Mark* VIe Controls
System Redundancy Options
Instruction Guide

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.

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

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.

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: Aug 2014
Issued: May 2008


* 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
Document Updates

<table>
<thead>
<tr>
<th>Revision</th>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Entire Document</td>
<td>Updated to new format</td>
</tr>
<tr>
<td></td>
<td>Throughout document</td>
<td>Updated all diagrams</td>
</tr>
</tbody>
</table>

Contents

1. Introduction .................................................................................................................. 3
2. Basic Redundancy Options ............................................................................................ 4
3. Power Redundancy ........................................................................................................... 6
4. Controller ....................................................................................................................... 7
5. I/O Network Redundancy ................................................................................................. 7
6. I/O Redundancy ................................................................................................................ 8
   6.1 Dual Redundancy ......................................................................................................... 8
   6.2 Triple Modular Redundancy ....................................................................................... 11
7. Tripping Reliability ....................................................................................................... 15
8. Digital Bus Reliability .................................................................................................. 17
   8.1 FOUNDATION Fieldbus .............................................................................................. 17
   8.2 PROFIBUS DP-V0 and DP-V1, Class 1 Masters .......................................................... 17
   8.3 HART Communications ............................................................................................ 17
   8.4 CANopen Communications ...................................................................................... 17
9. Relative Reliability ......................................................................................................... 18
1 Introduction

Control redundancy is used to improve the availability of the plant’s process. Its implementation varies with each application and the criticality of the process to the plant’s revenue.

The premise of redundancy is that all control equipment has a mean-time-between-failure (MTBF) that can be compensated for with redundancy, so that the mean-time-between-forced-outage (MTBFO) of the entire system is better than the MTBF of the individual components. Improvement in MTBFO depends on how the redundancy is applied and whether the inevitable failures can be detected and repaired online without interrupting the process. Field components (for example, sensors, actuators, and wiring) cause over half of forced outages. Therefore, redundancy of field components is an important consideration in the overall control system.

Most discussions of redundancy focus on its contributions to starting and running reliability. However, tripping reliability is another important safety aspect of all control systems, and there is usually some compromise between the two objectives. For example, two hydraulic trip solenoids provide better tripping reliability than one (that is, either solenoid trips), but less running reliability.

Basic reliability terminology:

- Mean-Time-Between-Failure (MTBF)
- Mean-Time-Between-Forced-Outage (MTBFO)
- Mean-Time-To-Repair (MTTR)
- Availability = \[ \frac{\text{MTBFO}}{\text{MTBFO} + \text{MTTR}} \] x 100%
Each of these system components can be supplied in Simplex, Dual, or Triple Modular Redundancy (TMR) configuration. Dual is more reliable than simplex, assuming that the component has a known failure mode. For example, if two pressure sensors are known to fail low, then the control can be preconfigured to select the higher of the two signals. If the sensors or the electronics that monitor the sensors have a less predictable failure mode, transiently or steady state, then dual redundancy is insufficient.

Triple redundancy continuously monitors and votes three parameters so a partial or unpredictable failure of one component is out-voted by the other two. In the case of three lube oil pressure switches, the protective system performs a simple logical vote with no need to predict in advance a probable failure mode.

Simplex, dual, and triple redundancy can be implemented according to the specific needs of each application and site. This is important for cost effective redundancy. For example, exhaust thermocouples are important inputs for running reliability and tripping reliability on gas turbine controls, but wheelspace thermocouples are monitored-only. Therefore, different redundancy strategies are used for exhaust and wheelspace thermocouples.
Typical Mark VIe Architecture

- Control Network (UDH)
- System Building Blocks
- Controller
  - 3 IONET Ports
  - 2 Control Network Ports
  - 1 COM Port
- IONET Switch
- I/O Module
  - I/O Pack
    - Local Processor
    - Data Acquisition
- Terminal Block
The terminology for power sources, supplies, and converters is often confused. An external power source is provided for the electronics, which have internal power supplies that convert the source voltage to low-level regulated busses for circuit boards. In many cases, there is also a wetting voltage required for contact inputs, analog inputs, and power feeds for field solenoids that are powered from the control.

