



GE Fanuc Automation

Programmable Control Products

***Genius[®] Modular Redundancy
Triple Modular Redundant System
Guide Form Specification***

GFT - 229

Nov 2002

1. SCOPE.....	5
2. GENERAL	5
2.1 HARDWARE/SOFTWARE.....	5
2.2 SUPPORT SERVICES.....	5
2.3 DISTRIBUTION NETWORK	5
2.4 DOCUMENTATION.....	5
3. CRITICAL REQUIREMENTS	6
4. SYSTEM ARCHITECTURE	6
4.1 GENERAL.....	6
4.2 MODULARITY/SCALABILITY	7
4.3 LOCAL AND DISTRIBUTED I/O	7
4.4 INTERFACE TO I/O SUB-SYSTEM.....	7
4.5 CAPACITIES	7
4.6 ON-LINE REPAIR	7
5. CPU SUB-SYSTEM	7
5.1 RACKS/CHASSIS	7
5.1.1 VME Standard	7
5.1.2 Rack/Chassis Isolation.....	8
5.2 CENTRAL PROCESSOR UNITS (CPUs).....	8
5.3 CENTRAL PROCESSOR UNIT PERFORMANCE	8
5.4 MEMORY	8
5.4.1 Memory Battery.....	8
5.5 MEMORY PROTECTION	8
5.5.1 Keyswitch Protection.....	8
5.5.2 Password Protection	8
5.5.3 Application Program Data Memory Protection.....	8
5.6 INTER-CPU COMMUNICATIONS.....	8
5.7 CONFIGURATION.....	9
5.7.1 System Degradation Path (3-2-1-0 and 3-2-0 Operation).....	9
5.7.2 On-Line Programming.....	9
5.7.3 Simplex Shutdown.....	9
5.7.4 Input/Output Autotest Interval.....	9
5.7.5 Input Discrepancy Filter	9
5.7.6 Fault Actions	9
5.7.7 Application Program Data Memory Protection	10
5.8 CPU SUB-SYSTEM DIAGNOSTICS	10
5.8.1 On-Line CPU Diagnostics	10
5.8.2 Presentation of Diagnostic Faults	10
5.8.2.1 Fault Logs.....	10
5.8.2.2 Application Program Interface to Diagnostics	10
5.8.2.2.1 I/O Fault Bits	10
5.8.2.2.2 System Fault Bits.....	10
5.8.3 CPU Diagnostic Participation.....	11
5.8.4 CPU Sub-System Repair	11
6. INPUT SUB-SYSTEM	11
6.1 INPUT CAPACITIES	11
6.2 GENERAL INPUT ARCHITECTURE.....	11

6.2.1 Remote I/O	11
6.3 INPUT SUB-SYSTEM ON-LINE REPAIR	11
6.4 INPUT FIELD WIRING	11
6.5 DIGITAL INPUTS.....	12
6.5.1 Digital Input Types/Density	12
6.5.2 Digital Input Voting	12
6.5.3 Digital Input Diagnostics.....	12
6.6 ANALOG INPUTS	13
6.6.1 Analog Input Types	13
6.6.2 Analog Input Voting.....	13
6.6.3 Analog Input Diagnostics	13
6.6.3.1 Analog Input Deviation (Discrepancy) Checking	14
6.6.4 Analog Input Scaling.....	14
7. OUTPUT SUB-SYSTEM.....	14
7.1 OUTPUT CAPACITIES	14
7.2 GENERAL OUTPUT ARCHITECTURE	14
7.2.1 “H” Pattern Fault Tolerant/ Fail Safe Outputs.....	14
7.2.2 “T” Pattern Fault Tolerant Outputs	14
7.2.3 “I” Pattern Fail Safe Outputs	15
7.2.4 Remote I/O	15
7.3 OUTPUT SUB-SYSTEM ON-LINE REPAIR.....	15
7.4 OUTPUT FIELD WIRING.....	15
7.5 DIGITAL OUTPUTS	16
7.5.1 Digital Output Types/Density.....	16
7.5.2 Digital Output Voting.....	16
7.5.2.1 Standard Majority Vote for Redundant Outputs (“H”, “T”, and “I”).....	16
7.5.2.2 Voting for Simplex Outputs	16
7.5.2.2.1 Majority Voting	16
7.5.2.2.2 Hot Standby Voting	16
7.5.3 Digital Output Diagnostics	17
7.5.4 Electronic Output Fusing.....	17
8. COMMUNICATION INTERFACE SUB-SYSTEM	18
8.1 BUILT-IN SERIAL PORTS	18
8.2 OPTIONAL COMMUNICATIONS INTERFACES	18
8.2.1 Serial RS-232 and RS-485.....	18
8.2.2 Ethernet	18
9. PROGRAMMING/CONFIGURATION SUB-SYSTEM	19
9.1 PROGRAMMING.....	19
9.1.1 General	19
9.1.2 Programming Languages	19
9.1.3 On-Line Changes.....	19
9.1.4 Instruction Set.....	19
9.1.5 Programming Organization	19
9.1.6 Security.....	20
9.1.7 Application Program Annotation.....	20
9.1.8 Application Program Documentation (Print Functions).....	20
9.1.9 Macro Keys	20
9.2 CONFIGURATION.....	20
9.2.1 General	20
9.2.2 Configuration Data Documentation (Print Functions)	20
10. ENVIRONMENTAL REQUIREMENTS.....	21

