

# Specification and Technical Data for Safety Manager R120

FS75-120  
10/2007



*The Next-Generation Safety Management System*

**Honeywell**

# Table of Contents

<b>Introduction</b> .....	<b>4</b>
Improves business results .....	4
Built on QMR technology .....	4
Benefits .....	5
Compliance to safety standards.....	5
Engineering environment .....	6
Process availability .....	6
Operation and maintenance performance .....	6
System reliability and robustness .....	7
<b>Safety Solutions</b> .....	<b>8</b>
Integration into Experion PKS .....	8
PlantScape Integration.....	9
Serial Communication with Process Computer Systems .....	9
Fire and Gas Safety Solution.....	10
<b>Functional Description</b> .....	<b>11</b>
Basic architecture.....	11
Safety vs. availability.....	12
Redundancy and availability .....	12
IO configurations.....	13
Multiple-Sensor and Transmitter Configurations .....	14
Fault detection and response .....	15
Principle of fault detection .....	17
Principle of fault response .....	18
Watchdog and redundancy .....	20
Peer to peer connections.....	21
Human Machine Interfaces .....	22
<b>System Features</b> .....	<b>27</b>
Safety Manager System Configurations .....	27
Safety Manager basic architectures .....	27
Network architecture .....	35
Safety Builder .....	39
Functional Logic Diagrams (FLDs).....	40
Multi User: Concurrent use of Safety Builder.....	43
Multi Site .....	44
Safety Manager Diagnostics.....	47
Flash-Memory Operation .....	47
On-Line Modification .....	48
Hot-swap of Safety Manager Controller Modules.....	48
Self Educating Safety Manager Controller Modules.....	48
Power System.....	48
Write Protection .....	49
IO Signal Forcing.....	49
Serial Communication with Process Computer Systems.....	49
Safety Manager SafeNet.....	50



Figure 1 — Safety Manager

**Physical Characteristics** ..... 52  
SM controller components ..... 52  
Controller chassis ..... 53  
Control Processor ..... 53  
Battery & Key switch Module (BKM) ..... 55  
SM IO components ..... 56  
Field interface ..... 59

**Safety Services** ..... 61  
System services ..... 61  
Training ..... 61  
Safety Consultancy ..... 62

**Standards Compliance** ..... 63

**Specifications** ..... 64

**Model Numbers** ..... 65  
Identification ..... 65  
Controller Modules ..... 65  
Analog Modules ..... 66  
Digital Modules ..... 67



## Introduction

The Honeywell Safety Manager™ is a highly reliable, high-integrity safety system for safety-critical control applications. As part of Honeywell's Experion™ PKS, integrated into PlantScape, or in stand-alone applications, Safety Manager forms the basis for *functional safety*, thus providing protection of persons, plant equipment, and the environment, combined with optimum availability for continuous plant operation.

Safety Manager is a user-programmable, modular, microprocessor-based safety system, which can perform a wide range of high-integrity process control and safety instrumented functions, including:

- High-integrity process control,
- Burner/boiler management systems,
- Process safeguarding and emergency shutdown,
- Turbine and compressor safeguarding,
- Fire and gas detection systems, and
- Pipeline monitoring.

## Improves business results

Safety Manager™ is the natural evolution of the current proven in use Fail Safe Controller (FSC®) safety system platform, which has gained global acceptance for more than 15 years. It embeds proven technology with two decades of Honeywell process safety management expertise in integrating process safety data, applications, system diagnostics and critical control strategies.

Safety Manager is designed to improve a company's business results by fundamentally enhancing process safety and protecting plant assets and people. Through tight integration with Experion™ Process Knowledge System (PKS), safety systems are unified into one single safety system architecture, assuring a unique opportunity to improve both safety and availability of processes.

Experion PKS provides unprecedented connectivity through all levels of process and business operations and optimizes work processes, improves routine maintenance efficiencies, enhances safety management, and releases personnel from manual processes.

## Built on QMR technology

Safety Manager™ is based on the unique and field proven Quadruple Modular Redundant (QMR™) diagnostic based technology with a 2oo4D architecture. QMR enhances system flexibility, increases diagnostic messaging capabilities and improves system fault tolerance for critical applications. It enables the handling of *multiple* system faults within Safety Manager, matching the needs of critical control applications.

Additionally Safety Manager provides the basis for integrating SIL (safety integrity level) rated sensors and valve actuators in the field ensuring that your safety instrumented functions are well in place to protect complex and hazardous processes. Whether it is integrating SIL1-2 safety transmitters (ST3000 and STT250) or safety valve positioners for improved safety and field

asset management, Safety Manager is the ideal enabler for your Safety Instrumented Systems (SIS).

## Benefits

- Improved engineering and design efficiency – designing safety networks has never been easier
- Improved system reliability and robustness – through rigorous Design for Six Sigma (DFSS) process and the IEC 61508 development criteria
- Improved process availability – applying the proven-in-use QMR technology allows uninterrupted process operation in case of any system degradation
- Improved operation and maintenance performance – through unification of critical process data and information with the process control information, allowing single window access for operation and maintenance
- Protection of investments – Safety Manager™ allows and supports migration of FSC to the latest QMR safety technology
- Compliance to safety standards – with all SIL3 safety compliance tools, hardware and software, Safety Manager provides excellent protection for safety applications across multiple industries throughout the lifetime of an installation.

## Compliance to safety standards

A major requirement for compliance to IEC 61508 is the availability of a change history of applications. With the new Safety Builder this is no longer an issue as the Safety Audit Tracker provides an automatically enabled audit trail. It will keep track of all the changes performed on an application automatically. Difficult procedures or extensive loggings are not required. The Safety Audit Tracker, together with the Application Verification Tool, is all that is necessary.

Safety Manager™ complies with the following international standards:

- For BMS: NFPA 85, 86, VDE 0116
- For ESD: IEC 61508, ISA S84.01, DIN V 19250, UL, FM, ATEX
- For F&G: EN54-2, NFPA 72, Lloyd's Register.

In summary, with all SIL3 safety compliance tools, hardware and software, Honeywell's Safety Manager provides excellent protection for safety applications across multiple industries throughout the lifetime of an installation. Together with Experion or any other process control systems, Safety Manager provides the basis for critical control and safety unification, reducing risks and installed costs, and improving plant safety.

## Engineering environment

The Safety Builder improves engineering and design efficiency. With the newly developed Network Configurator, designing safety networks has never been easier. With simple drag & drop functionality a complete network can be designed within minutes. Difficult and complex configurations no longer need to be programmed, as the Safety Builder will do this and will save valuable engineering and testing time. Moreover, the complete network design is available on a one-page view, no longer requiring additional documentation and programming.

The proven in use Functional Logic Diagram (FLD) Editor facilitates fast and effective application design allowing clear and distinct views of all logic, with full compliance to IEC 61131 standards. Logic inputs, outputs and symbols are placed with drag & drop functionality from the toolbar and are easily configurable.

Safety Manager R120, will provide several enhancements to make the life of a project engineer easier. Amongst others, the following features have been included:

- Copy application from another plant
- Bulk copy of points
- Bulk rename of points
- Bulk copy FLD
- Multi users using one Safety manager database
- Multi users connecting to one Safety manager controller
- Multi site support to allow for distributed logic development

## Process availability

By applying the proven-in-use QMR technology in Safety Manager™, unlimited run time for single channel operation is achieved. This invariably increases process availability, allowing uninterrupted process operation in case of any system degradation. Online system modification procedures have been redesigned and simplified, resulting in significantly improved application or system upgrades during plant start-ups or throughout the life-time of the process operation. It is estimated that up to 20% process uptime improvement can be achieved as a result of the above system enhancements.

## Operation and maintenance performance

Safety Manager™ unifies critical process data and information with the process control information, allowing single window access for operation and maintenance. When connected to the Experion Fault Tolerant Ethernet (FTE) network via TÜV SIL3 approved Universal Safety Interfaces (USI), multiple Safety Managers are unified into a single safety system architecture.

Extensive use of Ethernet for communication enables fast, safe and reliable data exchange with Experion, enhancing operator and maintenance performance. Additionally, with inherent extensive system self-testing and diagnostic capability, Safety Manager extends the system proof test interval, reducing operational and maintenance costs.

## System reliability and robustness

More than 60% of the proven-in-use safety system software coupled with the established QMR technology resides in the Safety Manager™ (SM) Controller. Software design robustness is achieved through the rigorous Design for Six Sigma (DFSS) process and the IEC 61508 development criteria. When it comes to safety, there is absolutely no compromise in Safety Manager.

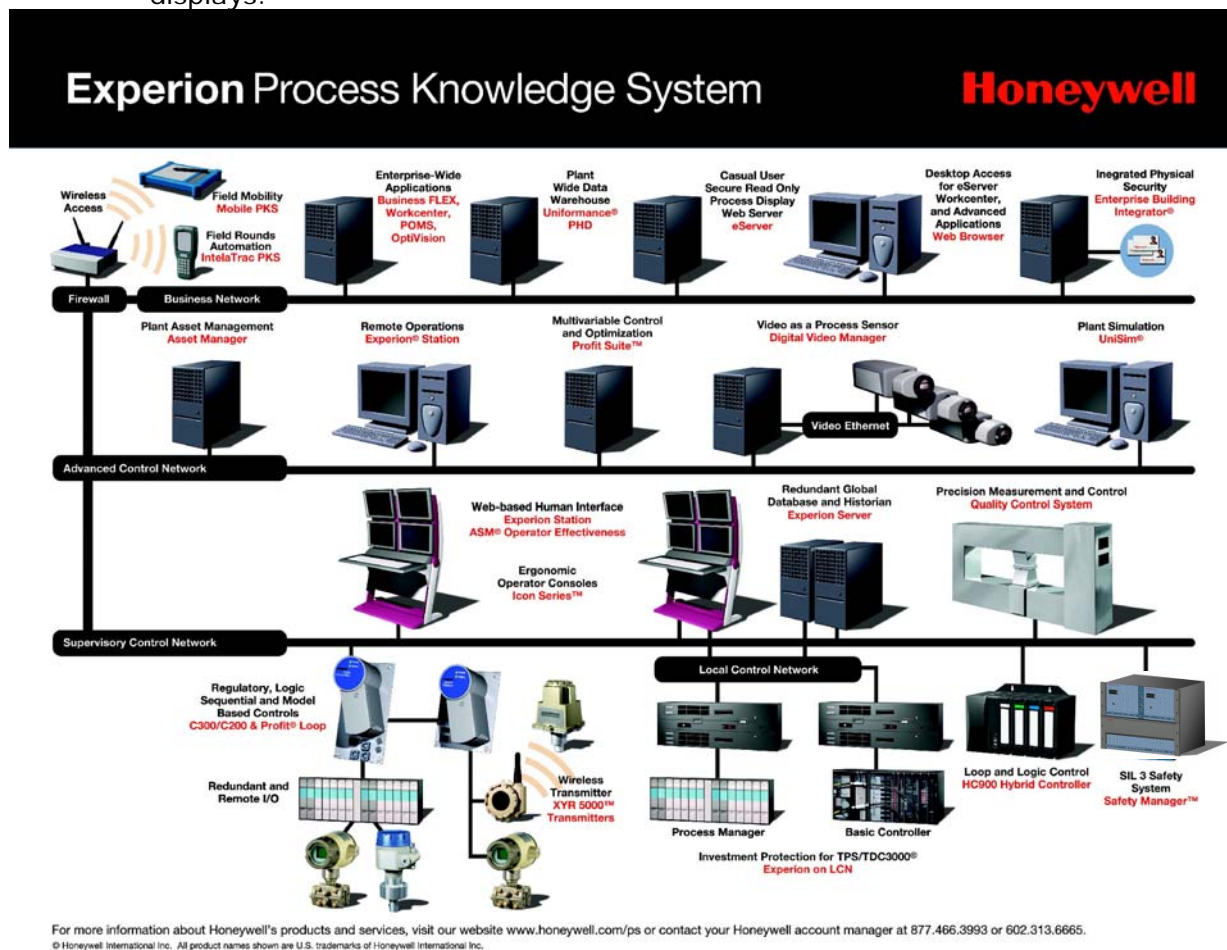
In addition, extensive design enhancement and simplification of the SM Controller hardware architecture reduces controller complexity, and promotes ease of use, system reliability and safety. Hardware robustness is enhanced through packaging using metallic enclosures for both controller and safety Ios. This improves EMC performance.

Additionally, with integrated 24 Vdc and 5 Vdc power supplies, adding either Ios or IO chassis will save valuable onsite activities reducing risks and costs for installation. Improperly operating circuit breakers are no longer an issue and cannot lead to a nuisance process trip. The system availability surpasses 99.99% and meets the stringent safety integrity SIL3 required in critical processes.

# Safety Solutions

## Integration into Experion PKS

Safety Manager™ supports the integration of Safety Manager into Experion™ PKS which unifies Honeywell's safety controller with its equally reliable Experion platform. The integration is realized through the Safety Manager Universal Safety Interface (USI) via High Speed Ethernet (HSE) on the Fault Tolerant Ethernet (FTE) layer, which is placed in the control processor of the Safety Manager Controller. This USI module makes Safety Manager an integrated part of the Experion architecture, which means that Safety Manager related information can easily be exchanged between Safety Manager and Experion. This allows information to be shared and made available on the Experion Server displays.



For more information about Honeywell's products and services, visit our website [www.honeywell.com/ps](http://www.honeywell.com/ps) or contact your Honeywell account manager at 877.466.3993 or 602.313.6665.  
© Honeywell International Inc. All product names shown are U.S. trademarks of Honeywell International Inc.

Figure 2 — Overview Experion PKS

Safety Manager integrates the sequence-of-event (SOE) features as supported by Safety Manager into the Experion server. Safety Manager supports SOE for digital inputs and outputs, analog inputs and outputs, and marker points. Each tag name that has been "SOE-enabled" is time-stamped by the Safety Manager controller and reported to the Experion Server, where it is incorporated into the standard Experion Server SOE list which allows for improved search, filter and automated archive functionality. Standard SOE displays are available to view the events as they are reported.



## PlantScape Integration

Safety Manager™ supports the integration of Safety Manager into PlantScape, which combines Honeywell's safety controller with its equally reliable hybrid control system. The integration is realized through the Safety Manager Universal Safety Interface module, which is placed in the control processor of the Safety Manager controller. This dedicated interface module makes Safety Manager an integrated part of the PlantScape system architecture, which means that Safety Manager related information, can easily be exchanged between Safety Manager and PlantScape. This allows information to be shared and made available on the PlantScape server displays.

Safety Manager integrates the sequence-of-event (SOE) features as supported by the Safety Manager controller into the PlantScape system. Safety Manager supports SOE for digital inputs and outputs, analog inputs and outputs, and marker points. Each tag name that has been "SOE-enabled" is time-stamped by Safety Manager and reported to the PlantScape server, where it is incorporated into the standard PlantScape SOE table. Standard SOE displays are available to view the events as they are reported.

Safety Manager integration into PlantScape requires PlantScape Release 300 or higher.

## Serial Communication with Process Computer Systems

Safety Manager™ supports the exchange of control program data with process computers via serial communication links, using the non-proprietary Modbus RTU communication protocol. The following information can be exchanged:

- analog process data as scanned by SM Controller through its input interfaces,
- trip settings,
- trip status, and
- Safety Manager Controller alarm status.

Data written to the Safety manager Controller is available in the Safety Manager control program via digital and numerical input variables, which allow the user to define the conditions of use in the control strategy.

## Fire and Gas Safety Solution

Honeywell Safety Manager™ provides an approved Fire and Gas Safety Solution that covers Safety Instrumented System requirements as part of the Mitigation Safety Layer described in the IEC 61508, IEC 61511 and ANSI/ISA S84.01 standards.

Safety Manager fire and gas safety system is designed to detect hazards like fires or gas leakage's in a fast and accurate way by using connections of a wide range of F&G detector devices. On detection system will perform the appropriate safety actions automatically and will alert about the detected hazard(s) in most efficient way.

Safety Manager supports standard connection of Fire and Gas detector devices of most major F&G field device suppliers. The supported connections are proven in use and/or are fully tested as part of the MVIP test program. For signal handling inside Safety Manager of these connected F&G devices, special function blocks are developed to create an optimum response from these devices. For connection of the devices special interfaces are developed to achieve the optimum connection.

Available interfaces are:

- TSGASH-1624 Fail-safe Gas/Flame detector input FTA with HART interface.
- TSFIRE-1624 Fail-safe Fire detector input FTA

In the Safety Manager Guides an approved basic Fire and Gas Safety application is included. This application provides a Fire and Gas Safety Solution that can easily be integrated into Honeywell's Experion™ PKS, Honeywell's TotalPlant Solution (TPS) system or into Honeywell's PlantScape system. The basic application can be developed and adjusted easily to design a project specific Fire and Gas Safety Solution.

The integrated layer of the F&G solution within Experion, TPS or PlantScape contains the integrated alarm listing and safety historian functionality that records all detected alarms, all actions initiated by the F&G Safety system and all actions executed by this system or connected integrated sub-systems. This layer also shows the actual situation of the F&G application by using overall plant displays and various detailed area displays that contain locations and actual status of all connected F&G field detectors.

# Functional Description

## Basic architecture

Two major system parts can be distinguished:

- SM Controller, and
- SM IO interfaces.

Figure 3 shows the basic components of Safety Manager™.

