GE Fanuc Automation

Programmable Control Products

Genius Modular Redundancy for Fire and Gas Applications

GFK-1649A *September 1999*

Warnings, Cautions, and Notes as Used in this Publication

Warning

Warning notices are used in this publication to emphasize that hazardous voltages, currents, temperatures, or other conditions that could cause personal injury exist in this equipment or may be associated with its use.

In situations where inattention could cause either personal injury or damage to equipment, a Warning notice is used.

Caution

Caution notices are used where equipment might be damaged if care is not taken.

Note

Notes merely call attention to information that is especially significant to understanding and operating the equipment.

This document is based on information available at the time of its publication. While efforts have been made to be accurate, the information contained herein does not purport to cover all details or variations in hardware or software, nor to provide for every possible contingency in connection with installation, operation, or maintenance. Features may be described herein which are not present in all hardware and software systems. GE Fanuc Automation assumes no obligation of notice to holders of this document with respect to changes subsequently made.

GE Fanuc Automation makes no representation or warranty, expressed, implied, or statutory with respect to, and assumes no responsibility for the accuracy, completeness, sufficiency, or usefulness of the information contained herein. No warranties of merchantability or fitness for purpose shall apply.

The following are trademarks of GE Fanuc Automation North America, Inc.

Alarm Master	GEnet	PowerMotion	Series Six
CIMPLICITY	Genius	ProLoop	Series Three
PowerTRAC	Helpmate	PROMACRO	VersaMax
CIMPLICITY 90–ADS	Logicmaster	Series Five	VersaPro
CIMSTAR	Modelmaster	Series 90	VuMaster
Field Control	Motion Mate	Series One	Workmaster

Contents

Chapter 1 Introduction

This document describes the requirements for Fire and Gas Systems based on E/E/PE systems. It explains how Genius Modular Redundancy (GMR) can be applied to produce Fire and Gas Systems that conform with the requirements of IEC 61508. Additional important information is provided in the *GMR User Manual* (GFK-1277B).

Assessment of the Genius Modular Redundancy system by TÜV Rheinland has been completed in accordance with IEC 61508 for a range of system configurations capable of meeting up to SIL3 requirements for both Fire and Gas, and, Emergency Shutdown applications. This assessment continues to build upon GE Fanuc's proven product manufacturing capabilities and Silvertech's experience in Fire and Gas applications.

This chapter provides background information about Fire and Gas Systems, their components and performance requirements. Later chapters highlight the issues of and configurations for creating Fire and Gas Systems using GMR. The appendices provide the information necessary to calculate individual Probability to Fail on Demand for each safety function, an example application and information concerned with the configuration of Fire and Gas Systems.

Terms and Abbreviations

1oo1	One out of One Voting
1oo1d	One out of One Voting with 2-0 Degradation
1oo2	One out of Two Voting
1oo2d	One out of Two Voting with 2-0-1 Degradation
2oo2	Two out of Two Voting
2oo3	Two out of Three Voting
DCS	Distributed Control System
E/E/PE	Electrical, Electronic and Programmable Electronic
ESD	Emergency Shutdown
F&G	Fire and Gas
GBC	Genius Bus Controller
GMR	Genius Modular Redundancy
HHM	Hand Held Monitor
HMI	Human Machine Interface
HSB	Hot Standby
HVAC	Heating Ventilation and Air Conditioning
I/O	Input/Output
IP	Ingress Protection
IR	Infra-Red
MAC	Manual Alarm Call Point
MCB	Miniature Circuit Breaker
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
N/C	Normally Closed
N/O	Normally Open
PFD	Probability of Failure on Demand
SIL	Safety Integrity Level

References

Standards

IEC61508	Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems
DIN VDE 0801	Principles for Computers in Safety Related Systems
DIN VDE 19250	Fundamental Aspects to be Considered for Measurement and Control Equipment
EN 50178	Electrical Equipment to be used in Electrical Power Installations and their assembly into Electrical Power Installations
DIN VDE 0116	Electrical Equipment for Furnaces
NFPA 72	National Fire Protection Association Part 72 Fire Suppression Systems
NFPA 85.01	National Fire Protection Association Part 85.01, standard for the prevention of Furnace explosions/implosions in single burner boilers.
NFPA 85.02	National Fire Protection Association Part 85.02, standard for the prevention of Furnace explosions/implosions in multiple single burner boilers.
ANSI/ISA S.84	International Society for Measurement & Control (ISA), Standards and Practices Committee No.84 Application of Safety Instrumented System for Process Industries
BS 5345/ IEC 79-10	Codes of Practice relating to the Selection, Installation and Maintenance of Electrical Equipment for use in hazardous areas
BS 5501/ EN50 015... EN50 020	Electrical Apparatus for Potentially Explosive Atmospheres
BS EN ISO 9001	Quality Systems
IEE Wiring Regulations	IEE 16th Edition Wiring Regulations

Related Documents

GFT-177	GMR Flexible Triple Modular Redundant (TMR) System - Technical Product Overview
GFK-1277B	GMR Flexible Triple Modular Redundant (TMR) System – User Manual
GEK-90486D-2	Genius I/O Discrete and Analog Blocks

Overview

Legislation throughout the world makes clear that businesses and individuals alike share a responsibility for the health and safety of other individuals and the environment. In addition, businesses have vested commercial interests in ensuring the safe operation of plant and processes.

The document IEC61508 *Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems* describes a Lifecycle Safety Management Framework from which to take a structured approach in the assessment and control of such hazards. Fire & Gas Systems fall under the scope of safety systems covered by this standard.

A Fire & Gas Systems is intended to detect and annunciate Fire and/or Gas hazards at the earliest possible time and to automatically initiate protective measures. Although primarily a physical measure, a Fire and Gas System requires procedural measures to ensure its effectiveness.

Components of a Fire and Gas System

A Fire and Gas System is mainly concerned with detection, annunciation and mitigation of fire and/or gas hazards. It must perform this function without itself creating further hazards.

Fire and Gas Systems typically have the following basic components and sub-systems:

- Detectors
- Barriers
- Input Units
- Logic/Control System
- Annunciation/Displays
- Audible Alarms
- Manual Controls
- Interface to other safety systems.
- Output Units
- Actuators

Each of these components/sub-systems is described on the following pages.

Detectors

Detectors are placed in areas or zones where a fire or gas hazard may exist. The document BS 5345/IEC 79-10 *Codes of Practice Relating to the Selection, Installation and Maintenance of Electrical Equipment for use in Hazardous Areas* provides guidance on the placement of detectors.

Using several detectors of the same type in an area provides protection against device failure. Combining the outputs of a group of detectors protects against spurious system response due to a fault in the detector or communications line.

Detectors are usually located where they may be exposed to explosive gas/air mixtures. Appropriate measures should be taken to prevent ignition. Such measures are described in BS 5345/IEC 79-10 & 11 and in BS 5501/EN50 015...EN50 020 *Electrical Apparatus for Potentially Explosive Atmospheres.*

Types of Fire and Gas Sensors

The common sensors for detecting Fire and Gas hazards include:

Gas Combustible	sensitive to combustible gases. The three most common types are catalytic or pellistor, electro chemical and IR absorption.
Gas Toxic	sensitive to toxic gases, e.g. hydrogen sulfide, carbon monoxide/dioxide, etc. The most common type is electro-chemical.
Smoke	sensitive to smoke particles. The two most common types are ionization and optical detectors.
Heat	sensitive to temperature. The two most common types are rate-of-rise and fixed-temperature detectors.
Flame detectors	sensitive to the flames of a fire. The most common type is IR.
Break-glass or MAC	simple switches.

Detector Interfaces to the Fire and Gas System

In a Fire and Gas System, detectors may be single devices, multiple devices on a loop, or multiple independently-addressable devices on a loop.

Addressable devices on a loop are interfaced to a Fire and Gas System by a proprietary unit from the detector manufacturer. This interface is usually external to the system, as described later in this section. Addressable schemes can localize a hazard to a single detector. They provide reduced wiring cost, but increase the risk of common-mode failure. Addressable systems are usually restricted to lower-risk areas such as the accommodation module in offshore installations.

Non-addressable devices on a loop are interfaced to a Fire and Gas System by a digital or analog signal. An analog interface can indicate line and detector faults by out-of-range readings. It is possible to use conditioning components for digital-type sensors to produce multiple signal states for varying field loop conditions, such as open circuit, short circuit, and normal or tripped states.

Digital input configurations are available that can indicate the presence of a fault such as a ground fault as a trip condition. A Genius block's tri-state discrete input improves this by being able to report a field fault, i.e. open wire or shorted wire, while allowing the input to respond to a trip condition.

A number of detectors latch an alarm condition. An example of this type of device is a smoke detector. Detectors that latch an alarm condition must be de-energized after a trip so that they can be reset and re-armed. If this is required, it is important to be sure that protective measures already taken by the system are not removed without positive confirmation that the hazards are no longer present.

Barriers

A barrier is a device that limits the amount of power present in a field circuit, so that it cannot ignite an explosive gas/air mixture. The normal field signals carried by a barrier are small analog voltage (<30V) or current (<100mA) signals. Two common types of barriers are safety barriers and isolation barriers.

Safety barriers are simple passive devices based upon zener diodes and resistors. They do not require a power supply to operate. Power to the field device is supplied from the protection system power supply and/or input unit. These devices require a reference potential for operation.

Isolation barriers are active electronic devices. They perform power-conversion and power-limiting functions and may require a separate power source. These devices do not require a reference potential for their operation.

If barriers are used, they must be correctly rated for the application, e.g. safety description (voltage/current/resistance ratings), cable properties, etc, and they must conform to any system certification requirements for the sensors.

Input Units

Input units condition and convert the detector signal for transfer to the logic/control unit. Many types of signal conversion are available, including analog-to-digital conversion, analog-level trip detection, and detector excitation with amplification and conversion.

In some Fire and Gas Systems, the input unit also indicates field conditions such as alarms, signal values, and faults, and permits manual testing and inhibiting of the field signal.

Depending upon the system architecture, input units can incorporate self-checking and diagnostic functional checks to ensure that the units are operating correctly.

In addition to interfacing field devices to the system, input units also interface internal protection system signals such as: fuse failure and over-temperature. In this way, the protection system provides a high level of diagnostic and fault reporting.

Logic/Control System

In the Fire and Gas System, the logic/control unit receives the input signal, performs the logic for annunciation and control actions, and interfaces to external systems.

The logic/control unit performs such functions as inhibiting I/O, alarm-tripping analog signals, handling detector/actuator faults, detector voting, control of local and field annunciation, control of extinguishing system, control of output devices such as fans and dampers, and interfacing to other systems such as HVAC, ESD systems. The critical role of the logic/control unit means that some type of redundancy is usually desirable.

