Honeywell

Safety Manager

Safety Manual

EP-SM.MAN.6283

Issue 4

10 July 2008

Release 131

Honeywell

Document	Release	Issue	Date
EP-SM.MAN.6283	131	4	July 2008

Notice

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell Safety Management Systems.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a 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 direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

Honeywell trademarks

Experion PKS®, PlantScape®, SafeBrowse®, TotalPlant® and TDC 3000® are U.S. registered trademarks of Honeywell International Inc.

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Conventions

Symbols

The following symbols are used in Safety Manager documentation:

Attention

This symbol is used for information that emphasizes or supplements important points of the main text.

Tip

This symbol is used for useful, but not essential, suggestions.

Note

This symbol is used to emphasize or supplement important points of the main text.

Caution

This symbol warns of potential damage, such as corruption of the database.

Warning

This symbol warns of potentially hazardous situations, which, if not avoided, could result in serious injury or death.

ESD

This symbol warns for danger of an electro-static discharge to which equipment may be sensitive.

Fonts

The following fonts are used in Safety Manager documentation:

Emphasis

- "... inform the reader on *how to* perform the task in terms of..."
- "...see the *Overview Guide"*

Emphasised text is used to:

- emphasise important words in the text,
- identify document titles.

Label

"The **Advanced** tab of the **Properties** window has.."

This font is used to identify labels and titles of (popup) windows.

Labels are used for Dialog box labels, menu items, names of properties, and so on.

Steps

Take the following steps:

1. **Create a plant and set its properties.**
2. **....**

This font is used to identify steps.

Steps indicate the course of action that must be adhered to, to achieve a certain goal.

`User Variable`

..create the ***`My Projects`*** folder and store the ***`readme.txt`*** file here.

..press the ***`Tab`*** key..

Next press ***`Enter`*** to..

This font is used to:

1. identify a user variable, a filename, an object or view.
2. highlight the keys the user should press on the keyboard.

`User variable` is a variable, an object or a view that the reader can call-up to view or to manipulate.

`Value`

"`Low` is the fault reaction state for digital inputs and digital outputs."

This font is used to indicate a value.

`Value` is a variable that the reader must resolve by choosing a pre-defined state.

`Variable`

"The syntax is: ***`filename`*** *`[-s] [-p]`*"

This font is used to identify a variable.

`Variables` are used in syntax and code examples.

`http://www.honeywellsms.com`

This font is used to identify a URL, directing a reader to a website that can be referred to.

Contents

The *Safety Manual* 1

Content of *Safety Manual*

The *Safety Manual* is a reference guide providing detailed information regarding safety aspects in Safety Manager.

A reference guide is a Safety Manager related guide and does not describe tasks in terms of *how to* perform the task in terms of steps to follow. A reference guide can provide input to support decisions required to achieve a certain objective.

Guide	subjects
Safety Manual	• "Architectural principle and standards of Safety Manager" on page 9 • "Safety Manager fault detection and response" on page 19 • "Safety Manager special functions" on page 37 • "Special requirements for TUV-approved applications" on page 47

References

The following guides may be required as reference materials:

Guide	Description
The *Overview Guide*	This guide describes the general knowledge required, the basic functions of, and the tasks related to Safety Manager.
The *Planning and Design Guide*	This guide describes the tasks related to planning and designing a Safety Manager project.
The *Installation and Upgrade Guide*	This guide describes the tasks related to installing, replacing and upgrading hardware and software as part of a Safety Manager project.
The *Troubleshooting and Maintenance Guide*	This guide describes the tasks related to troubleshooting and maintaining Safety Manager.
The *System Administration Guide*	This guide describes the task related to administrating the computer systems used in a Safety Manager project.
The *On-line Modification Guide*	This guide describes the theory, steps and tasks related to upgrading Safety Builder and embedded software and modifying an application online in a redundant Safety Manager.
The *Hardware Reference*	This guide specifies the hardware components that build a Safety Manager project.
The *Software Reference*	This guide specifies the software functions that build a Safety Manager project and contains guidelines on how to operate them.

