should define signal levels and classes of wiring (refer to the section, *Cable Separation and Routing*). This information should be listed in a separate column to help prevent installation errors.

The cable and conduit schedule should include the signal level definitions in the instructions. This provides all level restriction and practice information needed before installing cables.

The conduit and cable schedule should indicate shield terminal practice for each shielded cable (refer to the section, *Connecting the System*).
6.2 Equipment Receiving and Handling

GE inspects and packs all equipment before shipping it from the factory. A packing list, itemizing the contents of each package, is attached to the side of each case.

---

**Warning**

Only personnel who are adequately trained and thoroughly familiar with the equipment and instructions should install, operate, or maintain the equipment. To prevent damage to the equipment, personnel injury, or death, safe equipment lifting practices must be followed. For example, use adequate tie-off, load-sprea-ding mechanisms, precise lifting control, managed acceleration, the correct forklift/crane rated for equipment tonnage, and so forth.

---

Upon receipt, carefully examine the contents of each shipment and check them with the packing list. Immediately report any shortage, damage, or visual indication of rough handling to the carrier. Then notify both the transportation company and GE. Be sure to include the serial number, part (model) number, GE requisition number, and case number when identifying the missing or damaged part.

---

**Attention**

Immediately upon receiving the system, place it under adequate cover to protect it from adverse conditions. Packing cases are not suitable for outdoor or unprotected storage. Shock caused by rough handling can damage electrical equipment. To prevent such damage when moving the equipment, observe normal precautions along with all handling instructions printed on the case.

---

If technical assistance is required beyond the instructions provided in the documentation, contact the nearest GE Sales or Service Office or an authorized GE Sales Representative.

---

**Warning**

Junction boxes can weigh well over 45.36 Kg (100 lb). Installation should be planned to protect both the box and the personnel. The use of an overhead crane may be required. Consult the site specific shipping and junction box documents. Follow all standard safety practices.

Only personnel who are adequately trained and thoroughly familiar with the equipment and the instructions should install, operate, or maintain this equipment.
6.2.1 Storage

If the system is not installed immediately upon receipt, it must be stored properly to prevent corrosion and deterioration. Since packing cases do not protect the equipment for outdoor storage, the customer must provide a clean, dry place, free of temperature variations, high humidity, and dust.

Use the following guidelines when storing the equipment:

- Place the equipment under adequate cover with the following requirements:
  - Keep the equipment clean and dry, protected from precipitation and flooding.
  - Use only breathable (canvas type) covering material – do not use plastic.
- Unpack the equipment as described, and label it.
- Maintain the following environment in the storage enclosure:
  - Recommended ambient storage temperature limits for the Mark VIeS Safety controller are from -40 to 85°C (-40 to 185 °F).
  - Surrounding air free of dust and corrosive elements, such as salt spray or chemical and electrically conductive contaminants
  - Ambient relative humidity from 5 to 95% with provisions to prevent condensation
  - No rodents, snakes, birds or insects
  - No temperature variations that cause moisture condensation

---

**Attention**

Moisture on certain internal parts can cause electrical failure.

Condensation occurs with temperature drops of 15°C (59 °F) at 50% humidity over a four-hour period, and with smaller temperature variations at higher humidity.

If the storage room temperature varies in such a way, install a reliable heating system that keeps the equipment temperature slightly above that of the ambient air. This can include space heaters or cabinet space heaters (when supplied) inside each enclosure. A 100 W lamp can sometimes serve as a substitute source of heat.

---

**Attention**

To prevent fire hazard, remove all cartons and other such flammable materials packed inside units before energizing any heaters.
6.3 Power Requirements

The control cabinet can accept power from multiple power sources. Each power input source (30 A / 120 V ac, 15 A / 240 V ac, or 30 A / 125 V dc) should feed through its own external, two-pole, thermal, magnetic circuit breaker before entering the control system enclosure. The breaker should be supplied in accordance with required site codes. The circuit breaker must be included in the installation. If used as the panel disconnect, it must be suitably located and easily reachable. The circuit breaker must be marked as the disconnecting device and suitably located near the equipment for servicing.

Control panels and systems may use up to three mains supplies: two for redundant control power (ac and/or dc) and one auxiliary ac supply for accessories such as panel lights and fans. The mains power supply rating labels are provided on the front cabinet door where the panel mains power is to be connected.

The designators on the rating labels are explained as follows:

- AC1 and optional AC2 may be 120 V ac or 240 V ac, 50/60 Hz.
- DC1 and optional DC2 are 220 V dc supplies that may be used instead of AC1 and AC2. DC is an optional floating source 125 V dc supply, usually a battery.
- AUXAC is used only to supply internal auxiliary appliances, such as fans, heaters, lights, or socket outlets. The AC1, AC2, DC, DC1, or DC2 mains supplies may feed one or more Switch Mode Power Supplies to provide 28 V dc control power, or 24 or 48 V dc wetting for contact I/O circuits.

Note To comply with Low Voltage Directive (LVD) 2014/35/EU, all ac and dc power supply mains must connect through a Overvoltage Transient Protection and EMI Filter circuit. These OV and EMI filter circuits are built-in to the JPDB and JPDF Power Distribution Modules. If JPDB/JPDF are not used to distribute ac and dc power supply mains to the Mark VIeS Functional Safety System, then a separate GE Filter Module 246B8279Gx should be used to filter the mains. Refer to Mark VIeS Functional Safety Systems for General Market Volume II: System Guide for General-purpose Applications (GEH-6855_Vol_II), the chapter PDM Power Distribution Modules.

Power requirements for a typical large, four-cabinet turbine control containing controllers, I/O, and terminal boards are displayed in the following table. The total panel current ratings must include the current supplied to external loads, such as solenoids and ignition transformers as described in the notes below the table. Heat dissipation in a typical TMR turbine control is about 1600 watts. However, power supply mains and heat dissipation requirements must be calculated for each Mark VIeS Functional Safety System panel application based on the number and mix of controllers, I/O modules, IONet switches, power supplies, and external loading.

### Power Requirements for Cabinets

<table>
<thead>
<tr>
<th>Cabinet</th>
<th>Voltage</th>
<th>Frequency</th>
<th>Current Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large, four-cabinet</td>
<td>125 V dc</td>
<td>± 10%</td>
<td>N/A</td>
</tr>
<tr>
<td>Four-cabinet turbine</td>
<td>120 V ac</td>
<td>± 10%</td>
<td>50/60 Hz ± 3 Hz</td>
</tr>
<tr>
<td>Control</td>
<td>240 V ac</td>
<td>± 10%</td>
<td>50/60 Hz ± 3 Hz</td>
</tr>
</tbody>
</table>

1. Add 0.5 A dc † continuous for each 125 V dc external solenoid powered.
2. Add 6.0 A rms † for a continuously powered ignition transformer (2 maximum).
3. Add 3.5 A rms † for a continuously powered ignition transformer (2 maximum).
4. Add 2.0 A rms † continuous for each 120 V ac external solenoid powered (inrush 10 A).

Note † These are external and do not create cabinet heat load.
6.4 **Grounding**

This section defines grounding and signal-referencing practices for the control system. This can be used to check for proper grounding and signal reference structure (SRS) after the equipment is installed. If checking the equipment after the power cable has been connected or after power has been applied to the cabling, be sure to follow all safety precautions for working around high voltages.

---

**Warning**

To prevent electric shock, make sure that all power supplies to the equipment are turned off. Then discharge and ground the equipment before performing any act requiring physical contact with the electrical components or wiring. If test equipment cannot be grounded to the equipment under test, the test equipment's case must be shielded to prevent contact by personnel. Be sure to follow the site LOTO and safety practices.

---

6.4.1 **Equipment Grounding**

Equipment grounding and signal referencing have two distinct purposes:

- Equipment grounding protects personnel from risk of serious or fatal electrical shock, burn, fire, and/or other damage to equipment caused by ground faults or lightning.
- Signal referencing helps protect equipment from the effects of internal and external electrical noise, such as lightning or switching surges.

Installation practices must simultaneously comply with all codes in effect at the time and place of installation, and with all practices that improve the immunity of the installation. Code requirements for safety of personnel and equipment must take precedence in the case of any conflict with noise control practices.

---

**Note** In addition to technical regulations, guidance from IEEE Standard 142-2007 *IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems*, and IEEE Standard 1100-2005 *IEEE Recommended Practice for Powering and Grounding Electronic Equipment* are provided by the design and implementation of the system.

The control system has no special or non-standard installation requirements, if installed in compliance with all of the following:

- The NEC or local codes
- With SRS designed to meet IEEE Standard 1100
- Interconnected with signal/power-level separation as defined later

This section provides equipment grounding and bonding guidelines for control and I/O cabinets. These guidelines also apply to motors, transformers, brakes, and reactors. Each of these devices should have its own grounding conductor going directly to the building ground grid.

- Ground each cabinet or cabinet lineup to the equipment ground at the source of power feeding it.
  - See NEC Article 250 for sizing and other requirements for the equipment-grounding conductor.
  - For dc circuits only, the NEC allows the equipment-grounding conductor to be run separate from the circuit conductors.
- With certain restrictions, the NEC allows the metallic raceways or cable trays containing the circuit conductors to serve as the equipment grounding conductor:
  - This use requires that they form a continuous, low-impedance path capable of conducting anticipated fault current.
  - This use requires bonding across loose-fitting joints and discontinuities. See NEC Article 250 for specific bonding requirements. This chapter includes recommendations for high-frequency bonding methods.
  - If metallic raceways or cable trays are not used as the primary equipment-grounding conductor, they should be used as a supplementary equipment grounding conductor. This enhances the safety of the installation and improves the performance of the SRS.
• The equipment-grounding connection for the control cabinets is plated copper bus or stub bus. This connection is bonded to the cabinet enclosure using bolting that keeps the conducting path’s resistance at 1 ohm or less.
• There should be a bonding jumper across the ground bus or floor sill between all shipping splits. The jumper may be a plated metal plate.
• The non-current carrying metal parts of the equipment covered by this section should be bonded to the metallic support structure or building structure supporting this equipment. The equipment mounting method may satisfy this requirement. If supplementary bonding conductors are required, size them the same as equipment-grounding conductors.

6.4.2 Building Grounding System

This section provides guidelines for the building grounding system requirements. For specific requirements, refer to NEC article 250 under the heading Grounding Electrode System.

The guidelines below are for metal-framed buildings. For non-metal framed buildings, consult the GE factory.

The ground electrode system should be composed of steel reinforcing bars in building column piers bonded to the major building columns.

• A buried ground ring should encircle the building. This ring should be interconnected with the bonding conductor running between the steel reinforcing bars and the building columns.
• All underground, metal water piping should be bonded to the building system at the point where the piping crosses the ground ring.
• NEC Article 250 requires that separately derived systems (transformers) be grounded to the nearest effectively grounded metal building structural member.
• Braze or exothermically weld all electrical joints and connections to the building structure, where practical. This type of connection keeps the required good electrical and mechanical properties from deteriorating over time.
6.4.3 *Signal Reference Structure*

On modern equipment communicating at high bandwidths, signals are typically differential and/or isolated electrically or optically. The modern Signal Reference Structure (SRS) system replaces the older single-point grounding system with a much more robust system. The SRS system is also easier to install and maintain.

*Note* The provisions covered in this document may not apply to all installations.