Fire and Gas Systems are normally-dormant or inactive systems. In Fire and Gas Systems, input signals and internal logic states may remain unchanged for long periods of time. If a fault develops while the system is inactive, it is important to be sure the system will respond appropriately. Therefore, thorough periodic background diagnostic tests must be performed to be sure the system remains able to function on demand.

In addition, a Fire and Gas System should have built-in measures such as watchdog timers, to bring the system to a pre-determined state in the event of erroneous logic program operation.

Annunciation

Fire and Gas Systems often include both display panels and/or computer-generated displays to alert operators to problems. The display normally indicates the plant or process areas and the presence/absence of hazardous conditions. The display can also indicate faults with the field devices or the control system.

Indicators such as LEDs or lamps may flash or stay on. The operator interface usually includes controls to inhibit detection, disable or permit automatic actions, initiate manual actions, and acknowledge hazards.

Computer-generated displays can provide more information about alarm conditions and a greater degree of operator interaction with the system. They can also generate electronic or printed reports of alarms, faults, inhibits/overrides, trips, and other significant events.

Audible Alarms

The low incidence of hazards in a well-designed and operated plant usually means the operator's attention will have to be drawn to a potentially hazardous situation. This is normally done with an audible signal such as a buzzer. The operator can turn off the signal when responding to the problem. Some systems use different sounds to identify different types of hazards. In addition, Fire and Gas Systems often control plant-wide audible alarms to warn of hazards and protect personnel. These audible alarms are normally accompanied by visual signals such as flashing/rotating beacons.

Interfaces to External Systems

A Fire and Gas System can exchange data with an external system over a communications link and/or through the use of physical I/O devices. In distributed applications, data can be shared among multiple Fire and Gas Systems and other safety systems.

A communications interface allows the transfer of system data and system control (if enabled). This type of communications interface is needed when the system includes a HMI display system or data-logging capability. The interface can be dedicated communications units or a direct link to the logic controller. Typical examples of communications links are RS232/RS422/RS485 serial links running a variety of protocols, and high-performance links such as Ethernet, Genius, Modbus Plus, ProfiBus, etc.

Interfacing through physical I/O can be done using standard I/O units. This type of interface is useful where no convenient communication link exists or no compatible communication protocol can be conveniently provided. Physical I/O interfaces can also be used to bypass and/or trip the signals for maintenance or system test.

Sometimes a Fire and Gas System must interface with an ESD System. That should be done using normally-energized outputs, which can set up so that the receiving system requires a trip on two outputs to initiate an action (1oo2D voting). In addition to signaling the hazard, the Fire and Gas outputs would also be de-energized in the event of total Fire and Gas System failure. This could provide a fail-safe mechanism for a Fire and Gas System failure either by annunciation to allow operator action and/or by automatically de-energizing a signal to the Emergency Shutdown system.

Output Units

Output units convert signals from the logic/control system and use them to control or actuate output devices. Where logic controller redundancy is used, output units normally perform the voting function. They do that by combining information from two or more logic controllers to produce a single voted output signal. An output unit generally includes diagnostic capabilities to report both internal faults and output faults such as open circuit, short circuit, or out-of-range. An output unit can also indicate output status and permit manual control and testing of the output circuit/actuator.

Actuators

Output actuators provide control and protection for the plant. Fire and Gas actuator outputs are usually digital. Typical actuators include Solenoid Operated Valves, for controlling ventilation dampers or extinguishers and indicators.

Certain outputs are normally energized so that failure of the Fire and Gas System causes automatic action. Examples of normally-energized outputs include fire dampers and a shutdown interface to an Emergency Shutdown System.

On a Fire & Gas System, outputs for which failure is undesirable should be de-energized. Examples include extinguisher systems (Deluge/CO_2/Halon) systems, and outputs to annunciation devices.

Critical system outputs such as extinguishant release outputs permit manual initiation independent of the Fire and Gas System. This is sometimes described as “a diverse path”.

Performance

Typical performance figures for a Fire and Gas System are detailed below.

Response Time

The system executive action response time, not including field devices, is normally less than 1 second and should not exceed 2 seconds. Note that some types of detector have detection times of 10 seconds or more.

Reliability and Availability

Reliability is the probability that a component will fail to perform its intended function per unit time. System reliability is calculated on a loop-function basis using the individual failure rates of the components of the loop. A loop comprises the units and devices necessary for the intended function, taking account of any redundancy, from input to output for the executive path. Including all field devices.

If the failure of one component will result in the failure of the path, the reliability of path is:

$$\lambda = \sum (\text{MTBF})^{-1} \qquad \text{where } \lambda \ll 1$$

Calculation for other levels of redundancy is described in *Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems* (IEC61508).

Availability is the probability that a system will perform its intended function per unit time. It can be calculated using the Mean Time To Repair (MTTR) and Mean Time Between Failures (MTBF) as follows:

$$\text{Availability} = (1 + \text{MTTR}/\text{MTBF})^{-1} \qquad \text{where } \lambda \ll 1$$

Industry practice is to assume a MTTR of 8 hours.

Diagnostic Coverage

Diagnostic coverage is the ratio of revealed-to-unrevealed faults that will be detected by the internal diagnostic checks of the unit or system. The diagnostic coverage of a Fire and Gas System as a low-demand system is expected to be 90% or greater. The time interval between diagnostic runs should be significantly less than the proof test interval to ensure correct operation of the system safety functions. The usual time between diagnostic runs is 24 hours or less.

Demand Rate

Demand rate is the probability of a demand being placed upon the system per unit time. Fire and Gas Systems are low-demand systems. The expected demand rate for a Fire and Gas System is typically less than once per year ***per safety function***.

Proof-Test Interval

Proof-test interval is the number of hours between manual proof tests of each of the system's intended functions. Testing must include the system detectors and actuators that are normally dominant in calculations of system reliability. The proof test demonstrates correct system function and reveals dormant faults not detected by the system diagnostics. Industry expectations for proof test interval is between 6 and 12 months.

Probability to Fail on Demand

Probability to fail on demand is the likelihood that the system will fail to perform its intended function when demanded. A Fire and Gas System being a low demand system would normally be expected to meet per safety function, including the associated field devices, one of the following SIL in accordance with IEC61508.

Safety Integrity Level	Probability to Fail on Demand (Low Demand Mode of Operation)
SIL 1	10^{-1} to 10^{-2}
SIL 2	10^{-2} to 10^{-3}
SIL 3	10^{-3} to 10^{-4}

Chapter 2 System Design

The Fire and Gas System described in this document is based upon the Genius Modular Redundancy (GMR) system. GMR is a flexible system specifically designed for industrial control applications including applications with safety-related requirements.

TÜV Rheinland has approved GMR systems for safety-related applications in which the de-energized state is the safe state (ESD Systems). GMR systems can also be designed for Fire and Gas applications by utilizing the following features:

- Simplex, duplex or triplex redundant processing units utilizing Genius I/O Blocks
- Failsafe or Fault-tolerant input structures utilizing Genius I/O Blocks
- Failsafe or Fault-tolerant (H-block and I-block) output structures utilizing Genius I/O Blocks
- Interface to external systems using industry-standard communication modules
- Genius I/O units with extensive diagnostic and voting features

For more information about GMR, refer to GFK-1277B *Genius Modular Redundancy Users Manual* and GFT-177 *Genius Modular Redundancy Technical Guide*.

GMR Fire and Gas System Configurations

Several GMR configurations can be used for Fire and Gas Systems. The sections below list these configurations for each sub-system, together with their expected achievable SIL ratings in an application.

The SIL rating achieved for a safety function can only be determined by a complete analysis of the loop including the input and output field devices.

IEC61508 permits including a lower SIL function in a higher SIL-rated system if there is adequate separation of the safety functions, and if system operation and maintenance are based on the highest SIL rating.

Processor Configuration Options

The extensive diagnostics of the GMR CPU family have been examined by TÜV. The designation Simplex D describes a single CPU with dual Genius Bus Controllers providing two paths to shutdown the output via either an I-block/1oo1D output group or an H-block/1oo2D output group.

For SIL 2 rated systems, the minimum redundancy requirement is a simplex D or duplex (voting 1oo2d[†] in the output blocks) CPU. For SIL 3 rated applications the minimum redundancy requirement is duplex (voting 1oo2 in the output blocks) or triplex processor redundancy. For both SIL 2 and SIL 3 rated applications, dual Genius busses are required.

The details of these processor configurations are described in the *GMR User Manual*.

Processor Redundancy	Expected Safety Function SIL Rating
Simplex	1
Simplex D (1001d)/ Duplex (1oo2d[†])	2
Duplex (1oo2)/Triplex	3

[†] The voting option designation 1oo2d implies voting 2oo2⇒1oo1⇒Default Action.

Input Configuration Options

The following input configuration options meet the SIL ratings indicated if the associated detector reliability meets the PFD requirement for that SIL level. Under IEC61508 for SIL 3 requirements, simplex detector redundancy is not permitted for type B components with a safe failure fraction below 99%.

In the table below, digital input units are assumed to be two-state signals and include Genius tri-state. Analog inputs are more than two-state signal inputs. See Appendix D for information concerning configuration requirements for Fire and Gas applications.

The table shows the application voting required for a given sensor configuration. The data presented to the application is voted by GMR where duplex or triplex input unit redundancy is used. GMR voting offers 1oo2, 1oo2d[†] and 2oo3 for digital input, and, Mid-Value Select, High, Low and Average for analog inputs.

For Fire and gas applications, it is assumed that application voting is performed on the alarm signals produced by alarm processing the analog signal which is taken directly from the input reference tables for simplex input units, or from the GMR voted data for duplex or triplex input unit redundancy.

The details of the GMR voting for these input configurations are described in the *GMR User Manual*.

Detector Redundancy	Safety Function Voting	Input Unit Type	Minimum Input Channels per Detector	Minimum Number of Inputs Units	Expected Safety Function SIL Rating
Simplex	1oo1	Digital	1	1	1
		Analog	1	1	
Simplex	1oo1	Digital	1	1	2
		Analog	2	2	
Simplex[‡]	1oo1	Digital	2[§]	2	3
		Analog	3	3	
Duplex	1oo2	Digital	1	2	2
		Analog	1	2	
Duplex	1oo2	Digital	1	2	3
		Analog	2	2	
Triplex or Higher	2ooN	Digital	1	3	3
		Analog	1	3	

[§] GMR Voting must be set to 1oo2

[‡] This configuration is only permitted under IEC 61508 if it conforms with the requirements of IEC 61508 Part 2 Table 2 Architectural Constraints on Type A Safety Related sub-systems and Table 3 Architectural Constraints on Type B Safety Related sub-systems.