10.1 TEMPERATURE.....	21
10.2 HUMIDITY.....	21
10.3 VIBRATION.....	21
10.4 SHOCK.....	21
11. AGENCY APPROVALS	21
11.1 INTERNATIONAL STANDARDS ORGANIZATION.....	21
11.2 TÜV (TECHNISCHER ÜBERWACHUNGS - VEREIN).....	21
11.3 OTHER AGENCY APPROVALS AND STANDARDS COMPLIANCE.....	21

1. Scope

This specification encompasses the minimum technical requirements for a fault tolerant and fail-safe TMR system for Emergency Shut Down (ESD), Fire and Gas (F&G), Critical Control and Critical Monitoring. The specification scope includes but is not limited to the CPU sub-system, input sub-system, output subsystem communication interface subsystem and programming/configuration sub-system.

2. General

2.1 Hardware/Software

The system shall be based on a GE Fanuc Automation's standard "off the shelf" components. They shall be field proven and well accepted in the control industry in general. Individual custom components or configurations are not acceptable. Multiple application programming language capabilities shall be available with the primary language being an IEC-61131 compliant ladder logic programming language.

2.2 Support Services

Support services shall be made available by the manufacturer including but not limited to a technical hotline, headquarters and local technical training, headquarters and local application engineering, distribution network, repair and return facilities and project management capabilities.

2.3 Distribution Network

The system manufacturer shall have in place an extensive distribution network to provide spare parts and local technical support.

2.4 Documentation

System and component documentation shall be comprehensive and complete. It shall be available in both paper and CD-ROM media.

3. Critical Requirements

The programmable controller must conform to the following minimum specifications.

- 3.1 *The system must comprise of standard, commercially available PLC hardware. “Specialized” solutions are not acceptable..*
 - 3.2 *It shall be possible to locate expansion racks containing standard I/O modules up to a distance of 2000 metres from the CPU.*
 - 3.3 *To provide a completely open and standard solution, the controller shall be based on the VME bus (Versa Modular Eurocard) open platform. The controller must also support the use of 3rd party VME I/O and special function cards.*
 - 3.4 *The network communications to be used must be deterministic Ethernet based, employing a “producer-consumer” protocol.*
 - 3.5 *It shall be possible to program subroutines in the C language.*
 - 3.6 *The CPU shall include comprehensive diagnostics that continually monitor the system & I/O module functions and store any fault information into an internal table. All faults shall be time and date stamped. This fault table shall be displayed by the programming software.*
4. 3.8 *The PLC hardware set must include the following special-purpose modules, as a minimum :*
5. *High Density I/O modules – up to 64 channels of analog/ discrete I/O on one module.*
 6. *Reflective Memory module – allowing up to 256 independent nodes to share data at up to 6.2 Mbaud per second (data transfer speeds up to 2.5 times those of 100 Base-T Ethernet, making possible the creation of up to 170 Mbaud networks) without the need for any special protocols/ software and I/O overheads.*
 7. *Single Board Computer and Hard Drive modules.*

8. System Architecture

8.1 General

The system shall be capable of true Triple Modular Redundant (TMR) operation, using the widely accepted 2-out-of-3 (2oo3) voting technique and shall also be configurable to provide 2-out-of-2 (2oo2), 1-out-of-2 (1oo2) and 1-out-of-1 (1oo1) voting. The redundant hardware components shall be physically isolated from each other to prevent a common mode of failure due to physical damage. This means for example that the CPU modules shall be housed in separate racks or chassis capable of being mounted in different panels if desired. The controllers shall operate independently and execute the application programs in parallel , but in

an asynchronous manner (they shall NOT be synchronized) to eliminate a potential single point of failure.

8.2 Modularity/Scaleability

The system shall be capable of true modularity not only with respect to the I/O sub-system, but the CPU and communications sub-systems as well. This means that in addition to triple TMR operation, any portion of any sub-system shall also be capable of duplex and simplex operation and hardware configuration. Combinations of all operational modes and hardware configurations of triple (TMR), duplex and simplex shall be allowed in a single system for individual sub-systems. Additionally the input and output sub-systems shall allow all combinations of operational modes and hardware configurations for different groups of inputs or outputs in a system.