The goal of the SRS is to hold the electronics at or near case potential to prevent unwanted signals from disturbing operation. The following conditions must all be met by an SRS:

- Bonding connections to the SRS must be less than 1/20 wavelength of the highest frequency to which the equipment is susceptible. This prevents standing waves. In modern equipment using high-frequency digital electronics, frequencies as high as 500 MHz should be considered. This translates to about 30 mm (1 in).
- SRS must be a good high-frequency conductor. (Impedance at high frequencies consists primarily of distributed inductance and capacitance.) Surface area is more important than cross-sectional area because of skin effect. Conductivity is less important (steel with large surface area is better than copper with less surface area).
- SRS must consist of multiple paths. This lowers the impedance and the probability of wave reflections and resonance.

In general, a good signal referencing system can be obtained with readily available components in an industrial site. All of the items listed below can be included in an SRS:

- Metal building structural members
- Galvanized steel floor decking under concrete floors
- Woven wire steel reinforcing mesh in concrete floors
- Steel floors in pulpits and power control rooms
- Bolted grid stringers for cellular raised floors
- Steel floor decking or grating on line-mounted equipment
- Galvanized steel culvert stock
- Ferrous metallic cable tray systems
- Raceway (cableway) and raceway support systems
- Embedded steel floor channels

Connection of the protective earth (PE) terminal to the installation ground system must first comply with code requirements and second provide a low-impedance path for high-frequency currents, including lightning surge currents. This grounding conductor must not provide, either intentionally or inadvertently, a path for load current. The system should be designed so that there is no way possible for the control system to be an attractive path for induced currents from any source. This is best accomplished by providing a ground plane that is large and low impedance, so that the entire system remains at the same potential. A metallic system (grid) will accomplish this much better than a system that relies upon earth for connection. At the same time all metallic structures in the system should be effectively bonded both to the grid and to each other, so that bonding conductors rather than control equipment become the path of choice for noise currents of all types.

In the control cabinet, the base is insulated from the chassis and bonded at one point. The grounding recommendations call for the equipment grounding conductor to be 120 mm² (4/0 AWG) gauge wire of shortest possible length connected to the nearest point of building ground system. PE plated copper bus to Earth pit/connection point resistance should be 1 Ohm or less. The Functional Earth (FE) is bonded at one point to the PE ground using two 25 mm² (6 AWG or larger) green/yellow bonding jumpers. These grounding recommendations are illustrated in the following figure.
Grounding Recommendations for Single Control Cabinet

If acceptable by local codes, the bonding jumpers may be removed and a 4/0 AWG identified insulated wire run from FE to the nearest accessible point on the building ground system, or to another ground point as required by the local code.

The grounding method for a larger system is displayed in the following figure. Here the FE is still connected to the control electronics section, but the equipment-grounding conductor is connected to the center cabinet chassis. Individual control and I/O bases are connected with bolted plates.

For armored cables, the armor is an additional current carrying braid that surrounds the internal conductors. This type cable can be used to carry control signals between buildings. The armor carries secondary lightning-induced earth currents, bypassing the control wiring, thus avoiding damage or disturbance to the control system. At the cable ends and at any strategic places between, the armor is grounded to the building ground through the structure of the building with a 360° mechanical and electrical fitting. The armor is normally terminated at the entry point to a metal building or machine. Attention to detail in installing armored cables can significantly reduce induced lightning surges in control wiring.
6.4.3.1 Notes on Grounding

**Bonding to building structure** - The cable tray support system typically provides many bonding connections to building structural steel. If this is not the case, supplemental bonding connections must be made at frequent intervals from the cable tray system to building steel.

**Connected equipment** - Cable tray installations for connected equipment should pay special attention to good high-frequency bonding between the cable tray and the equipment.

**Cable spacing** - Maintain cable spacing between signal levels in cable drops, as recommended in the section [Cable Separation and Routing](#).

**Conduit sleeves** - Where conduit sleeves are used for bottom-entry cables, the sleeves should be bonded to the floor decking and equipment enclosure with short bonding jumpers.

**Embedded conduits** - Bond all embedded conduits to the enclosure with multiple bonding jumper connections following the shortest possible path.

**Galvanized steel sheet floor decking** - Floor decking can serve as a high-frequency signal reference plane for equipment located on upper floors. With typical building construction, there will be a large number of structural connections between the floor decking and building steel. If this is not the case, then an electrical bonding connection must be added between the floor decking and building steel. The added connections need to be as short as possible and of sufficient surface area to be low impedance at high frequencies.

**High-frequency bonding jumpers** - Jumpers must be short, less than 500 mm (20 in) and good high-frequency conductors. Thin, wide metal strips are best with length not more than three times width for best performance. Jumpers can be copper, aluminum, or steel. Steel has the advantage of not creating galvanic half-cells when bonded to other steel parts.

Jumpers must make good electrical contact with both the enclosure and the signal reference structure. Welding is best. If a mechanical connection is used, each end should be fastened with two bolts or screws with star washers backed up by large diameter flat washers.

Each enclosure must have two bonding jumpers of short, random lengths. Random lengths are used so that parallel bonding paths are of different quarter wavelength multiples. Do not fold bonding jumpers or make sharp bends.
Metallic cable tray - System must be installed per NEC Article 318 with signal level spacing per the section *Cable Separation and Routing*. This serves as a signal reference structure between remotely connected pieces of equipment. The large surface area of cable trays provides a low impedance path at high frequencies.

Metallic framing channel - Metal framing channel cable support systems also serve as parts of the SRS. Make certain that channels are well bonded to the equipment enclosure, cable tray, and each other, with large surface area connections to provide low impedance at high frequencies.

Noise-sensitive cables - Try to run noise-sensitive cables tight against a vertical support to allow this support to serve as a reference plane. Cables that are extremely susceptible to noise should be run in a metallic conduit, preferably ferrous. Keep these cables tight against the inside walls of the metallic enclosure, and well away from higher-level cables.

Power cables - Keep single-conductor power cables from the same circuit tightly bundled together to minimize interference with nearby signal cables. Keep 3-phase ac cables in a tight triangular configuration.

Woven wire mesh - Woven wire mesh can serve as a high-frequency signal reference grid for enclosures located on floors not accessible from below. Each adjoining section of mesh must be welded together at intervals not exceeding 500 mm (20 in) to create a continuous reference grid. The woven wire mesh must be bonded at frequent intervals to building structural members along the floor perimeter.

Conduit terminal at cable trays - To provide the best shielding, conduits containing level L cables (see Leveling channels) should be terminated to the tray's side rails (steel solid bottom) with two locknuts and a bushing. Conduit should be terminated to ladder tray side rails with approved clamps.

Where it is not possible to connect conduit directly to tray (such as with large conduit banks), conduit must be terminated with bonding bushings and bonded to tray with short bonding jumpers.

Leveling channels - If the enclosure is mounted on leveling channels, bond the channels to the woven wire mesh with solid-steel wire jumpers of approximately the same gauge as the woven wire mesh. Bolt the enclosure to leveling channel, front and rear.

Signal and power levels - Refer to section *Cable Separation and Routing*, for guidelines.

Solid-bottom tray - Use steel solid bottom cable trays with steel covers for low-level signals most susceptible to noise.
6.4.3.2 Unit Specific Grounding Examples

The control system is applied in a variety of situations, using enclosures that are tailored for the end customer. Field installers need to be well versed in best practices for grounding their equipment for the end customer. Various local guidelines should be followed, as well as the site-specific installation drawings to determine the exact procedures for grounding the unit controls.

With this in mind, it is not possible to provide specific procedures for all variations of field installations of the control system. Properly trained field installers must perform this evaluation, verifying that the frame ground and power ground only connect at one location prior to wiring the cabinet. When multiple installed cabinets are connected together with base grounding plates (as displayed in the figure, Grounding Recommendations for Control Cabinet Lineup), this could result in each cabinet bottom providing a separate parallel path for grounding. This may require opening ground path jumpers on the power distribution boards and disconnecting wiring at the bottom of the adjacent cabinets. By temporarily opening the connection from Functional Earth (FE) to the building grounding system, the installer can confirm if adjacent cabinet connections to ground still exist. Once testing is completed, only one connection to FE per bonded set of cabinets is allowed.

If during inspection of the cabinet (prior to wiring the field devices) there are identified places where jumpers on the power distribution system have ground connections, then pulling those jumpers could be a potential task. Normally, the grounding systems connect to each other at only one location. The following figures provide an example where actions were taken to disconnect wires and remove jumpers.

For this field installation example, these two wires were disconnected from the FE grounding bracket.

Unit Specific Grounding Example (1 of 2)
In the first cabinet, this jumper was removed from both of the JPDF power distribution boards.

Unit Specific Grounding Example (2 of 2)
6.5 **Cable Separation and Routing**

This section provides recommended cabling practices to reduce electrical noise. These practices include signal/power level separation and cable routing guidelines.

---

**Note** Electrical noise from cabling of various voltage levels can interfere with microprocessor-based control systems, causing a malfunction. If a situation at the installation site is not covered in this document, or if these guidelines cannot be met, please contact GE before installing the cable.

---

Early planning enables the customer’s representatives to design adequate separation of embedded conduit. On new installations, sufficient space should be allowed to efficiently arrange mechanical and electrical equipment. On revamps, level rules should be considered during the planning stages to help ensure correct application and a more trouble-free installation.

### 6.5.1 Signal and Power Level Definitions

Signal and power carrying cables are categorized into four defining levels; low, medium, high, and power. Each level can include classes.

#### 6.5.1.1 Low-level Signals (Level L)

Low-level signals are designated as level L. In general these consist of:

- Analog signals 0 through ±50 V dc, < 60 mA
- Digital (logic-level) signals less than 28 V dc
- 4 to 20 mA current loops
- Ac signals less than 24 V ac

The following are specific examples of level L signals used in the control cabling:

---

**Note** Signal input to analog and digital blocks or to programmable logic control (PLC)-related devices should be run as shielded twisted-pair (for example, input from RTDs).

- All analog and digital signals including LVDTs, Servos, RTDs, Analog Inputs and Outputs, and Pyrometer signals
- Thermocouples are in a special category (Level LS) because they generate millivolt signals with very low current.
- Network communication bus signals: Ethernet, IONet, UDH, PDH, RS-232C, and RS-422
- Phone circuits
6.5.1.2 Medium-level Signals (Level M)

Medium-level signals are designated as level M. MPU signals are examples of level M signals used in the controller. These signals consist of:

- Analog signals less than 50 V dc with less than 28 V ac ripple and less than 0.6 A current
- 28 V dc light and switching circuits
- 24 V dc switching circuits
- Analog pulse rate circuits

**Note** Level M and level L signals may be run together only inside the control cabinet.

6.5.1.3 High-level Signals (Level H)

High-level signals are designated as level H. These signals consist of:

- Dc switching signals greater than 28 V dc
- Analog signals greater than 50 V dc with greater than 28 V ac ripple
- Ac feeders less than 20 A, without motor loads

The following are specific examples of level H signals used in cabling:

- Contact inputs
- Relay outputs
- Solenoid outputs
- Potential transformer (PT) and current transformer (CT) circuits

**Note** Flame detector (GM) type signals, 335 V dc, and Ultraviolet detectors are a special category (Level HS). Special low capacitance twisted shielded pair wiring is required.