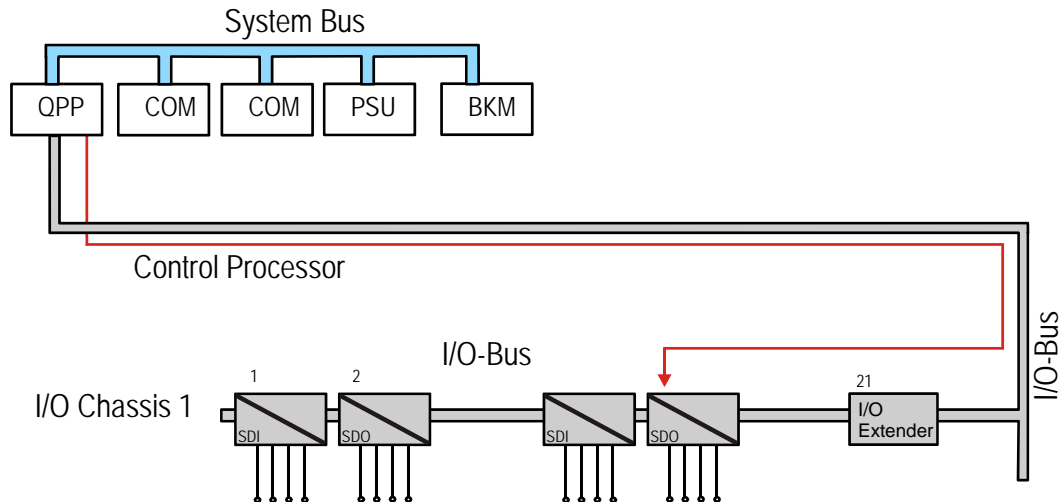


Figure 3 — Safety Manager basic components

### SM Controller

Its function is to run and control the Safety Manager™ application logic, communicate to other systems, perform diagnostics on safety-critical functions and respond to detected faults while maintaining safety. A SM Controller consists of a Control Processor, a Controller Chassis, a Battery and Keyswitch Module (BKM) and a Control Processor Backplane (CPB), which includes a speedy redundant system bus.

### Control Processor

A Control Processor consists of core components such as a Quad Processor Pack (QPP), a communication module (USI) and a Power Supply unit (PSU). For more information, see "SM Controller components".

### IO

Its function is to connect the SM Controller to the sensors and actuators in the field. The variety of IO modules includes safe modules, both analog and digital, redundant and non-redundant and different voltages. For more information, see "SM IO components".

### IO Bus

The IO bus is the interface to transport field data and diagnostic data between the IO and the controller. For more information, see "SM IO components".

## Safety vs. availability

Safety and availability do not easily coexist in the process industry:

- Safety means “Freedom from unacceptable risk”.  
To achieve safety it is mandatory to keep process away from its production limits.
- Availability is usually translated in productivity.  
To achieve optimum productivity, one must operate a process as close as possible to its production limits.

In a SIS, safety prevails over availability, meaning that when a SIS has to choose between safety and availability, safety is chosen.

### Safety

Safety Manager’ basic design allows the system to comply to SIL3, regardless the system architecture chosen.

SIL3 is the highest level of safety required for most process industries.

### Availability

Safety Manager is highly available due to the systems’:

- ability to locate faults accurately, and isolates faulty parts from the process whenever possible to continue a safe operating state with minimum effect on the remaining process parts. The fault location algorithm also reduces repair time and possible down time to an absolute minimum
- ability for on-line repair, such as on-line exchange of communication modules and all redundant components
- ability to automatically upload the required software in replaced modules, while being on-line.

### Note

This level of availability is referred to as “normal”.

## Redundancy and availability

Availability can be further increased by using redundancy in the architecture. Depending on the level of redundancy one refers to “increased availability” or “optimal availability”.

### Fault tolerancy

By applying redundancy the system becomes fault tolerant with respect to availability. This means that any single system fault shall NOT create a nuisance trip.

### Online repair and online modification

Redundancy also allows online repair of redundant components. When replacing Controller modules, these are automatically loaded with the required software. With a redundant Controller you can also perform online modifications.

### Availability levels

Table 1 shows the relation between applied redundancy within Safety Manager with the level of system availability.

**Table 1 Safety Manager architectures**

Controller configuration	IO Configuration	supports SIF up to and including	Availability
Redundant	Redundant	SIL3	Optimal
	Mixed redundant and non-redundant	SIL3	Mixed optimal and increased
	Non-redundant	SIL3	Increased
Non-redundant	Non-redundant	SIL3	Normal

## IO configurations

### Redundant IO configurations

Redundant IO configurations can be used in Safety Manager with a redundant Controller. In this fully redundant configuration, each Control Processor has its own IO system to which it has exclusive access. Each Control Processor reads its own input interfaces once every program cycle. After input matching, both Control Processors execute the user-defined control program and update their output interfaces according to the results. Before setting, the Control Processors compare the calculated output results to ensure identical operation. Redundant IO configurations are typically used for safety functions that require optimal availability. With Safety Manager R120, also Analog Outputs can be used in a redundant topology.

### Non-redundant IO configurations

Non-redundant IO configurations can be used in systems with a non-redundant Controller as well as in systems with redundant Controller. Fully non-redundant systems are typically used for safety applications where redundancy is part of the process. In a Safety Manager setup with a redundant Controller, and (partly) non-redundant IO, both Control Processors alternately assume responsibility for the non-redundant IO interfaces. This ensures both Control Processors can always access the IO interfaces correctly. Safety Manager configurations with a redundant Controller and non-redundant IO interfaces are typically used for safety critical applications with increased demands for system availability, for example because of redundancy in plant equipment. The combination of redundant and non-redundant IO interfaces is extremely powerful. Process safeguarding functions requiring optimal availability are controlled through the redundant IO interfaces, and less demanding safety functions through the non-redundant IO interfaces.

## Multiple-Sensor and Transmitter Configurations

Unlike earlier safety standards, the international standards ANSI/ISA S84.01 and IEC 61508 do not only focus on the safety system (called "logic solver", e.g. Safety Manager), but also demand compliance of the field equipment to the Safety Integrity Level (SIL) of the control loop. This may not always be possible. The control loop, for example, may be rated SIL3, whereas a transmitter that measures one of the loop input variables is only suited for SIL1 and SIL2. In such cases, the required level of safety can be realized by using multiple sensors or transmitters.

Safety Manager supports multiple input configurations for digital and analog input signals. The multiple-input function allows the use of two or three sensors or transmitters to measure the same process quantity. The resulting process value is fed to the control program on the basis of one of the available standard matching algorithms, e.g. 2-out-of-3 (2oo3). Safety Manager monitors if discrepancies occur between the values obtained from the independent sensors or transmitters, and reports any detected faults through its diagnostics. The diagnostic status is also available to the control program.

## Fault detection and response

### Concept

The fault detection-and-response technology is just one of the innovative concepts embodied by Safety Manager™, allowing it to operate in SIL3 per default.

Before we can discuss the actual fault detection and response principles, you should first learn about the concepts behind fault detection and response.

### Process safety time

The time a process can be left running uncontrolled without losing the ability to regain control.

### Example

As an example we discuss the process inside a furnace:

- If the main fuel valve is opened but the pilot burner is not ignited, the amount of fuel inside the burner chamber increases.
- If the pilot burner ignites within 3 seconds after the inlet of fuel started, then the burner starts in a controlled way and the furnace is operational.
- If the pilot burner does not ignite within 3 seconds, the amount of fuel inside the burner chamber increments to a critical level; if ignition should follow now, the furnace will be damaged.

Instead the burner should be purged and the ignition process restarted. In this example the Process Safety Time (PST) is 3 seconds, meaning that if we detect –and respond to- the failure (no ignition of the pilot burner) within 3 seconds after opening the fuel valve, control can be regained by purging the burner chamber.

### Concept

Safety Manager continuously tests all of its safety components (IO, software etc.) to verify that each safety component within the system functions as expected.

Since this takes time, and not all components can be tested at the same time, testing is a sequential process.

In order to detect –and respond to- a possible fault of a safety component in time to correct it, Safety Manager firmware tests all safety related hardware – and responds to a possible failure- within one diagnostic test interval (DTI).

### Diagnostic Test Interval (DTI)

A Diagnostic Test Interval is Safety Managers' response to Process Safety Time: DTI is the time period used by Safety Manager to cyclically locate and isolate safety related faults within on-line system components that could otherwise cause a hazardous situation.

### Fault

A fault is an abnormal condition that could lead to an error.

### Single fault

When reading, you should realize that when we discuss “a fault”, a single fault is often meant. If we would allow multiple faults to accumulate in a system, the combination of faults cause an accumulation of errors that cannot be anticipated upon.

It is therefore relevant to repair a fault after it has been detected, how irrelevant the fault may seem.

### Single fault tolerant

A system that is single fault tolerant is able to withstand the occurrence of a single fault, without losing its function.

When discussing SIS, you should refer to single fault tolerant for safety: A system is single fault tolerant for safety when safety can still be maintained after the occurrence of a single fault.

- The advantage of this capability is that the process’ safety is maintained, even with a single fault present in the system.
- The disadvantage of this capability lies in the lack of response of personnel, that thinks no urgent action is required, and does not respond to the fault report.

### Secondary means

Figure 4 shows that all safe output modules have a secondary means of de-energization (SMOD), to ensure “single fault tolerance for safety”. With this SMOD any faulty output channel can be isolated from the process.

The series connection of a SMOD and the channel output, combined with full functional testing, creates “single fault tolerance for safety”. Software driven full functional testing is executed by the QPP and the actual readback status is compared with the expected value. Any discrepancy found will result in safety corrective actions, meaning isolation of the fault from the process and notification of the operator while saving data in the diagnostics file.

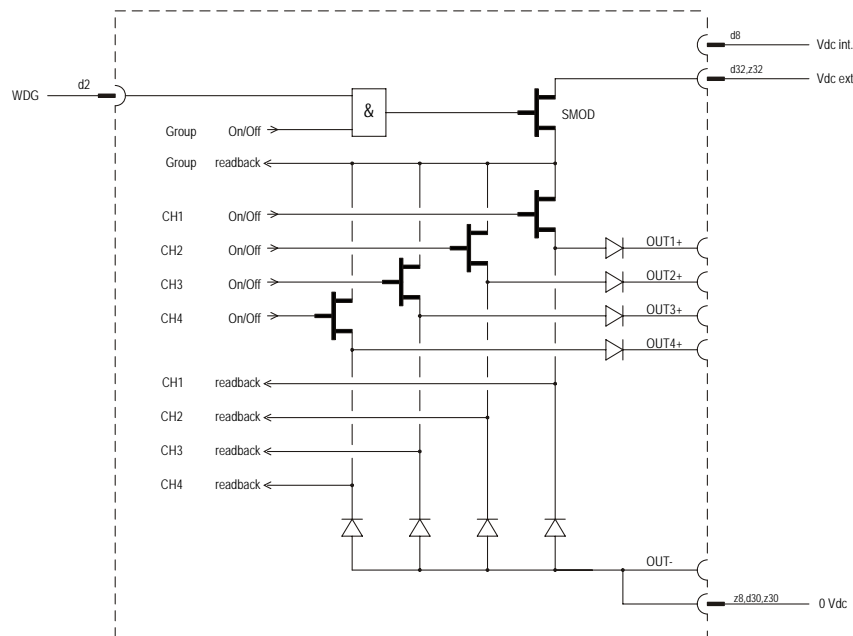


Figure 4 — Schematic diagram of a SMOD with 4 channels



### **Fault reaction**

Fault reaction is the systems' actual response towards detected faults. The response can depend on a number of things, such as the severity of the fault, the availability of a redundant component, the fault reaction setting. See "Principle of fault response".

Fault reaction for IO points is configurable.

### **Repair timer**

Safety Manager starts a repair timer upon the detection of very critical faults. This timer is started to urge maintenance personnel to fix the fault as soon as possible.

A repair timer protects the system from certain fault accumulations that may affect the safety of Safety Manager. The timer therefore only starts on detection of faults that can be categorized as "may affect safety when faults accumulate". The timer is a configurable count-down timer, which can be deactivated. The default repair window is 72 hours (3 days), which is more than sufficient if spare parts are available.

## **Principle of fault detection**

A Safety Instrumented System (SIS) operating in "high demand mode of operation" must detect and safely isolate any single fault within one PST.

#### **Note**

Fault detection and response is aimed at detecting and responding to faults that affect or endanger the safety of the system and the process under control.

### **Fault detection**

Fault detection is the first step towards fault response. Faults in Safety Manager™ are detected conform the Failure Mode and Effect Analysis (FMEA) model, which provides adequate diagnostics on any detected fault. Test algorithms and / or test circuits are embedded in the safety related software and hardware components, such to allow the detection of these faults.

A running SM Controller continuously performs a series of extensive diagnostic checks on all safety related software and hardware components. This way it will find faults before they can jeopardize the safety of the process and equipment under control.

### **Fault detection cycle**

The fault detection and diagnostic checks are executed during a fault detection cycle, which is usually split-up over a number of application cycles. A fault detection cycle always lasts less than one DTI.

### **Fault database**

Upon detection, a fault is stored in a fault database, where it is further processed by the Controller.

Upon the severity of the fault, the configuration settings, the redundancy in the Controller and other user settings, the Controller will decide what action is appropriate. To clear a fault from the fault database, the fault must be resolved and a fault reset must be initiated (e.g. turn and release the Reset key switch on the BKM).

## Principle of fault response

Each detected fault is reported by means of a diagnostic message, alarm markers and/or diagnostic markers.

If the nature of the fault requires the system to respond, Safety Manager™ will isolate the faulty component from the rest of the system.

At the same time the system acts on the effect of loosing the function of that component.

That action may be:

- none, a redundant component can cover for the lost function.
- none, loosing the function has no impact on safety.
- apply the fault reaction state to the affected IO.
- start the repair timer.
- halt the affected Control Processor.
- de-energize all non-redundant outputs via the watchdog
- de-energize all outputs via the watchdog.

Below explains these items in more detail.

### Redundancy

When available, the redundant component in the system will continue to perform that function. This means that, when redundancy is provided, the system remains available for the process.

### No impact on safety

The following examples show a number of faults that have no impact on safety:

- External power down.
- Loss of communication with a process control system.
- Failure of the Controller back-up battery.
- Loop faults

When such faults occur, the system will report the anomaly but take no action by itself. However the system can be programmed to initiate action if needed.

### Fault reaction state

If Safety Manager detects a fault related to the IO, this may result in the IO to go to the fault reaction state.

The fault reaction state is a state used as response to faults arising related to IO.

The fault reaction state is user configurable on module level, with exception of the communication IO. The following fault reaction states exist:

- 'High' is a fault reaction state for digital inputs:  
Upon a detected fault the input is energized, or –in other words, the input goes high or becomes '1'.
- 'Low' is a fault reaction state for digital inputs and digital outputs:  
Upon a detected fault the digital input or output is de-energized, or –in other words, the digital input or output goes low or becomes '0'.
- 'Top Scale' is a fault reaction state for analog inputs:  
Upon a detected fault the input is set to the top scale of the range.
- 'Bottom Scale' is a fault reaction state for analog inputs:  
Upon a detected fault the analog input is set to the bottom scale of the range.

- 'Scan' is a fault reaction state for tested (analog or digital) inputs and (non) tested digital outputs:  
 Upon a detected fault the input or output continues to carry the processing value, even if this value is not correct.
- 'Hold' is a fault reaction state for analog and digital inputs:  
 Upon a detected fault the input freezes to the last known good value.
- '0 mA' is a fault reaction state for analog outputs:  
 Upon a detected fault the analog output is de-energized.
- 'Appl' is a fault reaction state for analog outputs:  
 Upon a detected fault analog output continues to carry the processing value.
- 'Preset' is a fault reaction state for numeric inputs located on a communication channel:  
 Upon detected fault the numeric input is preset to a predefined value (not necessary being the startup value).

Table 2 shows the settings applicable to fault reaction for hardware IO.

**Table 2 — Fault Reaction settings for hardware IO**

Signal type		Fault Reaction settings
Digital Inputs	Tested	High/Low/Scan/Hold
	Not Tested	High/Low/Hold
Safe Digital Inputs with Line Monitoring		High/Low/Scan/Hold
Digital Outputs	Tested	Low/Scan
	Not Tested	Low/Scan
Tested Digital Outputs with Line Monitoring		Low/Scan
Tested Analog Inputs		Top Scale/Bottom Scale/Scan/Hold
Analog Outputs*	Tested	0 mA/Appl
	Not Tested	0 mA/Appl

**Table 4** The setting Tested or Not Tested is determined by the properties of the analog output module

Table 3 shows the settings applicable to fault reaction for communication IO.

**Table 3 — Fault reaction settings for communication IO**

Signal type	Fault Reaction settings
Digital Points (DI)	High/Low/Freeze
Numeric Points (BI)	Preset/Freeze

### **Repair timer**

All configurations of Safety Manager are single fault tolerant towards faults that affect safety: By using a secondary means Safety Manager is always able to bring a process to safe state, regardless of the fault.

However, given some time, a second fault may occur. This second fault may then disable the secondary means that keeps the process in a safe state.

To prevent such a scenario to develop, the system starts a repair timer if a secondary means becomes vulnerable to faults. Once started, this configurable timer counts down until the fault is repaired. If the timer is allowed to reach zero, the Control Processor halts.

### **Halt Control Processor**

A Control Processor halts if:

- A fault is detected in one of its safety functions.  
For example: corrupted software, safety processors out of sync, watchdog fault
- The repair timer runs out,
- The Control Processor is disabled by its own watchdog,
- The Control Processor is disabled by the watchdog of the other Control Processor.

### **Watchdog and redundancy**

The availability of the system after responding to a fault depends on the available redundancy in the system and if –and how- the watchdog interfered. As shown in Figure 5 each Control Processor has a watchdog with two watchdog lines to independently enable/disable the (non-) redundant outputs.

If the watchdog interferes, this can be caused by:

- • A fault in the Control Processor:  
This will halt the related CP and disable all output controls of that CP.
- • A fault in the non-redundant outputs:  
This will cause the watchdogs of both Control Processors to disable the non-redundant outputs.
- • A fault in one of the redundant outputs:  
This will cause the related watchdog to halt its CP and disable all outputs controlled by that CP.