Basic skills and knowledge

Before performing tasks related to Safety Manager you need to:

- Understand basic Safety Manager concepts as explained in the *Overview Guide* and the *Glossary.*
- Have a thorough understanding of the *Safety Manual*.
- Have had appropriate training related to Safety Manager that certifies you for your tasks (see the *Planning and Design Guide*).

Prerequisite skills

When you perform tasks related to Safety Manager, it is assumed that you have appropriate knowledge of:

- Site procedures
- The hardware and software you are working with. These may i.e. be: computers, printers, network components, Controller and Station software.
- Microsoft Windows operating systems.
- Programmable logic controllers (PLCs).
- Applicable safety standards for Process & Equipment Under Control.
- Application design conform IEC 61131-3.
- The IEC 61508 and IEC 61511 standards.

This guide assumes that you have a basic familiarity with the process(es) connected to the equipment under control and that you have a complete understanding of the hazard and risk analysis.

Training

Most of the skills mentioned above can be achieved by appropriate training. For more information, contact your Honeywell SMS representative or see:

- `http://www.automationcollege.com`.

Safety standards for Process & Equipment Under Control (PUC, EUC)

Safety Integrity level (SIL)

The IEC 61508 standard specifies 4 levels of safety performance for safety functions. These are called safety integrity levels. Safety integrity level 1 (SIL1) is the lowest level of safety integrity, and safety integrity level 4 (SIL4) the highest level. If the level is below SIL1, the IEC 61508 and IEC 61511 do not apply.

Safety Manager can be used for processing multiple SIFs simultaneously demanding a SIL1 up to and including SIL3.

To achieve the required safety integrity level for the E/E/PE safety-related systems, an overall safety life cycle is adopted as the technical framework (as defined in IEC 61508).

Application design conform IEC 61131-3

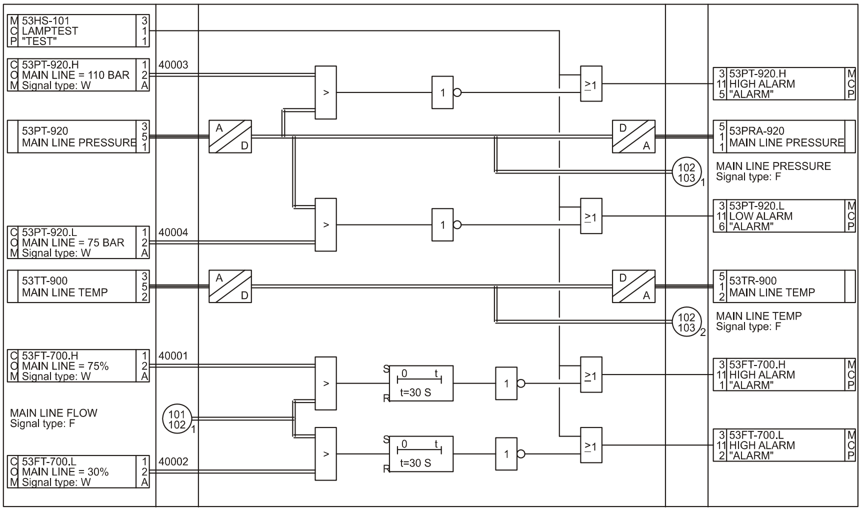
The IEC 61131 standard defines, as a minimum set, the basic programming elements, syntactic and semantic rules for the most commonly used programming languages, including graphical languages of:

- Ladder Diagram,
- Functional Block Diagram and,
- Textual languages of Instruction List and structured Text;

For more information see the IEC web site.

Figure 1 on page 5 shows how Safety Manager uses the graphical programming method, based on Functional Block Diagram as defined by the IEC 61131-3.