8.3 Local and Distributed I/O

The input and output sub-systems shall provide both local (or centrally located) I/O and a distributed I/O capability. The system shall be capable of supporting as few as 16 I/O points at a single remote location.

8.4 Interface to I/O Sub-System

In addition to a simplex or single interface for I/O data to/from the I/O sub-system, the system architecture shall provide for redundant interfaces to the I/O subsystem that can be duplex or triple dependent on the needs of each application.

8.5 Capacities

The system shall support at least 4096 redundant digital I/O points PLUS at least 1024 redundant analog input channels.

8.6 On-Line Repair

All components shall be modular and easily replaceable. All components shall be repairable or replaceable without affecting operation of the system or process.

9. CPU Sub-System

9.1 Racks/Chassis

The system's racks/chassis shall house a CPU module, I/O network interface modules, communications interface modules, power supply module and any other special purpose module required for a particular application. Both panel mount and rack mount versions of the chassis in 5 and 9 slot sizes shall be available.

9.1.1 VME Standard

The racks shall conform to a well known and accepted standard such as the VME bus to facilitate the integration of other manufacturer's special purpose modules that also conform to the same standard.

9.1.2 Rack/Chassis Isolation

Each of up to three racks in a system shall be completely separate physically, and electrically isolated from each other to allow mounting in different panels or even different buildings to reduce the chance of a catastrophic common mode failure. This shall not preclude the typical layout of mounting all CPU racks in the same panel if desired.

9.2 Central Processor Units (CPUs)

CPU Modules shall be based on the Intel microprocessor to gain the advantage of economy of scale of use of these devices and to benefit from future microprocessors based on the same technology. Multiple CPU modules offering different levels of performance and capacities shall be available to choose from depending on the needs of a particular application.

9.3 Central Processor Unit Performance

Basic CPU ladder logic execution shall occur at rates of 0.4 milliseconds per K of Boolean instructions or better. Non-Boolean instruction execution rates shall be dependent upon the individual CPU microprocessor type and speed.

9.4 Memory

A minimum of 200Kbytes of memory space shall be available for the application program. Memory shall be of the CMOS battery backed RAM type.

9.4.1 Memory Battery

The battery used to retain memory contents shall be readily available and have a minimum retention time of six months with a minimum shelf life of 10 years. The battery shall be replaceable on-line with no possibility of memory loss.

9.5 Memory Protection

9.5.1 Keyswitch Protection

Each CPU shall use a keyswitch to enable/disable memory protection. With memory protect enabled, no changes to the application program or run/stop mode shall be allowed.

9.5.2 Password Protection

The System shall provide a means of password protecting the application program. It shall also support multiple passwords - one for each section of an application program.

9.5.3 Application Program Data Memory Protection

The system shall provide via configuration, a method to select portions of the application program data areas to be written to from a host or operator interface device. The default shall be that all application program data memory areas be write protected (read only).

9.6 Inter-CPU Communications

The system shall provide Inter-CPU communications NOT for synchronization, but for the communication of diagnostic information between CPUs and for application program data

initialization during the start-up of a CPU coming on-line in the system. The communications path shall be redundant (2 channels) and the system shall have the ability to continue to operation without the inter-CPU communications operable.

9.7 Configuration

The CPUs optional parameters shall be selectable via software configuration to allow a system's operation to be tailored to the needs of each application.

9.7.1 System Degradation Path (3-2-1-0 and 3-2-0 Operation)

The system shall provide via configuration the ability to select CPU degradation paths of either Triple - Duplex - Simplex - Shutdown or Triple - Duplex - Shutdown.

9.7.2 On-Line Programming

The ability to make on-line program changes shall be configurable to be either enabled or disabled for safe operation to prevent un-intentional changes. In the enabled mode, the on-line programming function shall provide the option of verifying program operation before the new change takes effect in the system as a whole (i.e. before real world output states are affected).

9.7.3 Simplex Shutdown

The system shall provide the option of enabling or disabling an automatic shutdown when the system degrades to simplex CPU operation. If enabled, a configurable simplex shutdown time shall determine how long the system will be allowed to run in a simplex mode before the automatic shutdown occurs. This simplex shutdown time shall be in the range of 0 to 65,535 seconds (18.2 hours maximum).

9.7.4 Input/Output Autotest Interval

The interval between input and output subsystem diagnostic execution (autotesting) shall be selectable via configuration. In addition the system shall provide the ability to optionally modify the interval through the application program or through a host or operator interface.