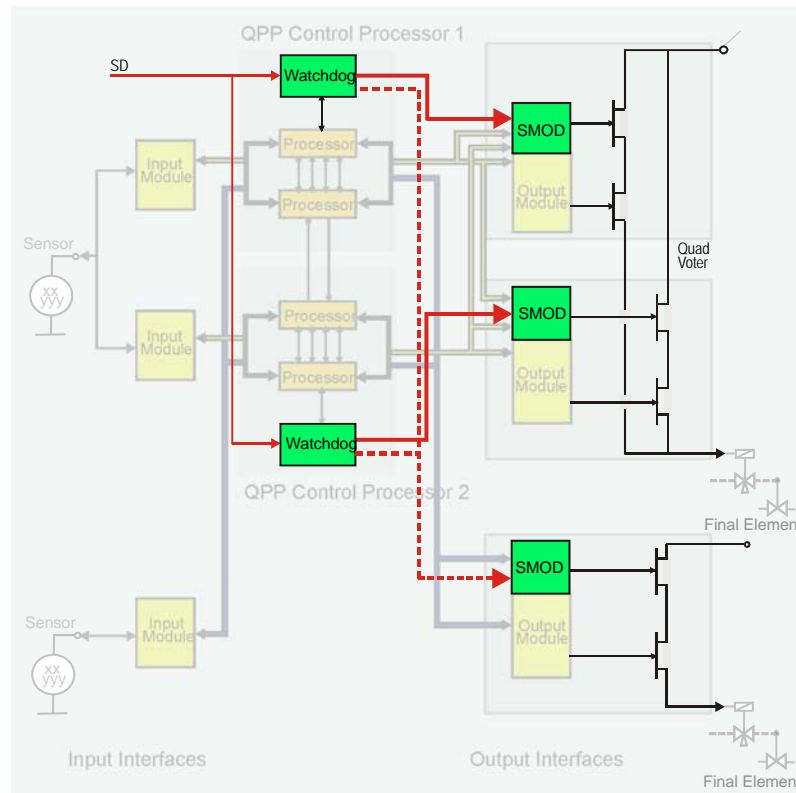


Figure 5 — Each watchdog has 2 outputs

### Peer to peer connections

Safety Manager™ communicates with its surroundings (for example a Safety Station or an Experion Station).

Table 4 on page 32 describes what information can be communicated and the supported protocols that can be used.

Table 4 — Overview of peer to peer connections

Connection	Logical network	Physical network	Safe?	Options
Safety Manager – Safety Station (Safety Builder)	Safety Builder protocol	RS232 RS485 RS422 Ethernet	no	data viewing diagnostics forcing loading
Safety Manager – Experion Server	Experion protocol	Ethernet	no	data viewing diagnostics soe
Safety Manager – Safety Manager (SafeNet)	SafeNet protocol	RS485 Ethernet	yes	data viewing diagnostics remote reset remote loading
Safety Manager – Safety Station (Safety Historian)	Experion protocol	Ethernet	no	soe

## Human Machine Interfaces

Within Experion PKS, different methods to retrieve process and system information are available.

When working with Safety Manager™:

- process information is available via stations and LEDs,
- system information, such as diagnostics and systems' temperature is available via both stations and hardware interfaces.

These interface options are discussed below.

### Hardware interfaces

The hardware interfaces are intended for basic information exchange between man and machine.

#### Display on Quad Processor Pack (QPP)

Figure 6 shows the user interface display, located on the Control Processor. It provides system status and diagnostic information.

The messages are language-independent and include (if applicable) UNICODE languages. This means that messages will be displayed in English as a default, but this depends on the configured language in the Safety Builder.



**Figure 6 — the user interface display of the QPP**

#### LED indicators

Most modules have one or more LED indicators at the front.

- Controller modules have a single bi-color LED with the word "status" written next to it. A green color means "OK".
- Communication modules and digital IO modules also have dedicated LEDs per channel, indicating the channel status.

#### Example

Figure 7 shows the module front of a 16 channel digital input module with line monitoring.

With this example, each channel has *two* LEDs to indicate its status.

- The green channel LED shows the channel status.
- The red channel LED indicates if a fault occurred in the channel, or the field wiring of that channel.

Furthermore the module is equipped with two bi-colored status LEDs; one to indicate the status of the built-in earth leakage detector, one to indicate the module overall status.

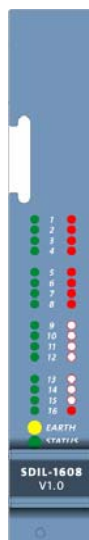


Figure 7 — Module front

### Key switches

Key switches are used for specific functions that require key access before they can be performed.



Figure 8 — Key switches at the front of the BMK

Safety Manager has 3 different key switches:

- Figure 8 shows the front view of the Battery and Key switch module (BKM), where the Reset and Force Enable key switch are installed.  
The key switches on the BKM are wired to both CP1 and CP2.
  - Under normal circumstances the Reset key switch is used to start the system or restart halted system components without switch-over effect. (Turning this key switch will not interrupt process safeguarding.)
  - When performing on-line modification (changing the application / system configuration on-line) the Reset key switch is used to switch applications.
  - The Force key switch is used to enable / disable the use of forcing of IO points. With this key switch in the "on" position, forcing via a safety station is allowed. With this key switch in the "off" position all forces are cleared
- Each Quadruple Processor Pack (QPP) has a 3 position key switch installed.
  - The key switch on the QPP is used to idle, halt or run the QPP. When idle, the QPP can be fitted with a new application program.

### Stations

The software interfaces are intended for extended information exchange between man and machine.

### Safety Stations and Experion Stations

Safety Manager can run software packages on different types of Stations (PCs) or use these Stations for interfacing.

The following Stations (PCs) can be distinguished:

Station name	Description
Safety Station	PC that runs Safety Builder and/or Safety Historian
Experion Station*	PC that runs the Process control application.

\* Safety Builder software may also be installed on an Experion Station

### Usability

Table 5 shows the main Station functions related to Safety Manager versus their availability on each Station type.

**Table 5 – Station functions**

Safety Station	Experion Station	Function
Yes	Yes	View Safety manager system status
Yes	Yes	View Safety Manager point status
Yes	Yes	View Safety Manager diagnostics
Yes	No	View Safety Manager functional logic diagrams
No	Yes	Integrate Safety Manager alarms in Experion alarm window
No	Yes	Integrate Safety Manager SOE in Experion SOE window
Yes	Nn	View Safety manager SOE in Safety Historian SOE window

The figures on the following pages provide screenshots of Experion Station displays, related to Safety Manager.



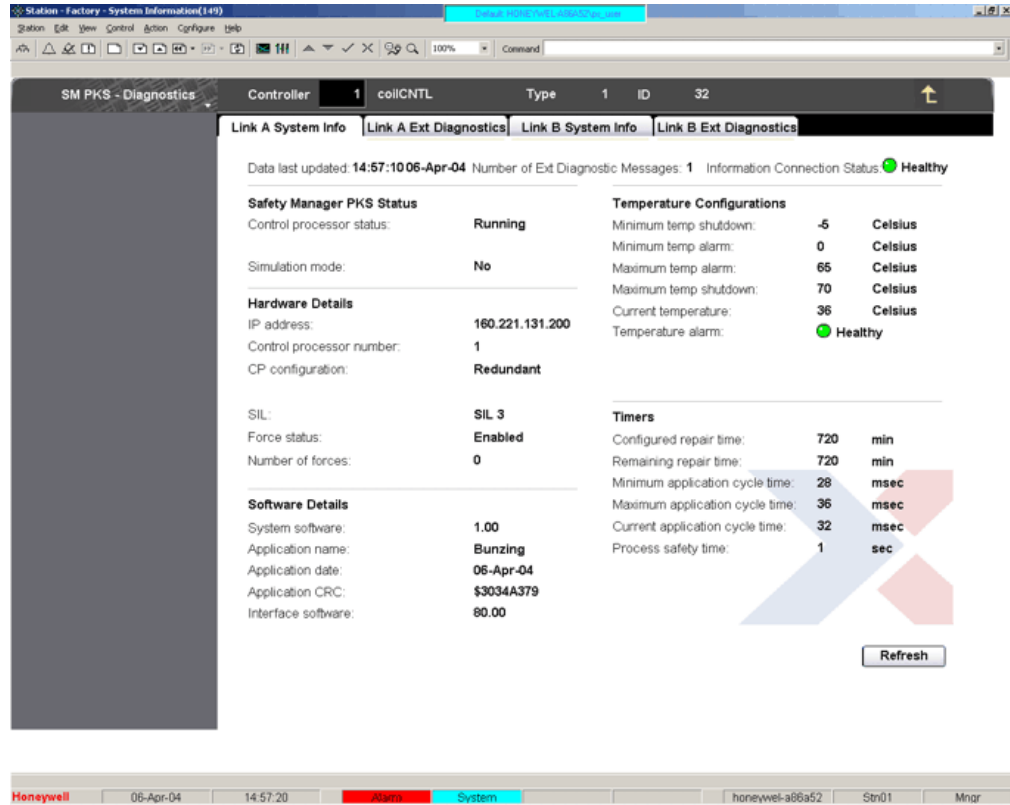


Figure 9 — Example of an Experion Station “system information display”

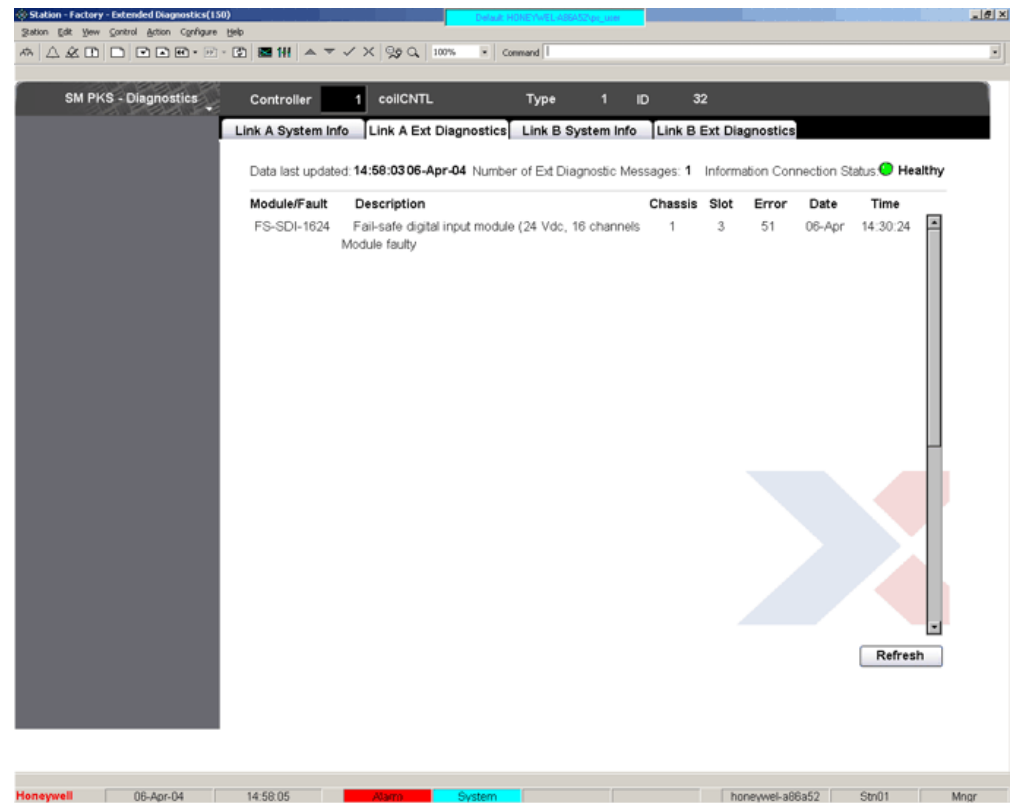


Figure 10 — Example of an Experion Station “diagnostics display”

### **Station requirements**

Basically any modern PC will qualify as Safety Station.

The minimum requirements for a Safety Station are:

- Windows 2000 with service pack 4 or Windows XP with service pack 2.
- Pentium 1Ghz, 256 MB RAM, 20 GB free disk space, CD ROM.
- Screen resolution 1024×768, 16-bit color.

As most Experion Stations have higher requirements, most Experion Stations are suitable to be upgraded as Safety Station.

# System Features

## Safety Manager System Configurations

Safety Manager™ is available in several configurations to suit virtually every process control requirement. Table 6 below lists the Safety Manager system configurations that are available, together with their main characteristics.

**Table 6 — Safety Manager System Configurations**

Type	Safety Manager Controller	Safety Manager IO Interface	Typical Application	Architecture
Non-redundant (single)	Non-redundant	Non-redundant	Critical process control with redundancy in field equipment	DMR
Redundant	Redundant	Non-redundant	Critical process control with redundancy in field equipment	QMR
	Redundant	Redundant	Critical process control	QMR
Combined	Redundant	Redundant & Non-redundant	Burner/Boiler Management System with Safety Manager - controlled alarm panel Fire & Gas	QMR

## Safety Manager basic architectures

Safety Manager can be configured for a number of architectures, each with its own characteristics and typical applications. Table 8 below provides an overview of the available architectures.

**Table 7 — Safety Manager architectures**

Controller configuration	IO configuration	Remarks
Non-redundant (DMR)	Non-redundant	DMR architecture; Applications up to and including SIL3
Redundant (QMR)	Non-redundant	QMR architecture; Applications up to and including SIL3
	Redundant	
	Redundant and non-redundant	

DMR = Dual Modular Redundant  
 QMR = Quadruple Modular Redundant

All Safety Manager architectures can be used for safety applications. The preferred architecture depends on the availability requirements.

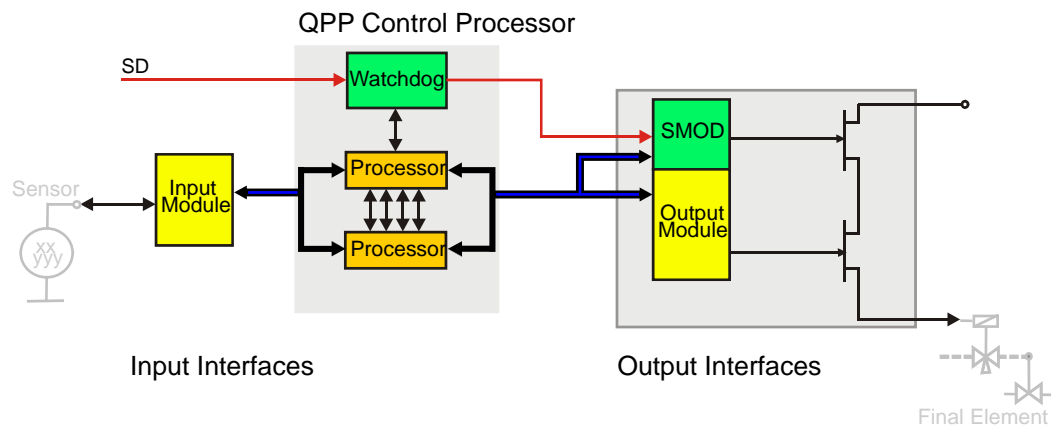
## Dual Modular Redundant (DMR) architecture

Typical applications of a DMR architecture are:

- Burner Management System
- Batch processing
- Machine safety

The Dual Modular Redundant (DMR) architecture provides 1oo2 voting in a non-redundant system. The DMR architecture with 1oo2 voting is based on dual-processor technology, and is characterized by a high level of self tests, diagnostics and fault tolerance.

The DMR architecture is realized with a non-redundant Controller. A non-redundant architecture contains only one QPP (see Figure 11), which contains a redundant processor with 1oo2 voting between the processors and memory.



**Figure 11 — Functional diagram: DMR architecture**

In IO configurations, each path is primarily controlled by the Control Processor and an independent switch (Secondary Means of De-energization, SMOD) which is controlled by an independent watchdog.

## Quadruple Modular Redundant (QMR) architecture

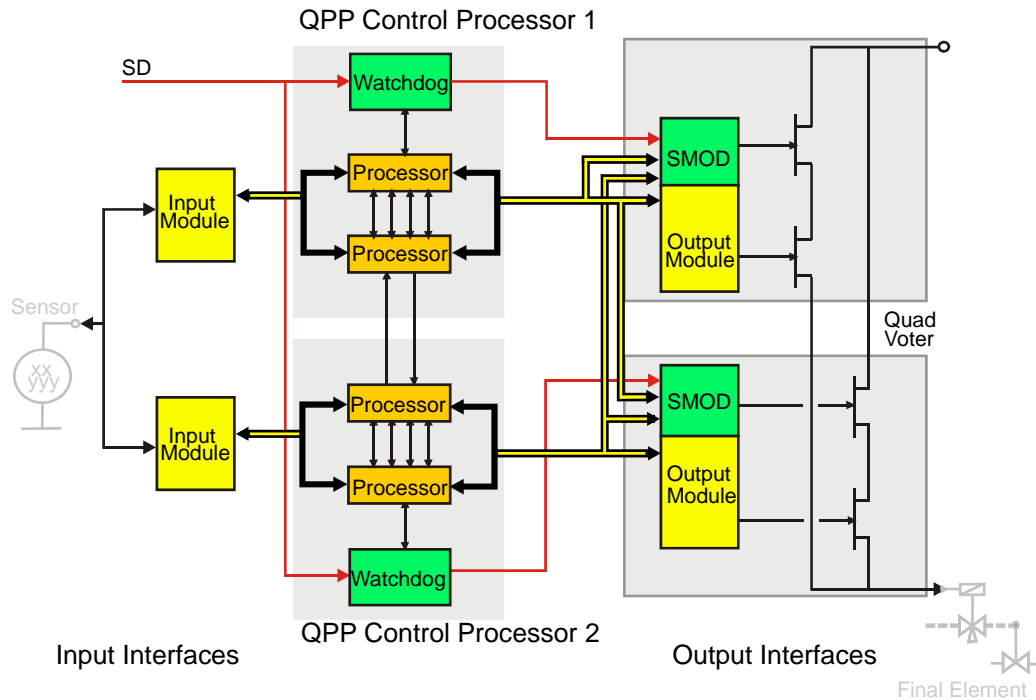
Typical applications of a QMR architecture are:

- process safeguarding applications for which continues operation is essential.