Figure 1 Example FLD layout


MCP 53HS-101 LAMPTEST "TEST" 3 1 1
COM 53PT-920.H MAIN LINE = 110 BAR Signal type: W 1 2 A
40003
53PT-920 MAIN LINE PRESSURE 3 5 1
COM 53PT-920.L MAIN LINE = 75 BAR Signal type: W 1 2 A
40004
53TT-900 MAIN LINE TEMP 3 5 2
COM 53FT-700.H MAIN LINE = 75% Signal type: W 1 2 A
40001
MAIN LINE FLOW Signal type: F
101 102 1
COM 53FT-700.L MAIN LINE = 30% Signal type: W 1 2 A
40002
A D
>
1
≥1
S R
0 t
t=30 S
D A
3 11 5 53PT-920.H HIGH ALARM "ALARM" MCP
5 1 1 53PRA-920 MAIN LINE PRESSURE
102 103 1
MAIN LINE PRESSURE Signal type: F
3 11 6 53PT-920.L LOW ALARM "ALARM" MCP
5 1 2 53TR-900 MAIN LINE TEMP
102 103 2
MAIN LINE TEMP Signal type: F
3 11 1 53FT-700.H HIGH ALARM "ALARM" MCP
3 11 2 53FT-700.L HIGH ALARM "ALARM" MCP

The IEC 61508 and IEC 61511 standards

SISs have been used for many years to perform safety instrumented functions e.g. in chemical, petrochemical and gas plants. In order for instrumentation to be effectively used for safety instrumented functions, it is essential that the instrumentation meets certain minimum standards and performance levels.

To define the characteristics, main concepts and required performance levels, standards IEC 61508 and IEC 61511 have been developed. The introduction of Safety Integrity level (SIL) is one of the results of these standards.

This brief provides a short explanation of each standard. Detailed information regarding IEC 61508 and 61511 can be found on the IEC web site `http://www.iec.org`.

What standard to use?

Tip:

You can use the IEC 61508 as stand-alone standard for those sectors where a sector specific standard does not exist.

- If you are in the process sector and you are an owner/user, it is strongly recommended that you pay attention to the IEC 61511 (ANSI/ISA 84.00.01). For details see “IEC 61511, the standard for the process industry” on page 7.
- If you are in the process sector and you are a manufacturer, it is strongly recommended that you pay attention to the IEC 61508. For details see “IEC 61508, the standard for all E/E/PE safety-related systems” on page 6.
- If you are in another sector, it is strongly recommended that you look for, and use, your sector specific IEC standard for functional safety (if there is one). If none exists, you can use the IEC 61508 instead. For details see “IEC 61508, the standard for all E/E/PE safety-related systems” on page 6

IEC 61508 and IEC 61511 terminology

This guide contains both IEC 61508 and IEC 61511 related terminology.

As the IEC 61511 sits within the framework of IEC 61508 most of the terminology used may be interchanged. Table 1 on page 6 provides an overview of the most common interchangeable terminology.

Table 1 IEC 61508 versus IEC 61511 terminology

IEC 61508 terminology	IEC 61511 terminology
safety function	safety instrumented function
electrical/electronic/programmable electronic (E/E/PE) safety-related system	safety instrumented system (SIS)

IEC 61508, the standard for all E/E/PE safety-related systems

The IEC 61508 is called “*Functional safety of electrical/electronic/programmable electronic safety-related systems*”

IEC 61508 covers all safety-related systems that are electrotechnical in nature (i.e. electromechanical systems, solid-state electronic systems and computer-based systems).

Generic standard

The standard is generic and is intended to provide guidance on how to develop E/E/PE safety related devices as used in Safety Instrumented Systems (SIS).

The IEC 61508:

- serves as a basis for the development of sector standards (e.g. for the machinery sector, the process sector, the nuclear sector, etc.).
- can serve as stand-alone standard for those sectors where a sector specific standard does not exist.

SIL

IEC 61508 details the design requirements for achieving the required Safety Integrity Level (SIL).

The safety integrity requirements for each individual safety function may differ. The safety function and SIL requirements are derived from the hazard analysis and the risk assessment.

The higher the level of adapted safety integrity, the lower the likelihood of dangerous failure of the SIS.

This standard also addresses the safety-related sensors and final elements regardless of the technology used.

IEC 61511, the standard for the process industry

The IEC 61511 is called "*Functional safety - Safety instrumented systems for the process industry sector*". It is also referred to as the ANSI/ISA 84.00.01.

This standard addresses the application of SISs for the process industries. It requires a process hazard and risk assessment to be carried out, to enable the specification for SISs to be derived. In this standard a SIS includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s).