9.7.5 Input Discrepancy Filter

To accommodate timing differences in real world input devices, the system shall provide a means of selecting an input discrepancy filter time. This time shall determine how long an individual input is allowed to be discrepant from the voted input value before a fault is logged and before vote adaptation takes effect. This time shall be selectable from 1 to 65,535 seconds and shall apply to both digital inputs and analog inputs.

9.7.6 Fault Actions

The system shall provide the option via configuration to select the actions of FATAL (Stop CPU) or DIAGNOSTIC (allow CPU to continue to run) for individual CPU Faults.

9.7.7 Application Program Data Memory Protection

The system shall provide via configuration, a method to select portions of the application program data areas to be written to from a host or operator interface device. The default shall be that all application program data memory areas be write protected (read only).

9.8 CPU Sub-System Diagnostics

The individual CPUs shall perform their own self diagnostics in addition to system wide diagnostics for the CPU sub-system and I/O sub-systems.

9.8.1 On-Line CPU Diagnostics

On-line CPU Diagnostics shall include but not be limited to the following: Memory pattern testing, Data and Address line testing, Processor testing, Interrupt testing, Timer testing, Time of Day Clock testing, Memory Battery testing, Firmware CRC testing, Application program Checksum testing, Operating system software policing, Configuration Data Checksum testing, Data fault, I/O Interface fault, Input Discrepancy Check (digital and analog), and Output Discrepancy Check.

9.8.2 Presentation of Diagnostic Faults

9.8.2.1 Fault Logs

Each CPU shall provide diagnosed fault information in easy to understand English language message format with a date and time stamp for each fault. Any corresponding address information (to determine location of the fault in the case of I/O for example) shall be included in the fault message that gets logged. Faults shall be listed in chronological order.

9.8.2.2 Application Program Interface to Diagnostics

9.8.2.2.1 I/O Fault Bits

In addition to fault logs of diagnostic information the system shall provide a fault bit for each I/O point the reflects the health of the I/O point. The fault bits shall be easily usable in a ladder logic application program in the form of relay contacts to allow the program to act on the diagnostic information. The fault bits shall also be available to be read by a host or operator interface device.

9.8.2.2.2 System Fault Bits

System faults bits shall also be provided including but not limited to the following information: CPU ID, CPU Online, Application Program Data Initialization Mismatch, Output Discrepancy, Simplex/Duplex/Triple Operation. The fault bits shall be easily usable in a ladder logic application program in the form of relay contacts to allow the program to act on the diagnostic information. The fault bits shall also be available to be read by a host or operator interface device.

9.8.3 CPU Diagnostic Participation

All functioning and healthy CPUs in a system shall participate in executing I/O diagnostics (I/O autotesting). Each CPU shall take its turn (in a “round-robin” fashion) executing the I/O diagnostics to ensure that in the event of a CPU failure the remaining CPU(s) continue to perform I/O diagnostics.

9.8.4 CPU Sub-System Repair

All components of the CPU Subsystem shall be modular and easily replaceable. All components shall be repairable or replaceable without affecting operation of the system or process.

10. Input Sub-System

10.1 Input Capacities

The system shall support at least 2048 redundant digital input points PLUS at least 1024 redundant analog input channels.

10.2 General Input Architecture

TMR Inputs shall be physically configured to read a signal from an input device (or triple input device) up to three times by three individual and physically separate input circuits. The three separate input circuits shall be capable of being physically mounted together (centrally or remotely) or optionally mounted remotely in separate physical locations. The three separate input circuits shall transmit their input data individually to each CPU via three separate I/O networks. Each CPU shall contain three I/O network interfaces to receive the triplicated input data from each of the I/O circuits and their corresponding I/O networks. Majority voting of the input data shall be performed separately by each CPU before use by the application program.

10.2.1 Remote I/O

All I/O shall be capable of being mounted locally (or centrally) in a main control panel. Optionally, all I/O shall be capable of being mounted remotely up to 7500 feet from the CPU sub-system. For longer distances fiber optic networks shall be available.

10.3 Input Sub-System On-Line Repair

All components of the input subsystem shall be modular and easily replaceable. All components shall be repairable or replaceable without affecting operation of the system or process. Input modules (blocks) shall be replaceable hot (without removing power).

10.4 Input Field Wiring

All Input field wiring shall be terminated at each module (block) or optionally at a termination board. Input modules (blocks) shall be removable without the need to disconnect field wiring or field wiring terminals. Each module (block) type shall be uniquely keyed to ensure correct placement.

10.5 Digital Inputs

10.5.1 Digital Input Types/Density

The Following digital input types and densities shall be available. The ability to use either simplex input field devices connected to TMR inputs or to use redundant (Triple or Duplex) input field devices connected to TMR inputs shall be provided.