The Quadruple Modular Redundant (QMR) architecture is based on 2oo4D voting, dual-processor technology in each QPP. This means that it is characterized by a ultimate level of self diagnostics and fault tolerance.

The QMR architecture is realized with a redundant Controller. This redundant architecture contains two QPPs (see Figure 12), which results in quadruple redundancy.

The 2oo4D voting is realized by combining 1oo2 voting of both CPUs and memory in each QPP, and 1oo2D voting between the two QPPs. Voting takes place on two levels: on a module level and between the QPPs.



**Figure 12 — Functional diagram: QMR architecture**

In redundant IO configurations, each path is controlled by one of the Control Processors and an independent switch (Secondary Means of De-energization, SMOD), which is controlled by the diagnostic software and an independent watchdog.

Furthermore, each Control Processor is able to switch off the output channels of the other Control Processor.

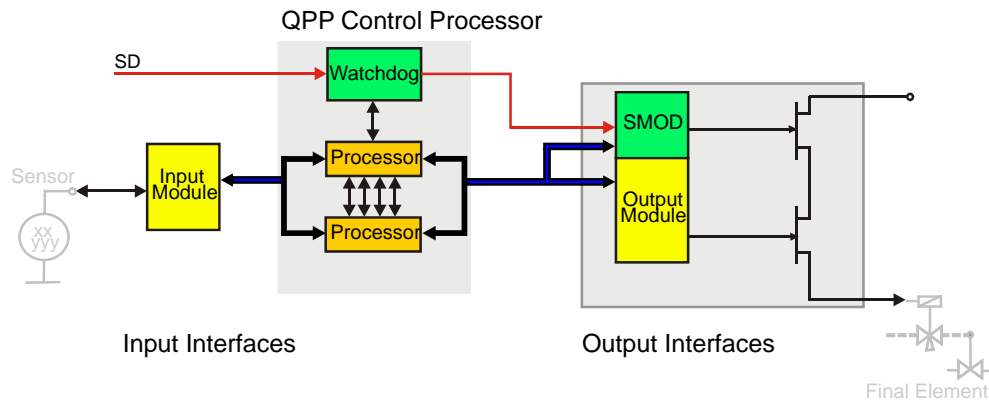
## System architectures

### Non-redundant Controller and non-redundant IO

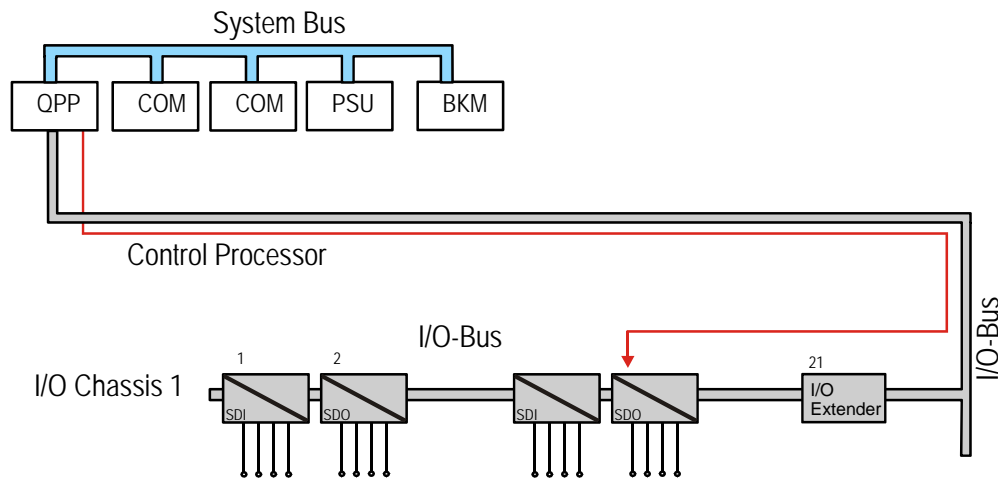
This Safety Manager architecture has a non-redundant Controller and non-redundant input and output (IO) modules (see Figure 13 and Figure 14).

The IO modules are controlled via the IO bus drivers (located in the QPP) and the IO Bus, which can control up to 8 IO chassis per cabinet. Each IO chassis is controlled via the IO Extender. There is no redundancy except for those modules with built-in redundancy (QPP, memory and watchdog).

This architecture can be applied up to and including SIL3.



**Figure 13 — Functional diagram: non-redundant Controller, non-redundant IO**



**Figure 14 — Non-redundant Controller, non-redundant IO configuration**

### Redundant Controller and non-redundant IO

This Safety Manager architecture has a redundant Controller and non-redundant input and output (IO) modules (see Figure 15 and Figure 16 below).

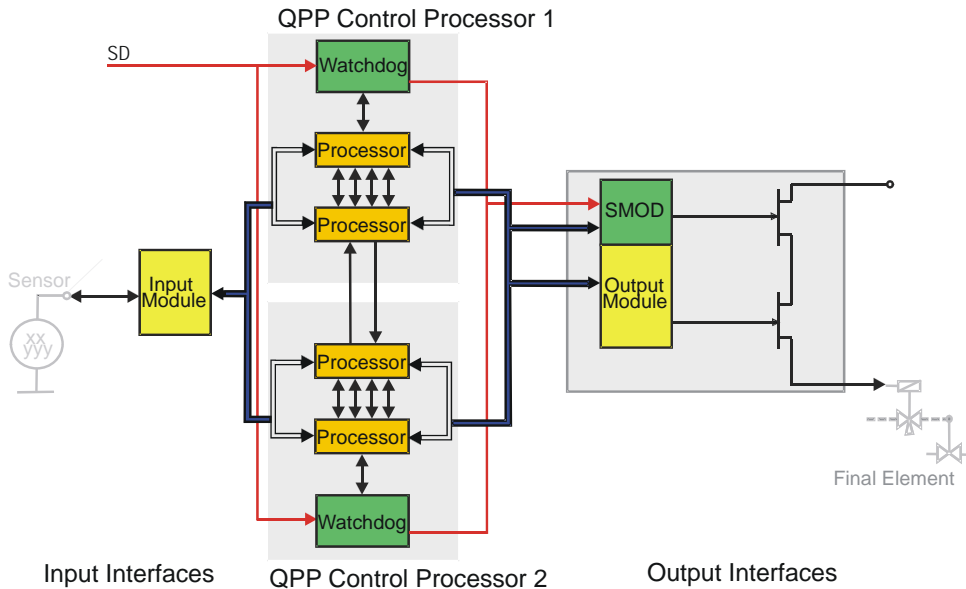
The IO modules are controlled via the IO bus drivers (located in the QPP) and the IO Bus, which can control up to 8 IO chassis per cabinet. Each IO chassis is controlled via the IO Extender.

This architecture can be applied up to and including SIL3.

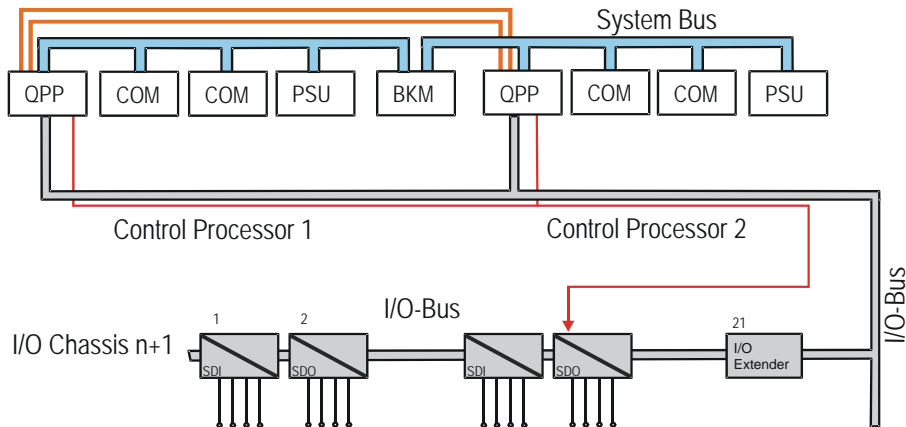
**Interaction between Control Processors**

Both Control Processors run in parallel, meaning that they simultaneously read input states and write output states. Via the redundant link both Control Processor s continuously inform each other about the achieved IO states, application states. The redundant link is used to synchronize actions and compare results.

A redundant Controller is single fault tolerant with respect to availability.



**Figure 15 — Functional diagram: redundant Controller, non-redundant IO**



**Figure 16 — Redundant Controller, non-redundant IO configuration**

### Redundant Controller and redundant IO

This Safety Manager architecture has a redundant Controller and redundant input and output (IO) modules (OR function outputs) (see Figure 17 and Figure 18 below).

The IO modules are controlled via the IO bus drivers (located in the QPP) and the IO Bus, which can control up to 8 IO chassis per cabinet. Each IO chassis is controlled via the IO Extender. The processor and IO are fully redundant, which allows continuous operation and smooth (zero-delay) transfer of the control in case of a Control Processor or IO failure.

This architecture can be applied up to and including SIL3.

### Interaction between Control Processors

Both Control Processors run in parallel, meaning that they simultaneously read input states and write output states. Via the redundant link both Control Processor's continuously inform each other about the achieved IO states, application states. The redundant link is used to synchronize activities and compare results.

### Interaction between redundant IO

Both IO modules reside next to each other in the same IO chassis. On the backplane they are wired parallel.

- In principle, when a fault is detected in an input channel, this channel is deactivated by its corresponding Control Processor. The correct value is obtained from the IO module connected to the other Control Processor via the redundant internal link before the application cycle is started.
- In principle, when a fault is detected in an output channel, this channel is de-energized by the SMOD. The correct value is driven into the field by the other Control Processor, but not after both Control Processors have agreed on its value via the redundant internal link.

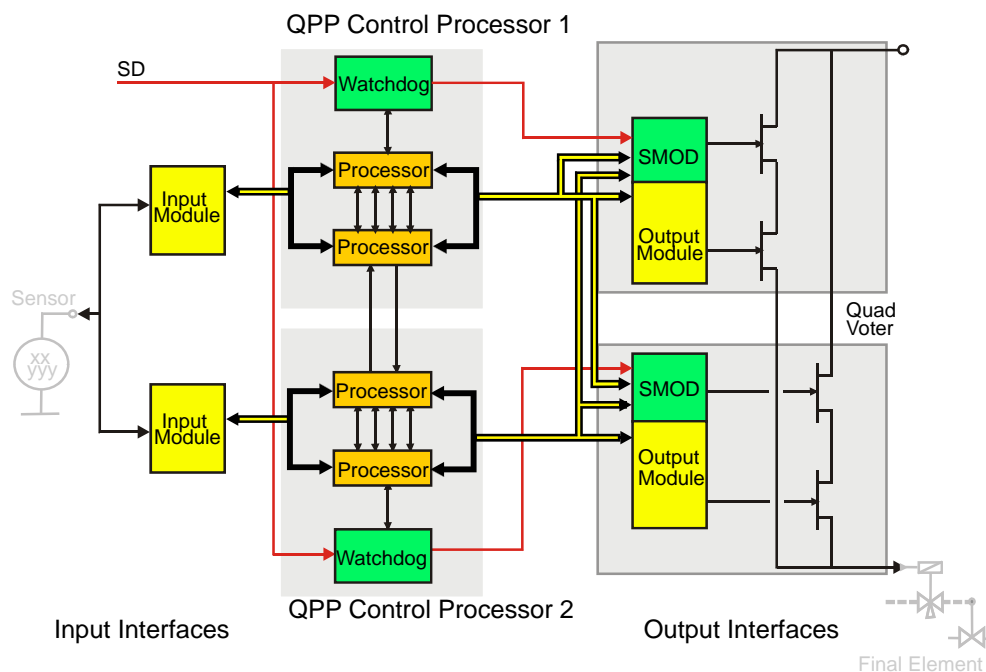
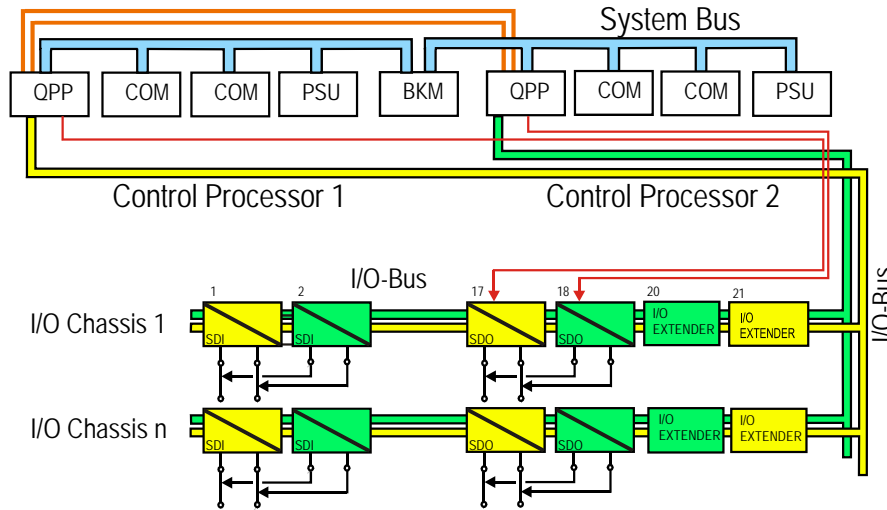


Figure 17 — Functional diagram: redundant Controller, redundant IO





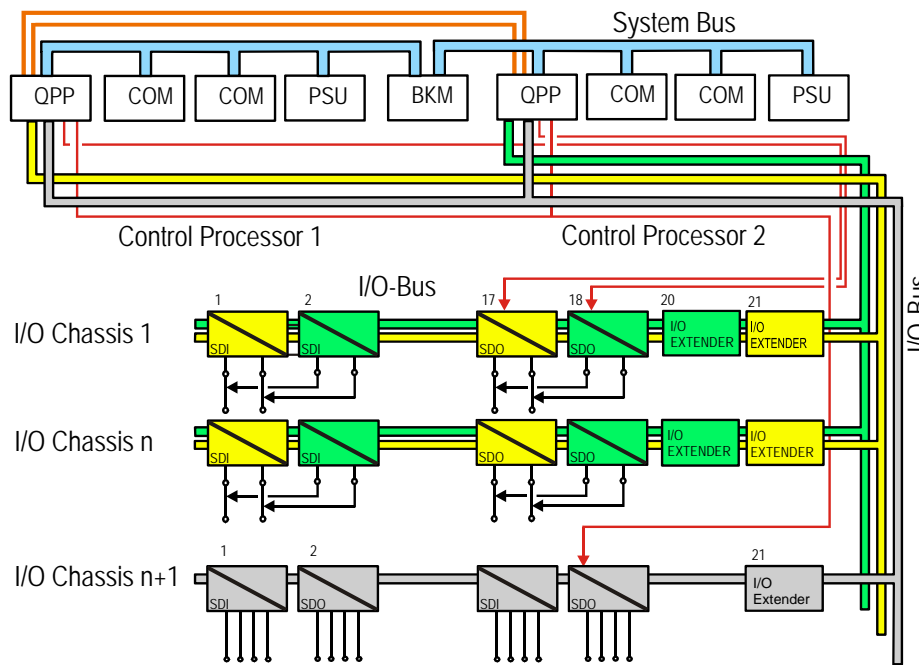
**Figure 18 — Redundant Controller, redundant IO configuration**

**Redundant Controller with redundant and non-redundant IO**

This Safety Manager architecture has a redundant Controller and redundant input and output (IO) modules (OR function outputs) combined with non-redundant input and output modules (see Figure 19 and Figure 20 below). This architecture can be applied up to and including SIL3.

This architecture is a mix of the described:

- Redundant Controller and non-redundant IO
- Redundant Controller and redundant IO".



**Figure 19 — Redundant Controller with redundant and non-redundant IO configuration**

### Selective watchdog

In a system with combined redundant and non redundant IO 3 watchdog lines are active:

- **WD1**  
This is the Watchdog line dedicated for Control Processor 1.
  - De-energizes upon a safety related fault in Control Processor 1 or an output module of Control Processor 1.
  - When de-energized, Control Processor 1 and the related outputs are halted.
- **WD2**  
This is the Watchdog line dedicated for Control Processor 2.
  - De-energizes upon a safety related fault in Control Processor 2 or an output module of Control Processor 2.
  - When de-energized, Control Processor 2 and the related outputs are halted.
- **WD3**  
This is the combined watchdog line, controlled by both Control Processors.
  - De-energizes upon a safety related fault in a non redundant output.
  - When de-energized, the non-redundant outputs are de-energized, but the redundant outputs and the Control Processors remain operational.