The control system accepts one, or redundant, 24 V dc, 125 V dc, and 115/230 V ac sources that can be mixed in any combination. Internal power supplies convert the source voltage to 28 V dc for the controller, IONet switches, and the distributed I/O modules. Internal supplies are normally non-redundant for simplex control systems, but can be provided as dual redundant, if required. Dual redundant power supplies are provided for dual redundant control systems, and dual/triple redundant power supplies are provided for triple redundant controls systems. An exception is remote I/O panels with non-critical I/O. These panels normally have a single power supply regardless of whether the controllers are redundant or non-redundant. But, they can be supplied in redundant pairs too, if required. Additional redundancy options are available.

Different power sources can be provided for the internal electronics and the wetting voltage for contact inputs, transducers, and solenoid power. For example, redundant 230 V ac sources can be converted to 28 V dc for the internal electronics. If 125 V dc wetting voltage is needed for contact inputs or field solenoids, it can be provided directly from the station battery or from redundant 230 V ac to 125 V dc converters in the control.

Diagnostics monitor power sources and power supplies for fault detection and to enable online repair.
4 Controller

A single-board controller is the heart of the system. It includes the main processor and three Ethernet drivers for communications with networked I/O and two additional Ethernet drivers for the control network. One, two, or three controllers are provided as required for redundancy.

Some suppliers support redundant processors and communication boards in a common rack with a split backplane for improved fault tolerance. Another form of redundancy has two controllers with two processors in each of the two controllers in a quad configuration. If one of the processors has a partial failure, there will be a discrepancy between the data from the two processors on one board, and the other board takes control.

A key evaluation point for any redundant control system is the failover time from one controller to the other. If one controller normally drives the control valve and the other is on standby in a hot-backup configuration, then there is a finite time for the backup to determine that the main controller has failed so that it can take over. This failover time is critical to the process.

Another method is to have both controllers continuously reading inputs, running application software, and providing outputs to the control valves and relays, so there is no failover time between controllers. Somewhere between the controllers and the control valves/relays a decision is made to follow the commands from one controller or the other. This decision point is a critical item in determining failover time, failure mode, and overall system fault tolerance.

5 I/O Network Redundancy

All control systems have internal communications between the main processor(s) and the I/O regardless of whether the I/O is separate from the controller board rack, or mounted inside the rack with communication on the backplane. The I/O network consists of active electronics at both ends and multiple failure modes, so its redundancy is just as important as the main processors and the I/O electronics that interface with field devices.

In a Mark VIe control system, IONET provides communication between the main processor(s) in the controller(s) and the local processors in the I/O packs that are located on the I/O modules. This communication architecture is a star configuration with the network switch(s) in the middle. Switches manage communication traffic to eliminate data collisions and increase network determinism. Networks conform to IEEE 802.3 for 100Base-Tx and 100Base-Fx (fiber).

Typically, simplex controls have one IONet, dual controls have two IONets, and triple redundant controls have three IONets. However, even in simplex controls a second IONet is often provided.

Switches send their input data to all controllers, which are continuously online. Each dual redundant controller uses the data from its designated switch, but uses the data from the other switch, with no delay, if the data from the first switch is not received or if the data has a bad checksum. Each triple redundant controller receives data from all three switches, individually votes the data from contact inputs, and selects the median value of analog inputs. In addition, diagnostics identify any discrepancy between the three inputs. This is important to minimize MTTR and enable online repair.

Output data is sent from each controller to its designated switch and then to the output electronics. The methodology for selection of output data from the redundant controllers for driving control valves, solenoids, and other components varies widely between control systems and is significant for determining the system reliability. These details are discussed in the next section.
6 I/O Redundancy

6.1 Dual Redundancy

A basic dual redundant control has a sensor connected to an I/O module with one I/O pack that communicates data to two IONET switches (Refer to the following figure). Each IONET switch transmits the data to both controllers, which are online and running the same application software.

This configuration has the advantage of network and controller redundancy but no redundancy for the sensor or I/O module. Another option is adding a second sensor and a second I/O module. This increases the fault tolerance and the ability to perform online repair at least to the module and possibly to the sensor assuming that the sensor can be replaced while the process is running. Note that online repair is at the I/O pack level. Therefore, replacement of I/O has minimal impact on monitoring and control of the overall control system. An extension of this is to add a third sensor whose value can be voted in the application software. This is an example of triple redundant sensors and I/O modules with dual networks and dual controllers.