- 24/48VDC - 16 point Sink (TMR, Duplex or Simplex)
- 24/48VDC - 16 point Source (TMR, Duplex or Simplex)
- 12/24VDC - 32 point Sink (TMR, Duplex or Simplex)
- 12/24VDC - 32 point Source (TMR, Duplex or Simplex)
- 115VAC - 8 point (Simplex)
- 115VAC - 16 point (Simplex)
- 115VAC/125VDC Isolated - 8 points (Simplex)

10.5.2 Digital Input Voting

TMR digital inputs shall be voted using the standard 2-out-of-3 algorithm. Upon a failure of one leg of a TMR digital input, voting shall adapt to either 2-out-of-2 or 1-out-of-2 (configurable). Upon a failure of two legs of a TMR digital input, voting shall adapt to either 1-out-of-1 or Default (configurable). Upon the failure of all 3 legs of a TMR digital input, voting shall adapt to supply the configured default value of on, off or hold last state to the application program.

10.5.3 Digital Input Diagnostics

Input faults shall be logged in easy to understand English language message format with a date and time stamp for each fault. Any corresponding address information (to determine location of the fault) shall be included in the fault message that gets logged. Faults shall be listed in chronological order. In addition to fault logs of input faults, the system shall provide a fault bit for each I/O point the reflects the health of the I/O point. The fault bits shall be easily usable in a ladder logic application program in the form of relay contacts to allow the program to act on the diagnostic information. The fault bits shall also be available to be read by a host or operator interface device. Diagnostic LED indicators shall be viewable at each physical module (block). Also each point on a module (block) shall include an LED indicating the on/off state of the circuit. Digital input diagnostics shall include but not be limited to:

- Stuck on input circuit.
- Stuck off input circuit.
- Input-to-input short circuit.
- Input shorted high.
- Input shorted to 0V.
- Input discrepancy.

- Loss of input module (block).

10.6 Analog Inputs

10.6.1 Analog Input Types

The Following analog input types shall be available. All shall be configurable as TMR, Duplex or Simplex. The ability to use either simplex input field devices connected to TMR inputs or to use redundant (Triple or Duplex) input field devices connected to TMR inputs shall be provided.

- 4 - 20 ma
- R.T.D. (Platinum, Nickel, Copper, Linear)
- Thermocouple (Type J, K, T, E, B, R, S, N)
- 0 - 10V
- -10 - +10V
- 0 - 5V
- -5 - +5V

10.6.2 Analog Input Voting

TMR analog inputs shall be voted using the mid-value select algorithm. Upon a failure of one leg of a TMR analog input, voting shall adapt to either average the remaining 2 legs, select the high value or select the low value of the remaining 2 legs (configurable). Upon a failure of two legs of a TMR analog input, voting shall adapt to either 1-out-of-1 or Default (configurable). Upon the failure of all 3 legs of a TMR analog input, voting shall adapt to supply the configured default of hold last value, minimum value or maximum value to the application program.

10.6.3 Analog Input Diagnostics

Input faults shall be logged in easy to understand English language message format with a date and time stamp for each fault. Any corresponding address information (to determine location of the fault) shall be included in the fault message that gets logged. Faults shall be listed in chronological order. In addition to fault logs of input faults, the system shall provide a fault bit for each I/O point the reflects the health of the I/O point. The fault bits shall be easily usable in a ladder logic application program in the form of relay contacts to allow the program to act on the diagnostic information. The fault bits shall also be available to be read by a host or operator interface device. Diagnostic LED indicators shall be viewable at each physical module (block). Analog input diagnostics shall include but not be limited to:

- Input wiring error.
- Input shorted.
- Input open wire.
- Input underrange.
- Input overrange.

- Input deviation (discrepancy).
- Loss of input module (block).

10.6.3.1 Analog Input Deviation (Discrepancy) Checking

Analog input deviations (or discrepancy) shall be diagnosed when a configurable percentage of the full scale deflection of the input is exceeded by a single leg of a TMR analog input. The percentage shall be based on scaled engineering units (those units used in the application program) minimum and maximum values. Both a fixed and a proportional deviation percentage shall be selectable for each individual TMR analog input.

10.6.4 Analog Input Scaling

The system shall provide a means of scaling each individual analog input so that the values used in the application program directly represent the real world units used by the application. These “engineering units” shall be configurable to be in the range of -32768 to +32767.

11. Output Sub-System

11.1 Output Capacities

The system shall support at least 2048 redundant digital output points.