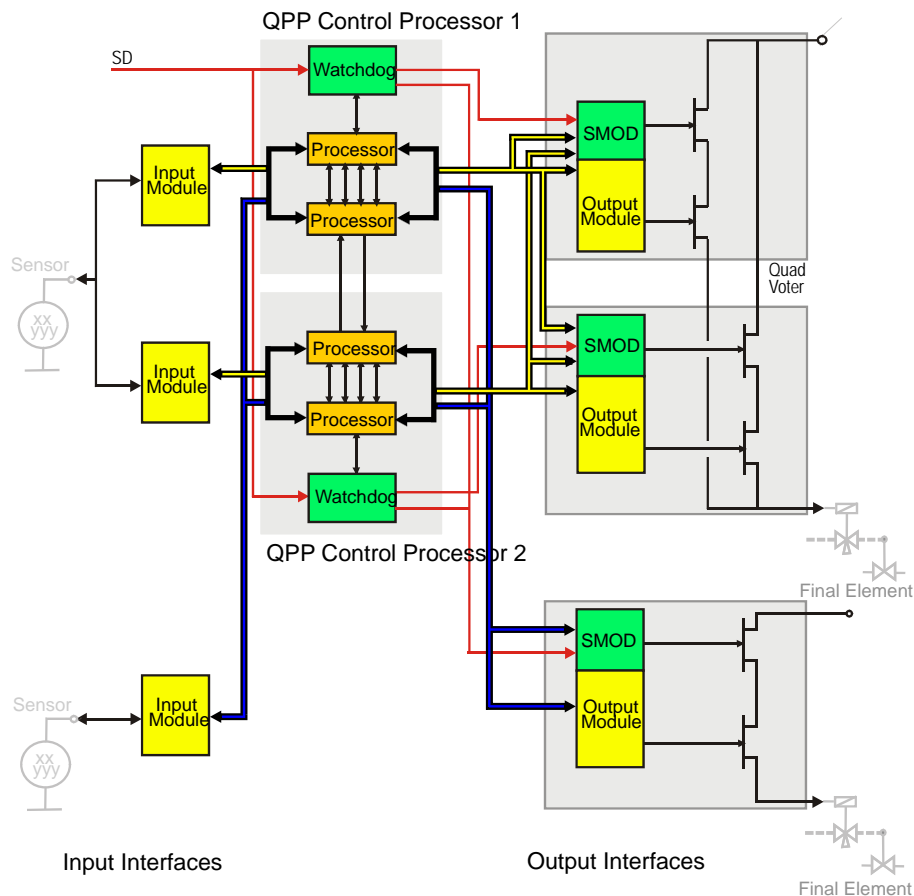


Figure 20 — Functional diagram: redundant Controller with redundant and non-redundant IO

## Network architecture

Process control and safeguarding functions in today's process industry are highly automated via computerized systems. One advantage of computerization is the possibility of gathering and exchanging digitized information of process parameters.

In order to make optimal use of this information and to be able to provide adequate information to plant operators, both the process control systems and the safeguarding systems must have communication capabilities to exchange process information.

Safety Manager can communicate with the following devices:

- Safety Station
- Other Safety Managers
- Experion PKS Server
- SOE station

This section contains a brief description of all communication architectures.

## Network components

### Time master

A time master is a system in the network that determines the network time. It has the responsibility to provide all other systems in a network with the network time.

- A time master can be a master or a slave system.
- If a system can choose from multiple time masters a hierarchical protocol is applied.

If multiple time sources are available in a network it is possible to define in Safety Manager the time source with the highest priority.

Time sources of a lower priority are ignored as long as time sources of a higher priority are available.

### Note

When a higher-level source of time synchronization becomes available again, the Safety Manager network automatically switches back to the source with the highest priority.

### Station

A Station is a human machine interface for the process control and safeguarding components connected to the network.

- A Station is a network master

Using Safety Builder as Station software for Safety Manager enables a number of functions:

- Monitoring the application.
- Monitoring the system status.
- Viewing extended diagnostics
- Clock synchronization
- Loading software
- Rebuilding a Safety Manager database on-line.
- Verifying the application as present in Safety Manager.
- Forcing and writing of variables.

### Link types

#### Point to point link

A point to point link is a physical link that interconnects one master and one slave only. Within the context of the SafeNet communication, a point to point link is the connection between a single master and a single slave.

#### Multidrop link

A multidrop link is a physical link that interconnects multiple systems (see Figure 21). Within the context of the SafeNet communication, a multidrop link is the connection of a single master with multiple slaves.

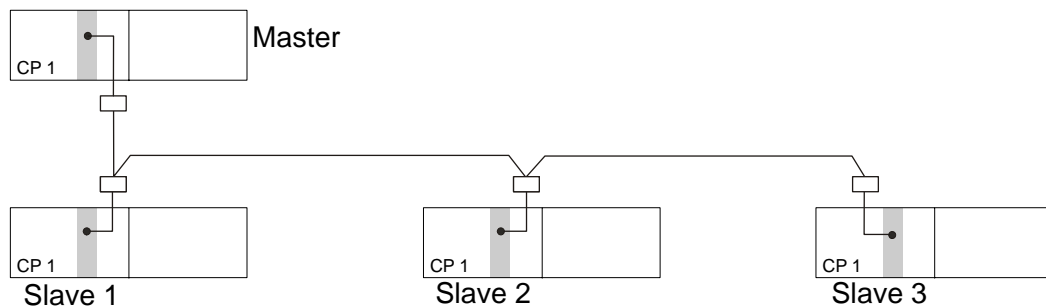


Figure 21 — Multidrop link

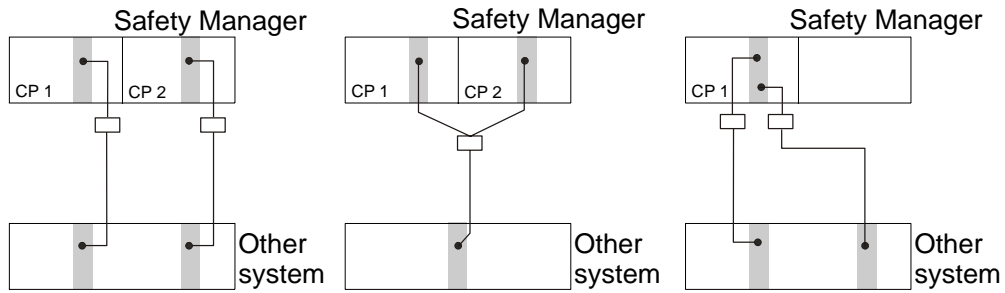
#### Redundant link

A redundant link is a communication link based on two independent physical links.

### Redundant communication with other systems

Figure 22 below shows the three options of redundant communication with other systems.

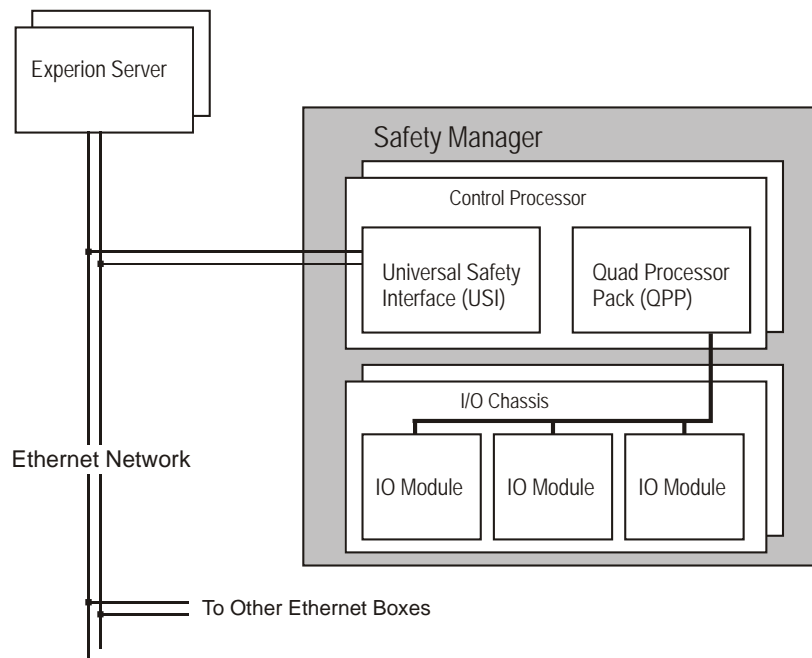
The middle configuration is also known as “connected Control Processors”, as the actual link to the other system is *not* redundant.



**Figure 22 — Example of redundant communication with other systems**

### Communication with Experion PKS

Experion PKS is directly connected to Safety Manager as shown in Figure 23. The Universal Safety Interface (USI) exchanges information with Experion PKS via Ethernet.



**Figure 23 — Experion communication**

## Time synchronization

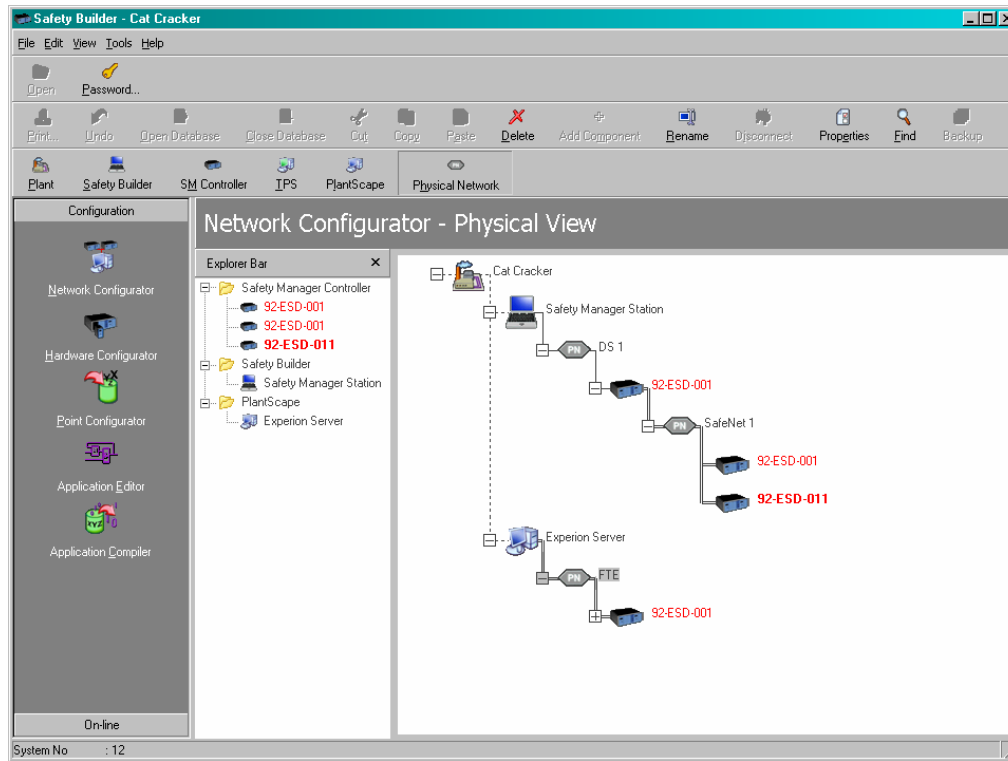
To ensure accurately time-stamped process event data, the real-time clocks of Safety Managers in a network need to be synchronized by a time master.

Safety Manager can use the following external sources to synchronize their real-time clock:

- Experion system (connected via Ethernet)
- GPS receiver via IEEE 1588 protocol
- Safety Station
- Time master
- Simple Network Time Protocol (SNTP)
- Time sync input (plant clock)

## Safety Builder

Safety Builder is a powerful software package that runs on PCs with a Microsoft Windows 2000 or Windows XP operating system. It provides a user interface with Safety Manager and supports the user in performing a number of design and maintenance tasks (see Figure 24 below).



**Figure 24 — Safety Builder function: Network Configurator**

Safety Builder's design and implementation features include:

- Intelligent user interface, presenting menu items only when applicable,
- Network Configurator,
- Hardware Configurator,
- Point Configurator,
- Application Editor,
- Database import and export,
- Automatic control program documentation,
- FLD revision control, and
- Easy loading of system software and control program into the Control Processors.

Safety Builder's maintenance support features include:

- Live viewing of Application execution,
- Detailed monitoring of process signal behavior,
- Collection of diagnostics of Safety Manager, automatically or on user demand,
- Diagnostic message storage, with user-definable browsing functions, and
- Forcing of Safety Manager input and output interfaces.

## Functional Logic Diagrams (FLDs)

Safety Manager™ safety-critical control functions (contained in the control program) are determined by the safety instrumented functions assigned to the system for the specific application. Safety Builder supports the design of the control program by the user.

The control functions are defined via graphical Functional Logic Diagrams (IEC 61131-3: Continuous Function Charts). Figure 25 below shows an example of a Functional Logic Diagram (FLD).

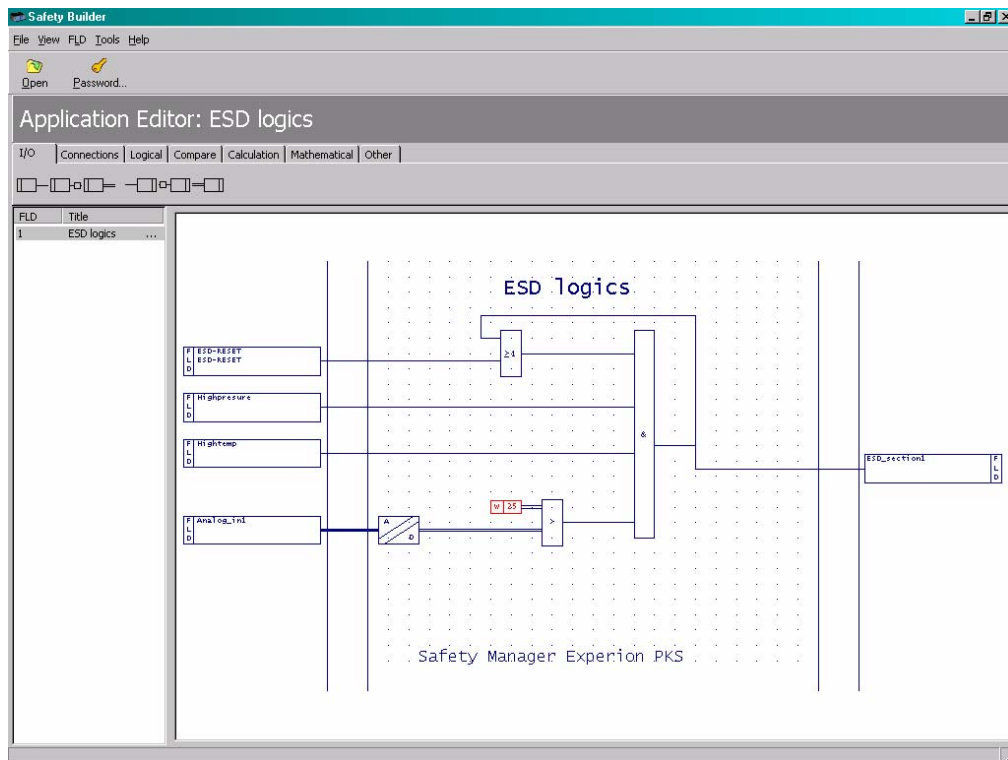


Figure 25 — Functional Logic Diagram (FLD)

An FLD is split into four main areas:

- Information area (bottom) *(on hardcopy only)*,
- Input area (left),
- Control function area (center), and
- Output area (right).

The **FLD information area**, at the bottom of the FLD, is included on printouts, and provides information to identify the Functional Logic Diagram, including revision data.

The **FLD input area**, on the left-hand side of the FLD, contains all the variables that serve as the input to the control function. Input variables may originate from the field equipment or from other computer equipment (Experion server, Safety Manager).



Special input functions are provided for:

- Diagnostic status of the Safety Manager IO interfaces,
- Status of field loops, and
- System alarm summary, e.g. temperature pre-alarm or device communication failure.

Data can be exchanged between FLDs via sheet transfer functions. This allows a structured design of complex functions across multiple diagrams.

Table 8 below lists the input functions that are available in Safety Manager functional logic diagrams, together with their source.

**Table 8 — FLD Input Functions**

Input Type	Source
Analog Input	Field Equipment
Boolean Input	Field Equipment, Process Computer, Other Safety Manager.
Numerical Input	Field Equipment, Process Computer, Other Safety Manager
Diagnostic Input	Diagnostic status of Safety Manager safe IO interfaces
Loop Status Input	Field loop status of Safety Manager IO interfaces with loop monitoring
System Alarm Input	Safety Manager controller
Sheet Transfer	Other FLDs

The **FLD control function** area, which is the central area of the FLD, contains the actual implementation of the control function. The function is realized by interconnecting predefined symbols, which provide a variety of functions including logical, numerical and time-related functions.

Apart from these standard functions, user-definable blocks are supported:

- Function Blocks  
standard FLDs for repetitive use within the control program, and
- Equation Blocks  
for tabular definition of complex functions, e.g. non-linear equations.

Table 9 below lists the control functions that are available in Safety Manager functional logic diagrams.

**Table 9 — FLD Control Functions**

Data type conversion functions	INT → SINT DINT → INT, SINT REAL → DINT, INT, SINT
Boolean functions	Boolean Constant, AND, OR, XOR, NOT, NAND, NOR, XNOR, flip-flop set and reset dominant
Arithmetical functions	Numerical Constant, AND filter, ADD, SUB, MUL, DIV, SQR, SQRT, ln(x), e <sup>x</sup>
Comparison functions	EQ, NEQ, GT, GTE, LT, LTE
Timer functions (with constant or variable time value)	Pulse, Pulse-retriggerable, Delayed-ON, Delayed-OFF, Delayed-ON memorize
Count & storage functions	Counter, Register
User-definable blocks	Equation Block Function Block

The supported data types are: Boolean, Integer ( $-2^{32} \dots 2^{32}-1$ ), Real ( $-10^{38} \dots 10^{38}$ ).

The **FLD output area**, on the right-hand side of the FLD, contains the results of the control function. These variables may be used to drive the field equipment or may be transferred to other computer equipment, e.g. a process computer or another Safety Manager.

Table 10 below lists the output functions that are available in Safety Manager functional logic diagrams, together with their destination.

**Table 10 — FLD Output Functions**

Output Type	Destination
Analog Output	Field Equipment
Boolean Output	Field Equipment, Process Computer, Other Safety Manager.
Numerical Output	Field Equipment, Process Computer, Other Safety Manager.
Sheet Transfer	Other FLDs

## Multi User: Concurrent use of Safety Builder

### **Safety Builder:**

On a Safety Station (PC) one Safety Builder can be started. Five different Safety Builders will be able to connect to one Safety Manager database via the Network Configurator program as a maximum.