An example of this configuration is in a heat recovery steam generator (HRSG) control that has minimal critical I/O except for the drum level. Triple redundant sensors can be added just for the drum level control to optimize system availability for the least cost.
Two Sensors & Dual Controllers

Sensor A +24Vdc
Sensor B +24Vdc

Sensor diagnostics enable on-line repair assuming on-line process access

On-line replacement of I/O Packs & auto reconfiguration

Option: communication to second IONET port

Two Sensors & Dual Controllers

Sensor A +24Vdc
Sensor B +24Vdc
Sensor C +24Vdc

Analog – Median select
Contacts – Logical vote
Disagreement diagnostics
Can be mixed with dual & simplex inputs

Three Sensors & Dual Controllers

Three sensors are beneficial when the sensor has an unpredictable failure mode.

Data outputs from dual redundant controllers are normally implemented with each controller sending its signal to its switch and each switch forwarding the signal to one of the two ports on an I/O pack on an I/O module. The pack uses the first healthy reference that it sees and continues to use it until it is not available or the pack determines that the signal is unhealthy. This results in a transfer to the second reference with no latency in driving outputs. In the unlikely event that an output pack loses communication with both IONETs, it defaults to one of three pre-configured states: 0 = Power Down State, 1 = Preset Value State, 2 = Last Value State.

Designated Controller
1. Provides the master clock
2. Supplies initialization data
3. Provides recovery data
4. Receives external commands
5. Creates process alarms
If redundancy is required for the I/O pack, three (not two) I/O packs can be mounted on the I/O module to provide a reliable two-out-of-three reference for each driven component. For general-purpose 4 - 20 mA outputs, the three I/O packs drive a common, passive, current-sharing circuit on the I/O module that produces a single 4 - 20 mA output. This is the median signal from the three I/O packs. There are also 0 – 200 mA outputs available to drive valve positioners.

A customized (application-specific) implementation of current outputs is used for servos. These outputs are similar to the 4 - 20 mA outputs and can have one or three I/O packs, for redundancy, that drive three bi-polar servo coils on the same control valve actuator. The advantage of three coil servos is that there is no single component in the electronics that selects between the redundant valve commands and is vulnerable to failure.

 Relay outputs are available in three redundancy levels:

- **Level 1** provides dual redundant controllers, IONET switches, and Ethernet ports on a common I/O pack, which controls a relay driver and a relay.
- **Level 2** also provides dual redundant controllers and IONET switches, but extends the redundancy to three redundant I/O packs, which are voted by a common relay driver feeding a relay.
- **Level 3** extends the voting to three sets of mechanical relays, which vote with their contacts. This is available with 36 relays voting to create 12 contact outputs that are available as form “A” (normally open) and form “B” (normally closed) configuration. Application-specific versions of this are available for interface with hydraulic trip solenoids on turbines, which vary in quantity, rating, and specific implementation.

Many other factors should be considered when choosing the proper contact output circuit for reliability. For example, magnetic relays and solid-state outputs are available. Magnetic relays have form “C” contacts (1 open and 1 closed with a common point). This allows preplanning for the most common failure mode, de-energize, for a magnetic relay. In this scenario, a normally-closed contact can energize a Motor Control Center starter, which is not available on solid-state outputs. If the starter is for the lube oil pump, then it probably warrants the highest level of redundancy. However, if there is an emergency lube oil pump to back-up the auxiliary pump, then there is less need for redundant electronics. Other considerations are whether the relays are sealed for hazardous locations, leakage current in the case of solid-state relays, suppression for solenoid applications and so forth.
6.2 Triple Modular Redundancy

Controllers, power supplies, networks, and I/O are physically separate, which is the origin of the term triple modular redundancy (TMR) that is often used when describing the control system. Triple redundancy controls offer a higher degree of fault tolerance than dual redundant controls. The primary advantages are the ability to ride-through a soft (partial) failure of a controller, network, or I/O component with an unexpected failure mode, and the ability to identify the origin of the fault with greater precision.

Since triple redundant controls are applied in a wide variety of applications, the I/O is flexible and can be implemented with single, dual, or triple sensors that are connected to one or multiple I/O modules. Obviously, triple redundant sensors are more fault tolerant than dual redundant or single sensors, but there is also a tradeoff between the cost of redundant sensors and the historical reliability of a particular sensor type for a specific application. Identical application software in each controller read sensor inputs, and diagnostics compares the data. Discrepancies are reported as system/process alarms.