[†] The voting option designation 1oo2d implies voting 2oo2⇒1oo1⇒Default Action.

Output Configuration Options

The following digital output configuration options meet the SIL ratings indicated shown if the actuator reliability meets the PFD requirement of that SIL level. Since Fire and Gas Systems seldom include analog output safety functions, these have not been included.

TÜV carefully assessed the I-block and H-block configurations and confirmed that these configurations correspond to the industry designations of 1oo1d and 1oo2d, respectively, on an individual channel basis. Accordingly they are shown in the tables for completeness.

The details of the simplex, I-block and H-block output configurations are described in the *GMR User's Manual.*

Actuator Redundancy	Safety Function Voting	Output Configuration (per actuator)	Expected Safety Function SIL Rating
Simplex	1oo1	Simplex	1
Simplex	1oo1	I-block/1oo1d , H-block /1oo2d†	2
Simplex‡	1oo1	I-block/1oo1d , H-block /1oo2d†	3
Duplex or Higher	1oo2	Simplex¥, I-block/1oo1d , H-block /1oo2d†	3

† The voting option designation 1oo2d implies voting 2oo2⇒1oo1⇒Default Action.

‡ This configuration is only permitted under IEC 61508 if it conforms with the requirements of IEC 61508 Part 2 Table 2 Architectural Constraints on Type A Safety Related sub-systems and Table 3 Architectural Constraints on Type B Safety Related sub-systems.

¥ Output signals must be on different output units.

The corresponding safe state for these options is shown below.

Safe State	Output Configuration
Energized	Simplex, H-block/1oo2d†
De-energized	Simplex, I-block/1oo1d,/H-block/1oo2d†

† The voting option designation 1oo2d implies voting 2oo2⇒1oo1⇒Default Action.

Chapter 3 Application Design

Software Lifecycle Techniques And Methods

GE Fanuc and Silvertech are ISO9001 accredited companies with declared design and development processes and procedures.

The existing GMR system has successfully been designed, developed and released into the marketplace using these processes and procedures. The product has been independently inspected and approved by TÜV Rheinland to a number of recognized standards as noted in chapter 1.

The GMR system is based upon field-proven Series 90-70 PLCs and Genius I/O blocks. The installed base is in excess of tens of thousands of PLC CPUs and several hundred thousand Genius blocks.

Building on these proven components, GE Fanuc and Silvertech jointly developed the design concepts for the GMR system. The system design and implementation followed the principles and ideals set out in IEC61508.

Application Design Principles

As required by IEC61508, a Fire and Gas System design must consider the complete safety lifecycle. GMR-based Fire and Gas Systems should be designed and implemented by skilled practitioners who are knowledgeable in the theory of operation of the GMR system and its components.

To implement a Fire and Gas System using GMR, the following system design principals should be observed. Some of these principles are generic to Fire and Gas SysGas Systems; others are specific to GMR.

System Architecture

A well-designed Fire and Gas System achieves a balance between the PFD (Probability of Failure on Demand) and spurious trip rate. Simple configurations may achieve the required performance target for one of these parameters at the expense of the other. However, over-specification can lead to increased costs, and result in an overly-complex system with greater risk of configuration and maintenance induced errors.

A key design consideration is selecting the performance requirements of each safety function. System performance must be viewed in the context of all safety measures. System performance must also consider such contributing factors as detectors and actuators.

Fire & Gas SysGas Systems are typically SIL1 or SIL2 rated systems however GMR is approved up to SIL3 rating. The usual configuration of the executive control path of a typical Fire and Gas SysGas System is:

- Redundant/simplex sensors with simplex input unit.
- High-reliability simplex sensors with dual input unit redundancy voting 1oo2.
- Dual Processors/CPUs.
- Normally de-energized duplex (1oo2D) voting simplex output block for initiating fire protection measures, for example deluge/CO2 systems and annunciation.
- Normally energized outputs voting 2oo2⇒1oo1 for signaling higher-order safety systems, for example ESD, and other actuators that have a de-energized safe state.
- Manual controls for override/initiation of critical outputs, acting upon the output signal.

This type of system is easily operated and maintained, achieving the required PFD while avoiding an excessive spurious trip rate.

Environment

The environment where the system will be installed must be considered for such factors as temperature, shock, vibration, EMC, and dust/water.

The Series 90-70 PLC and Genius equipment are designed and rated for the wide range of industrial environments. Special measures are not normally required. Note that if CPU model IC697CPM790 is used, fan kit IC697ACC721 (for AC) or IC697ACC724 (for DC) should be installed for cooling where the ambient temperature may exceed 40°C.

Protection against particle/water infiltration and mechanical damage are provided by mounting the equipment in suitable IP-rated cabinets. Where high shock and vibration levels are expected, for example marine based applications, anti-vibration mounts can be used on the cabinets.

The EMC rating of the equipment is suitable for industrial environments when it is installed in accordance with GE Fanuc's installation instructions.

Power Supply

In accordance with EN54 *Fire Detection and Fire Alarm Systems,* the power source for a Fire and Gas System should incorporate battery backup so system detection is retained if the power supply fails. The power supplied to the Fire and Gas System can be DC or AC from suitable inverters. Where AC power is supplied, two or more independent feeds should be provided. The state of the power sources and battery backup should be monitored and reported.

Most of the I/O devices and I/O units used in Fire and Gas Systems are low-voltage and DC-operated. The GMR system requires close matching (<5%) of the Genius block power supplies to assure correct operation.

To minimize the problem of matching/tracking supply voltages, an AC powered GMR-based Fire and Gas System should use a high-integrity DC distribution bus bar supply based on a M+N arrangement (see below). This is done by combining the outputs of the power supplies through suitable blocking diodes. The blocking diodes prevent internal faults within a supply from affecting the bus bar.

The base number of supplies required (M) is determined by calculating the load demand and dividing the load demand by the individual power supply capacity. To accommodate individual supply failures an additional (N) units are added. The design and calculation must accommodate the loss of one of the AC supplies. A simple technique to avoid excessive numbers of power supplies is to share the load equally on the AC feeds and provide a fast switchover to an alternate supply in the event of a loss of a supply feed.

The system must monitor each of the supplies to check that its output remains within limits, and to warn of failures.

Power wiring must meet with the requirements of control equipment. Wire capacity and wire color, AC/DC segregation, temperature rating, MCB, fusing, etc, should be in accordance with internationally recognized standards. Fuse and MCB trip must be reported to the system for annunciation purposes.

"Hot" insertion/removal of Series 90-70 PLC equipment is not recommended. Power to the modules is controlled by the power switch on the Series 90-70 power supply module. To replace the power supply itself requires an isolation switch in the power feed to the power supply module.

It is recommended that individual Genius I/O blocks be de-powered for replacement. Follow the instructions in GFK-1277 (*Genius Modular Redundancy User's Manual,* revision A or later) for block power isolation.

With careful system design and selection of appropriate I/O configuration, replacement of faulty units will not affect system operation.

Genius Bus

The Genius bus must be connected so as to permit addition or removal of a Genius I/O block or Bus Controller on the bus without affecting integrity of the bus connections. When installing the bus cable, the Shield In/Shield Out connections must be made to the correct terminals and Serial 1/2 must not be swapped from device to device. Rules for topology, cable type, length and baud-rate must be adhered to.

Sensors

Sensors must be located according to the manufacturer's recommendations, and the guidance provided in BS 5345/IEC 79-10, *Codes Of Practice Relating To The Selection, Installation And Maintenance Of Electrical Equipment For Use In Hazardous Areas.* Suitable weatherproof fixings/mountings must be used where the sensor is located in exposed positions.

Sensors must be accessible for maintenance and testing. For example, it may be necessary for gas sensors located in the ceilings to be provided with a tube for facilitating remote gassing from floor level.

System Inputs

For best PFD (Probability of Failure on Demand) and spurious trip performance, detector redundancy is recommended. Detector redundancy combines the advantages of spurious trip rejection, easier maintenance, and generally high SIL ratings. Input unit redundancy is not normally required for multiple-sensor voting group configurations, such as voted gas detectors.

Redundant sensors within a voting group must be distributed across different input modules and Genius busses to avoid common cause failure.

Because hazard-detection times can differ significantly depending on detector locations, the discrepancy function within the GMR logic will declare the first up signal as discrepant and reject it. Therefore application voting is recommended for redundant Fire & Gas sensors where alternate appropriate responses are required.

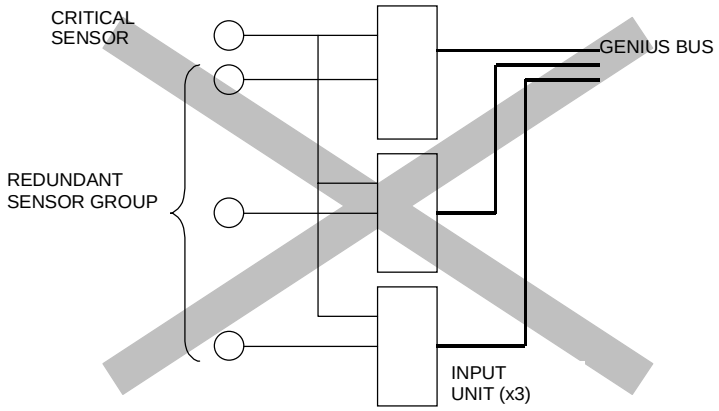
For critical high-reliability non-redundant input sensors, use duplex or triplex input unit redundancy with GMR voting.

For Voted DC discrete inputs, the GMR termination boards (or equivalent devices) provide de-coupling between input blocks with the option for asynchronous autotest. The autotest feature must be activated for SIL2 and SIL3 applications using discrete inputs.

For input signals requiring line monitoring for either analog and discrete sensors, consider using analog inputs or tri-state discrete inputs (16 channel Genius blocks). Non-line monitored inputs can be input via 32 channel Genius blocks. Ground Fault Detectors per EN54 *Fire Detection and Fire Alarm Systems* are not normally required because field faults such as short circuit to ground are detected by the Genius block diagnostics.

Redundant sensors using simplex analog input unit redundancy can be accommodated alongside sensors using duplex/triplex input unit redundancy, as illustrated below, by setting the input discrepancy limits to their maximum and using the input signal directly from the block in the configured reference address.

Mixing redundant sensors with input unit redundancy, as shown below, cannot be done for discrete inputs. This is a feature of GMR input voting that may cause erroneous fault reports, due to sustained differences in the input signal states.