### **Migrate:**

During the migration of the Safety Manager plant database, the Safety Builder plant database is opened exclusively, which means that no other Safety Builder session is able to access the plant or one of the controllers within the plant. During the Migration of the Safety Manager Controller databases, the plant is opened exclusively and all other Safety Builder sessions are locked out for this plant and all its Safety Manager Controllers. If the lock on the plant database is not possible then the Migration will not proceed.

### **Network Configurator:**

The network configuration can be modified by one Safety Builder. The plant is opened exclusively by default (with "Start configuration"). If the plant is opened in exclusive mode, all other Safety Builder sessions are locked out for this plant and all its Safety Manager Controllers, except for plant and Safety Manager Controller selection via the Network Configurator.

If exclusive open fails, then the user is informed and the plant is opened in view only mode. The plant and Safety Manager Controller selection will be possible. The "Start Configuration" function remains enabled to allow the user to retry opening the plant exclusively.

### **Hardware Configurator, Application Editor, Application Compiler:**

The controller configuration can be modified by one Safety Builder per Safety Manager Controller.

The Safety Manager plant database is opened for shared use. Other Safety Builder sessions are allowed to also open the plant in shared mode. Exclusive access to the plant by other Safety Builder sessions is denied.

The Safety Manager Controller database is opened exclusively. Access to the same controller by other Safety Builder sessions is denied.

If the lock on the plant or controller fails the program function will not proceed.

### **Point Configurator:**

The concurrent access behavior of the Point Configurator is in line with the behavior applicable for Hardware Configurator, Application Editor and Application Compiler except:

1. When a point is modified that affects a SafeNet allocation then the peer Safety Manager Controller will also be locked temporarily to prevent database inconsistencies. This lock will remain active until Point Configurator is closed. If the peer Safety Manager Controller database can not be locked, the SafeNet allocation will not be changed.
2. During point import, the plant is opened in exclusive mode and all other Safety Builder sessions are locked out for this plant and all its controllers until the import is finished. This is to prevent any database inconsistencies when SafeNet allocations are updated during import. If the plant can not be locked, the import function will not proceed.

**Controller Management: System Information, COM Statistics, Diagnostics:**

One Safety Manager Controller can be viewed by 4 Safety Builders per configured Safety Builder Ethernet connection concurrently.

The Safety Manager Controller can be viewed by 1 Safety Builder per configured Safety Builder serial connection concurrently.

Note: When a Safety Builder session is configuring the Safety Manager Controller (e.g. during download of a new application) you can not view the Safety Manager Controller with an Application Viewer installed on another Safety Station.

**Application Viewer:**

The plant is opened for shared use. Other Safety Builder sessions are allowed to also open the plant in shared mode. Exclusive access to the plant by other Safety Builder sessions is denied.

The Safety Manager Controller is opened for shared use. Other Application Viewer and Controller Management sessions can be started for the same Safety Manager Controller. Exclusive access to the Safety Manager Controller by other Safety Builder sessions is denied.

If the lock on the plant database or Safety Manager database fails the Application Viewer will not proceed.

**Controller Management: Load**

The concurrent access behavior of the Point Configurator is almost equal to the behavior applicable for the Application Viewer. Except:

During Load the Safety Manager Controller database is opened in exclusive mode and all other Safety Builder sessions for the same Safety Manager Controller are denied until Load finishes. If exclusive access to the database can not be obtained, load will not proceed.

## Multi Site

**Copy Controller:**

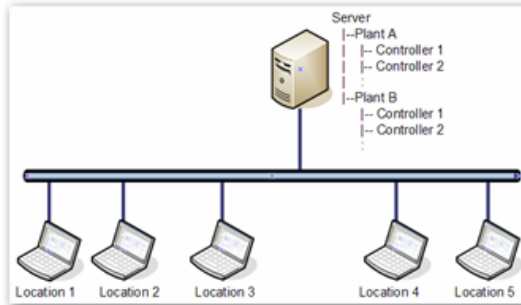
The following restrictions apply when you want to copy a Safety Manager Controller database in Safety Builder:

- Safety Manager Controllers that already have logical connections cannot be copied.
- Physical connections configured in a Safety Manager Controller database are removed
- Copy and paste of a Safety Manager Controller database back in the same Plant is not allowed.
- The Safety Manager Controller name must be unique per plant
- The Safety Manager Controller cabinet name must unique per plant.
- Safety Builder R120 is only able to copy a Safety Manager Controller from another plant.
- Safety Builder R120 is only able to copy a Safety Manager from the same software release.
- Copying a Safety Manager Controller can not be undone. (the controller can always be deleted afterwards)

Following table described the possible copy controller scenarios.

**SM R120 copy controller scenarios**

Plant & Controller databases are located on a file server where all PC's have access to



Scenario	Location	Plant	Controller	Action	Plant	Controller	Result	Comment
1	1	A	1	Configure	-	-	OK	
	1	A	2	Configure	-	-	OK	
	1	B	1	Configure	-	-	OK	
	1	B	2	Configure	-	-	OK	
2	1	A	1	Configure	-	-	OK	
	1	A	2	Configure	-	-	OK	
	2	B	1	Configure	-	-	OK	
	2	B	2	Configure	-	-	OK	
3	1	A	1	Configure	-	-	OK	
	1	A	2	Configure	-	-	OK	
	2	B	1	Is Copied from	A	1	OK	
	2	B	2	Is Copied from	A	2	OK	
4	1	A	1	Configure	-	-	OK	
	1	B	1	Configure	-	-	OK	
	2	A	2	Is Copied from	B	1	OK	
	2	B	2	Is Copied from	A	1	OK	
	3	A	3	Is Copied from	B	1	Failed	Has previously been copied
	3	B	3	Is Copied from	A	1	Failed	Has previously been copied
6	1	A	1	Configure	-	-	OK	
	2	A	2	Is Copied from	A	1	OK	Only Controller node copied, No content
7	1	A	1	Configure	-	-	OK	
	2	B	1	Is Copied from	A	1	OK	
	2	A	2	Is Copied from	B	1	Failed	Has previously been copied
8	1	A	1	Configure	-	-	OK	Create a "template"
	2	B	1	Is Copied from	A	1	OK	
	3	C	1	Is Copied from	A	1	OK	
	4	D	1	Is Copied from	A	1	OK	
	1	E	1	Is Copied from	A	1	OK	
	1	E	2	Is Copied from	B	1	Failed	Has previously been copied
	1	E	3	Is Copied from	C	1	Failed	Has previously been copied
	1	E	4	Is Copied from	D	1	Failed	Has previously been copied

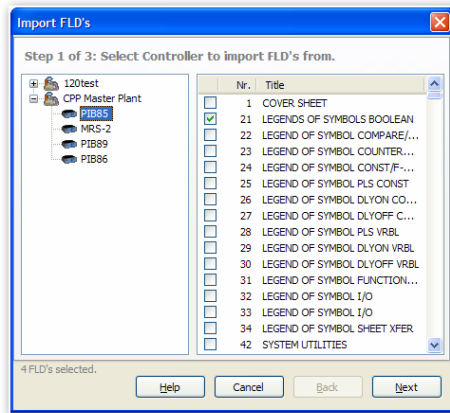
As can be seen: copy controller from another plant is possible. Copy controller within one plant is not possible.

**Bulk copy:**

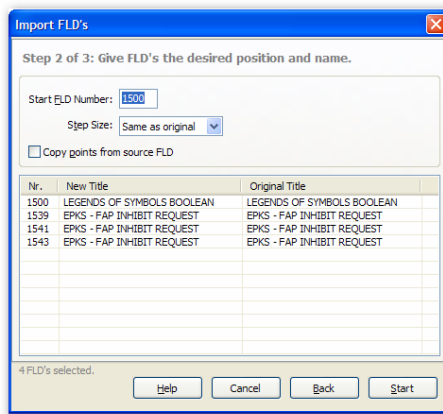
Safety Manager R120.4 supports bulk copy of Safety Manager Controller applications from any plant. This allows for easy configuration of multiple similar controllers and limits the possibility of human errors during the application design. By default, all point data will be copied.

Copy multiple FLD's from another Safety Manager Controllers with the import wizard in an easy 3-step procedure:

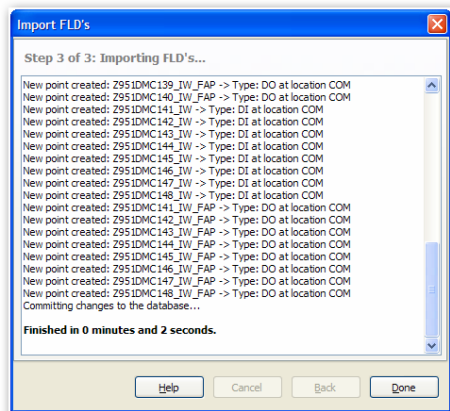
Select the Safety Manager Controller to import FLD's from.



Define the FLD's desired position and name.



Import the FLD's



**Bulk rename:**

Safety Manager R120.4 supports bulk rename of Safety Manager Controller applications from any plant. This allows for easy bulk renaming of tagnumbers in a Safety Manager Controller database and limits the possibility of human errors during the application design.

Use the extended function of the import: "Rename of I/O Point tagnumber" to change tagnumbers of IO points on newly imported FLD's.

PointType	TagNumber	NewTagNumber	Lo
DO	Z951DMC104_IW_FAP	Z951DMC104_IW_Change	C
DO	Z951DMC105_IW_FAP	Delete	C
DO	Z951DMC106_IW_FAP		C

## Safety Manager Diagnostics

Safety Manager™ continuous self-tests enable the system to collect valuable information on the diagnostic status of its own hardware and the field equipment. The system uses this information to ensure uninterrupted *functional safety* of the plant. In addition, the system provides the diagnostic information to the user, via the diagnostic displays of Safety Builder. Through its diagnostics, Safety Manager supports maintenance engineers in allocating and resolving failures effectively, thus reducing the Mean Time To Repair (MTTR) and minimizing the risk of a plant trip.

## Flash-Memory Operation

Safety Manager™ uses flash memory to store all system-related software. This feature combines the flexibility of RAM with the data integrity of EPROM. It allows direct downloading of the system firmware, system software, application software, and system configuration from Safety Station (with Safety Builder running) to Safety Manager. This functionality is in full accordance with TÜV approvals, and is protected against unauthorized use by a password and key-lock protection mechanism.

Another advantage of flash-memory operation is that it reduces the time to do an On-Line Modification (OLM). After the first full download, only the changes will be loaded after a modification. This should not be confused with the 'download changes' option that other vendors are offering. Safety Manager allows you to download unlimited changes, even in a running installation while continuing plant operation in a safe manner.

## On-Line Modification

On-Line Modification (OLM) is a TÜV-approved Safety Manager™ option that is supported by Safety Manager configurations with redundant Controller. It enables modification of the application software, system software and Safety Manager hardware configuration, while maintaining the system's critical control function for the operational plant. This means that the system can be upgraded without the need of a plant shutdown. During on-line modification, the changes are carried out in one Control Processor at a time. Meanwhile, the other Control Processor continues to monitor the process. The system will always perform a compatibility check across the control program in order to guarantee a safe changeover from the old control function to the new one. It will also report the numbers of the functional logic diagrams (FLDs) that have been changed, which complies with the 'verification requirements' of IEC 61508 and ANSI/ISA S84.01.

## Hot-swap of Safety Manager Controller Modules

The user is able to exchange "not safety-related" Safety Manager Controller modules while the Safety Manager Controller continues operation. The communication module type USI-0001 and the battery and key switch module type BKM-0001 can be swapped on-line without stopping the affected control processor

## Self Educating Safety Manager Controller Modules

If required, the user can replace the QPP-0001, QPP-0002 and / or the USI-0001 with a spare module. If the other control processor is running, the spare modules inserted will automatically be updated with all the software (including embedded software), which is already used in the running Control Processor. Note: If the controller number in the spare QPP is equal to the already running controller number, the update will not take place: reset the controller number first.

## Power System

Reliability of process data depends on the reliability of **all** related hardware of the process loop, i.e. sensing device, IO wiring, IO channel hardware and the required power supply voltages. Where possible, Safety Manager™ provides the supply power to the electronics of the entire loop, including the field instrumentation. The result is a fully integrated solution for reliable (safety) data gathering and related safeguarding actions, with the following advanced features:

- Electronically short-circuit proof,
- Loop-monitoring for short-circuiting and lead breakage, and
- Checking of the operational band of analog transmitters.

Where other systems require linkage of several externally mounted parts to establish the entire data collection chain, Safety Manager solution offers the fully integrated and tested loop approach as demanded by IEC 61508 and ANSI/ISA S84.01.



## Write Protection

To maintain safe and reliable operation of Safety Manager™, the system does not allow direct write access to its hardwired IO via communication links. Write requests, which are received via the Universal Safety Interface (USI) (serial and or Ethernet communication), are passed on to the Safety Manager control program via dedicated boolean and numerical inputs. The inputs appear in the input area of the Functional Logic Diagrams, where the conditions for write access have been defined.

## IO Signal Forcing

For maintenance reasons, it may be desirable to force an input or an output signal to a certain fixed state, e.g. when exchanging a defective input sensor. This allows the sensor to be exchanged without affecting the continuation of the production. During the exchange, the applicable input is forced to its normal operational state. While being desirable in some situations, forcing a signal to a specific, fixed value may also create a potentially hazardous condition.

Safety Manager™ provides a force function which supports maintenance personnel in applying forces consciously. It only allows forcing of signals that were specifically selected during the system design. During operation, the system is protected against unauthorized forces via a key switch. Forcing of Safety Manager signals is only possible via Safety Builder, using a password-protected software function. All forcing actions are included in Safety Manager event reports for trace ability purposes.

## Serial Communication with Process Computer Systems

Safety Manager supports the exchange of application and diagnostic data with DCS systems or other equipment via serial communication links, using the non-proprietary Modbus RTU communication protocol. All point data available within the Safety Manager application can be made available via Modbus RTU. Data written to the Safety Manager Controller via Modbus RTU is available in the Safety Manager application via digital and numerical input variables, which allow the user to define the conditions of use in the safety application.

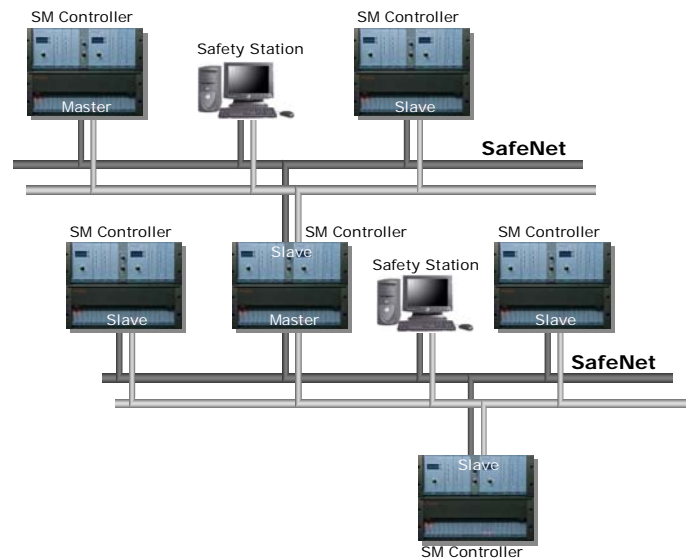
## Safety Manager SafeNet

Safety Manager™ supports Distributed Safety Solutions (DSS™) through its extensive networking capabilities. Safety Manager networks provide the means to decentralize process safeguarding with central process monitoring and control capabilities.

In a DSS network, multiple Safety Managers are interconnected via dedicated Ethernet (or serial) communication links. Both point-to-point and multidrop networks are supported.

For optimum availability of the communication, the redundant Safety Manager configurations require the use of redundant communication links.

The communication is based on the Honeywell proprietary, TÜV-approved SIL 4 SafeNet communication protocol. This protocol includes a high level of error detection and recovery, which makes it suitable for exchanging safety-related information while maintaining optimum availability. The network is also used to route diagnostic data to central operator stations and maintenance workstations.



Communication within Safety Manager networks is based on the master-slave concept. In this concept, the master system is responsible for all communication activities. It initiates requests for data from the slave systems, and sends data to the slaves.

Safety Manager networks also support communication server systems. These are Safety Managers that are interconnected between the communicating master and slave system(s). Their task is to route the data that is exchanged between master and slave(s).

The DSS concept supports safety solutions in line with the plant design, with every independent process unit being safeguarded by a separate Safety Manager. This minimizes the risk of nuisance plant trips during unit maintenance.

Safety Manager supports SafeNet communication via Ethernet, RS232, RS485 and Fiber optic. This allows easy integration of fail-safe networking via third-party equipment (black channel), enabling the use of existing media, equipment, and cabling to exchange safety-critical Safety Manager data, e.g. using public telephone lines, satellites, or radio links. This TÜV-approved function provides flexible solutions for FPSOs, pipelines, and other remote system applications. It is completely embedded into the Safety Manager design, and no additional effort is needed to configure this type of communication.