Each sensor can be transmitted in parallel to the three IONETs (fanned) or transmitted individually. Fanned inputs are transmitted on the IONET with three I/O packs on the I/O module. Therefore, a failure of an I/O pack does not inhibit any controller from seeing all of the sensors. In addition, any disagreement between the data values for the same sensor in the three controllers is identified as an internal diagnostic fault. Non-fanned inputs have less electronics (lower MTBF) but also less diagnostic precision, because there is only one I/O pack per sensor. Since the precision of the diagnostics impacts the MTTR, it also impacts the availability of the control system and the process.

The Mark VIe is also available as a SIL-3 capable safety controller, Mark VIeS, in simplex, dual, and triple redundant configurations. Both systems share common architectures, configuration and diagnostic software tools, and can share input data from I/O modules on a common IONET to simplify operations and maintenance. When sharing I/O, the controllers from the Mark VIe and Mark VIeS can read inputs from all I/O modules, but write outputs only to their own I/O modules.
Non-critical data that is being used for non-essential monitoring is usually implemented without redundancy. Redundant and non-redundant I/O coexists in most control systems.

The overall scheme of software voting, diagnostics, and online repair capability is known as Software Implemented Fault Tolerance (SIFT). Its significance is that application software in each of the three control sections performs the voting rather than a single hardware voter that would compromise reliability by introducing a potential single point failure.
Basic forms of output module:
Relays – Voting occurs at a relay driver
Relays – Voting occurs with 2/3 contact voting
Analog – Median select with a passive, current-sharing circuit
Analog – Voting occurs with a 3-coil servo

Voting at I/O Module

Extended Voting at Field Device
(Example: 3 Coil Servo Valve Actuator)
Typical nuclear configuration
A good redundant control system has a solution for handling faults all the way to the control valves and trip solenoids. Any compromise in fault tolerance prior to the final output device seriously degrades the MTBFO of the entire system. Therefore, outputs are voted in hardware and preferably as close as possible to the final output device that is being controlled.

An example of extending the voting to the field component is driving three-coil servo valve actuators. The flux from the three coils moves the valve, and LVDTs provide position feedback to the valve regulators that are located in each I/O pack. In normal operation, each current driver is slightly off null, and in the event of a fault, the remaining two current drivers compensate for the loss. This is hardware voting of the current outputs at the control valves.

Standard GE triple redundant control systems are highly fault tolerant but not devoid of single point failures. As an example, I/O packs are mounted on I/O modules with passive components and high corresponding MTBF. Some applications, such as nuclear, require no single point failures. Requirements for no single point failures must be evaluated on a case-by-case basis to determine the best way to approach this from the system level. The preceding figure displays a variation of outputs to three coil servos where each coil is driven from a separate I/O module. This eliminates single point failures from this circuit and demonstrates the flexibility of the controls to meet this objective. However, it also demonstrates the additional size and cost that may be required to eliminate single point failures when field devices are considered, as they should be.

Similarly, a triple redundant control system uses the contacts from three relays to vote each output to each hydraulic trip solenoid. In some high-availability applications such as nuclear, the voting is extended to dual TMR hydraulic trip manifolds that support on-line repair.

DN1600N Hydraulic Trip Assembly
- (2) sets of 2-out-of-3 hydraulic trip circuits A & B
- Parallel operation with both normally operating
- Enables isolation and maintenance of 1 during normal operation
- Remote control on-line test capability: 1 of 3 elements of A & B
- A & B joined with shut-off continuous flow transfer valve assembly
- Fully instrumented with trip and reset position transducers
Turbine control applications have primary and backup trip protection for tripping reliability. The controller and its corresponding I/O control, protect, and monitor the turbine. Primary protection includes a full set of all trip functions, and backup protection includes a small subset of the protection functions to backup the primary. Typical backup functions include emergency overspeed protection, manual-emergency trip, and synch check protection for generator drives. Additional backup functions can be added as required for specific applications or industry code requirements.