6.5.1.4 Power (Level P)

Power wiring is designated as level P. This consists of ac and dc buses 0 – 600 V with currents 20 A – 800 A. The following are specific examples of level P signals used in plant cabling:

- Motor armature loops
- Generator armature loops
- Ac power input and dc outputs
- Primary and secondary wiring of transformers above 5 kVA
- SCR field exciter ac power input and dc output
- Static exciters (regulated and unregulated) ac power and dc output
- 250 V shop bus
- Machine fields
6.5.1.5 Class Codes

Certain conditions can require that specific wires within a level be grouped in the same cable. This is indicated by class codes, defined as follows:

S Special handling of specified levels can require special spacing of conduit and trays. Check dimension chart for levels. These wires include:
  - Signals from COMM field and line resistors
  - Signals from line shunts to regulators

U High voltage potential unfused wires over 600 V dc

PS Power greater than 600 V dc and/or greater than 800 A

If there is no class code, there are no grouping restrictions within designated levels

6.5.1.6 Marking Cables to Identify Levels

Mark the cableway cables, conduit, and trays in a way that clearly identify their signal/power levels. This helps ensure correct level separation for proper installation. It can also be useful during equipment maintenance.

Cables can be marked by any means that makes the level easy to recognize (for example, coding or numbering). Conduit and trays should be marked at junction points or at periodic intervals.

6.5.2 Cableway Spacing Guidelines

Spacing (or clearance) between cableways (trays and conduit) depends on the level of the wiring inside them. For correct level separation when installing cable, the customer should apply the general practices along with the specific spacing values for tray/tray, conduit/tray, conduit/conduit, cable/conduit, and cable/cable distances as discussed below.
### 6.5.2.1 General Practices

The following general practices should be used for all levels of cabling:

- All cables of like signal levels and power levels must be grouped together in like cableways.
- In general, different levels must run in separate cableways, as defined in the different levels. Intermixing cannot be allowed, except as noted by exception.
- Interconnecting wire runs should carry a level designation.
- If wires are the same level and same type signal, group those wires from one cabinet to any one specific location together in multiconductor cables.
- When unlike signals must cross in trays or conduit, cross them in 90° angles at maximum spacing. Where it is not possible to maintain spacing, place a grounded steel barrier between unlike levels at the crossover point.
- When entering terminal equipment where it is difficult to maintain the specific spacing guidelines displayed in the following tables, keep parallel runs to a minimum, not to exceed 1.5 m (5 ft) in the overall run.
- Where the tables display tray or conduit spacing as 0, the levels can be run together. Spacing for other levels must be based on the worst condition.
- Trays for all levels should be solidly grounded with good ground continuity. Conduit should provide shielding.

The following general practices should be used for specific levels of cabling:

- When separate trays are impractical, levels L and M can be combined in a common tray if a grounded steel barrier separates levels. This practice is not as effective as tray separation, and may require some rerouting at system startup. If levels L and M are run side-by-side, a 50 mm (1.97 in) minimum spacing is recommended.
- Locate levels L and M trays and conduit closest to the control panels.
- Trays containing level L and level M wiring should have solid galvanized steel bottoms and sides and be covered to provide complete shielding. There must be positive and continuous cover contact to side rails to avoid high-reluctance air gaps, which impair shielding.
- Trays containing levels other than L and M wiring can have ventilation slots or louvers.
- Trays and conduit containing levels L, M, and H(S) should not be routed parallel to high power equipment enclosures of 100 kV and larger at a spacing of less than 1.5 m (5 ft) for trays, and 750 mm (2.5 ft) for conduit.
- Level H and H(S) can be combined in the same tray or conduit but cannot be combined in the same cable.
- Level H(S) is listed only for information since many customers want to isolate unfused high voltage potential wires.
- Do not run levels H and H(S) in the same conduit as level P.
- Where practical for level P and/or P(S) wiring, route the complete power circuit between equipment in the same tray or conduit. This minimizes the possibility of power and control circuits encircling each other.
6.5.2.2 Tray and Conduit Spacing

The following tables display the recommended distances between metal trays and metal conduit carrying cables with various signal levels, and the cable-to-cable distance of conduit and trays.

Table 1. Spacing Between Metal Cable Trays, inches (mm)

<table>
<thead>
<tr>
<th>Level</th>
<th>L</th>
<th>M</th>
<th>H</th>
<th>H(S)</th>
<th>P</th>
<th>P(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>0</td>
<td>1(25)</td>
<td>6(150)</td>
<td>6(150)</td>
<td>26(660)</td>
<td>26(660)</td>
</tr>
<tr>
<td>M</td>
<td>0</td>
<td>6(150)</td>
<td>6(150)</td>
<td>18(457)</td>
<td>26(660)</td>
<td></td>
</tr>
<tr>
<td>H</td>
<td>0</td>
<td>0</td>
<td>8(302)</td>
<td>12(305)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H(S)</td>
<td>0</td>
<td>0</td>
<td>8(302)</td>
<td>12(305)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P(S)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recommended minimum distances between trays from the top of one tray to the bottom of the tray above, or between the sides of adjacent trays.

Table 2. Spacing Between Metal Trays and Conduit, inches (mm)

<table>
<thead>
<tr>
<th>Level</th>
<th>L</th>
<th>M</th>
<th>H</th>
<th>H(S)</th>
<th>P</th>
<th>P(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>0</td>
<td>1(25)</td>
<td>4(102)</td>
<td>4(102)</td>
<td>18(457)</td>
<td>18(457)</td>
</tr>
<tr>
<td>M</td>
<td>0</td>
<td>4(102)</td>
<td>4(102)</td>
<td>12(305)</td>
<td>18(457)</td>
<td></td>
</tr>
<tr>
<td>H</td>
<td>0</td>
<td>0</td>
<td>4(102)</td>
<td>8(203)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H(S)</td>
<td>0</td>
<td>0</td>
<td>4(102)</td>
<td>8(203)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P(S)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recommended minimum distance between the outside surfaces of metal trays and conduit.

Use Table 1 if the distance between trays or conduit and power equipment up to 100 kVA is less than 1.5 m (5 ft).

Table 3. Spacing Between Metal Conduit Runs, inches (mm)

<table>
<thead>
<tr>
<th>Level</th>
<th>L</th>
<th>M</th>
<th>H</th>
<th>H(S)</th>
<th>P</th>
<th>P(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>0</td>
<td>1(25)</td>
<td>3(76)</td>
<td>3(76)</td>
<td>12(305)</td>
<td>12(305)</td>
</tr>
<tr>
<td>M</td>
<td>0</td>
<td>3(76)</td>
<td>3(76)</td>
<td>9(229)</td>
<td>12(305)</td>
<td></td>
</tr>
<tr>
<td>H</td>
<td>0</td>
<td>0</td>
<td>3(76)</td>
<td>6(150)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H(S)</td>
<td>0</td>
<td>0</td>
<td>3(76)</td>
<td>6(150)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P(S)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recommended minimum distance between the outside surfaces of metal conduit run in banks.

Table 4. Spacing Between Cable and Metal Conduit, inches (mm)

<table>
<thead>
<tr>
<th>Level</th>
<th>L</th>
<th>M</th>
<th>H</th>
<th>H(S)</th>
<th>P</th>
<th>P(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>0</td>
<td>2(51)</td>
<td>4(102)</td>
<td>4(102)</td>
<td>20(508)</td>
<td>48(1219)</td>
</tr>
<tr>
<td>M</td>
<td>0</td>
<td>4(102)</td>
<td>4(102)</td>
<td>20(508)</td>
<td>48(1219)</td>
<td></td>
</tr>
<tr>
<td>H</td>
<td>0</td>
<td>0</td>
<td>12(305)</td>
<td>18(457)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H(S)</td>
<td>0</td>
<td>0</td>
<td>12(305)</td>
<td>18(457)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P(S)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recommended minimum distance between the outside surfaces of cables and metal conduit.

Table 5. Spacing Between Cable and Cable, inches (mm)

<table>
<thead>
<tr>
<th>Level</th>
<th>L</th>
<th>M</th>
<th>H</th>
<th>H(S)</th>
<th>P</th>
<th>P(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>0</td>
<td>2(51)</td>
<td>6(150)</td>
<td>6(150)</td>
<td>28(711)</td>
<td>84(2134)</td>
</tr>
<tr>
<td>M</td>
<td>0</td>
<td>6(150)</td>
<td>6(150)</td>
<td>28(711)</td>
<td>84(2134)</td>
<td></td>
</tr>
<tr>
<td>H</td>
<td>0</td>
<td>0</td>
<td>20(508)</td>
<td>29(737)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H(S)</td>
<td>0</td>
<td>0</td>
<td>20(508)</td>
<td>29(737)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P(S)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recommended minimum distance between the outside surfaces of cables.

Cable, Tray, and Conduit Spacing

Installation Guidelines GEH-6855_Vol_I_A System Guide 119
Public Information
6.5.3 Cable Routing Guidelines

6.5.3.1 Pullboxes and Junction Boxes

Keep signal and power levels separate inside pullboxes and junction boxes. Use grounded steel barriers to maintain level spacing. Tray-to-conduit transition spacing and separation are a potential source of noise. Be sure to cross unlike levels at right angles and maintain required separation. Use level spacing. Protect transition areas according to the level spacing recommendations.

6.5.3.2 Transitional Areas

When entering or leaving conduit or trays, ensure cables of unlike levels are not mixed. If the installation needs parallel runs over 1.5 m (5 ft), grounded steel barriers may be needed for proper level separation.

6.5.3.3 Cabling for Retrofits

Reducing electrical noise on retrofits requires careful planning. Lower and higher levels should never encircle each other or run parallel for long distances. It is practical to use existing conduit or trays as long as the level spacing can be maintained for the full length of the run. Existing cables are generally of high voltage potential and noise producing. Therefore, route levels L and M in a path apart from existing cables when possible. Use barriers in existing pullboxes and junction boxes for level L wiring to minimize noise potential. Do not loop level L signals around high control or level P conduit or trays.

6.5.3.4 Conduit Around and Through Machinery Housing

Care should be taken to plan level spacing on both embedded and exposed conduit in and around machinery. Runs containing mixed levels should be minimized to 1.5 m (5 ft) or less overall. Conduit running through and attached to machinery housing should follow level spacing recommendations. This should be discussed with the contractor early in the project.

Trunnions entering floor mounted operator station cabinets should be kept as short as possible when used as cableways. This helps minimize parallel runs of unlike levels to a maximum of 1.5 m (5 ft) before entering the equipment. Where different signal/power levels are running together for short distances, each level should be connected by cord ties, barriers, or some logical method to prevent intermixing.

6.5.3.5 RF Interference

To prevent radio frequency (RF) interference, take care when routing power cables near radio-controlled devices (for example, cranes) and audio/visual systems (public address and closed-circuit television systems).

6.5.3.6 Suppression

Unless specifically noted otherwise, suppression (for example, a snubber) is required on all inductive devices controlled by an output. This suppression minimizes noise and prevents damage caused by electrical surges. Standard relay and solenoid output boards have adequate suppression.
6.6  **Power and I/O Field Wiring**

### 6.6.1 General Requirements

- Maximum length (unless specified) 300 m (984.25 ft)
- Individual minimum stated wire size is for electrical needs
- Clamp-type terminals accept two 14 AWG wires or one 12 AWG wire
- Terminal blocks accept two 12 AWG wires
- PTs and CTs use 10 AWG stranded wire

**Note** Wires with appropriate temperature ratings must be used, especially in applications where the internal panel ambient temperature can exceed 60°C (140 °F).