11.2 General Output Architecture

11.2.1 “H” Pattern Fault Tolerant/ Fail Safe Outputs

Outputs shall be wired in the standard “H” Pattern fault tolerant and fail-safe configuration. No single point of failure shall exist in this type of output configuration. Two redundant sourcing output circuits shall drive one side of the load while two redundant sinking output circuits shall connect the other side of a critical load to the common of the power source. The four circuits that make up the “H” pattern output shall exist on physically separate output modules (blocks). Each module (block) shall receive output data from each of the CPUs over three separate I/O networks. The separate output circuits shall be capable of being physically mounted together (centrally or remotely) or optionally mounted remotely in separate physical locations. Each CPU shall contain three I/O network interfaces to transmit the triplicated output data to the output circuits. Majority voting of the output data shall be performed by each group of 4 output circuits.

11.2.2 “T” Pattern Fault Tolerant Outputs

Outputs shall be wired in a “T” Pattern fault tolerant configuration. Two redundant sourcing output circuits shall drive one side of the load while the remaining load connection shall be made to the common of the power source. The two circuits that make up the “T” pattern output shall exist on physically separate output modules (blocks). Each module (block) shall receive output data from each of the CPUs over two separate I/O networks. The separate output circuits shall be capable of being physically mounted together (centrally or remotely)

or optionally mounted remotely in separate physical locations. Each CPU shall contain two I/O network interfaces to transmit the triplicated output data to the output circuits. Majority voting of the output data shall be performed by each group of 2 output circuits.

11.2.3 “I” Pattern Fail Safe Outputs

Outputs shall be wired in a “I” Pattern fail safe configuration. One sourcing output circuit shall drive one side of the load while a redundant sinking output circuit shall connect the other side of a critical load to the common of the power source. The two circuits that make up the “I” pattern output shall exist on physically separate output modules (blocks). Each module (block) shall receive output data from each of the CPUs over two separate I/O networks. The separate output circuits shall be capable of being physically mounted together (centrally or remotely) or optionally mounted remotely in separate physical locations. Each CPU shall contain two I/O network interfaces to transmit the triplicated output data to the output circuits. Majority voting of the output data shall be performed by each group of 2 output circuits.

11.2.4 Remote I/O

All I/O shall be capable of being mounted locally (or centrally) in a main control panel. Optionally, all I/O shall be capable of being mounted remotely up to 7500 feet from the CPU sub-system. For longer distances fiber optic networks shall be available.

11.3 Output Sub-System On-Line Repair

All components of the Output subsystem shall be modular and easily replaceable. All components shall be repairable or replaceable without affecting operation of the system or process (except in the case of the “I” pattern fail safe output). Output modules (blocks) shall be replaceable hot (without removing power).

11.4 Output Field Wiring

All output field wiring shall be terminated at each module (block) or optionally at a termination board. Output modules (blocks) shall be removable without the need to disconnect field wiring or field wiring terminals. Each module (block) type shall be uniquely keyed to ensure correct placement.

11.5 Digital Outputs

11.5.1 Digital Output Types/Density

The Following digital output types and densities shall be available.

- 24/48VDC - 16 point (Fault Tolerant, Fail Safe, Fault Tolerant & Fail Safe or Simplex)
- 12/24VDC - 32 point (Fault Tolerant, Fail Safe, Fault Tolerant & Fail Safe or Simplex)
- 115VAC - 8 point (Simplex)
- 115VAC/125VDC Isolated - 8 points (Simplex)
- Relay - 16 point (Simplex)

11.5.2 Digital Output Voting

11.5.2.1 Standard Majority Vote for Redundant Outputs (“H”, “T”, and “I”)

Digital Outputs shall be voted using the standard 2-out-of-3 algorithm. Upon a failure of CPU or one leg of a digital output, voting shall adapt to either 2-out-of-2 or 1-out-of-2 (configurable). Upon a failure of two CPUs or legs of a digital output, voting shall adapt to either 1-out-of-1 or Default (configurable). Upon the failure of all three CPUs or legs of a digital output, voting shall adapt to supply the configured default value of on, off or hold last state to the output devices.

11.5.2.2 Voting for Simplex Outputs

11.5.2.2.1 Majority Voting

Simplex digital outputs shall take advantage of the redundant CPU architecture and be able to perform voting using the standard 2-out-of-3 algorithm. Upon a failure of one CPU, voting shall adapt to either 2-out-of-2 or 1-out-of-2 (configurable). Upon a failure of two CPUs, voting shall adapt to either 1-out-of-1 or Default (configurable). Upon the failure of all three CPUs, voting shall adapt to supply the configured default value of on, off or hold last state to the output devices.

11.5.2.2.2 Hot Standby Voting

Simplex digital outputs shall take advantage of the redundant CPU architecture and be able to perform voting using a triple Hot Standby algorithm. Under normal operation the outputs shall use data from CPU “A”. Upon a failure of CPU “A”, voting shall adapt so that the outputs use data from CPU “B”. Upon a failure of two CPUs, both “A” and “B”, voting shall adapt so that outputs use data from CPU “C”. Upon the failure of all three CPUs, voting shall adapt to supply the configured default value of on, off or hold last state to the output devices.