The input signal sense of tri-state discrete inputs (normally open or normally closed) must be the same for all points on a Genius block. The correct block mode (GMR for N/C or non-GMR for N/O) must be configured.

Field loops should provide a way to electrically isolate field circuits for maintenance. It should be possible to inhibit field inputs. This can be done at a physical level, for example, by maintaining the discrete input active, or it can be done by providing a control input to act upon the system logic.

The system should indicate/report if an inhibit is active. The system should incorporate measures to rapidly remove inhibits on critical inputs under operator control, for example by means of a “remove all inhibits” keyswitch. This function is particularly important where software-based inhibits are used.

Forcing I/O at the Genius block is only recommended for non-commissioned loops, because such forces cannot easily be removed by operator command on a system basis.

“Intrinsically-Safe” (I.S.) circuits must be adequately-separated from non-I.S. circuits in the hazardous environment, in accordance with the separation requirements laid down by the IS and IS Installation standards. Note that the PDF calculations described in Appendix B do not include I.S. circuits; this additional hardware with its associated MTBF figures will change the results of PFD calculations.

Logic Units

AC-powered redundant logic units should be powered from separate power sources, so that loss of a power supply would only affect one processor. The Series 90-70 PLC can tolerate a 20mS interruption in its supply. A fast switch to an alternate supply can maintain full system operation if the primary power supply fails.

In determining the system response time the interaction of the Genius bus and CPU sweep times should be examined. Calculation of Genius bus time and CPU sweep time can be made as instructed in the Series 90-70 PLC and Genius I/O system documentation. For the CPU sweep time include the GMR base scan time into the calculations as detailed in the *GMR User's Manual*.

Genius bus scan times greater than 60mS are to be avoided. Longer scan times can cause problems with the operation of the autotest functions, especially if the Genius bus is also the inter-PLC communications bus. Consider re-distributing the Genius devices or adding more busses to lower the scan time if necessary.

The application must determine what data has to be synchronized when a PLC is brought on line where other PLC's are online. Typical data that will need to be synchronized are latched states and timer/counters.

Annunciation

The annunciation sub-system must provide the basic annunciation requirements of

- alarms (by zone)
- overrides/inhibits (by zone)
- system faults (e.g. Fault Table Entry, CPU Table Entry, Fuse Fail, etc.)
- audible(s)

The annunciation sub-system must also provide the basic system control requirements of

- reset (to clear latching detectors and system faults)
- manual trips/permissives (by zone)
- manual overrides (by zone)
- mute audible(s)

Output Units

Output units should be selected on rating and diagnostic capability. Several redundant output configurations are available to provide reduced PFD (Probability of Failure on Demand).

For outputs with a high SIL requirement, 16-channel Genius DC discrete output blocks should be considered. These blocks' no-load detection and pulse test capabilities provide a high level of diagnostic coverage for the output actuator and associated field wiring. Output points on these blocks are rated for 2 Amp duty with a high surge capacity. The block rating of 16 Amp total load current should not be exceeded on a continuous basis.

The 8-point Genius AC discrete block provides a no-load diagnostic of the state of the output load. Output points are rated for a 2 Amp with a high surge capacity. The block rating of 15 Amp total

load current should not be exceeded, and the leakage current should not cause any problem with low-powered loads.

For annunciation purposes and low-power load ratings, 32-point Genius DC blocks may be suitable. The block diagnostic capabilities provide detection of field wiring faults. Output point rating is 0.5 Amp per channel and 16 Amps per block.

If No-load reporting is enabled on 16-point DC blocks, the minimum load for an H-block group is 100mA; for an I-block group it is 50mA.

The appropriate normal state for the load (On or Off) must be configured for H/T-block and I-block output groups.

For the I-block configuration to avoid unnecessary shutdowns/control actions during maintenance activities, some way of maintaining energized outputs active is needed during replacement of a block. This can be done with bypass links. For example, on the GMR termination boards, the "unused" connectors provide a convenient bypass access point.

For SIL2 and SIL 3 rated outputs, the output autotest must be configured. The GMR output autotest uses the block pulse test feature, which is performed on all outputs of a block. Pulse test can only be enabled or disabled on a per-block basis. The pulse test can activate small or high-speed loads, so it may be necessary to pre-load the output or fit high-inertia output relays.

- For 16-point blocks, output pulses start at 1 mS and if the load current is below the no-load threshold, the block progressively increases the duration in several steps to approximately 18 mS as it searches for a load demand.
- For the 32 point blocks the pulse test is of a fixed duration (approximately 1mS).

Critical system outputs may be provided with manual bypass and trip capabilities, with trip normally taking precedence over bypass. The system should provide the ability to remove manual bypasses on critical outputs. Outputs that have been bypassed must be annunciated.

Due to the asynchronous nature of GMR, frequently-changing outputs can exhibit phasing effects if the Genius block voting is either GMR or duplex. For this reason, frequently-changing outputs should be voted using the Genius Hot Standby voting which is incompatible with H-block and I-block groups. Also, output discrepancy reporting is only available with the Genius block in GMR mode.

It is important to make sure that the Genius I/O block configuration selections for Redundancy Mode (GMR, Duplex, Hot Standby, or "No Redundancy") and Duplex Default (On or Off) are consistent with the output group type. See GFK-1277 for detailed information on configuring Genius I/O Blocks in output groups.

PFD calculations should also account for any additional output devices such as I.S. barriers and interposing relays.

Chapter 4 Operation and Maintenance

The operation and maintenance of a Fire and Gas System requires consideration of the complete safety lifecycle. The development of operation and maintenance procedures is the responsibility of operators/maintainers. It should be done by skilled practitioners who are knowledgeable in the application of Fire and Gas Systems.

The development of these procedures is outside the scope of this document. However general information about generic and GMR-specific Fire and Gas System operation and maintenance is given below.

CAUTION

Maintenance on a live system requires careful planning, adherence to operating and maintenance procedures, and the appropriate permits and permissions.

These matters are the responsibility of the owner/operator of the system and are outside the scope of this document.

Overview

The GMR system builds upon the extensive diagnostic features of the Series 90-70 PLC. These diagnostic features facilitate straight-forward maintenance of a GMR Fire and Gas System.

These diagnostic features include:

- I/O Fault Table; identifies module faults and field faults with locating reference and online help.
- CPU Fault Table; identifies system faults with locating reference and online help.
- System Status References; flags indicating system status, e.g. any force present
- Fault locating references; these indicate fault status to an I/O channel level.

In addition to these features, the GMR executive software adds the following diagnostics capabilities:

- Fault reporting module; this is a user accessible program block that can be used to access specific fault data.
- GMR fault table messages; the executive software logs a number of messages to the fault tables.
- GMR system status bit references; these provide status on such points as autotest, PLCs online, etc.

Full details of these standard features can be found in the GE Fanuc Series 90-70, Genius I/O block and GMR User Manuals

Maintenance

The maintenance of a system requires that no unintended changes in state occur when performing a maintenance action. If possible, the system should not be inhibited from responding to a demand. If an inhibit is necessary, appropriate measures must be taken to provide alternative protection during the period any inhibits are active.

TÜV Rheinland has provided a number of recommendations, re-printed in GFK-1277B (*Genius Modular Redundancy User's Manual)* Appendix B, concerning procedural and other measures including checklists pertaining to the use of maintenance overrides.

Fire and Gas Systems are normally multi-sensor with no input unit redundancy, dual processors and de-energized outputs voting 1oo2. Such system can normally be easily maintained without inhibiting the system.

The maintenance actions required for a Fire & Gas System that is in service typically include:

- Replacing a defective unit, such as a sensor, input unit, processor unit, output unit or actuator.
- Handling an abnormal/facility plant operating condition, for example: arc welding, deluge pump taken out of service.
- Upgrading the application software and/or adding new units.
- Routine Proof Testing of each system safety function including field devices.

A GMR Fire & Gas System can accommodate maintenance actions as described below.

Sensor Maintenance

The system must allow isolating and inhibiting of the input signal. It should be possible to remove inhibits on critical inputs upon operator command.

Input Unit Maintenance

GMR adapts input voting of a redundant input group if a block in the group is removed or powered down. Make sure that removing an input unit does not cause undesired outputs to change state due to pre-existing discrepancies (check PLC I/O tables and system logic). Also make sure that removing an input unit does not cause an unexpected output trip as a consequence of an I/O shutdown (check no pending I/O shutdown and temporarily disable autotest).

After analyzing the effect of the removal of an input unit, bypass any critical outputs that are expected to change state. It should be possible to manually activate critical outputs that are inhibited by the removal of the unit.

Check that input units can be de-powered and removed without electrically affecting the other redundant channels. Take care to include the effects of power being fed through the field device. The GMR termination input boards provide the necessary de-coupling.

The GMR system adapts the input voting to ignore an input unit that has been removed from a voted input group, so the system can still respond to a genuine plant alarm condition.

Restoring an input unit may require system Reset and/or Force Logon before the unit can resume normal operation.

Logic Unit Maintenance

GE Fanuc recommends isolating power before removing modules. Take care to consider the effects and bypass any outputs that are expected to change state where this is undesired. The output block will adapt its voting to ignore a logic unit that is stopped or powered down.

Note that for Fire & Gas Systems, Simplex CPU Shutdown would normally be disabled.

GMR configuration changes can only be performed with the system stopped. Program changes can be performed with the system operational. However great care must be taken to ensure that there are no unexpected output actions.

Online program changes are possible if there is enough free memory for the CPU to load the revised program software and then switch over. It is important to be sure that all application logic states are correctly initialized by the application. In accordance with the guidance of IEC61508 *Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems*, development of program changes with a live system is possible but is not advised for anything beyond minor changes.

When re-starting a PLC, the log-on control feature is intended to prevent unexpected changes in block outputs arising for including the newly-initialized CPU in the block vote. Before forcing a log-on, check for and resolve any latent discrepancies that could cause block outputs to change state as a consequence of enabling the CPU in the block voting.

Output Unit Maintenance

GE Fanuc recommends isolating output block power before removing modules. Take care to consider the effect of removing output modules. Bypass energized outputs that would otherwise experience an undesired change of state.

For the redundant H-block and I-block output groups, check that the correct block is to be removed and that the remaining units can correctly control the load. If in doubt, set the outputs to a designated state using the bypass/inhibit facilities.

Output bypass/inhibit is required for I-block maintenance to prevent spurious tripping of energized outputs during block removal.

Actuator Maintenance

For manual proof-testing of the output device, lamps should be illuminated, audible alarms sounded, and mechanical acting devices set to travel and return to the rest position.