It is standard practice to use shielded cable with control equipment. Shielding provides the following benefits:

- Generally, shielding protects a wire or combination of wires from its environment.
- Low-level signals may require shielding to prevent signal interference due to the capacitive coupling effect between two sources of potential energy.

### 6.6.2 I/O Field Wiring Restrictions

<table>
<thead>
<tr>
<th>Board</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBAI</td>
<td>15 Ω maximum two-way cable resistance, cable length up to 300 m (984 ft)</td>
</tr>
<tr>
<td>STAI</td>
<td>15 Ω maximum two-way cable resistance, cable length up to 300 m (984 ft)</td>
</tr>
<tr>
<td>SAII</td>
<td>15 Ω maximum two-way cable resistance, cable length up to 300 m (984 ft)</td>
</tr>
<tr>
<td>TBAO</td>
<td>Driven devices should not exceed a resistance of 900 Ω and can be located up to 300 m (984 ft) from the control cabinet</td>
</tr>
<tr>
<td>STAO</td>
<td>Driven devices should not exceed a resistance of 900 Ω and can be located up to 300 m (984 ft) from the control cabinet</td>
</tr>
<tr>
<td>PSCA</td>
<td>GEH-6855_Vol_II lists cable distance and maximum baud rate for the three supported communication standards</td>
</tr>
<tr>
<td>YVIB</td>
<td>Often sensors used with this input module impose their own cabling requirements</td>
</tr>
</tbody>
</table>

### 6.6.3 Wire Sizes

The recommended current carrying capacity for flexible wires up to 1,000 V, PVC insulated, based on DIN VDE 0298 Part 4, is displayed in following table. Cross section references of mm² versus AWG are based on EN 60204 Part 1, VDE 0113 Part 1. NFPA 70 (NEC) may require larger wire sizes based on the type of wire used.

<table>
<thead>
<tr>
<th>Wire Area (mm²)</th>
<th>Wire Area (Circular mils)</th>
<th>Max Current (Approx. Amp)</th>
<th>Wire Size AWG No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.75</td>
<td>1,480</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>0.82</td>
<td>1,618</td>
<td>16</td>
<td>18</td>
</tr>
<tr>
<td>1</td>
<td>1,974</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>1.31</td>
<td>2,585</td>
<td>22</td>
<td>16</td>
</tr>
<tr>
<td>1.5</td>
<td>2,960</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>2.08</td>
<td>4,105</td>
<td>29</td>
<td>14</td>
</tr>
<tr>
<td>2.5</td>
<td>4,934</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>3.31</td>
<td>6,532</td>
<td>37</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>7,894</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>Wire Area (mm²)</td>
<td>Wire Area (Circular mils)</td>
<td>Max Current (Approx. Amp)</td>
<td>Wire Size AWG No.</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------</td>
<td>---------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>5.26</td>
<td>10,381</td>
<td>50</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>11,841</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td>8.36</td>
<td>16,499</td>
<td>65</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>19,735</td>
<td>73</td>
<td></td>
</tr>
<tr>
<td>13.3</td>
<td>26,248</td>
<td>87</td>
<td>6</td>
</tr>
<tr>
<td>16</td>
<td>31,576</td>
<td>98</td>
<td></td>
</tr>
<tr>
<td>21.15</td>
<td>41,740</td>
<td>116</td>
<td>4</td>
</tr>
<tr>
<td>25</td>
<td>49,338</td>
<td>129</td>
<td></td>
</tr>
<tr>
<td>33.6</td>
<td>66,310</td>
<td>154</td>
<td>2</td>
</tr>
<tr>
<td>35</td>
<td>69,073</td>
<td>158</td>
<td></td>
</tr>
<tr>
<td>42.4</td>
<td>83,677</td>
<td>178</td>
<td>1</td>
</tr>
<tr>
<td>50</td>
<td>98,676</td>
<td>198</td>
<td></td>
</tr>
<tr>
<td>53.5</td>
<td>105,584</td>
<td>206</td>
<td>1/0</td>
</tr>
<tr>
<td>67.4</td>
<td>133,016</td>
<td>239</td>
<td>2/0</td>
</tr>
<tr>
<td>70</td>
<td>138,147</td>
<td>245</td>
<td></td>
</tr>
<tr>
<td>85</td>
<td>167,750</td>
<td>273</td>
<td>3/0</td>
</tr>
<tr>
<td>95</td>
<td>187,485</td>
<td>292</td>
<td></td>
</tr>
<tr>
<td>107</td>
<td>211,167</td>
<td>317</td>
<td>4/0</td>
</tr>
<tr>
<td>120</td>
<td>236,823</td>
<td>344</td>
<td></td>
</tr>
<tr>
<td>127</td>
<td>250,000</td>
<td>354</td>
<td>250 MCM</td>
</tr>
<tr>
<td>150</td>
<td>296,029</td>
<td>391</td>
<td></td>
</tr>
<tr>
<td>185</td>
<td>365,102</td>
<td>448</td>
<td></td>
</tr>
<tr>
<td>240</td>
<td>473,646</td>
<td>528</td>
<td></td>
</tr>
<tr>
<td>253</td>
<td>500,000</td>
<td>546</td>
<td>500 MCM</td>
</tr>
<tr>
<td>300</td>
<td>592,058</td>
<td>608</td>
<td></td>
</tr>
<tr>
<td>400</td>
<td>789,410</td>
<td>726</td>
<td></td>
</tr>
</tbody>
</table>
6.6.4 **Low-voltage Shielded Power Cables**

This section defines the minimum requirements for low-voltage shielded cable. These guidelines should be used along with the level practices and routing guidelines provided previously.

*Note* The specifications listed are for sensitive computer-based controls. Cabling for less sensitive controls should be considered on an individual basis.

---

### 6.6.4.1 Single-conductor Shielded Cable, Rated 300 V

- 18 AWG minimum, stranded single-conductor insulated with minimum 85% to 100% coverage shield
- Protective insulating cover for shield
- Wire rating: 300 V minimum
- Maximum capacitance between conductor and shield: 492 pF/m (150 pF/ft)

### 6.6.4.2 Multi-conductor Shielded Cable, Rated 300 V

- 18 AWG minimum, stranded conductors individually insulated per cable with minimum 85 to 100% coverage shield
- Protective insulating cover for shield
- Wire rating: 300 V minimum
- Mutual capacitance between conductors with shield grounded: 394 pF/m (120 pF/ft) maximum
- Capacitance between one conductor and all other conductors and grounded shield: 213 pF/m (65 pF/ft)

### 6.6.4.3 Shielded Twisted Pair (STP) Cable, Rated 300 V

- Two 18 AWG minimum, stranded conductors individually insulated with minimum 85 to 100% coverage shield
- Protective insulating cover for shield
- Wire rating: 300 V minimum
- Mutual capacitance between conductors with shield grounded: 394 pF/m (120 pF/ft) maximum
- Capacitance between one conductor and the other conductor and grounded shield: 213 pF/m (65 pF/ft) maximum

### 6.6.4.4 Instrument Cable, 4 – 20 mA

- With Tefzel® insulation and jacket: Belden® catalog no. 85231 or equivalent
- With plastic jacket: Belden catalog no. 9316 or equivalent
6.7 Connecting Power to the System

The cabinets come complete with internal cabling. Power cables from the power distribution module to the control modules, interface modules, and terminal boards are secured by plastic cable cleats located behind the riser brackets. The mounting brackets and plates cover most of this cabling.

6.7.1 I/O Wiring

I/O connections are made to terminal blocks on the control system terminal boards. Shielding connections to the shield bar located to the left of the terminal board are displayed in the following figure.

The grounded shield bars provide an equipotential ground plane to which all cable shield drain wires should be connected, with as short a pigtail as practical. The length should not exceed 5 cm (2 in) to reduce the high-frequency impedance of the shield ground. Reducing the length of the pigtail should take precedence over reducing the length of exposed wire within the cabinet. Pigtails should not be connected except at the grounding bars provided, to avoid loops and maintain a radial grounding system. Shields should be insulated up to the pigtail. In most instances, shields should not be connected at the far end of the cable, to avoid circulating power-frequency currents induced by pickup.

A small capacitor can be used to ground the far end of the shield, producing a hybrid ground system, improving noise immunity. Shields must continue across junction boxes between the control and the turbine, and should match up with the signal they are shielding. Avoid hard grounding the shield at the junction boxes, but small capacitors to ground at junction boxes may improve immunity.
6.8 **Startup Checks**

All control system panels have cables pre-installed and factory-tested before shipment. However, final checks should be made after installation and before starting the equipment.

---

**Warning**

This equipment contains a potential hazard of electrical shock or burn. Power is provided by the control system to various input and output devices. External sources of power may be present in the control system that are NOT switched by the control power circuit breaker(s). Before handling or connecting any conductors to the equipment, use proper safety precautions to ensure all power is turned off.

---

Inspect the cabinet components for any damage possibly occurring during shipping. Check for loose cables, wires, connections, or loose components, such as relays or retainer clips. Report all damage that occurred during shipping to GE Product Service.

---

**Attention**

Deposits containing ionic contaminants such as salt are difficult to remove completely, and may combine with moisture to cause irreparable damage to the boards.
6.8.1 Power Wiring and Circuit Checks

The 125 V dc supply must be installed and maintained so that it meets requirements of IEC 61010-1 cl. 6.3.1 to be considered Not Hazardous Live. The BJS berg jumper must be installed in the JPDF to provide the monitored ground reference for the 125 V dc. If there are multiple JPDFs connected to the dc mains, only one should have the Berg jumper installed. The dc mains must be floated (isolated from ground) if they are connected to a 125 V dc supply (battery).

---

**Note** The JPDF module must provide the single, monitored, ground reference point for the 125 V dc system.

---

**Warning**

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

---

The following steps should be completed to check the cabinet wiring and circuits.

➢➢

**To check the power wiring**

1. Ensure that all incoming power wiring agrees with the electrical drawings, supplied with the panel, and is complete and correct.

2. Ensure that the incoming power wiring conforms to approved wiring practices as described previously.

3. Ensure that all electrical terminal connections are tight.

4. Ensure that no wiring has been damaged or frayed during installation. Replace if necessary.

5. Check that incoming power (125 V dc, 115 V ac, 230 V ac) is the correct voltage and frequency, and is clean and free of noise. Make sure the DACA converters, if used, are set to the correct voltage by selecting the JTX1 (115 V ac) or JTX2 (230 V ac) jumper positions on the top of the converter.

6. If the installation includes more than one JPDF on an interconnected 125 V dc system, the BJS jumper must be installed in one and only one JPDF. This is because the parallel connection of more than one ground reference circuit will reduce the impedance to the point where the 125 V dc no longer meets the not hazardous live requirement.

Verifying that the 125 V dc is properly grounded. A qualified person using appropriate safety procedures and equipment should make tests. Measure the current from first the P125 V dc, and then the N125 V dc, using a 2000 Ω, 10 W resistor to the protective conductor terminal of the Mark VIeS Functional Safety System in series with a dc ammeter. The measured current should be 1.7 to 2.0 mA, (the tolerance will depend on the test resistor and the JPDF tolerances). If the measured current exceeds 2.0 mA, the system must be cleared of the extra ground(s). A test current of about 65 mA, usually indicates one or more hard grounds on the system, while currents in multiples of 1 mA usually indicate more than one BJS jumper is installed.