Safety Manager SafeNet network supports up to 1024 Safety Manager Controllers in one Plant. A maximum of 63 Safety Manager Controllers is supported per Safety Manager segment.  
The maximum number of Safety Manager Controllers per plant can be calculated using the following formula

$$n + n \times (63 - n) = MaxSM ,$$

with:  $n = MasterSMControllers$

and:  $2 \leq n \leq 63$

If  $n = 1$  than  $MaxSM = 63$

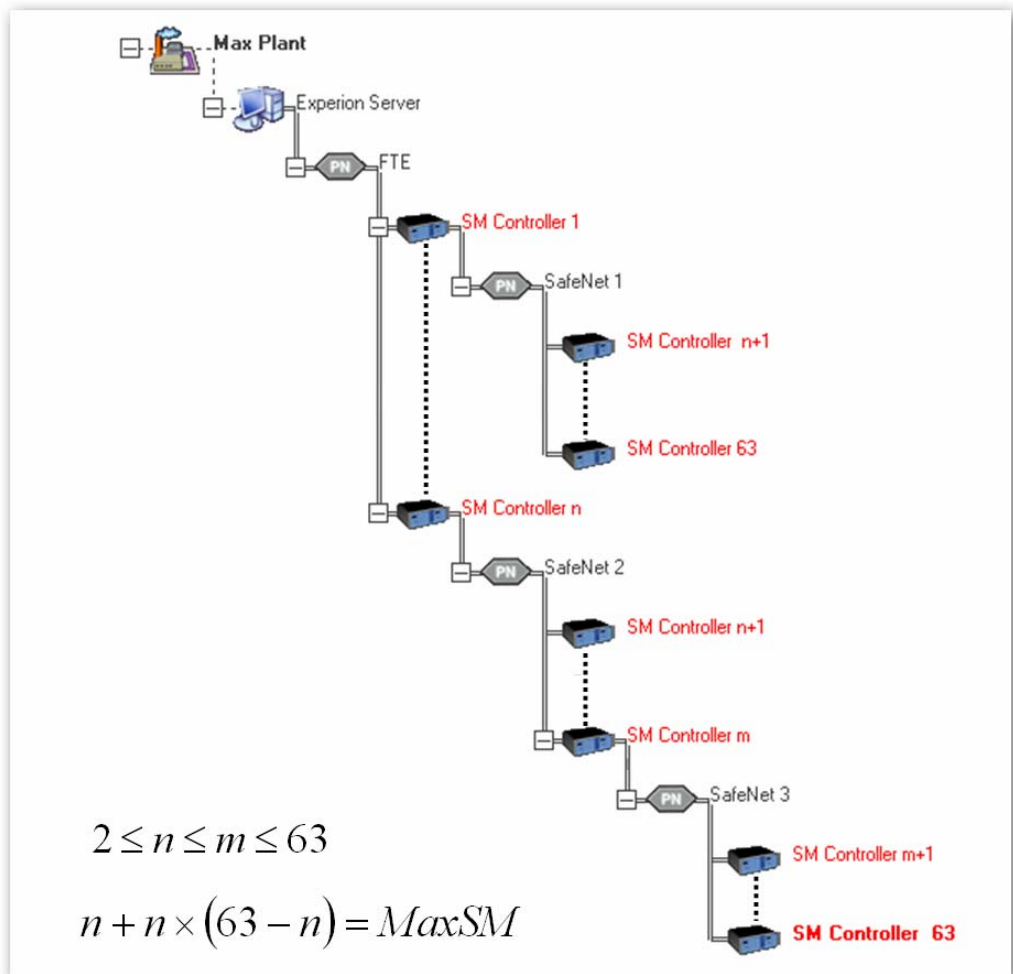


Figure 26 - Typical SafeNet Network

## Physical Characteristics

Safety Manager™ consist of:

- SM controller,
- SM IO, and
- Field interface

Figure 27 shows the components of Safety Manager.

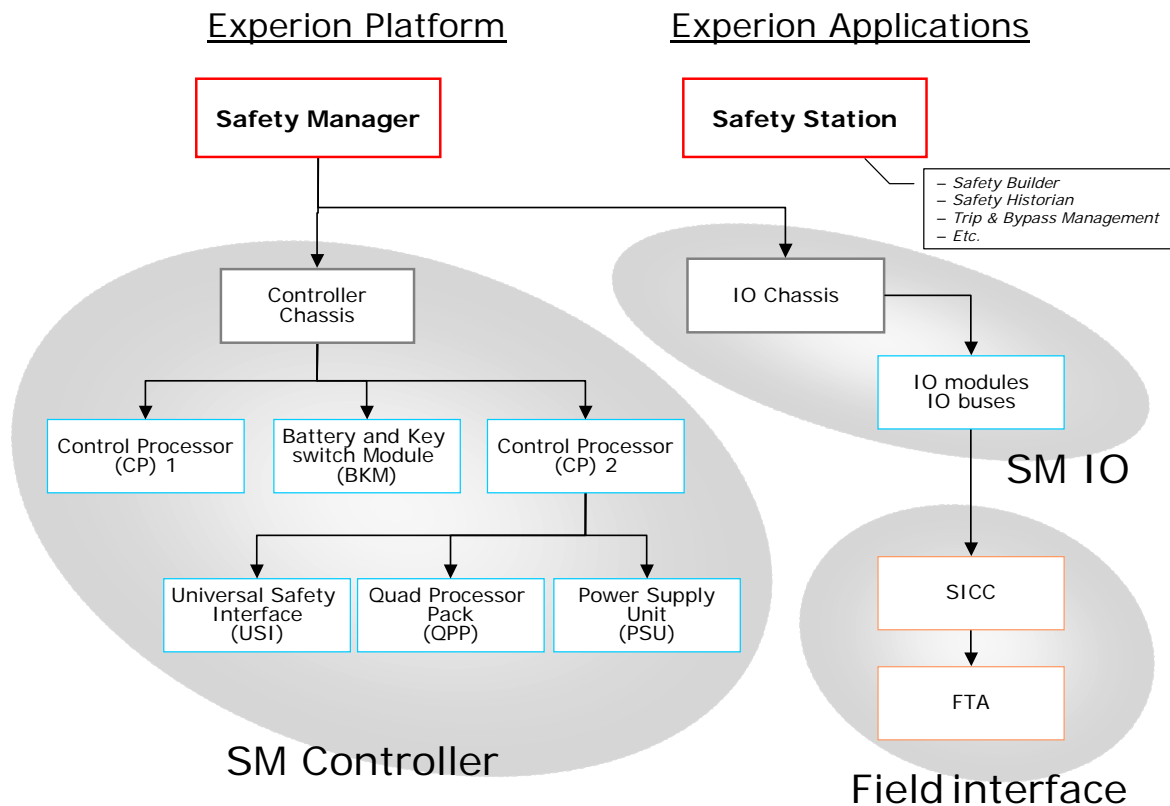


Figure 27— Safety Manager Components

### SM controller components

The SM Controller consists of:

- Controller chassis
- Control Processor (one or two)
- Battery & Key switch Module

## Controller chassis

The SM controller is placed in the **CP chassis** (CPCHAS). The **CP backplane** (CPB), which is integrated into the CP chassis, has the following functions:

- A 32 bit Redundant System Bus between the Control Processors
- 5 Vdc and WD distribution to the IO chassis,
- IO bus connections,
- Communication connections,
- Incoming 24Vdc power for both Control Processors,
- ESD input, and
- Three common system inputs.

Figure 28 shows also that the CP chassis is covered at the back.

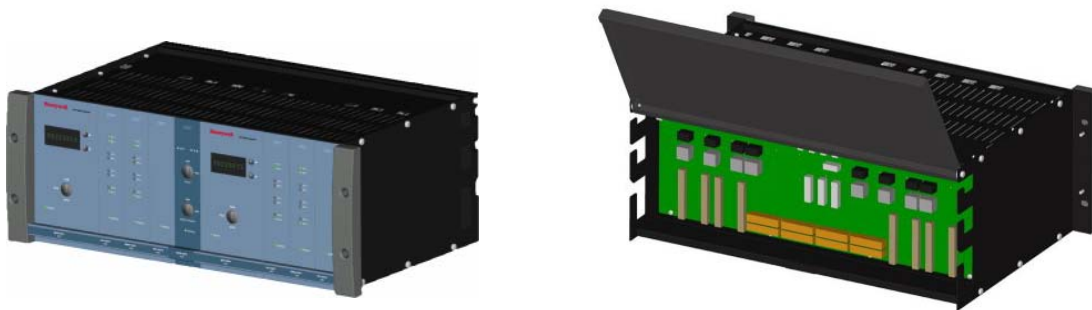


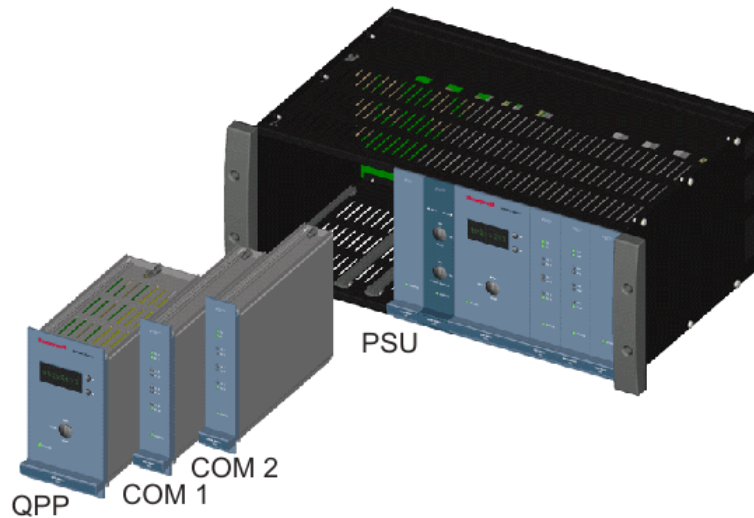
Figure 28 — Front and rear view of the CP chassis

## Control Processor

The Control Processor (CP) is the heart of the SM controller. It is a modular microprocessor system specifically designed for safety-critical applications and can be tailored to the requirements of many applications. The main Control Processor modules are:

- Quad Processor Pack (QPP)
- Universal Safety Interface (USI)
- Power Supply Unit (PSU)

The Control Processor modules are constructed on a European standard size instrument card. The height of the front panel of the modules is 4 HE (4U), their width is 8 TE (8 HP) (USI, SMM, PSU and BKM module), and the QPP module is 16 TE wide. The Control Processor modules are placed in the CP Chassis (19" chassis), which are generally located in the top section of the cabinet.



**Figure 29 — Control Processor modules**

### **Quad Processor Pack (QPP)**

The QPP reads the process inputs and executes the application program created with the Application Editor. The results of the control program are transmitted to the output interfaces. In Safety Manager configurations with a redundant Controller, both QPPs synchronize their operation through a dedicated redundant communication channel, integrated in the Controller backplane. Through continuous testing of Safety Manager hardware and software integrity, the QPP ensures safe operation as well as extensive diagnostics.

The QPP contains a watchdog circuit. It automatically monitors the correct functioning and the operating conditions of the QPP safety processors. The watchdog circuits include the following functions:

- A unique feature of the Safety Manager watchdog is that it verifies if the processor executes its tasks within the defined cycle time.
- The monitored operating conditions include the data integrity check of the processor memory and the voltage range check of the supply power (under voltage and over voltage).
- Deactivate the safety-critical outputs of Safety Manager, regardless of the QPP status, whenever required.

The QPP is also equipped with the following items:

- 4 bus drivers to drive the IO chassis
- A status LED
- Display to show time, date, system information, system status and diagnostics
- Key switch

### Universal Safety Interface (USI)

USI is a communication module with universal safety interfaces. Safety Manager™ uses the USI to exchange information with other equipment. The USI is equipped with 2 Ethernet interfaces and 2 serial interfaces, for either RS232 or RS485 (configurable). A Control Processor can accommodate two USI modules with a maximum of eight external communication links.

**Table 11 — Safety Manager Communication Interfaces**

Equipment	Physical Interface	Protocol
Process Servers	Experion	High Speed Ethernet (HSE)
	UCN (TPS Network)	UCN Token Bus
	PlantScape	Ethernet
Safety Station	RS-232, RS-485, HSE	Development System
HMI, DCS	RS232, RS485	Modbus RTU Slave
Other Safety Manager	Ethernet, RS-485, Fiber Optic	SafeNet

All communication interfaces are galvanically isolated. If Safety Manager configuration contains redundant Control Processors, the system supports redundant communication. Each Control Processor then has its dedicated connection to the communication peer system.

### Power Supply Unit (PSU)

The PSU is galvanically isolated and supplies 5Vdc power to the SM controller, SM IO and communication FTA.

### Battery & Key switch Module (BKM)

The Battery and Key switch Module (BKM) contains:

- a redundant backup battery, to retain a number of system parameters during power outage,
- Reset and Force Enable key switches with redundant contacts.

Only one BKM is required in a Controller chassis. It serves both redundant and non-redundant configurations.

## SM IO components

Safety Manager™ IO consists of:

- IO chassis
- IO bus
- IO modules

### IO chassis

The **IO chassis** (IOCHAS) is one mechanical housing, which contains the horizontal IOBus back plane, the IO module housing, the IO backplane, a cable tray, and is covered at the back.

The **IO chassis** containing 18 IO slots. It also contains an IO backplane, IO extenders and IO busses. IO chassis are available for redundant and non-redundant IO.

The **IO backplane** (IOB) consists of a multi-layer PCB, with one layer being an earth plane to improve EMC/RFI immunity. The front side of the IO backplane contains the Eurocard connectors to install the IO modules and the IO extender module(s). At the back, the IO backplane provides female connectors for the system interconnection cables (SICs), which also connect to the FTA modules. The backside also provides programming connectors, which allow the IO interfaces to be tailored to the specific signal characteristics of the field equipment, e.g. digital line-monitored output impedance, Low, Medium, High or Spare.

Integrated in the IO backplane is the internal and external power distribution to the IO modules,

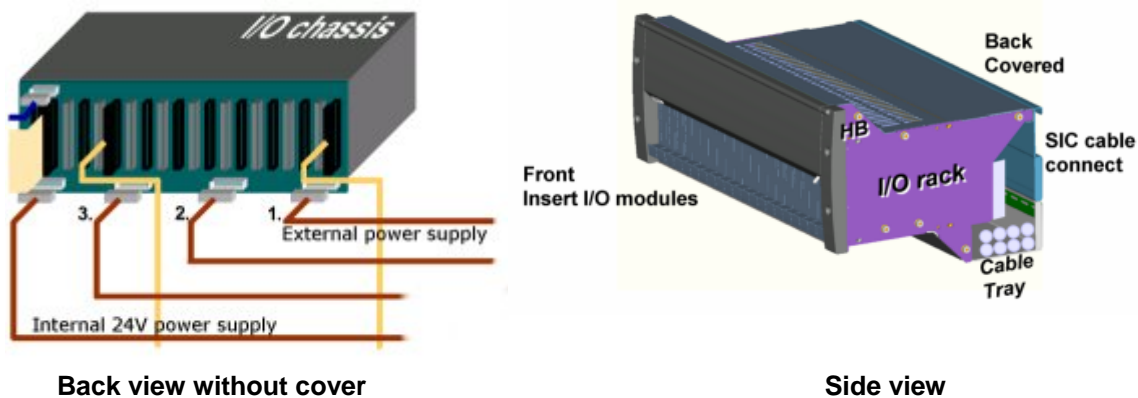


Figure 30 — Back and side view Safety Manager IO chassis

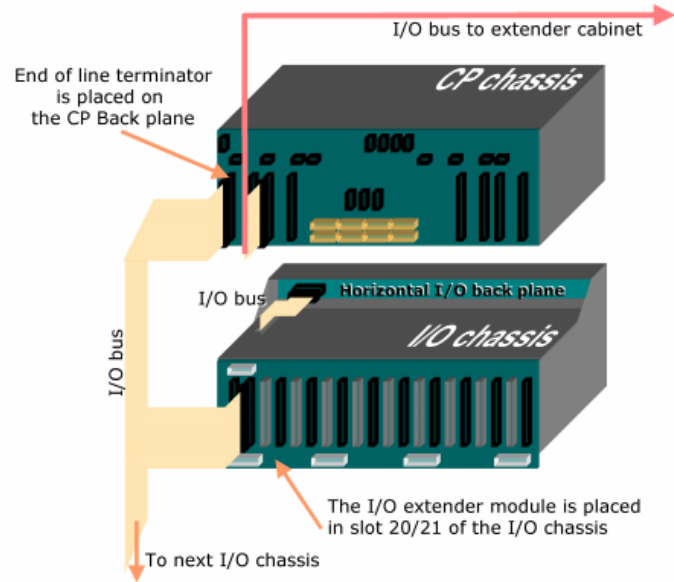
### IO bus

The Control Processor controls IO (located in the IO chassis) via an IO bus. An IO extender (located in the IO chassis) communicates with the individual IO modules via a horizontal IO bus.

The Control Processor interfaces with the IO system through a **IO bus**, which is a flatcable that runs vertically in the cabinet. The IO-bus is controlled by the **IO Bus Driver** function, which is part of the QPP module.



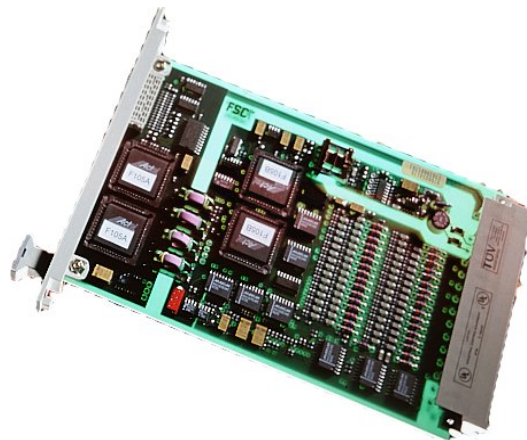
Each of the IO chassis contains a **IO extender IO-0001** module, which connects to the IO-bus. The IO extender module drives the **Horizontal IO Bus**, which relays the signals from the IO-bus to the IO modules via a flatcable. The Horizontal IO bus back plane is located on top of each IO bus chassis. The Horizontal IO bus and the flatcables of the IO modules are covered with a sheet steel cover which provides optimum EMC/RFI immunity. The cover plate contains a paper strip which holds the relevant process tagging for signal identification.



**Figure 31 — Back view of typical Safety Manager with redundant Controller and a IO chassis**

### IO modules

The **IO modules** are constructed on a European standard-size instrument card. The height of the front panel of the modules is 3 HE (3U), their width is 4 TE (4 HP). A total of 18 IO modules can be placed per IO chassis. All IO modules are equipped with standard 32-pin DIN 41612F connectors. All IO chassis are provided with an IO backplane, which contains matching 32-pin connectors with key coding to prevent mis-insertion of the IO modules.