Appendix A Reliability Data

Calculation of system reliability and availability as well as safety function PFD and spurious trip rates requires module specific reliability data. GE Fanuc has a well-established procedure for determining module reliability data. This data is available on request from GE Fanuc.

GE Fanuc calculates failure rate based on modules returned in warranty. Factory tests are performed on returned modules. The results place returned modules in one of three categories:

- No Defect
- Customer Induced Failure
- Proven Product Failure

Only proven product failures are included in the failure rate calculation. Modules not tested are assumed to have the same ratio of proven defects as those for which test results are available.

Calculation of the number of in-warranty operating hours for a given module type is based on a model that predicts the fraction of shipped modules operating as a function of the number of months since the module was shipped.

The model was developed through field experience and makes the following assumptions:

- 90% of total months shipments are used
  - 5% of shipments cover warranty returns
  - 5% of shipments never go into use (User stock, etc)
- 693 hours per operation month (95% of time)
- Processes
  - CPU/Memory continuous cycling
  - I/O holding or cycling

MTBF calculations are based on one year (12 months) accumulated run hours and warranty returns for a corresponding 12-month period. To gain statistical validity, each module type must have accumulated a minimum of 500,000 run hours during this 12-month period before a reliable prediction will be made. MTBF and reliability are not calculated for modules with less than 500k run hours.

Appendix B PFD Calculations

The following assumptions have been used for the basis of calculating the Probability to Fail on Demand as determined in *IEC61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems*.

To avoid excessive number of configurations, the PFD calculations have been made by computing individual sub-system PFD based on the worst case channel/path reliability figures within the sub-system for the specified configuration. By combining the PFD results of these sub-systems, the PFD of a safety function can be computed.

Standard Parameters

Parameter	Value	Comment
Proof Test Period, T_1	6 months	Industry accepted value
Mean Time To Repair, MTTR	8 hours	Repair within shift
Diagnostic Coverage, DC	90%	All GE Fanuc units incorporate extensive internal diagnostic.
Fraction of failures with common cause, β	1%	Common cause design failures have been minimized through mature design and long service combined with a high degree of segregation between paths and modules.
Average probability of failure per hour, λ	Module Specific	Contact GE Fanuc for module reliability data
Probability of dangerous failure per hour, λ_D	see calculation	Value depends on Architecture
Probability of undetected dangerous failure per hour, λ_{DU}	see calculation	Value depends on Architecture
Probability of detected dangerous failure per hour, λ_{DD}	see calculation	Value depends on Architecture
Device equivalent mean down time, t_{DE}	see calculation	Value depends on Architecture
System equivalent mean down time, t_{SE}	see calculation	Value depends on Architecture
Average probability of failure on demand, PFD_{AVG}	see calculation	Value depends on Architecture

The formulas for calculating the PFD for various architectures have been taken or are based on those in IEC61508 as follows;

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2} \qquad \lambda_{DU} = \frac{\lambda}{2}(1-DC) \qquad \lambda_{DD} = \frac{\lambda}{2}DC$$

PFD Formula 1oo1

$$t_{DE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$\underline{PFD_{AVG} = (\lambda_{DD} + \lambda_{DU})t_{DE}}$$

PFD Formula 1oo2

$$t_{DE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$t_{SE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$\underline{PFD_{AVG} = 2\left((1-2\beta)\lambda_{DD} + (1-2\beta)\lambda_{DU}\right)^2 t_{DE} t_{SE} + \beta\lambda_{DD} MTTR + 2\beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)}$$

PFD Formula 2oo2

$$t_{DE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$\underline{PFD_{AVG} = 2\lambda_D t_{DE}}$$

PFD Formula 1oo2d

$$t_{DE}' = \frac{\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SU}}$$

$$t_{DE}' = \frac{\lambda_{DU}\left(\frac{T_1}{3} + MTTR\right) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}$$

$$\underline{PFD_{AVG} = 2(1-2\beta)\lambda_{DU}\left((1-2\beta)\lambda_{DU} + (1-\beta)\lambda_{DD} + \lambda_{SD}\right)t_{DE}' t_{SE}' + \beta\lambda_{DD} MTTR + 2\beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)}$$

PFD Formula 2oo3

$$t_{DE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$t_{SE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$PFD_{AVG} = 2(1-2\beta)\lambda_{DU}\left((1-2\beta)\lambda_{DU} + (1-\beta)\lambda_{DD} + \lambda_{SD}\right)t_{DE}\,'t_{SE}\,' + \beta\lambda_{DD} MTTR + 2\beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$$

Genius Input PFD

The worst case PFD for various Genius input configurations per channel are shown below. The calculations assume the probability of failure of the I/O power supply is at least a magnitude better than path for the arrangement under consideration.

Configuration	PFD (Per Channel)	Comment
Simplex	6.81×10^{-05}	
Duplex (1oo2d)	1.34×10^{-06}	
Duplex (1oo2)	1.35×10^{-06}	
Triplex	1.36×10^{-06}	

Series 90-70 Logic Unit PFD

The worst case PFD for Series 90-70 Logic Units are shown below. The calculations assume that only 10% of rack PSU failures are “fail to danger”.

Configuration	PFD (Per Path)	Comment
Simplex	7.11×10^{-04}	Configuration is 9 Slot Rack, PSU, CPU and Simplex GBC. Voting occurs in output block
SimplexD	8.24×10^{-04}	Configuration is 9 Slot Rack, PSU, CPU and Duplex GBC. Voting occurs in output block
Duplex (1oo2d)	1.63×10^{-05}	Configuration is 9 Slot Rack, PSU, CPU and Duplex GBC. Voting occurs in output block
Duplex (1oo2)	1.71×10^{-05}	Configuration is 9 Slot Rack, PSU, CPU and Duplex GBC. Voting occurs in output block
Triplex	2.19×10^{-05}	Configuration is 9 Slot Rack, PSU, CPU and Triplex GBC. Voting occurs in output block

Genius Output PFD

The worst case PFD for various Genius output groups are shown below. The calculations assume the probability of failure of the I/O power supply is at least a magnitude better than path for the arrangement under consideration.

Configuration	PFD (per channel)	Comment
Simplex	6.81×10^{-05}	
I-Block/1oo1d	1.34×10^{-06}	Calculated per 1oo2
H-Block/1oo2d	1.35×10^{-06}	Calculated per 1oo2d

PFD Summary

The following table provides a range of typical Fire and Gas subsystem configurations and indicates the worst-case safety function PFD for each of these subsystems for the electronic control system only. It is intended to provide a quick-check/cross-reference for system designers.

Note that only the Logic Unit PFD is additive to the total PFD of each safety function under consideration. The input and output PFD has to be re-calculated including the field devices and associated control modules/barriers with due consideration for environmental factors.

Genius Input		90-70 Logic Unit		Genius Output	
Configuration	PFD	Configuration	PFD	Configuration	PFD
Simplex	6.81×10^{-05}	Simplex	7.11×10^{-04}	Simplex	6.81×10^{-05}
Simplex	6.81×10^{-05}	Duplex (1oo2)	1.63×10^{-05}	Simplex	6.81×10^{-05}
Simplex	6.81×10^{-05}	Duplex (1oo2d)	1.71×10^{-05}	Simplex	6.81×10^{-05}
Simplex	6.81×10^{-05}	Triplex (2oo3)	2.19×10^{-05}	Simplex	6.81×10^{-05}
Simplex	6.81×10^{-05}	SimplexD	8.24×10^{-04}	I-Block/1oo1d	1.34×10^{-06}
Duplex (1oo2d)	1.34×10^{-06}	SimplexD	8.24×10^{-04}	I-Block/1oo1d	1.34×10^{-06}
Duplex (1oo2d)	1.34×10^{-06}	Duplex (1oo2d)	1.63×10^{-05}	I-Block/1oo1d	1.34×10^{-06}
Duplex (1oo2d)	1.34×10^{-06}	Duplex (1oo2d)	1.63×10^{-05}	H-block/1oo2d	1.35×10^{-06}
Simplex	6.81×10^{-05}	SimplexD	8.24×10^{-04}	I-Block/1oo1d	1.34×10^{-06}
Duplex (1oo2)	1.35×10^{-06}	SimplexD	8.24×10^{-04}	I-Block/1oo1d	1.34×10^{-06}
Duplex (1oo2)	1.35×10^{-06}	Duplex (1oo2)	1.71×10^{-05}	I-Block/1oo1d	1.34×10^{-06}
Duplex (1oo2)	1.35×10^{-06}	Duplex (1oo2)	1.71×10^{-05}	H-Block/1oo2d	1.35×10^{-06}
Triplex (2oo3)	1.36×10^{-06}	Triplex (2oo3)	2.19×10^{-05}	I-Block/1oo1d	1.34×10^{-06}
Triplex (2oo3)	1.36×10^{-06}	Triplex (2oo3)	2.19×10^{-05}	H-Block/1oo2d	1.35×10^{-06}

Appendix C An Example System

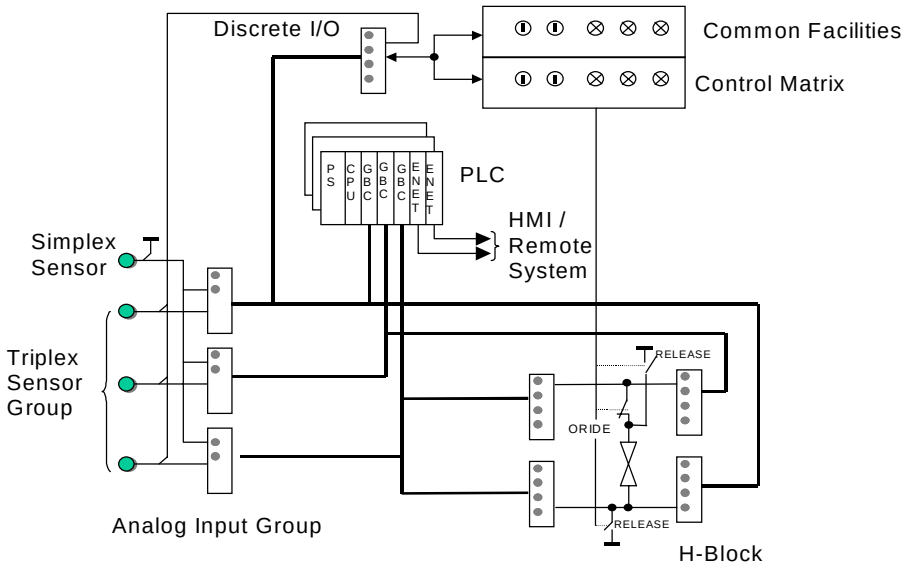
This section describes a simple example of a Fire and Gas System to illustrate how the GMR system can be applied. The example includes:

- Single Heat sensor with system inhibit
- 2oo3 voting Smoke sensor group with system inhibit and detector reset
- Triplex Processors
- H-Block/1oo2d Extinguishant Output with manual overrides/release
- Matrix Indications
- Common Facilities
- Interface to HMI and/or Remote System

The example does not cover the wider aspects of engineering a Fire and Gas System such as evaluating the system safety functions and SIL level(s) required to meet the safety functions. Information about the principles and methodologies is contained in IEC61508. Other sections of this document provide information needed to determine the required system architecture for a given application.