---

**Note** At this point the system is ready for initial application of power.
6.8.2 **Control Cabinet Hardware Checks**

Before and after applying power to a Mark VIeS Functional Safety System control cabinet, perform the following hardware components checks. Refer to *Mark VIe and Mark VIeS Safety Systems Power Distribution Modules (PDM) Application Guide* (GEI-100861) for more information on architecture and components.

**Note** The control cabinet should be in a dust-free environment; the controllers, I/O packs, and IONet switches are sensitive to dust.

---

**Warning**

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

➢➢

**To check the control hardware before initial power on**

1. Follow all site safety practices as defined by EHS, including LOTO.
2. Put the cabinet in a safe state and verify that power has been removed from the PDM.
3. From within the enclosure, verify that all the control equipment 28 V dc power connectors are connected or disconnected as expected.
4. Verify that any of the J-type boards with switches (JPDB for example) have them in the ON or OFF positions as expected.
5. Verify that the control power supplies are properly configured.
6. If present, verify that the DACA is properly configured. Check that the power connector is attached for the correct input voltage level.
7. Verify that Cat 5e cables for IONet are connected properly from switches ESWA or ESWB to the controllers, I/O packs, and PPDA (if present).
8. Verify that the Cat 5e cables for UDH or other networks are properly connected to the Mark VIeS Safety controllers.
9. Check every field wire coming into the enclosure to the specified terminal board screw using GE supplied site-specific wiring diagrams.

➢➢

**To check the control hardware after initial power on**

1. Use the GE supplied site-specific wiring diagram for the cabinet to verify that the expected component’s power is on. The chapter *Troubleshooting* provides help if needed.
2. From the ToolboxST Component Editor Hardware tab, verify that the I/O packs and controllers have been properly configured and then complete the procedures to setup, download, and go online with the system.
3. Visually inspect the LED indicators on the components. (Refer to the *Mark VIeS Functional Safety Systems for General Market Volume II: System Guide for General-purpose Applications*, GEH-6855_Vol_I, for specific component LED information.)
• IONet switches display network activity only if the incoming network cable has network traffic.

Example Network Switch Activity LED Indicators

• I/O pack’s ATTN LED is on when beginning to boot. Once booted, the I/O pack displays other LED indicators.

Example I/O Pack LED Indicators
• Controller’s Boot LED indicates if the Network IP address has been properly configured.
Notes
7 Alarm Overview

Alarm management is a vital component to operating and maintaining equipment in power generation or other industrial plants. Reporting of abnormal conditions and trips (with accurate descriptions and high-resolution time tags to identify the origin) are vital to minimizing mean-time-to-repair (MTTR). The Mark VIeS Functional Safety System with the ControlST Software Suite provides solutions for alarm management, prioritization, classification, measurement, and reporting.

Each unit control (such as a turbine control) has its own embedded alarm detection and management system to ensure the integrity of its data. Alarm logic is embedded in the overall unit control logic, and runs at the same frame rate, synchronous with the control logic. Therefore, any trip emanating from the control due to a condition such as low lube oil pressure will have a first-out alarm time tag assigned during the same data frame as the trip command. Since trips are significant events, they are initiated locally from sensor inputs and internal algorithms. The unit alarm management system is immune to failures of peripheral networks and supervisory equipment. Should a network malfunction occur, local alarm logic, time tags, and messages are retained in the local controller and are available to operator stations upon restoration of the network.

In normal operation, each unit control communicates its alarm messages and local high-resolution time tags to operator stations where they are combined into the overall plant alarm management system. The integrity of the time stamps that the operator sees depends on the system time synchronization, which consists of time coherence and time accuracy. Within a unit control, there is ±1 ms time coherence between time stamps in controllers due to the distributed nature of its I/O. Time synchronization on the I/O networks is implemented with IEEE-1588 Precision Clock Synchronization Protocol. In addition, there is ±2 ms time coherence between any two units on the control network (UDH), which is implemented with Network Time Protocol (NTP).

A time-server is normally provided for plant-wide time synchronization. The server communicates on the control network (UDH) and information network (PDH) with ±1ms accuracy between a plant data point and a time source such as a global positioning satellite (GPS). IRIG-B is a commonly used synchronization protocol.
Example of the Alarm System Showing Multiple Alarm Display Mechanisms
Plant operators need to prioritize alarms, filter data, lockout nuisance alarms, analyze data, and more effectively apply the available data to plant operation. To meet this need, the Mark VIeS Functional Safety System with ControlST is based on ANSI/ISA-18.2, Management of Alarm Systems for the Process Industries to assist in improving the safety, quality, and productivity of the facility. HMIs running WorkstationST and ToolboxST applications provide a user-friendly environment for visualization, navigation, change management, and analysis of alarm and event conditions with a common, time-coherent data set for the plant.

The comprehensive plant alarm system provided by the ControlST software suite allows operator stations to see alarms from both GE controls and third-party components, using OPC to integrate alarm messages and time stamps from third-party servers with native Mark VIeS alarm data. The OPC Alarm and Events (AE) has typically been used for this purpose, but now with ControlST V05.03 or later, the newer OPC Unified Architecture (UA) protocol can be used. OPC UA combines the features of OPC DA, AE, and HDA with the flexibility to include some or all of these features.

An operator needs to be able to see and react to alarms and events from any of the equipment within his jurisdiction. The WorkstationST Alarm Server gathers alarms from the controllers or other sources and makes them available to alarm clients such as WorkstationST Alarm Viewer displays. Alarms are also recorded and made available to the WorkstationST Alarm Viewer for historical viewing and statistical analysis. The WorkstationST Alarm Viewer may run on the same computer as the WorkstationST Alarm Server or on a separate computer. Refer to the WorkstationST Alarm Server Instruction Guide (GEI-100626) for further details.
7.1 Alarm Types

Standards for alarming define five types that occur in the Mark VIeS Functional Safety System as follows:

- **Process alarms** are created to announce abnormal conditions in the plant equipment that the operator needs to be aware of or take action on. The focus of the alarm management system is based on capturing, filtering, visualizing, and analyzing these process alarm messages. Typically, the word alarm is used to mean a process alarm, since that type is most commonly used and experienced in the field.

- **Hold list alarms** advise the operator that an automatic sequence is on hold. Then, the operator can choose to override the hold if permitted by the protective logic. Holds are typically used in steam turbine controls. An example hold list alarm is the notification used with controlling the thermal expansion in steam turbines.

- **Diagnostic alarms** alert the operator to fault conditions in the control equipment (such as a power supply failure) or an interruption in network communications (issue with cabling or switches).

- **Events** are important normal occurrences in the operation of a plant such as the closure of the generator breaker.

- **Sequence of Events (SOE)** provide a ±1 ms time stamped message whenever a field contact opens or closes. This precision is particularly useful in determining the root cause of trips in a power plant that is subject to trips from electrical equipment and grid dynamics. To be effective, time synchronized sequence-of-events reporting is needed throughout the plant. In general, ±1 ms resolution is available on native Mark VIe and Mark VIeS discrete input modules for dc contacts and available with less resolution for ac contacts. Time resolution for third-party I/O on fieldbus networks is application-specific.

The maximum number of new alarms that can be processed are as follows:

- A burst load of 400 alarm transitions are supported in a single frame without missing a transition in the internal queue.
- A constant load of 100 alarm transitions per second are supported without missing a transition in the internal queue.

7.2 Controller Alarm Subsystem

The Mark VIeS Safety controllers contain an embedded alarm subsystem that can handle the following data types:

- Boolean Alarms
- Boolean Events
- Boolean Holds

Beginning with ControlST V04.04, the following limits to the number of data types are enforced by the ToolboxST application during the build operation of the Mark VIe, EX2100e, and LS2100e controller:

- There can be a maximum of 4096 Boolean Alarms, Analog Alarms, and Holds, but this includes a limit of 512 Holds
- Boolean Events are limited to 2048

The state information of each alarm, including the Hold state and the Acknowledged state, is stored in the alarm queue of the controller. There are several benefits to having the persistent alarm state information stored in the controller itself rather than in the HMI:

- If an HMI fails, the alarms are still in the controller. Another HMI can obtain the information from the controller making all the alarms and their state available for viewing. Neither alarms nor their state are lost.
- Multiple HMIs may be used to view alarms simultaneously since each HMI only needs to get information directly from the controller.
- Each alarm has a timestamp of when it became active. If an alarm transitions to inactive and then back to active, the latest time stamp of when the alarm became active is retained.
- In a redundant controller set, the alarm queue is synchronized so that if one controller fails the other(s) have the alarms. During normal operation, the designated controller sends the alarm states to the HMI and to the other controllers to keep them in sync. If a controller fails and is replaced, the new controller will initialize its state from the designated controller. Therefore, alarms are not lost if one of the controllers in a redundant set reboots.
7.3 Diagnostic Alarms

Controllers and I/O packs generate diagnostic alarms to indicate potential issues with control system equipment or the connections to it (power, networks, and so forth). I/O pack firmware checks raw inputs from hardware and creates alarm bits at frame rate, queueing any resulting alarms.

- Each type of I/O pack has hardware limit checking based on high and low levels set near the ends of the operating range. When the limit is exceeded, a logic signal is set. (ATTN_xxxx).
- In TMR systems, a limit alarm called TMR Diff Limt is created if any of the three inputs differ from the voted value by more than a preset amount. This limit value is configured by the user creating a voting alarm indicating a problem exists with a specific input.
- If any one of the hardware limits is set, a pack composite diagnostic alarm, L3DIAG_xxxx, where xxxx is created in the board name. This signal can be used to trigger a process alarm.
- The diagnostic signals can be individually latched, and then reset with the RESET_DIA signal from the HMI.

In addition to inputs, each board has its own diagnostics. The I/O boards have a processor stall timer, which generates the signal, SYSFAIL. This signal lights the red LED on the front panel and queues and alarm. The watchdog timers are set at 150 ms. If an I/O board times out, the outputs go to a fail-safe condition which is zero (or open contacts) and the input data is put in the default condition, which is zero.

7.3.1 Viewing Controller Diagnostics from the ToolboxST Application

From the ToolboxST application, the Controller Diagnostics View displays errors or warnings that occur in the hardware component and could cause the component to function improperly. Retrieving these messages should be the first step in diagnosing any hardware or communication issues.

➢➢ To open Controller Diagnostics view: from the View menu, select Diagnostics and Controller Diagnostics.
7.3.2 Resetting Diagnostic Alarms

There are three ways to reset a diagnostic alarm:

- from the ToolboxST Application (as displayed in the figure on the previous page of the document)
- from the Alarm Viewer (right-click the alarm and select Reset) (refer to GEI-100620)
- using a SYS_OUTPUTS block and the RSTDIAG input pin (refer to GEI-100682)

Note Application engineers often program a CIMPLICITY push-button to allow for a diagnostic reset using the RSTDIAG input pin.

7.3.3 Time Stamping

The time stamp applied to an I/O pack diagnostic alarm is the time when that diagnostic originated. When a diagnostic has been reset, a subsequent occurrence of the same diagnostic then creates a new time stamp. If a diagnostic alarm occurs several times without being reset by the operator, it retains the original time stamp.