11.5.3 Digital Output Diagnostics

Output faults shall be logged in easy to understand English language message format with a date and time stamp for each fault. Any corresponding address information (to determine location of the fault) shall be included in the fault message that gets logged. Faults shall be listed in chronological order. In addition to fault logs of output faults, the system shall provide a fault bit for each I/O point that reflects the health of the I/O point. The fault bits shall be easily usable in a ladder logic application program in the form of relay contacts to allow the program to act on the diagnostic information. The fault bits shall also be available to be read by a host or operator interface device. Diagnostic LED indicators shall be viewable at each physical module (block). Also each point on a module (block) shall include an LED indicating the on/off state of the circuit. Digital output diagnostics shall include but not be limited to:

- Stuck on output circuit.
- Stuck off output circuit.
- Output-to-output short circuit.
- Load shorted high.
- Load shorted to 0V.
- Open circuit load.
- Open circuit output leg.
- Output circuit overload (> 2 Amps)
- Output circuit overtemp.
- Output discrepancy.
- Loss of Output module (block).

11.5.4 Electronic Output Fusing

Output circuits shall make use of internal electronic fusing in lieu of the traditional external destructive fuses. The electronic fusing shall provide the same or better protection as a destructive fuse, and also provide these benefits:

- Reduction in wiring and terminations within a panel.
- Resetting of overcurrent or short circuits remotely or locally without the need to replace a physical fuse.
- Automatic fault reporting of an overcurrent or short circuit condition with physical location and date/time stamp.

The option of using traditional external destructive fuses shall also be available.

12. Communication Interface Sub-System

12.1 Built-in Serial Ports

Each CPU shall provide a built-in RS-422/485 serial port supporting at least the following functions in combination with the programming and configuration software:

- Storing/Loading of configuration and application program to/from CPUs
- Read/Writing of application program data
- On-line monitoring of program and data
- Monitoring and acknowledge/clearing of faults
- Selection of system mode of operation (Run/Stop)
- Optional on-line program changes

Forcing/overriding I/O for troubleshooting or testing purposes

The built-in port shall be software configurable allowing selection of Baud rate, Parity, Stop bits, Data bits and Modem turn around time.

The built-in port shall support a Message mode whereby the application program can transmit ASCII messages to another device (example: printer) and shall support optional use as a connection for a host computer or MMI when not being used with the programming and configuration software. A proprietary protocol is acceptable for this port.

For the purpose of host or MMI connections, redundant ports shall be inherent in the system as each of up to three CPUs shall include it's own built-in port and the same application data and I/O fault information shall be available through any of the ports.

12.2 Optional Communications Interfaces

12.2.1 Serial RS-232 and RS-485

The system shall support multiple and redundant communications interfaces in addition to the primary built-in communications port. The optional communications interfaces shall be configurable allowing selection RS-232 or RS-422/485 operation, Baud rate, Flow Control, Parity, Stop bits and turn around time. Protocols supported can be proprietary but shall include Modbus RTU and the ability to create a custom protocol via application programming in the Basic or "C" programming languages.

12.2.2 Ethernet

Redundant Ethernet interfaces shall be supported for host or MMI communications. TCP/IP protocol shall be used with MMS available as an optional protocol.

13. Programming/Configuration Sub-System

13.1 Programming

Program development software shall operate on an Personal Computer with minimum requirements of an Intel 80386 or higher microprocessor, 2 Megabytes of RAM memory, 4 megabytes of free hard disk space and MS-DOS[®] version 5.0 or later. The programmer

hardware shall interface to the controllers using standard serial ports commonly available in personal computers; no special interface hardware shall be required.

13.1.1 General

The programming software shall be capable of operation in both on-line and off-line modes. On-line mode shall provide the ability to view the status of an operating application program. In addition, for safe operation, an on-line “monitor only” mode shall be provided which prevents any un-intentional changes. Full program development and program documentation capability shall also be provided in an off-line mode.

13.1.2 Programming Languages

Multiple program language capability shall be supported including ladder logic (primary language), Sequential Function Chart (SFC) and the “C” programming language.

13.1.3 On-Line Changes

The ability to make on-line program changes shall be provided. This ability shall be configurable to be either enabled or disabled for safe operation to prevent un-intentional changes. In the enabled mode, on-line the change function shall provide the option of verifying program operation before the new change takes effect in the system as a whole (i.e. before real world output states are affected).

13.1.4 Instruction Set

Multiple application programming language capabilities shall be available with the primary language being an IEC-1133 compliant ladder logic. The ladder logic instruction set shall include as a minimum the following groups of instructions: contacts, coils, timers, counters, relational functions, math functions, bit operations, conversion operations, control operations (including PID control), data table operations and data move operations.