It is further to be noted that to meet a given SIL rating, in accordance with IEC61508, requires detailed evaluation of the complete lifecycle of the system, as described in IEC61508, from conception through to de-commissioning and covering all aspects of design, operation and maintenance.

Example F&G System Block Diagram

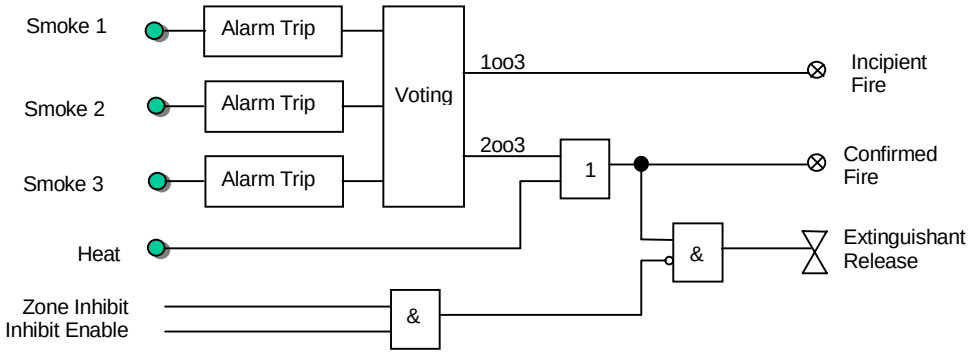


Application Logic

The example F&G system illustrates the basics of a simple F&G system implemented using GMR. The application logic is correspondingly simple and is shown in the figure below.

The application comprises a single fire zone with a heat detector, 3 smoke detectors and extinguishant system. The extinguishant is released if any 2 smoke detectors are tripped or the heat detector is tripped. Facilities are to be provided for manual release of the extinguishant together with warnings if any single smoke has tripped.

Example F&G System Application Logic



Redundancy

This example illustrates the ability of GMR to optimize the degree of I/O redundancy.

The example Fire & Gas application is an extension to an existing triplicated Emergency Shutdown system that features triplicated processors. For most F&G applications, duplex processors are adequate to meet the system PFD requirements.

The heat sensor, a high reliability device, is not redundant. To meet the system PFD requirements, the example uses triplicated input units.

The smoke sensors provide smoke detection in a single area forming a redundant sensor group. In this case only a single input unit is required to interface each detector to meet the PFD.

The example output configuration is the H-block/1oo2d form. It conveniently provides external (manual) override and release capabilities. For most normal F&G system outputs, no output redundancy is required, however the GMR system provides the I-block/1oo1d as an alternatives to the H-block.

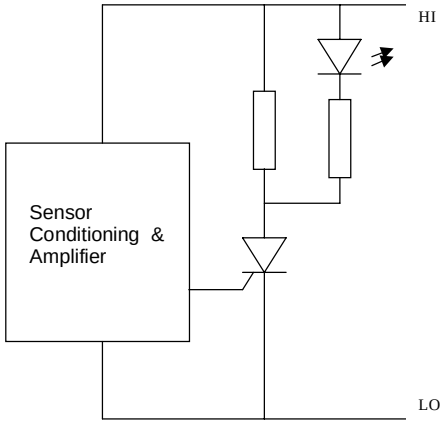
Input Configurations

The example Fire & Gas application requires full line monitoring for open and short circuit faults on input devices. The sensors used are two-state devices, i.e. normal and alarm. Because Genius 16 point tri-state input blocks can only detect one of these faults at a time, the example instead uses analog inputs to interface to the sensors.

Thus the input signals to the GMR system are analog, not discrete. Because the GMR software provides signal voting but not alarm level processing, that function must be included in the application program logic.

To illustrate interfacing discrete sensors consider a convention ionization smoke detector. A simplified equivalent circuit of a smoke detector is shown below.

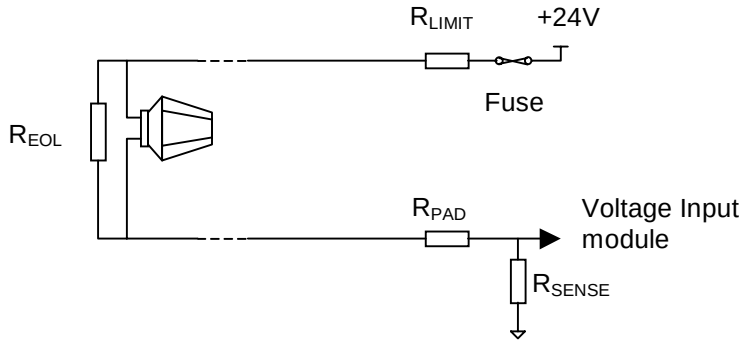
Typical Smoke Detector Equivalent Circuit



These sensors generally require a minimum operating voltage of 18V. To operate a remote indicating LED requires a source impedance capable of delivering 20mA or more. The detector draws about 50µA in the non-alarm state and will sink 60mA with a standoff voltage of 6V in the alarm state. Several detectors can be placed on a single input loop for greater coverage, however, there will be a loss of discrimination.

Typical NON-I.S. Smoke Detector Loop Analog Interface

To interface this detector to the system using analog interface requires that four discrete signal bands be defined corresponding to open circuit, normal, alarm and short circuit. This can easily be accomplished using resistors.



The elements of this interface are:

- R_{LIMIT} : sets the short circuit current/limits input voltage for the loop
- FUSE : sets the short circuit current for the loop
- R_{EOL}: sets the normal loop current
- R_{PAD}: sets the short circuit current/limits input voltage
- R_{SENSE}: current sensing resistor/sets the short circuit current

With the detector in the quiescent state, the combination of R_{EOL} , R_{PAD} and R_{SENSE} resistors sets the "normal" loop current. A typical normal loop current is 4mA. There must also be sufficient operating voltage for the detector, typically 18v minimum. With the detector tripped, the loop current rises as determined by the combination of $V_{DET\ ALM}$, R_{LIMIT}, R_{PAD} and R_{SENSE} . A typical loop current with the detector in the alarm state is 25mA.

An open circuit or ground short will cause the input current seen at the system input to drop to zero. A line-to-line short will either cause the input current to rise the maximum set by the resistor or if this exceeds the fuse rating, zero.

The example uses a 6 channel analog input block (IC697BBA020). The R_{LIM} was 560Ohms and R_{SENSE} was 250Ohms, R_{PAD} and FUSE were not used. In this example for a 24VDC supply rail, the maximum loop current is 29mA and the maximum input voltage is 7.4V. For the heat detector interface the internal current sense resistor was not connected and an single external resistor used. For the smoke detector the internal 250 Ohms sense resistor was used.

The input range for all channels was selected to be 0-10V. The scaling factor of the channels was set to 0..3071 corresponding to 0..30000. The effect of which is to give an output reading in µA. The Genius block signal fault detection was disabled as this is being handled by the application logic.

F&G circuits often need explosion hazards protection, the most common form of which uses Intrinsic Safety techniques. Barriers have a safety description that defines the maximum voltage and current that can be delivered to the field. A typical barrier safety description for a smoke detector would be 28V and 93mA. The input signal in this example is ground referred, so it would be necessary to use either a dual zener barrier or an isolation barrier.

Smoke detectors latch in the alarm state until power is removed. Therefore some means of removing power is required. In this example, a single output of the common facilities discrete I/O block has been used to remove power to the smoke detector under operator control. In a real application, this function should also have some form of redundancy. While power is removed, the loop current drops to zero. This situation must be handled by the application to avoid erroneous fault reports.

When interfacing two-state detectors, it is important to ensure that alarms and faults are correctly reported. This requires adequate analog signal and timing margins. For example, a short circuit fault causes the input signal to traverse the alarm region, so it is important that there be proper discrimination between stable and transient states.

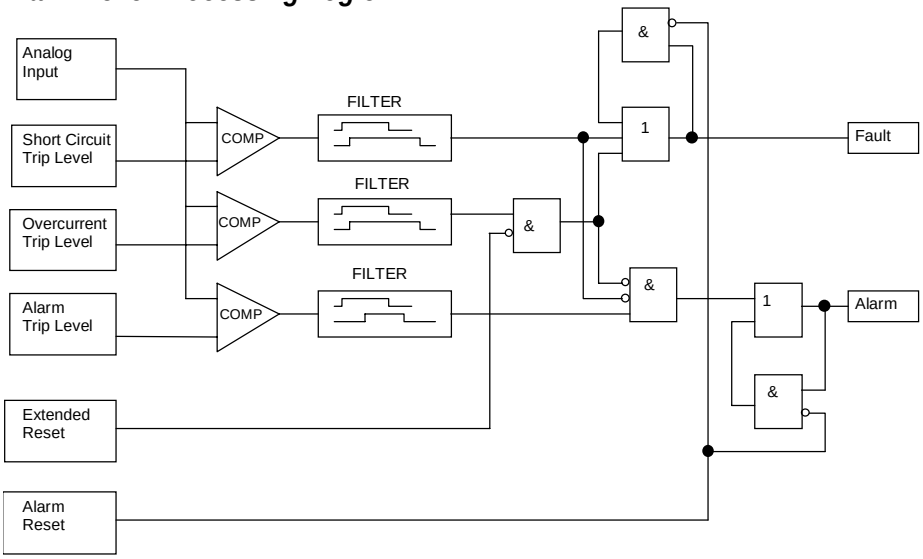
In this example the heat sensor is subject to voting by GMR as a standard triplex analog input group. The voted result is then subjected to the alarm logic processing.

Although the smoke sensors are a triplex group, their inputs are individual signals that are not GMR-voted. The analog input signals are directly processed by the alarm processing logic. Because these signals have been wired on the same blocks as the heat sensor signals in this example, GMR performs a vote on the smoke signals. However, this data is not used in the application. A side effect of this voting is that it would generate apparent voting discrepancies based on time differences in detecting a smoke hazard. This would cause unnecessary fault table messages. This can be avoided by setting the discrepancy thresholds for a channel to the limits of the input range.