The WorkstationST* Alarm Viewer Live View displays the diagnostic time when each transition to the active state occurs. If a diagnostic alarm occurs several times, a new time stamp is applied by the WorkstationST Alarm Server for display in the WorkstationST Alarm Viewer. However, if the Alarm Server is restarted, or if the connection to the I/O pack's owning controller is lost, then the Alarm Server must get an updated dump of the current state of all I/O pack diagnostics from the controller. Since the I/O pack only retains the original time when the diagnostic first occurred, the Alarm Server and Alarm Viewer would then show the original time after the restart and reconnect. Refer to GEI-100620, WorkstationST Alarm Viewer.

The ToolboxST application has an I/O Diagnostic Viewer for displaying the I/O pack's current diagnostics alarm status. It displays the I/O pack's known time stamp, which is the time of the first occurrence of the diagnostic. Each time the user refreshes the viewer, the pack's time stamp is obtained. Refer to ToolboxST User Guide for Mark VIeS Functional Safety Systems (GEH-6862), the section I/O Diagnostic Viewer.

7.3.4 Voter Disagreement Diagnostics Detection (VDDD)

Each I/O pack produces diagnostic alarms when it is configured as TMR and any of its inputs disagree with the voted value of that input by more than a configured amount. This feature allows the user to find and fix potential problems that would otherwise be masked by the redundancy of the control system. The user can view these diagnostics the same way one views other diagnostic alarms. The designated controller triggers these diagnostic alarms when an individual input disagrees with the voted value for a number of consecutive frames. The diagnostic clears when the disagreement clears for a number of frames.

The user configures voter disagreement diagnostics for each variable. Boolean variables are all enabled or disabled by setting the DiagVoteEnab signal to enable under the configuration section for each input. Analog variables are configured using the TMR_DiffLimit setting under configuration for each point. This difference limit is defined in one of two ways. It is implemented as a fixed engineering units (EU) value for certain inputs and as a percent of configured span for other variables. For example, if a point is configured as a 4-20 mA input scaled as 0-40 EU, its TMR_DiffLimit is defined as a percent of (40-0). The type of limit checking used is spelled out in the dialog box for the TMR_DiffLimit for each board type. The following table provides some examples of TMR limit checking.
### Type of TMR Limit Checking

<table>
<thead>
<tr>
<th>I/O Processor Board</th>
<th>Type of I/O</th>
<th>Delta Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>YAIC</td>
<td>Analog</td>
<td>% of Configured Span</td>
</tr>
<tr>
<td>YDIA</td>
<td>Contact Input</td>
<td>Voting Disagreement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Diagnostic Enable/Disable</td>
</tr>
<tr>
<td>YDOA</td>
<td>Relay feedback</td>
<td>Voting Disagreement</td>
</tr>
<tr>
<td></td>
<td>Fuse feedback</td>
<td>Diagnostic Enable/Disable</td>
</tr>
<tr>
<td>YVIB</td>
<td>Vibration Inputs</td>
<td>Engineering Units</td>
</tr>
</tbody>
</table>

**Note**  All unused variables will have the voter disagreement checking disabled to prevent nuisance diagnostics.
7.4 Process Alarms

Process alarms are generated by the transition of Boolean or analog variables configured by the ToolboxST application with the alarm attribute. The variables are driven by sequencing or tied to input points to map values directly from I/O boards. Process alarm variables are scanned during each frame after the sequencing is run. In TMR systems, process alarm variables are voted and the resulting composite is present in each controller.

Process alarms are time stamped and stored in a local queue in the controller. Changes representing alarms are time stamped and sent to the alarm queue. Reports containing alarm information are assembled and sent over the UDH to the HMIs. Here the alarms are again queued and prepared for operator display by the alarm viewer.

Operator commands from the HMI, such as alarm Acknowledge, Reset, Lock, and Unlock, are sent back over the UDH to the alarm queue where they change the status of the appropriate alarm. An alarm entry is removed from the controller queue when it has returned to normal and has been acknowledged by an operator. The operator or the controller can take action based on the process alarms setup.

Process alarms can also be created by having the WorkstationST application scan variables and create alarms. This is useful when alarms need to be created from data coming from third-party equipment.

7.4.1 Process Alarm States and Queue in Controller

Once alarms are generated by the controller (the alarm source), they are placed and maintained in a queue in the controller. The controller maintains the active alarms with controller state (Active, HI, Low, and so forth) and with the command given from the operator (acknowledged, silenced, and so forth). The queue structure holds the alarm state, process value, priority, and shelved, inhibited, silenced, locked, and acknowledged states as well as a timestamp. For a simple Boolean alarm, the controller alarm state indicates if the process value is beyond alarm limits. Because analog alarms are configured with more detailed threshold information, analog alarms also have additional information attached to the alarm state relating to those threshold limits, such as if the process value is below the LO threshold or above the HI threshold.

7.4.2 Process Alarm Development

Process Alarms are typically developed in the Mark VIeS Safety controller by using the ToolboxST application. An application engineer creates Mark VIeS application code in Relay Ladder Diagram (RLD) or Function Block language. Alarms are configured using individual variables in the controller. An Alarm Class, defined at a system level, can be created and referenced by each alarmed variable to control aspects of the alarm such as priority and color indications. Refer to GEH-6808, the section How to Configure Alarm Capability in the ToolboxST Application.

Every Boolean variable used in the controller application code has a set of properties including an alarmed property. An application engineer can set the alarmed property of a Boolean variable so that the variable will cause an alarm anytime its value transitions to True. For example, if the application code has a Boolean variable called OVERSPD, the user need only set the Alarm property of OVERSPD to cause an alarm to be generated any time OVERSPD transitions to True.

Analog variables such as integers and floating point REAL values can also be configured for alarming. An application designer can set High, Low, and other threshold limits of an Analog variable (such as an Integer or REAL) so that an alarm is generated whenever those thresholds are crossed. This configuration creates child variables in the control logic, and those variables can be accessed and modified by application code created by the user. For example, if an integer PRES02 variable exists and the user enables the High threshold limit, a PRES02.H variable is created in application code. The user can write other application code to change the value of the PRES02.H threshold limit dynamically as the controller is running, and can use the PRES02.H to drive other control logic. This supports alarm rationalization techniques advocated by ISA 18.2 to reduce the number of false positive alarms.
The application designer can use as much Relay Ladder or Function Block Diagram logic as is needed to condition the Boolean or Analog variable such that alarms are not triggered unless conditions truly warrant creation of an alarm. This ability to use arbitrary control logic to condition alarm generation in real-time at fast sample rates is a very powerful capability afforded by creating alarms in the controller itself. Alarm detection happens as part of the Mark VIeS Safety controller frame (part of the outputs phase of processing and synchronous to the control logic). Because of this, timestamps of alarms are very accurate, and can easily be compared to other data collected from the controller since that data is time stamped with exactly the same time as the alarm. Specialized alarm blocks are also available, effectively capturing many design patterns for pre-alarm signal conditioning in a reusable library form.

The alarm system collects exactly what the controller logic detects so there are no losses in resolution and there is no resampling. The Mark VIeS Safety controller can run frames as fast as once every 10 milliseconds, and uses POSIX timestamps with nanosecond resolution and sub millisecond accuracy. Comparison of timestamps from alarms that originate from different controllers devices is possible since the controllers and HMIs are all time synchronized with NTP.

When an alarm Boolean first transitions to True, the controller creates a new instance of an alarm record structure and places it in the alarm queue of the controller. Later, the Boolean might transition to False, but unless the operator takes action, the alarm queue entry remains. If the Boolean again transitions to True, the alarm queue entry is updated. The alarm queue entry will not be deleted unless the alarm is set for Auto Acknowledge. The operator can acknowledge the alarm, the alarmed Boolean can change to False, and the operator can reset the alarm. The acknowledge and reset may be accomplished in single keystroke if the auto-acknowledge feature is enabled.

Events and Holds can be created in a fashion that is very similar to that of process alarms. Sequence of Events (SOEs) are created by setting a similar property on an IO Point. Diagnostic Alarms can also be created in the controller by transmission from other subsystems. Diagnostic Alarms are created by firmware itself, not by the application engineer.

### 7.4.2.1 Intrinsic Variables and Totalizers

Intrinsic variables allow alarm manager commands to be generated when a variable changes state. Totalizers are timers and counters that store critical data such as number of trips, number of starts, and number of fired hours. The controller provides a special block, Totalizer, which maintains values in a protected section of non-volatile RAM (NVRAM). ControlST V07.04 and lower supports 64 totalizers. ControlST V07.05 and higher supports 128 totalizers. This Totalizer block should be placed in a protected macro to prevent the logic driving its counters from being modified. Users can set and clear Totalizer counter values from the ToolboxST application. The standard block library instruction guide (GEI-100682) provides more details on using the Totalizer block. Refer to ToolboxST User Guide for Mark VIeS Functional Safety Systems (GEH-6862), the section Intrinsic Variables.

### 7.4.2.2 External Process Alarms

Process alarms may also enter the alarm system through the WorkstationST application rather than through the Mark VIeS Safety controller. The WorkstationST application can scan Boolean variables and create alarms in a manner similar to the Mark VIeS Safety controller. Additionally, the WorkstationST application can import alarms from other systems using OPC AE or OPC UA.
7.5 Alarm Communication Flow

One goal of the alarm system communications infrastructure is to replicate each alarm queue at the point of visualization. Each Mark VIeS Safety controller has an alarm queue and each Alarm Viewer must have a copy of those alarm queue entries in order to display them. The Alarm Viewers get their information from one or more Alarm Servers, which in turn get queue entries from the source of the alarms. Each system has at least one Alarm Server. Many systems have a pair of Alarm Server for redundancy, and these Alarm Servers communicate to synchronize their state machines. The control systems can support up to a maximum of 10 supervisory PCs with individual alarm server connections to a unit controller (not including OSM and Historian if present).

A custom TCP/IP based protocol named SDI is used to transfer alarms from the Mark VIeS Safety controller to the Alarm Server. Other custom protocols are used to communicate between the Alarm Server and alarm clients such as the Alarm Viewer. A change based communication mechanism is used by these protocols, so a client must connect to a server and request an alarm dump to get the current state of all the alarms maintained by the server. Subsequent changes to that state are communicated to the client by transition messages. If the connection is lost or if there is any question that the client has the correct state, the process must be repeated. This is the nature of all change detect protocols, including those used by OPC; the client must first learn the current state before change of state notifications are useful.

Configuration information about variables, including alarmed variables, is preloaded into the WorkstationST device by using the ToolboxST application, and is updated automatically by a WorkstationST service that monitors the controller and uploads configuration information. This mechanism provides WorkstationST devices and their clients with metadata like variable data types, descriptions, units, display limits, and all of the other attributes of variables and objects that hold variables. Such metadata is displayed in the CIMPLICITY and Alarm Viewer screens. Keeping this metadata accurate even as the controllers and other parts of the system are modified is aided by the unidirectional data flow afforded by having the controllers own the variables and alarms and their generation. Each HMI can have the same view of the alarm information because each HMI gets the data and metadata from an alarm server which in turn gets the information from the alarm source, typically the Mark VIeS Safety controller. Synchronization issue with alarm state that can be caused by having multiple alarm sources for the same alarm are thereby eliminated.
8 Troubleshooting

The following sections are provided to aid in common troubleshooting of control system equipment.