The standard is intended to lead to a high level of consistency in underlying principles, terminology and information within the process industries. This should have both safety and economic benefits.

The IEC 61511 sits within the framework of IEC 61508.

Need to know more?

For more information regarding, or help on, implementing or determining, the applied safety standards for your plant/process please contact your Honeywell affiliate. Our Safety Consultants can help you to e.g.:

- perform a hazard risk analysis
- determine the SIL requirements
- design the Safety Instrumented System
- validate and verify the design
- train your local safety staff

Architectural principle and standards of Safety Manager

2

Safety Manager basic architectures

Safety Manager can be configured for a number of architectures, each with its own characteristics and typical Safety Instrumented Functions. Table 2 on page 9 provides an overview of the available architectures.

Table 2 Safety Manager architectures

Controller configuration	IO configuration	Remarks
Non-redundant (DMR)	Non-redundant	DMR architecture; Supports SIF for SIL1, SIL2 and SIL3 applications.
Redundant (QMR)	• Non-redundant • Redundant • Redundant and non-redundant	QMR architecture; Supports SIF for SIL1, SIL2 and SIL3 applications.

Dual Modular Redundant (DMR) architecture

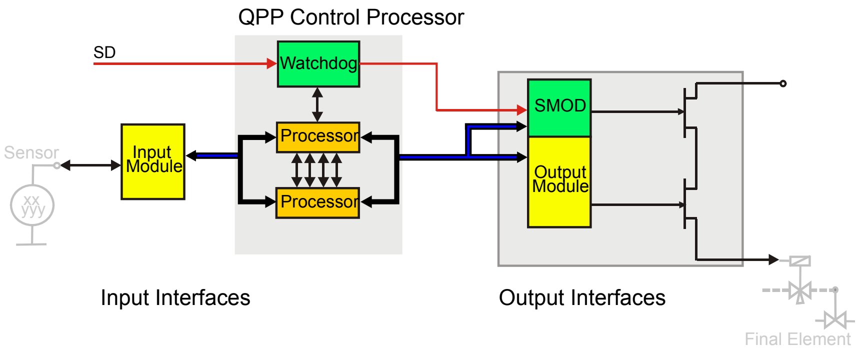
Typical applications of a DMR architecture are:

- Burner Management System
- Batch processing
- Machine protection

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 2 on page 10), which contains a redundant processor with 1oo2 voting between the processors and memory.

Figure 2 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:

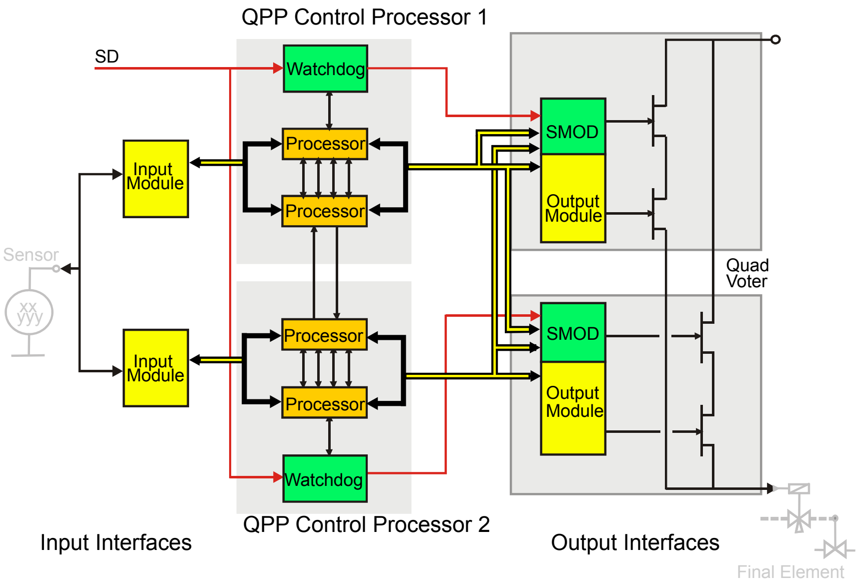
- process safeguarding applications for which continues operation is essential.