In summary the issues for interfacing a F&G detector are:

- Loop operating current and voltages
- Explosion Hazards Protection
- Fault v. Alarm signal detection margins
- Fault v. Alarm timing detection margins
- Resetting of latching detectors.
- GMR/Application Voting

Alarm Level Processing Logic



The block compares each analog input to fixed thresholds for open circuit, alarm and short circuit. The output of these comparisons is filtered with the open circuit and short circuit filters having a shorter leading time constant and longer falling time constant than the alarm filter. This difference provides the discrimination to allow transition between states.

The output signals are latched in a resettable seal circuit. These latches give priority to the set term, the reset timing ensures that the logic stabilizes after power has been removed, before an attempt is made to reset the latches.

Common Facilities

The example uses a common facilities panel to monitor the status of the Fire and Gas hazards as well as the GMR system operation. This type of panel is normally located in one of the equipment cabinets. The common facilities panel gives operators/maintenance staff a range of indications, via LED's, such as alarm and fault status. In the example system the panel is controlled by a non-voted Genius I/O block.

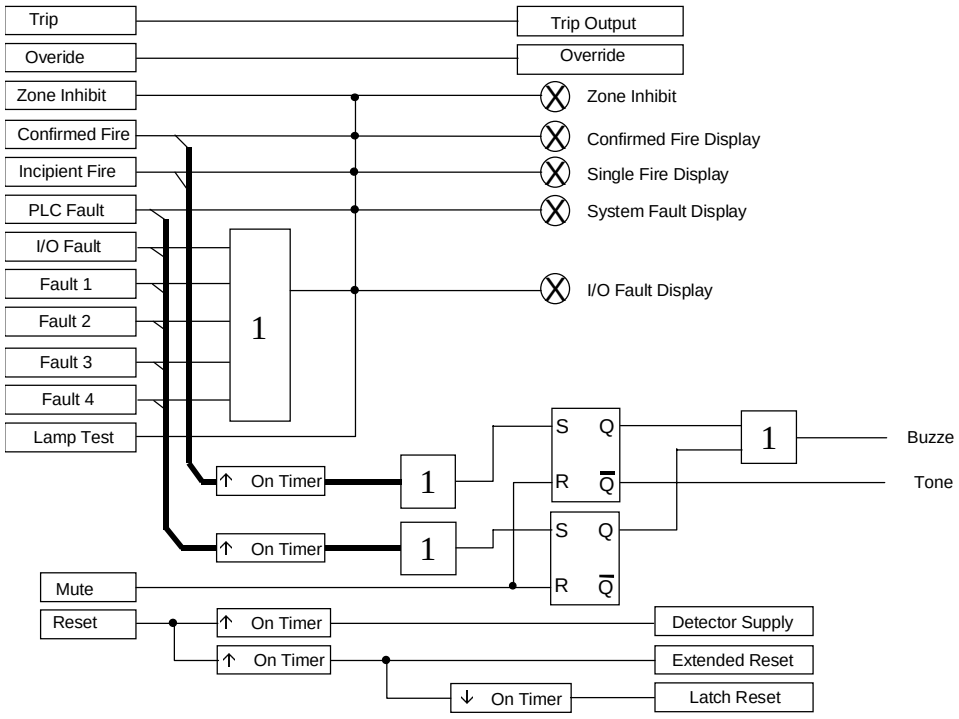
The common facilities matrix implements the following operator functions:

Description	Function	I/O Type	Comment
Single Fire LED	F&G	O/P	Indicates one of the three smoke detectors tripped in zone
Confirmed Fire LED	F&G	O/P	Indicates any two smoke or heat tripped in zone
Zone Inhibit LED	F&G	O/P	Illuminated when valid Zone Inhibit present
Zone Inhibit S/W	F&G	I/P	When enabled (see Zone Inhibit Enable) prevents automatic release of extinguishant. Does not affect incipient/confirmed fire indications
Zone Inhibit Enable S/W	F&G	I/P	Enables Zone inhibit switch
Manual Override	F&G	I/P	Is used to prevent an output device from activating (i.e. for maintenance of the device). Its operation is independent of the GMR system. The status of this switch is monitored by the GMR system for autotest reporting purposes.
Manual Release	F&G	I/P	Is used to force an output device to activate. Its operation is independent of the GMR system and has priority over manual override. The status of this switch is monitored by the GMR system for autotest reporting purposes.
System fault LED	CF	O/P	Indicates entry in PLC fault table entry
I/O fault LED	CF	O/P	Indicates field fault or I/O fault table entry
Buzzer	CF	O/P	Activates two tone sounder.
Tone	CF	O/P	Two tone sounder. High tone has priority and indicates single/confirmed fire, low tone indicates system or I/O fault.
Reset P/B	CF	I/P	Resets latching detectors and attempts to clear input fault and alarm latches. During this time system outputs do not change until it is certain that there are no standing alarms. This ensures that devices activated by the alarm condition are not turned off then back on again
Mute P/B	CF	I/P	Silences audible

In addition the common facilities implements the control logic to handle resetting the detector (i.e. Detector Reset) and alarm level processing logic (i.e. Extended Reset and Latch Reset).

Common Facilities Logic

The common facilities logic is shown below.



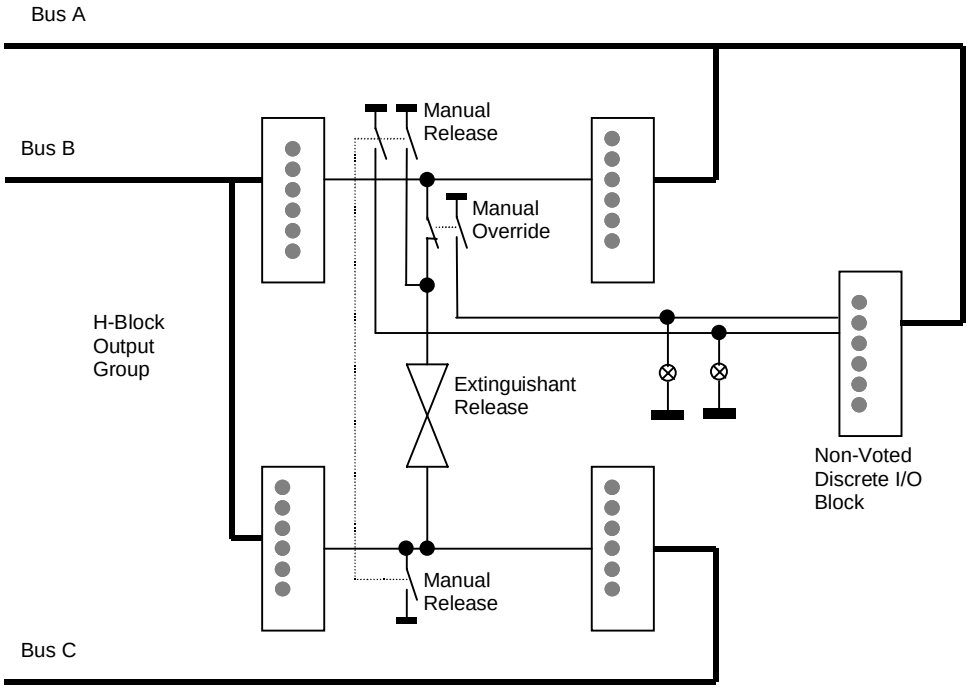
HMI/Remote System Interface

Optionally, Series 90-70 PLC Ethernet Modules could be used to facilitate the interface to an HMI system, e.g. CIMPLICITY® HMI or a remote system, e.g. DCS system. Alternatives for remote system interfacing include Genius Bus and other GE Fanuc Series 90-70 communication modules.

Output Configuration

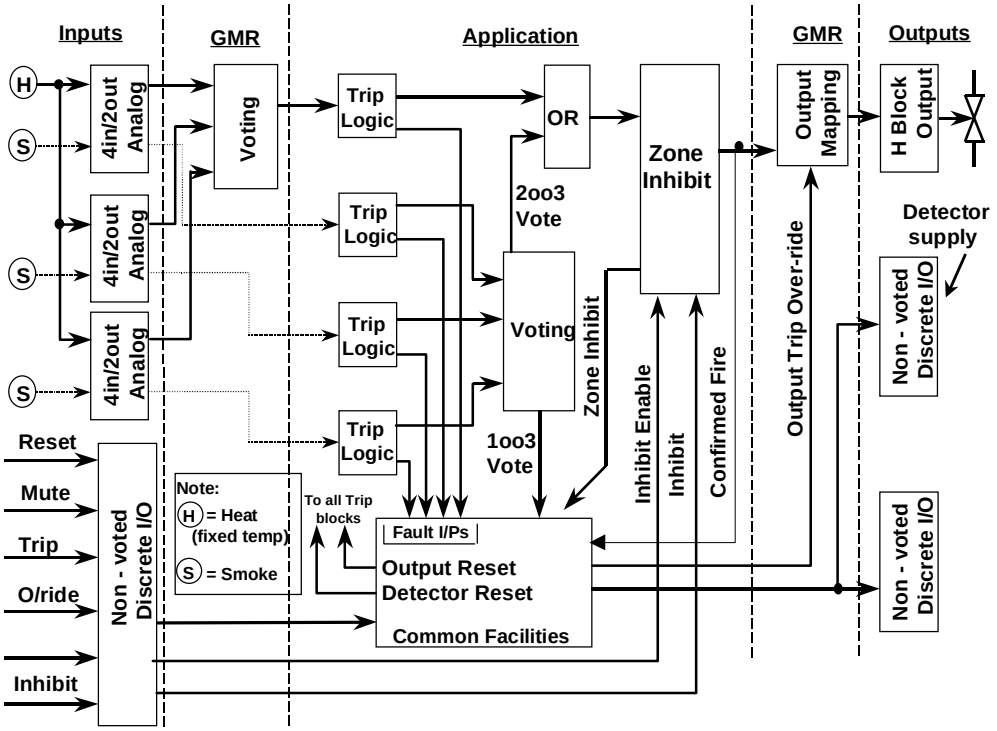
The extinguishant output for the example application is implemented using an H-block output group. This allows manual override and/or manual release of the extinguishant output. Independent indications are provided for these switches, at the same time the individual signals are input to the GMR system via a non-voted discrete I/O block. These inputs are used to prevent autotest faults from being reporting on this output when either of these controls are activated.

Extinguishant Output



System Logic

The complete system logic includes the application logic and the common facilities/matrix logic for the system. The following figure gives the simplified block diagram.