8.1 Controller, I/O Pack, IONet Switch Not Powering On

The following figure provides a decision making flow to aid in troubleshooting power loss to controllers, I/O packs, or IONet switches.

---

**Warning**

Follow all site safety requirements and precautions, including PPE to diagnose the issue while maintaining power to the enclosure.

---

Troubleshooting GEH-6855_Vol_I_A System Guide 141 Public Information
Troubleshooting Power Loss to Controllers, I/O Packs, or IONet Switches
## 8.1.1 I/O Pack Power LED Not Lit

### I/O Pack Power Troubleshooting

<table>
<thead>
<tr>
<th>Condition</th>
<th>Potential Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>All other I/O packs on same terminal board have power lights lit</td>
<td>I/O pack power connector</td>
</tr>
<tr>
<td></td>
<td>I/O pack failure</td>
</tr>
<tr>
<td>Some other I/O packs on same terminal board have power LED lit (or simplex board)</td>
<td>I/O pack power connector</td>
</tr>
<tr>
<td></td>
<td>I/O pack failure</td>
</tr>
<tr>
<td></td>
<td>Terminal board failure</td>
</tr>
<tr>
<td>No other I/O packs on same terminal board have power LEDs lit</td>
<td>Terminal board power</td>
</tr>
<tr>
<td></td>
<td>Terminal board failure</td>
</tr>
</tbody>
</table>
8.2 Unable to Download to Controller

Note Before downloading, the controller IP address must be setup. Refer to GEH-6808 for more information.

Diagram:

Unable to download to controller

Flashing

Is the boot LED lit continuously or flashing?

Troubleshoot the flashing codes

Continuous

Are you able to ping to the controller?

Check communication between HMI and controller

Yes

Re-flash and download to the controller

Is download successful?

Yes

Finish

No

Replace the controller keeping the existing Flash card

Is download successful?

Yes

Finish

No

Replace Flash card
8.3 **Controller Not In Controlling State**

Pre-requisites for attaining a controlling state include:

- The controller should have the base load, firmware, and application code downloaded.
- All controllers (in dual or TMR) should communicate with each other over the IONet.
- All I/O modules (if configured as required) should be able to communicate with the controllers.

**Note** The control system may not reach a controlling state due to faults in either the I/O module, the IONet switch or the controller itself. A single faulty controller can prevent the other two controllers from reaching a controlling state.

Perform the following procedures if the controller is not attaining a controlling state.
8.3.1 Controller States

The controller states are as follows:

- Power On
- d0-MASTER_INITIALIZATION
- d1-DC_DETERMINATION
- d2-DATA_INITIALIZATION
- d3-INPUTS_ENABLED
- d5-EXCH_INITIALIZATION
- d6-EXCHANGING
- d7-SEQUENCING
- d8-STANDBY
- dA-CONTROLLING

Perform the following procedures if the controller is stalled at Master Installation state.

1. Replace the controller keeping the existing flash card
2. Re-flash and download to the controller

Has it crossed Master Initialization?

Yes → Finish
No → Replace flash card

Has it crossed Master Initialization?

Yes → Finish
No → Replace flash card
Perform the following procedures if the controller is stalled at DC determination state.

1. Connect a computer to an IONet 1 switch
2. Set the computer IP address to 192.168.1.xxx

Are you able to ping 192.168.1.8 [RY9 (SY10 (T)]?

1. Yes
   1. Connect a computer to an IONet 2 switch
   2. Set the computer IP address to 192.168.2.xxx
   Check IONet communication between computer, switch and controllers

2. No
   Are you able to ping 192.168.2.8 [RY9 (SY10 (T)]?
   2. Yes
      2.1. Connect a computer to an IONet 3 switch
      2.2. Set the computer IP address to 192.168.3.xxx
      Are you able to ping 192.168.3.8 [RY9 (SY10 (T)]?
      2.2.1. Yes
          Finish
      2.2.2. No
          Are you able to ping the controllers?
          2.2.2.1. Yes
              Re-flash and download to the controller
          2.2.2.2. No
              Replace controller

   1. No
   Are you able to ping the controllers?
   1.1. Yes
       Finish
Perform the following procedures if the controller is stalled at Input Enabled state.

The following diagram displays the possible causes if the controller is not reaching the controlling state.

1. Check the I/O pack connection and configuration to the controller. If necessary, replace the I/O pack.
2. Build and download the application code.
Perform the following troubleshooting steps if needed:

- It is not possible to connect to the designated controller if the controllers are set in the dc determination state. Going online with each individual controllers is required.
- The ToolboxST application may not display any information in the Status tab for the faulty Mark VIeS Functional Safety System if it is set in the Power on/d0-MASTER_INITIALIZATION state. The other two controllers are suspended at d1-State Designated Controller Determination state.

![Graphical representation of controller status]

- If the controller halts before d0-MASTER_INITIALIZATION (at power on state), the problem could be with the controller. If the controller halts at d0-MASTER_INITIALIZATION state, the controller may have lost its IP address.
- If the controllers halt at the d1-dc_DETERMINATION state, one of the controllers may be unable to communicate to either IONet 1, 2, or 3 port.
- If all the controllers halt at the d3-INPUTS_ENABLED state, at least one of the I/O modules configured as a required module may not be communicating with the controllers.
8.4 Unable to Download to I/O Modules

Perform the following procedures if you are unable to download to I/O packs.

- **Unable to download to I/O module**
  - A "?" symbol displays on the I/O module for which the download is not possible.
  - **Does the module/terminal board hardware form match the installed hardware?**
    - No: Correct the hardware form, build, and download.
    - Yes:
      - **Is the module connected to correct jack (JR1/SJ1/JT1) and ICNet?**
        - No:
          - 1. Correct I/O module connections
          - 2. Build and download to module
        - Yes:
          - **Is the terminal board barcode entered correctly?**
            - No:
              - 1. Correct barcode
              - 2. Build and download
            - Yes:
              - **Go online. Is there any unassigned barcode?**
                - Yes:
                  - 1. Assign the unassigned barcode
                  - 2. Build and download
            - No:
              - **Simplex module**
                - No:
                  - **TMR module**
                    - No:
                      - 1. Check pack communication between module and controller
                    - Yes:
                      - 1 module
                        - **Unable to download to 1 or all 3 modules?**
                          - 3 modules
                            - 2. Replace faulty module
                            - 3. Replace faulty terminal board

8.5 Unable to Communicate with I/O Module

In the ToolboxST application, Component Editor, Hardware tab, a red X symbol on an I/O module indicates that the controller is unable to communicate with that I/O module. If multiple modules have red X symbols, the problem may be with the IONet switch or the I/O module power supply.

➢ To view I/O communication failures between an I/O pack and the controller diagnostic

1. From the ToolboxST application, open the system .tcw file.
2. From the Component Editor, select the Hardware tab and right-click on the I/O pack with a red X.
3. Select View Diagnostics.

Note In TMR I/O modules, the diagnostic displays for the faulty module only.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Potential Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other I/O packs on same IONet switch still communicating</td>
<td>I/O pack power&lt;br&gt;Ethernet cable from I/O pack&lt;br&gt;Incomplete downloads to pack or controller&lt;br&gt;Improper ToolboxST configuration&lt;br&gt;Bad IONet switch port&lt;br&gt;I/O pack failure</td>
</tr>
<tr>
<td>No other I/O packs on same IONet switch are communicating</td>
<td>Switch power&lt;br&gt;Switch communication&lt;br&gt;Improper switch configuration&lt;br&gt;Switch failure</td>
</tr>
</tbody>
</table>
8.6 Unable to Download to Controller or I/O Module

If intermittent communication loss occurs between the HMI and the controllers, the downloading process could be interrupted at intermediate stages. It is recommended that the download be carried out for base load, firmware, and application/parameters individually to the controllers and the I/O packs. Firmware download to the controllers could be interrupted due to issues related to incorrect library references.

The Model Predictive Control (MPC) block libraries are not supported by the UCSA/UCSB/UCSC controller. Therefore, if the application is configured for the UCSA/UCSB/UCSC controller and the MPCBlockLib is used as a reference library, the firmware download is interrupted.

The Status tab displays error messages.

152 GEH-6855_Vol_I_A   GEH-6855_Vol_I Mark VleS Functional Safety Systems Vol I System Guide
Public Information
8.7 Communication Loss Between Controller and I/O Module

➢ To resolve communication loss between the controller and I/O module

1. If there are diagnostic alarms on an I/O module related to .xml files, download the base load, firmware, and parameters to the module.

2. If an I/O module is unable to go online with the controller when powering on a Mark VIeS Functional Safety System, cycle power to the module.

3. If there are diagnostic alarms on an I/O module related to configuration files, download the base load, firmware, and parameters to the module.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Potential Problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>No other I/O packs on same IONet switch are losing communication</td>
<td>I/O pack power</td>
</tr>
<tr>
<td></td>
<td>I/O pack communication diagnostic</td>
</tr>
<tr>
<td></td>
<td>Incomplete downloads</td>
</tr>
<tr>
<td></td>
<td>Improper ToolboxST configuration</td>
</tr>
<tr>
<td></td>
<td>I/O pack failure</td>
</tr>
<tr>
<td>Some other I/O packs on same IONet switch are losing communication</td>
<td>I/O pack power</td>
</tr>
<tr>
<td></td>
<td>I/O pack communication diagnostic</td>
</tr>
<tr>
<td></td>
<td>Incomplete downloads</td>
</tr>
<tr>
<td></td>
<td>Improper ToolboxST configuration</td>
</tr>
<tr>
<td></td>
<td>Improper IONet switch configuration</td>
</tr>
<tr>
<td></td>
<td>I/O pack failure</td>
</tr>
<tr>
<td>All other I/O packs on same IONet switch are losing communications</td>
<td>IONet switch power</td>
</tr>
<tr>
<td></td>
<td>IONet switch communication</td>
</tr>
<tr>
<td></td>
<td>Improper IONet switch configuration</td>
</tr>
<tr>
<td></td>
<td>IONet switch failure</td>
</tr>
</tbody>
</table>
8.8 Collecting Boot Log

➢ To collect a boot log

1. From the Windows® Start menu, select Programs, Accessories, Communications, and HyperTerminal.

![Connection Description](image)

Enter a session name and click OK.

---

**Note**  HyperTerminal is not included in Windows 7.

---

![Connect To](image)

From the Connect using drop-down list, select COM1 and click OK.

---

**Note**  The serial cable between the computer COM port and the controller COM port must be connected.
2. Reboot the controller and save the boot log collected in the HyperTerminal session.

8.9 I/O Module Replacement or Upgrade Issues

After upgrading or replacing an I/O module, the following conditions require additional troubleshooting to resolve:

- Communication Errors
- Download Errors
- Active Diagnostics
- Mismatched Revision

**Note** If one I/O pack has different diagnostics than the other two in a TMR set, it is typically due to an incomplete download or mismatched revision. If neither of these issues can be resolved, try replacing the I/O pack with a new one of the same hardware form as the other two in the TMR set.

8.9.1 Communication Errors

When firmware and application is downloaded to an I/O module, it can take several minutes to install, restart, and re-establish communication to the Mark VIe controller. If the ATTN LED is red and flashing at 2 Hz 50%, the IP address has not been received from the controller. For information on ATTN LED flash codes, refer to the Help file for the specific I/O module and the section Diagnostics.