**Figure 32 — Example of the high density SAI-1620m module**

Safety Manager provides an extensive selection of digital and analog input and output interfaces, with different characteristics, to meet the demands of a wide range of field equipment. Table 12 on the next page lists the input and output interfaces available with Safety Manager.

**Table 12 — Safety Manager input and output interfaces**

Interface	Properties
Digital Input	24 Vdc, 48 Vdc and 110 Vdc 24 Vdc (loop-monitored) 120-230 Vac Class I, Division 2, Groups ABCD; Class II, Division 2, Groups FG Class [Eex ia] IIC intrinsically safe (Through external devices)
Digital Output	24 Vdc, 48 Vdc, 60 Vdc and 110 Vdc 24 Vdc, 48 Vdc (loop-monitored) 120-230 Vac Dry contact outputs Class [Eex ia] IIC intrinsically safe (Through external devices)
Analog Input	0-20 mA, 4-20 mA, 0-25mA 0-20 mA and 4-20 mA with HART support (Through external devices) 0-5 V, 1-5 V, 0-10 V and 2-10 V Class I, Division 2, Groups ABCD; Class II, Division 2, Groups FG Resistance Temperature Device (RTD) (Through external devices) Thermocouple, types E, J, K and T (Through external devices)
Analog Output	0-20 mA and 4-20 mA Class I, Division 2, Groups ABCD; Class II, Division 2, Groups FG

All Safety Manager IO modules are galvanically or optically isolated between external and internal power supply. Safe IO modules can be used for safety loops up to and including SIL3.  
Safe modules can also be used for control applications, offering the benefits of Safety Manager diagnostic and fault-reporting functions with or without automatically isolating faults. (Automatic isolation of faults is configurable.)

## Field interface

Safety Manager™ uses Field Terminal Assemblies (FTA) and internal cabling to connect IO and communication channels to field terminals.

### IO FTA

An FTA module for IO converts input field signals to values appropriate for the Safety Manager input module that is used, or Safety Manager output module signals to values that can be used in the field. To enable this conversion, FTAs can be used in combination with input converter modules or output converter modules.

FTA modules are 70 mm (2.76 in) or 109 mm (4.29in) wide, and their length varies between 90 mm and 300 mm (3.54 and 11.81 in), depending on the FTA type. The modules are mounted on standard DIN EN rails (TS32 or TS35 x 7.5).

An FTA may contain electronic circuitry to convert standard Safety Manager signals to specific signals with characteristics required by field equipment. For the connection to the Safety Manager IO modules a standard system interconnection cable FS-SIC-0001 is used for all FTAs. The field cables are connected to terminals. (see Figure 33).

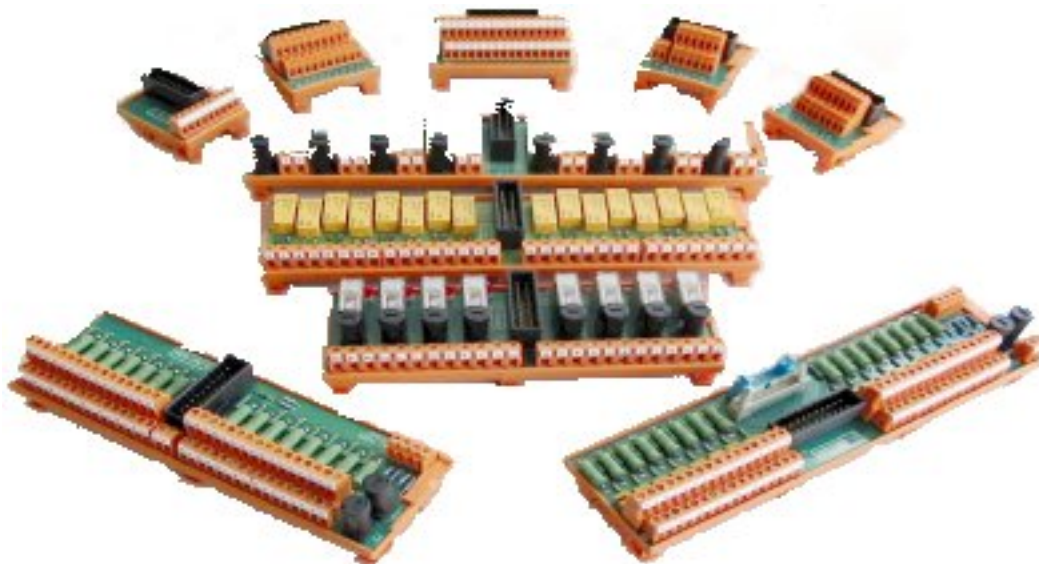


Figure 33 — Overview of some terminal type FTA's

### **Communication FTA**

An FTA for communication purposes is wired to a channel of the Universal Safety Interface (USI).

Two types of communication FTAs exist:

- Ethernet FTA, UCOM-HSE or SDW-550 EC providing:
  - auto-switching 10Mb/100Mb Ethernet interface.
- general purpose FTA, DCOM-232-485 providing:
  - RS232
  - RS485

### **Cabling**

System Interconnection Cables (SIC) connect field signals to IO modules. Depending on the type of SIC cable, an FTA is required to establish the connection.

## Safety Services

### System services

Safety Manager™ based safety solutions are supported from Honeywell locations worldwide. To guarantee optimum system operation and performance throughout the system lifecycle, a comprehensive services portfolio is available that helps users optimize their safety strategy. Users can choose between various support options and service contracts, which enable them to customize their service requirements:

- Software Enhancement & Support Program (SESP),
- Site Support Services,
- Spare Parts Management,
- Emergency Technical Assistance, and
- Software Updates.

Safety Manager service contracts are more than just emergency backups — they add value to the safety solution, and enhance the performance and reliability of the safeguarded process:

- Guaranteed fast response to service requests,
- Reduced hourly rates for on-site servicing,
- Expert assistance during all stages of the system lifecycle,
- Support from locations around the world,
- Continuous availability of the latest software, and
- Compliance with IEC 61508 and ANSI/ISA S84.01.

### Training

Various training programs are available which enable users to become familiar with Safety Manager™. The training courses can be given at Honeywell locations, but they can also be organized on site, if required. In addition to the standard programs below, there is also the option of having a training course tailored to the customer's specific needs. This allows extra options to be added to the training, or it can be used to focus on specific segments.

The following standard training courses are available:

- Managers Overview Course,
- Introduction to IEC 61508,
- Safety Manager Implementation Course,
- Safety Manager Maintenance Course
- Safety Manager On-Line Modification Course
- Safety Manager Advanced Course
- Safety Manager Total Package Course

## Safety Consultancy

In addition to a services and training portfolio, a full range of safety consultancy services that help customers manage all their safety and risk management needs also backs Safety Manager based solutions. The Honeywell safety experts have the expertise and experience to guide and assist end users in the implementation of new international safety standards such as IEC 61508 and ANSI/ISA S84.01.

Honeywell can help customers:








- Formulate and manage their safety lifecycle model,
- Carry out hazard and risk analysis and definition of safety functions,
- Define safety requirements,
- Provide expertise on failure rate assessments,
- Perform safety and availability calculations, and
- Provide advice on optimal proof test intervals.

## Standards Compliance

Since functional safety is at the core of the Safety Manager™ design, the system will be certified for use in safety applications all around the world. The predecessor of Safety Manager, Fail Safe Controller (FSC) was developed specifically to comply with the strict German DIN/VDE functional safety standards, and has been certified by TÜV for use in AK 1 to 6 applications. FSC was also the first safety system to obtain certification in the United States for the UL 1998 and ANSI/ISA S84.01 standards.

FSC based and Safety Manager based safety solutions and related Honeywell services can also help you comply with the new ANSI/ISA S84.01 standard for safety-instrumented systems up to and including Safety Integrity Level (SIL) 3, as well as the new international standard IEC 61508 for functional safety. These new standards address the management of safety throughout the entire life cycle of your plant.

### Certifications and Compliance with International Standards and Safety Codes

	<p><b>TÜV Bayern (Germany)</b> — Certified to fulfill the requirements of "Class 6" (AK6) safety equipment as defined in the following documents:                  DIN V VDE 19250, DIN V VDE 0801 incl. amendment A1, DIN VDE 0110, DIN VDE 0116, DIN VDE 0160 incl. amendment A1, DIN EN 54-2, DIN VDE 0883-1, DIN IEC 68, IEC 61131-2.</p>
	<p><b>Instrument Society of America (ISA)</b> — Certified to fulfill the requirements laid down in ANSI/ISA S84.01.</p>
	<p><b>Canadian Standards Association (CSA)</b> — Complies with the requirements of the following standards:                  CSA Standard C22.2 No. 0-M982 General Requirements – Canadian Electrical Code, Part II;                  CSA Standard C22.2 No. 142-M1987 for Process Control Equipment.</p>
	<p><b>Underwriters Laboratories (UL)</b> — Certified to fulfill the requirements of:                  UL 508, UL 991, UL 1998 and ANSI/ISA S84.01.</p>
	<p><b>Factory Mutual (FM)</b> — Certified to fulfill the requirements of FM 3611 (non-incendive field wiring circuits for selected modules).</p>
	<p><b>Safety Manager Functional Logic Diagrams</b> for Control Program design are compliant with IEC 61131-3.</p> <p>The <b>design and development of Safety Manager</b> are compliant with IEC 61508:1999, Parts 1-7 (as certified by TÜV).</p>
	<p><b>CE compliance</b> — Complies with CE directives 89/336/EEC (EMC) and 73/23/EEC (Low Voltage).</p>

## Specifications

The following specifications apply to Safety Manager™ systems and modules mounted in a standard Safety Manager cabinet:

### Safety Manager SFF values

SFF (Safe Failure Fraction)	≥ 99%
-----------------------------	-------

### Safety Manager Environmental Conditions

Operating Temperature:	−5°C to 70°C (14°F to 158°F), ambient <sup>(1)</sup>
Storage Temperature:	−25°C to +80°C (−13°F to +176°F)
Relative Humidity:	5% to 95%, non-condensing
Vibration, Sinusoidal:	IEC 60068-2-6; 1 G at 57 Hz to 150 Hz; 10 Hz to 57 Hz: 0.075mm
Shock:	IEC 60068-2-27; 15 G for 11 ms, 3 axes
Electrostatic Discharge:	IEC 61000-4-2, Level 4 (15 kV)
Conducted Susceptibility:	IEC 61000-4-4, Level 3, Fast Transient/Burst IEC 61000-4-5, Level 3, Surge Withstand IEC 61000-4-6, Level 3, Conducted Field
Rated Susceptibility:	IEC 61000-4-3, Level 3
Conducted Emissions:	Measured per CISPR 11 & CISPR 22
Rated Emissions:	Measured per CISPR 11 & CISPR 22

<sup>(1)</sup> "Ambient" refers to the air temperature measured in the Safety Manager Control Processor chassis (CPCHAS-0001).

### Safety Manager Mechanical Specifications

Safety Manager cabinet dimensions (Rittal, model TS 8):	2000 x 800 x 800 mm (H x W x D) 78¾ x 31½ x 31½ in (H x W x D)
Chassis size (incl. horizontal bus):	height: 4 HE (4U), width: 84 TE (84 HP)
Module sizes:	
– IO modules height and width	height: 3 HE (4U), width: 4 TE (4 HP)
– QPP module	height: 4 HE (3U), width: 16 TE (16 HP)
– USI, SMM, BKM, PSU modules	height: 4 HE (3U), width: 8 TE (8 HP)
– Eurocard dimensions	100 x 160 mm (3.94 x 6.30 in)

### Safety Manager Electrical Specifications

Supply voltages:	24 Vdc: +30% / −15% 48 Vdc: +15% / −15% 110 Vdc: +25% / −15% 220 Vdc: +10% / −15%
------------------	--



## Model Numbers

### Identification

All non-conformal coated products have type numbers starting with 'FS-'. All conformal-coated products have type numbers starting with 'FC-'. E.g. FS-QPP-0001

In this way materials related to Safety Manager can always be recognized directly in overall Honeywell SMS product listings.

### SM Controller Modules

#### SM Controller Modules

Description	Model Number
Quad Processor Pack (QPP)	QPP-0001
Enhanced Performance Quad Processor Pack (QPP)	QPP-0002
Universal Interface Module (USI)	USI-0001
Battery and Key-switch Module (BKM)	BKM-0001
24 Vdc to 5 Vdc DC/DC converter, 16 A	PSU-240516

#### Power Supply Modules

Description	Model Number
System Power supply Input 115/230VAC Output 24Vdc, 50A	FC-PSU-UNI2450
System Power supply Input 115/230VAC Output 48Vdc, 25A	FC-PSU-UNI4825
System Power supply Input 115/230VAC Output 110Vdc, 11A	FC-PSU-UNI110
24 Vdc Power Supply Unit, 45 A, input: 100-264 Vac, 230-340 Vdc	1200 S 24 P067
48 Vdc Power Supply Unit, 25 A, input: 100-264 Vac, 230-340 Vdc	1200 S 48 P067
110 Vdc Power Supply Unit, 13 A, input: 90-265Vac	SM120-13

## Analog Modules

### Analog Input Modules

Description	Model Number
Safe analog input module (4 channels)	SAI-0410
Safe high-density analog input module (24 Vdc, 16 channels)	SAI-1620m

### Analog Input Field Termination Assemblies (FTAs)

Description	Model Number
Safe input FTA (24/48/60 Vdc, 24 channels)	TSAI-0410
Safe 0(4)-20 mA analog input FTA (16 channels)	TSAI-1620m
Safe 0(4)-20 mA analog input FTA (16 channels) with HART support	TSHART-1620m

### Fire and Gas Detector Input Field Termination Assemblies (FTAs)

Description	Model Number
Safe Gas/Flame detector input FTA (24 Vdc, 16 channels)	TSGAS-1624
Safe Gas/Flame detector input FTA (24 Vdc, 16 channels) with HART interface	TSGASH-1624
Safe Fire detector input FTA (16 channels)	TSFIRE-1624

### Analog Output Modules

Description	Model Number
Safe analog output module (0(4)-20 mA, 2 channels)	SAO-0220m

### Analog Output Field Termination Assemblies (FTAs)

Description	Model Number
Safe analog output FTA (0(4)-20 mA, 2 channels)	TSAO-0220m
Safe analog output FTA (0(4)-20 mA, 2 channels) with HART interface	TSAOH-0220m

## Digital Modules

### Digital Input Modules

Description	Model Number
Safe digital input module (24 Vdc, 16 channels)	SDI-1624
Safe digital input module (48 Vdc, 16 channels)	SDI-1648
Safe line-monitored digital input module with earth fault monitor (16 ch.)	SDIL-1608

### Digital Input Field Termination Assemblies (FTAs)

Description	Model Number
Safe digital input FTA (24Vdc, 16 channels)	TSDI-1624
Safe digital input FTA (NAMUR, 16 channels)	TSDI-16UNI
Isolated passive digital input FTA (16 channels)	TIDI-1624
Safe digital input FTA with line-monitoring (16 channels)	TSDI-16UNI
Current-limited digital input FTA (24 Vdc, 16 channels)	TSDI-1624C
Safe digital input FTA (48Vdc, 16 channels)	TSDI-1648
Safe active/passive digital input FTA (115 Vac/dc, 16 channels)	TSDI-16115

### Digital Output Modules

Description	Model Number
Safe digital output module (24 Vdc, 550 mA, 8 channels)	SDO-0824
Digital output module (24 Vdc, 550 mA, 12 channels)	DO-1224
Relay output module (contacts, 10 channels)	RO-1024
Digital output module (24 Vdc, 100 mA, 16 channels)	DO-1624
Safe digital output module (110 Vdc, 325 mA, 4 channels)	SDO-04110
Safe digital output module (48 Vdc, 750 mA, 4 channels)	SDO-0448
Safe digital output module (24 Vdc, 2 A, 4 channels)	SDO-0424
Safe loop-monitored digital output module (24 Vdc, 1 A, 4 ch.)	SDOL-0424
Safe loop-monitored digital output module (48 Vdc, 0.5 A, 4 ch.)	SDOL-0448

### Digital Output Field Termination Assemblies (FTAs)

Description	Model Number
Safe digital output FTA (24/48/60/110 Vdc, 4 channels)	TSDO-04UNI
Safe digital output FTA (24 Vdc, 4 channels)	TSDO-0424
Safe digital output FTA (24 Vdc, 8 channels)	TSDO-0824
Safe digital output FTA, Current limited (24 Vdc, 4 channels)	TSDOL-0424C
Safe digital output FTA, Current limited (24 Vdc, 8 channels)	TSDO-0824C
Digital output (relay) FTA for AK5/6 applications (8 channels)	TSRO-0824
Digital output (relay) FTA for AK5/6 applications common power (8 channels)	TSRO-08UNI
Digital output FTA (24 Vdc, 16 channels)	TDO-1624
Digital output (relay contact) FTA (8 channels, NO/NC)	TRO-0824
Digital output (relay contact) FTA (10 channels)	TRO-1024
Digital output FTA, loop monitoring (24 V, 7 channels)	TDOL-0724
Digital output FTA, loop monitoring (120 V, 7 channels)	TDOL-07120

## **Copyright, Trademarks, and Notices**

© 2007 — Honeywell Industrial Inc., Honeywell Safety Management Systems a division of Honeywell Aerospace B.V. The Netherlands.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any indirect, special or consequential damages. The information and specifications in this document are subject to change without notice.

Honeywell, TotalPlant, TDC 3000 and Universal Control Network are U.S. registered trademarks of Honeywell International Inc.  
Experion, PlantScape and Safety Manager are a trademark of Honeywell International Inc.

FSC, DSS and QMR are trademarks of Honeywell International Inc., Honeywell Safety Management Systems a division of Honeywell Aerospace B.V.

Other brand or product names are trademarks of their respective owners.