13.1.5 Programming Organization

The programming software shall provide a structured programming capability which facilitates organization of the overall program into blocks that contain the logic for a functional or logical part of the process. A librarian function shall also be provided which facilitates the re-use of these program blocks in other applications with export, import and variable address offset capability.

13.1.6 Security

The programming software shall provide the ability to password protect each program block individually. Also general programming software functions shall be optionally enabled or disabled by the use of passwords. The password protected functions shall include program logic changes, Input/Output overrides, application variable data changes, Run/Stop mode

changes and clearing of faults. The application program memory shall also be keyswitch protected.

13.1.7 Application Program Annotation

The programming system shall provide full application program annotation functions including rung explanations, element names, element descriptions, program block descriptions and program descriptions.

13.1.8 Application Program Documentation (Print Functions)

The programming system shall provide full automatic documentation capability. Printouts shall optionally include application program, rung explanations, element names, element descriptions, program block structure, program block descriptions, program descriptions, variable table, variable values, I/O cross references, I/O reference use tables, and configuration data.

13.1.9 Macro Keys

The programming software shall support the creation of key macros to facilitate the re-use of commonly used keystroke sequences or to insure that a commonly used key sequence is always executed consistently and correctly.

13.2 Configuration

Configuration software shall operate on an Personal Computer with minimum requirements of an Intel 80386 or higher microprocessor, 2 Megabytes of RAM memory, 4 megabytes of free hard disk space and MS-DOS version 5.0 or later. The hardware shall interface to the controllers using standard serial ports commonly available in personal computers; no special interface hardware shall be required.

13.2.1 General

Configuration of the system shall be via software; no hardware switches or jumpers shall be used. The software shall graphically represent the hardware and allow selection of all configuration parameters.

13.2.2 Configuration Data Documentation (Print Functions)

The configuration software shall provide full and automatic documentation capability. Printouts shall include graphical representation of the system's rack (chassis) and module (block) layout and full configuration parameter detail.

14. Environmental Requirements

14.1 Temperature

The TMR system shall be designed for and be capable of full operation within the temperature range of 0° to 60° C (32° to 140° F). The TMR CPU components shall also be capable of

withstanding storage temperatures of -40° to 85° C (-40° to 185° F). I/O components shall be capable of withstanding storage temperatures of -40° to 100° C (-40° to 212° F).

14.2 Humidity

The TMR system shall be designed for and be capable of full operation within the humidity range of 5% to 95% (non-condensing).

14.3 Vibration

The TMR CPU components shall be capable of withstanding vibration of 5 to 9 Hz with 3.5mm displacement and 9 to 150 Hz at 1.0 G. I/O components shall be capable of withstanding vibration of 5 to 10 Hz with 5.08mm displacement and 10 to 200 Hz at 1.0 G.

14.4 Shock

The TMR system shall be capable of withstanding Shock of up to 15 Gs for 11msec.

15. Agency Approvals

15.1 International Standards Organization

The TMR system shall be provided by a manufacturer which is both ISO 9000 certified and ISO 9001 registered.

15.2 TÜV (Technischer Überwachungs - Verein)

The TMR system shall be certified by TÜV for use in the following basic configurations:

- TMR fault tolerant and fail safe up to class 5
- Duplex (2oo2) fail safe up to class 5
- Duplex (1oo2) fault tolerant and fail safe up to class 4

15.3 Other Agency Approvals and Standards Compliance

Appropriate components or portions of the TMR system shall also be certified by and/or comply to the following agencies standards:

- IEC 435,380
- CSA C22.2 No. 142, C22.2
- JIS C 0912, JIS C 0911
- ANSI/IEEE C-37.90A-1978
- DIN 435, 380
- VDE 805, 806, 871-877
- UL 508, 1012
- FCC 15J Part A
- NEMA/ICS 2-230.40
- VME C.1

- IEC 68-2-1 Cold test
- IEC 68-2-2 Dry Heat test
- IEC 68-2-27 Shock test
- IEC 68-2-14 Change of Temp test
- IEC 68-2-30 Damp Heat Cyclic test
- IEC 68-2-6 Vibration test
- IEC 801-2 Electrostatic Discharge
- IEC 801-3 RF & Electromag. Immunity
- IEC 801-4 Burst test
- ANSI/IEEE 37.90.1 Surge test
- DIN VDE 0160 - 7.3 Overvoltage test
- DIN VDE 0116 P.S. Interrupt test
- DIN VDE 0116 P.S. Variation test

Genius is a registered trademark of GE Fanuc Automation North America, Inc. MS-DOS is a registered trademark of Microsoft Corporation.