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 3 on page 11), which results in quadruple redundancy making it dual fault tolerant for safety.

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 3 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.

Watchdog architecture in mixed IO configurations

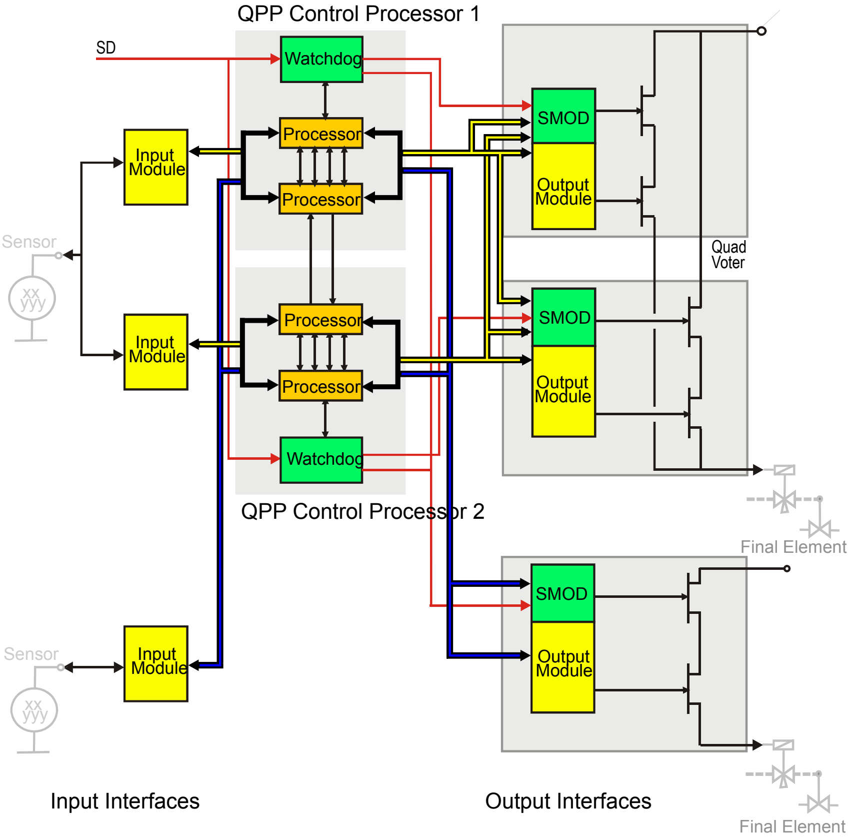
In a system with combined redundant and non redundant IO 3 watchdog lines are active:

- **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 4 Functional diagram: redundant Controller with redundant and non-redundant IO



Certification

The advantage of applying and complying to standards is obvious:

- International standards force companies to evaluate and develop their products and processes according a consistent and uniform way.
- Products certified conform these international standards guarantee a certain degree of quality and product reliability that other products lack.

Since functional safety is the core of the Safety Manager design, the system has been certified for use in safety applications all around the world. Safety Manager has been developed specifically to comply with the IEC61508 functional safety standards, and has been certified by TUV for use in SIL1 to SIL3 applications.

Safety Manager has also obtained certification in the United States for the UL 1998 and ANSI/ISA S84.01 standards.

For a full list of all these and other certifications see “Certification” on page 13.

Certification

Safety Manager has been certified to comply with the following standards:

International Electrotechnical Commission (IEC) — The design and development of Safety Manager are compliant with IEC 61508 (as certified by TUV).

Instrument Society of America (ISA) — Certified to fulfill the requirements laid down in ANSI/ISA S84.01.

CE compliance — Complies with CE directives 89/336/EEC (EMC) and 73/23/EEC (Low Voltage), 89/392/EEC (Machine Safety)

European Committee for Standardization — CEN, CENELEC

TUV (Germany) — Certified to fulfill the requirements of SIL3 safety equipment as defined in the following documents: IEC61508, IEC60664-3, EN50156, EN 54-2, EN50178, IEC 60068, IEC 61131-2, IEC 61131-3, IEC60204.

Canadian Standards Association (CSA) — 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.