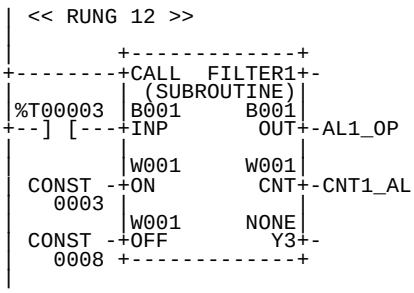
Silvertech has many years of experience in designing Fire and Gas applications using GMR and other GE Fanuc PLC's. This knowledge has been captured in a library of software Function Blocks for Fire and Gas, ESD and other safety related systems and process control systems. Contact Silvertech International for further information.

Ladder Listing

Ladder Logic for the Alarm Processing Logic

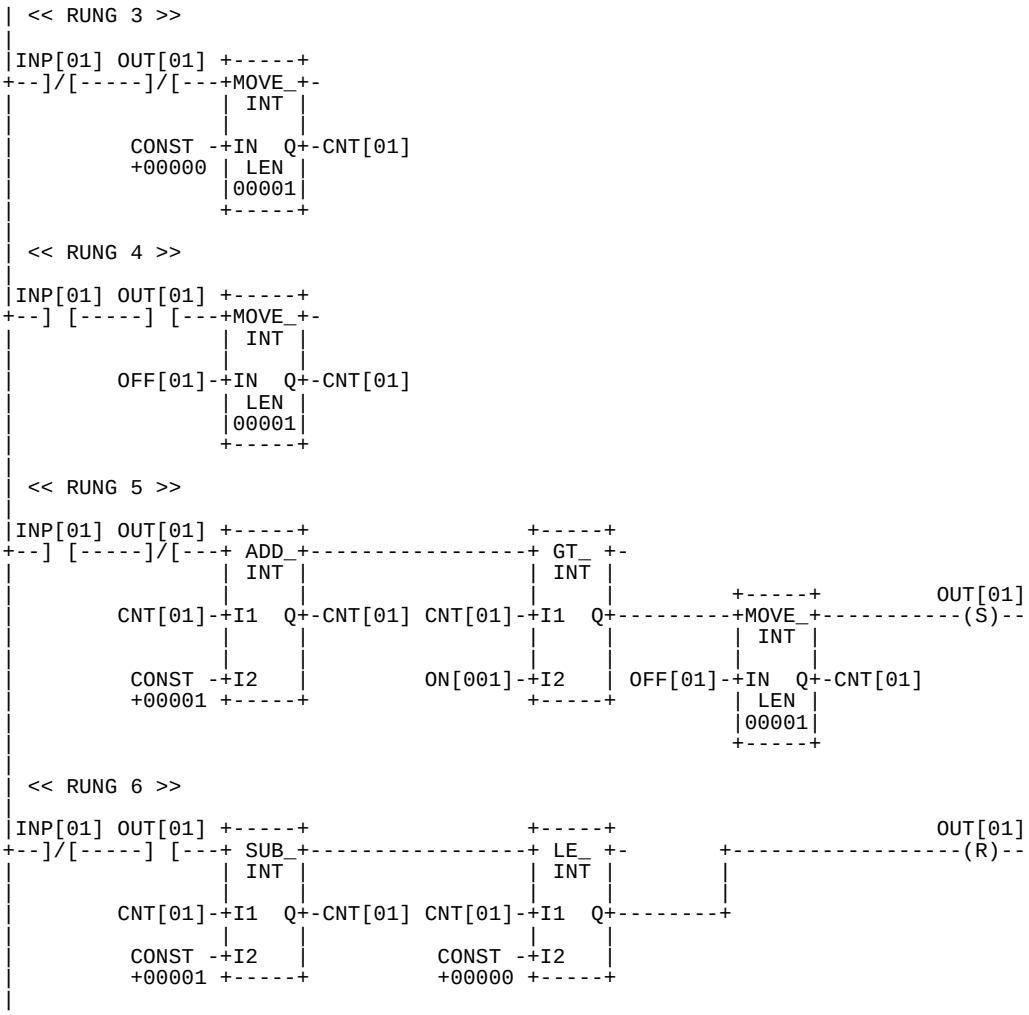
In the example logic below, rungs 7, 9, and 11 are the comparators for short circuit, open circuit, and alarm conditions respectively. In each case, the filter block is called to perform the operations described in the filter logic pseudo-code. (in this case, Analog 1 is the Heat Detector).

```
|  << RUNG 7 >>
|
|          +-----+
+---------+ GT_ +-
|          | INT |
|          |     |                                                          %T00001
|ANALOG1--+I1  Q+-----------------------------------------------------------( )--
|          |     |
|  CONST --+I2   |
|  +28000 +-----+
|
|  << RUNG 8 >>
|
|          +-------------+
+---------+CALL  FILTER1+-
|          | (SUBROUTINE)|
|%T00001  |B001     B001|
+--] [----+INP       OUT+-SC1_OP
|          |             |
|          |W001     W001|
|  CONST --+ON         CNT+-CNT1_SC
|    0003  |             |
|          |W001     NONE|
|  CONST --+OFF         Y3+-
|    0008 +-------------+
|
|  << RUNG 9 >>
|
|          +-----+
+---------+ LT_ +-
|          | INT |
|          |     |                                                          %T00002
|ANALOG1--+I1  Q+-----------------------------------------------------------( )--
|          |     |
|  CONST --+I2   |
|  +02000 +-----+
|
|  << RUNG 10 >>
|
|          +-------------+
+---------+CALL  FILTER1+-
|          | (SUBROUTINE)|
|%T00002  |B001     B001|
+--] [----+INP       OUT+-OC1_OP
|          |             |
|          |W001     W001|
|  CONST --+ON         CNT+-CNT1_OC
|    0003  |             |
|          |W001     NONE|
|  CONST --+OFF         Y3+-
|    0008 +-------------+
|
|  << RUNG 11 >>
|
|          +-----+
+---------+ GT_ +-
|          | INT |
|          |     |                                                          %T00003
|ANALOG1--+I1  Q+-----------------------------------------------------------( )--
|          |     |
|  CONST --+I2   |
|  +15000 +-----+
|
```



Ladder Logic from the Example Filter Block

The logic from the filter block is shown below.



Appendix D TUV Guidance for Fire and Gas Systems

This section describes the changes to the GMR Configuration Utility from those described in GFK-1277B and TÜV conditions relevant to Fire and Gas applications.

A list of the certified components for use in GMR systems is maintained by GE Fanuc, and regularly verified by TÜV in the TÜV Change Log. It is available online at www.gefanuc.com.

Configuration Utility

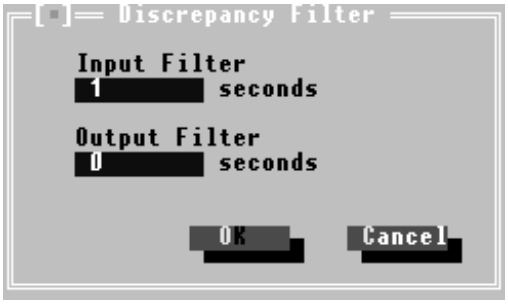
Version 7.01 of the configuration utility introduces a new configuration option from that described in GFK-1277B for output discrepancy filtering.

Configuration Update

Configurations created with previous versions of the configuration utility should be imported into the latest version and saved to a new file. The configuration should then be carefully checked to confirm that all settings are identical to the original version and where new configuration options have been introduced, the default settings are appropriate for the application.

Output Discrepancy Filter

The output discrepancy filter is found under [S]ystem, [D]iscrepancy Filter. The dialog box is shown below.



The output discrepancy filter can be set to increase the time interval needed to detect an output discrepancy. This time defaults to 0 seconds.

Configuration Settings for Fire and Gas

The following specific settings are recommended for Fire and Gas applications.

- The normal state for redundant outputs must be set to OFF (check box clear) for normally de-energized outputs,

TÜV Guidance for Fire and Gas Systems

The following guidance from TÜV should be observed when applying GMR to Fire and Gas Systems in addition to that provided in Appendix A of GFK-1277B.

System

Fire & Gas application CPU simplex shutdown should be disabled for 3-2-1-0 operation.

For safety relevant applications a safe state must exist (e.g. de-energized for ESD systems) or the demand to trip must be defined.

If a simplex redundancy system configuration is used for applications requiring SIL2 performance then additional measures must be specified and implemented to maintain the safe state during the time that it takes to restore the system to normal operation. Due to this requirement a simplex redundancy system can only be used with applications having a high process safety time.

Inputs

16 channel blocks configured for tri-state operation can be used for discrete inputs that require line monitoring and/or earth fault detection. Operation of the inputs is as follows;

BLOCK	FAULT	GMR MODE (normally on)	NON-GMR MODE (normally off)
Source	Open Wire	Off	Fault
Source	Shorted Wire	Fault	On
Source	Ground Short	Off†	Fault
Sink	Open Wire	Off	Fault
Sink	Shorted Wire	Fault	On
Sink	Ground Short	Fault	On

† Assumes a ground short to positive line interrupts power flow to the field

Additionally, or alternatively, other special measures may be applied for the detection of earth faults by for example an earth leakage detection unit. The system ground should be connected to earth unless otherwise required by the earth leakage measure.

If line monitoring is not used and no other special measures are applied then field wiring must be checked within or during the proof test.

The test interval for analog inputs as described in Appendix A of GFK-1227A shall be aligned with the proof test.

For each discrete input used with a safety related function, the vote adapt mode (i.e. 3-2-0 or 3-2-1-0), duplex default (i.e. 0 or 1) and default state (i.e. 0 or 1) must be set according to the safe state.

For each analog input used with a safety related function, the vote adapt mode (i.e. 3-2-0 or 3-2-1-0), duplex default (i.e. high, low or average) and default state (i.e. min, max or hold) must be set according to the safe state or demand state respectively.

Outputs

For discrete output groups, the normal state must be set to:-

- ON for outputs with a de-energized safe state
- OFF for outputs with an energized safe state

Critical normally de-energized outputs should be located on 16 point H-block with no load reporting enabled. Output loads that fall below the minimum required 100mA load current should include an additional resistive load in the field to fulfill the minimum load requirement.

Definitions

Fire & Gas System

These types of safety systems are defined as low demand mode of operation in IEC61508. TÜV's inspection of GMR for use in Fire and Gas System application was made on this basis.

1oo1d/1oo2d

TÜV have carefully assessed the I-block and H-block configurations, and, confirmed these correspond to the industry designations of 1oo1d and 1oo2d, respectively on an individual channel basis.

Simplex D Processor

The designation Simplex D Processor describes a single CPU with dual GBCs providing two paths to shutdown the output via either an I-block/1oo1D or H-block/1oo2D.

P

R

S

T