- Verify that the terminal board bar code configured in the ToolboxST configuration matches the actual hardware.
- Verify that the terminal board type, including **HW Form**, in the ToolboxST configuration matches the terminal board in the actual I/O module.
- Verify that the network cables and switches to the I/O module are plugged in correctly, and that the Link and Activity LEDs are active.

➢➢ To view more troubleshooting information: from the **Diagnostics** tab, select each diagnostic alarm and press F1.
8.9.2 Download Errors

Download errors are typically caused by a mismatch between the I/O module hardware form in the ToolboxST configuration and the hardware form of the actual I/O module.

➢➢

To correct a hardware form mismatch between the I/O module and the ToolboxST configuration

1. From the Mark VIe Component Editor Hardware tab, right-click the affected I/O module and select Modify.

Change the HW Form and click OK.
2. From the ToolboxST application, perform a manual Download of the firmware.

**Note** If the Download is not successful, manually restart the I/O module and perform the Download again.

3. If an I/O module displays 🔄 during the download, complete the following:
   - Check the Component InfoView Log tab for errors. If there is a mismatch between the I/O module configured in the ToolboxST application and the actual hardware, the I/O module configuration must be updated to match the hardware.
   - If there is still an issue with the download and the hardware configuration has been verified, restart the I/O module, wait one minute, and perform the download again.
   - When the download has completed successfully, open the Download wizard and verify that all I/O modules are equal (display green). Check the InfoView log and resolve any Communication Errors.

### 8.9.3 Active Diagnostics

If the Warning symbol 🔄 displays on an I/O module:

- I/O module has active diagnostic alarms
- Firmware and/or application revisions in the I/O module do not match the ToolboxST configuration

➢➢➢ **To clear active diagnostics**

1. From the Component Editor Hardware tab, select the Diagnostics tab.
2. Select the diagnostic alarm with the red icon and press F1 to display the Help file.
3. Use the possible causes and solutions provided for the specific alarm number to correct the problem.
8.9.4 Mismatched Revision

A revision mismatch is indicated by a ≠ icon on the I/O module Status tab.

➢➢➢ To resolve a revision mismatch

1. From the Component Editor Device menu, select Download and Download Wizard.
2. From the wizard page, select Next and scan the I/O module to verify that all unequal items are selected for download.
3. Perform a Download to the I/O module. When the Download is complete, wait for the I/O module to go online and verify that all revisions are equal.

If the configuration being downloaded contains I/O modules with different module IDs than the configuration currently running, the download may install incorrect firmware to some I/O modules. If this occurs, make sure the controller is running the new configuration, restart the entire system, then start the ToolboxST Download Wizard again.

When communication has been successfully established, the I/O module displays with no errors.
8.10 Controller Status LEDs

The UCSC controller status LEDs are as follows:

- **Link** displays solid green if Ethernet connection has been established.
- **Act** indicates packet traffic on an Ethernet interface. This LED may flash if the traffic is low, but is solid green in most systems.
- **On** indicates the status of restore process
- **FAOK** displays solid green when the Embedded Field Agent (EFA) is connected to the cloud.
- **Boot** displays solid red or flashing red during the boot process.
- **ONL** displays solid green when the controller is online and running application code.
- **UFP** indicates status of FPGA program updates.
- **DC** displays solid green when the controller is the designated controller.
- **Diag** displays solid red when the controller has a diagnostic available.
- **OT** displays solid amber when temperature of internal components exceeds recommended limit.
- **VDC** indicates power status.

The boot LED is on continuously during the boot process unless an error is detected. If an error is detected, the LED flashes at a 1-Hz frequency. The LED, when flashing, is on for 500 ms and off for 500 ms. The number of flashes indicates the failed state. After the flash section, the LED turns off for three seconds.
The boot LED flash codes are:

- 1: Failed Serial Presence Detect (SPD) EEPROM
- 2: Failed to initialize DRAM or DRAM tests failed
- 3: Failed NOR flash file system verification
- 4: Failed to load FPGA or PCI failed
- 5: CompactFlash device not found
- 6: Failed to start IDE driver
- 7: CompactFlash image not valid

If the CompactFlash image is valid but the runtime firmware has not been loaded, the Boot LED flashes continuously at a 1-Hz frequency. When the firmware is loaded, the boot LED turns off.

The I/O pack status LEDs are:

- Green LED labeled PWR indicates the presence of control power.
- Red LED labeled ATTN indicates pack status, with the following conditions.
  - LED off - no detectable problems with the pack
  - LED solid on - a critical fault is present that prevents the pack from operating. Critical faults include detected hardware failures on the processor or acquisition boards, or no application code is loaded.
  - LED flashing quickly (¼ cycle) - an alarm condition is present in the pack (for example, the wrong pack on the terminal board), or there is no terminal board, or there were errors loading the application code.
  - LED flashing at medium speed (¾ cycle) - the pack is not online.
  - LED flashing slowly (2 cycle) - the pack has received a request to flash the LED indicating that the pack is used during factory test, or as an aid to confirm the physical location against the ToolboxST application settings.

- Green LED labeled LINK is provided for each Ethernet port to indicate that a valid Ethernet connection is present.
- Yellow LED labeled TxRx is provided for each Ethernet port to indicate when the pack is transmitting or receiving data over the port.
**Glossary of Terms**

**Application code**  Software that controls the machines or processes, specific to the application.

**Balance of Plant (BOP)**  Plant equipment other than the turbine that needs to be controlled.

**Baud**  A unit of data transmission. Baud rate is the number of bits per second transmitted.

**Bit**  Binary Digit. The smallest unit of memory used to store only one piece of information with two states, such as One/Zero or On/Off. Data requiring more than two states, such as numerical values 000 to 999, requires multiple bits (see Word).

**Block**  Instruction blocks contain basic control functions, which are connected together during configuration to form the required machine or process control. Blocks can perform math computations, sequencing, or continuous control. The toolbox receives a description of the blocks from the block libraries.

**Board**  Printed wiring board.

**Boolean**  Digital statement that expresses a condition that is either True or False. In the ToolboxST application, it is a data type for a logical variable.

**Broadcast**  In computer networking broadcast is traffic that is simultaneously addressed to all computers connected to the network.

**Bus**  An electrical path for transmitting and receiving data.

**Byte**  A group of binary digits (bits); a measure of data flow when bytes per second.

**CIMPLICITY**  Operator interface software configurable for a wide variety of control applications.

**Configure**  To select specific options, either by setting the location of hardware jumpers or loading software parameters into memory.

**Control Data Highway (CDH)**  Redundant Ethernet communication network allows two separate controllers to communicate with each other.

**Cyclic Redundancy Check (CRC)**  Detects errors in Ethernet and other transmissions.

**Data server**  A computer that gathers control data from input networks and makes the data available to computers on output networks.

**Device**  A configurable component of a process control system.

**Distributed Control System (DCS)**  Control system, usually applied to control of boilers and other process equipment.

**Ethernet**  LAN with a 10/100 M baud collision avoidance/collision detection system used to link one or more computers together. Basis for TCP/IP and I/O services layers that conform to the IEEE 802.3 standard, developed by Xerox®, DEC®, and Intel®.

**Ethernet Global Data (EGD)**  Control network and protocol for the controller. Devices share data through EGD exchanges (pages).

**EX2100e Excitation Control**  Latest version of GE generator exciter control; regulates the generator field current to control the generator output voltage.

**Fanned input**  An input to the terminal board that is connected to all three TMR I/O boards.
**Firmware**  The set of executable software that is stored in memory chips that hold their content without electrical power, such as EEPROM.

**Flash**  A non-volatile programmable memory device.

**Forcing**  Setting a live variable to a particular value, regardless of the value blockware or I/O is writing to that variable.

**Frame rate**  Basic scheduling period of the controller encompassing one complete input-compute-output cycle for the controller. It is the system-dependent scan rate.

**Function**  The highest level of the blockware hierarchy, and the entity that corresponds to a single .tre file.

**Gateway**  A device that connects two dissimilar LANs or connects a LAN to a wide-area network (WAN), computer, or a mainframe. A gateway can perform protocol and bandwidth conversion.

**I/O device**  Input/output hardware device that allows the flow of data.

**I/O drivers**  Interface the controller with input/output devices, such as sensors, solenoid valves, and drives, using a choice of communication networks.

**IONet**  The I/O Ethernet communication network.

**IP Address**  The address assigned to a device on an Ethernet communication network.

**Logical**  A statement of a true sense, such as a Boolean.

**LS2100e Static Starter control**  GE’s current state-of-the-art control for static starter control systems, used to bring a gas turbine up to starting speed.

**Macro**  A group of instruction blocks (and other macros) used to perform part of an application program. Macros can be saved and reused.

**Modbus**  A serial communication protocol developed by Modicon for use between PLCs and other computers.

**Module**  A collection of tasks that have a defined scheduling period in the controller.

**Multicast**  The delivery of a message or Information to a group of destination computers simultaneously in a single transmission from the source.

**Online**  Online mode provides full CPU communications, allowing data to be both read and written. It is the state of the toolbox when it is communicating with the system for which it holds the configuration. Online is also, a download mode where the device is not stopped and then restarted.

**Period**  The time between execution scans for a Module or Task. Also a property of a Module that is the base period of all of the Tasks in the Module.

**Pin**  Block, macro, or module parameter that creates a variable used to make interconnections.

**Plant Data Highway (PDH)**  Ethernet communication network between the HMI Servers and the HMI Viewers and workstations.

**Potential Transformer (PT)**  Measures voltage in a power cable.

**Programmable Logic Controller (PLC)**  Designed for discrete (logic) control of machinery. It also computes math (analog) function and performs regulatory control.

**QNX**  A real time operating system used in the controller.

**Relay Ladder Diagram (RLD)**  A ladder diagram that represents a relay circuit. Power is considered to flow from the left rail through contacts to the coil connected at the right.
**Sequence of Events (SOE)**  A high-speed record of contact transitions taken during a plant upset to allow detailed analysis of the event.

**Server**  A computer that gathers data over the Ethernet from plant devices, and makes the data available to computer-based operator interfaces known as viewers.

**Simplex**  Operation that requires only one set of control and I/O, and generally uses only one channel. The entire control system can operate in simplex mode.

**Simulation**  Running a system without all of the configured I/O devices by modeling the behavior of the machine and the devices in software.

**Software Implemented Fault Tolerance (SIFT)**  A technique for voting the three incoming I/O data sets to find and inhibit errors. Note that control also uses output hardware voting.

**TCP/IP**  Communication protocols developed to inter-network dissimilar systems. It is a de facto UNIX standard, but is supported on almost all systems. TCP controls data transfer and IP provides the routing for functions, such as file transfer and e-mail.

**ToolboxST**  A Windows-based software package used to configure the control systems, exciters, and drives.

**Trend**  A time-based plot to show the history of values, similar to a recorder, available with the ControlST Historian and the ToolboxST application.

**Triple Module Redundancy (TMR)**  An operation that uses three identical sets of control and I/O (channels R, S, and T) and votes the results.

**Unit Data Highway (UDH)**  Connects the controllers, static starter control system, excitation control system, PLCs, and other GE provided equipment to the HMI Servers.