Backup protection is completely separate and independent from the primary protection, including separate power supplies, processors, and I/O. In addition, the hardware and application software are sufficiently dissimilar from the primary to dramatically reduce the probability of common mode failures between the primary and backup protection due to common technology. Backup protection is frequently supplied as triple redundant regardless of the redundancy configuration of the primary controllers.
A key tripping reliability feature is cross-tripping. The primary and backup systems initiate a trip independently, but can also initiate a cross-trip for additional tripping redundancy. For example, a trip that originates in the backup protection can be sent to the primary protection to close the control valves and de-energize the trip solenoids from the primary side. Another example, the backup protection monitors communications from each controller, so it can be configured to initiate a trip on behalf of the controllers.

Functionality for the backup protection system is application-specific and subject to the safety requirements dictated by code and/or GE design practices for specific turbine types. In general, it complies with most industry standards. It is separate and independent from the primary protection, with more functionality than required by most codes. As an example, ANSI/API-670 requirements for overspeed protection are written for an (one) independent, triple redundant system. The standard GE overspeed system for a heavy-duty gas turbine or a combined-cycle steam turbine consists of two triple redundant protection systems with cross-tripping.
8 Digital Bus Reliability

In addition to the variety of classic Mark VIe I/O modules, additional I/O modules are available for digital busses such as FOUNDATION Fieldbus™, PROFIBUS®, HART®, and CANopen®. These modules share a common design with other I/O modules consisting of a local processor that communicates on the IONET to switches and then to the controllers. Similarly, they share a common ControlST* software suite with ToolboxST* configuration and diagnostic tools. It is beyond the scope of this paper to review the redundancy options for each specific digital bus. However, some basic principles are provided for reference.

8.1 FOUNDATION Fieldbus

For reliability, two linking devices (I/O modules) can be connected with a RS-232C null modem cable to form one logical linking device (a redundant set) in a primary / secondary configuration. Both linking devices are connected to the same H1 field devices and IONET. If the primary device were to fail, the secondary device would provide a backup. The original primary could then be replaced and automatically reconfigured to match the new primary device.

For a typical application with redundant controllers, there is a primary controller (the designated controller) and a secondary controller. Therefore, the primary linking device is the one connected to the primary controller. Less common are applications with a single controller and redundant linking devices. In this scenario, the first linking device to be powered becomes the primary.

8.2 PROFIBUS DP-V0 and DP-V1, Class 1 Masters

The I/O module can be configured for three types of redundancy:

- One I/O module with one I/O network
- One I/O module with dual I/O networks
- HotBackup I/O modules with dual I/O networks

The active master communicates with the slaves while the backup master is in standby mode. The backup is ready to automatically switchover in less than 200 ms if any of the following conditions occur:

- All master/slave communication is lost
- Master/controller communication is lost on both I/O
- The master is powered down

8.3 HART Communications

Highway Addressable Remote Transducer (HART) communications provide diagnostics and remote communications to smart field devices with standard 4-20 mA wiring. Each I/O module can communicate with dual redundant IONET switches.

8.4 CANopen Communications

The protocol specifications are developed and maintained by the Controller Area Network (CAN) in Automation standards organization comprising. Each I/O module can communicate with dual redundant IONET switch.
9 Relative Reliability

The contribution of redundancy to improving reliability varies greatly between applications, but some basic guidelines are useful. Field devices and wiring are the major cause of forced outages. Therefore, adding redundant electronics to a system with historic field device problems accomplishes little. Improving the quality of the devices and adding redundancy will help.

Two surveys of GE turbine control installations indicated that field devices and wiring contributed to 57% and 69% of forced outages. Redundancy was applied to both the field devices and the electronics at these sites to mitigate the overall control system forced outages.

<table>
<thead>
<tr>
<th>Causes of Forced Outages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Devices &amp; Wiring 57%</td>
</tr>
<tr>
<td>Electronics 31%</td>
</tr>
<tr>
<td>Survey Diff. 12%</td>
</tr>
</tbody>
</table>

Adding redundancy to the electronics can improve the MTBFO of the electronics by approximately 15:1 from a completely non-redundant control to a fully triple redundant control. Between these extremes are redundancy options that can be added to simplex and dual redundant controls that add to their fault tolerance, as previously discussed. The option with the biggest impact on the reliability of the electronics is redundant I/O. Control systems with large I/O quantities have a significant amount of electronics (I/O processors, A/D converters, relays, and so on) that are in the critical path for running and starting reliability. Selective addition of redundancy to these systems can have a dramatic impact on the reliability of the electronics.