Underwriters Laboratories (UL) — Certified to fulfill the requirements of UL 508, UL 991, UL 1998, and ANSI/ISA S84.01.

Factory Mutual (FM) — Certified to fulfill the requirements of FM 3611 and FM3600 (non-incentive field wiring circuits for selected modules and installation in Class 1 Div 2 environments).

Standards compliance

This subsection lists the standards Safety Manager complies with, and gives some background information on the relevant CE marking (EMC directive and Low Voltage directive).

Table 3 Safety Manager compliance to standards

Standard	Title	Remarks
IEC61508 (S84.01)	Functional safety of electrical/electronic/ programmable electronic (E/E/PE) safety-related systems.	
VDE 0116 (10/89)	Electrical equipment of furnaces. *(German title: Elektrische Ausrüstung von Feuerungsanlagen)*	
EN 54 part 2 (01/90)	Components of automatic fire detection systems, Introduction. *(German title: Bestandteile automatischer Brandmeldeanlagen)*	
EN 50081-2-1994	Electromagnetic compatibility – Generic emission standard, Part 2: Industrial environment.	
EN 50082-2-1995	Electromagnetic compatibility – Generic immunity standard, Part 2: Industrial environment.	
IEC 61010-1-1993	Safety Requirements for Electrical Equipment for Measurement, Control and Laboratory Use, Part 1: General Requirements.	
IEC 61131-2-1994	Programmable controllers. Part 2: Equipment requirements and tests.	
NFPA 72/2002	National Fire Alarm Code Handbook	
NFPA 85/2001	Boiler and Combustions Systems Hazards Code	
UL 1998	Safety-related software, first edition.	Underwriters Laboratories.
UL 508	Industrial control equipment, sixteenth edition.	Underwriters Laboratories.

Table 3 Safety Manager compliance to standards

Standard	Title	Remarks
UL 991	Test for safety-related controls employing solid-state devices, second edition.	Underwriters Laboratories.
FM3600, FM 3611 Class I, Division 2, Groups A, B, C & D Class II, Division 2, Groups F & G	Electrical equipment for use in • Class I, Division 2, • Class II, Division 2, and • Class III, Division 1 and 2, hazardous locations.	Factory Mutual Research. Applies to the field wiring circuits of the following modules: SDI-1624, SAI-0410, SAI-1620m, SDIL-1608 and SAO-0220m, and installation of the Controller in these environments.
CSA C22.2	Process control equipment. Industrial products.	Canadian Standards Association No. 142 (R1993).
IEC 60068-1	Basic environmental testing procedures.	
IEC 60068-2-1	Cold test.	0°C (32°F); 16 hours; system in operation; reduced power supply voltage: (–15%): U=20.4 Vdc or (–10%): U=198 Vac.
IEC 60068-2-1	Cold test.	–10°C (14°F); 16 hours; system in operation.
IEC 60068-2-2	Dry heat test.	up to 65°C (149°F); 16 hours; system in operation; increased power supply voltage: (+15%): U=27.6 Vdc or (+10%): U=242 Vac.
IEC 60068-2-3	Test Ca: damp heat, steady state.	21 days at +40°C (104°F), 93% relative humidity; function test after cooling.
IEC 60068-2-3	Test Ca: damp heat, steady state.	96 hours at +40°C (104°F), 93% relative humidity; system in operation.
IEC 60068-2-14	Test Na: change of temperature – withstand test.	–25°C—+55°C (–13°F—+131°F), 12 hours, 95% relative humidity, recovery time: max. 2 hours.

Table 3 Safety Manager compliance to standards

Standard	Title	Remarks
IEC 60068-2-30	Test Db variant 2: cyclic damp heat test.	+25°C—+55°C (+77°F—+131°F), 48 hours, 80-100% relative humidity, recovery time: 1—2 hours.
IEC 60068-2-6	Environmental testing – Part 2: Tests – Test. Fc: vibration (sinusoidal).	Excitation: sine-shaped with sliding frequency; Frequency range: 10—150 Hz. Loads: • 10—57 Hz; 0.075 mm. • 57—150 Hz; 1 G. Duration: 10 cycles (20 sweeps) per axis. No. of axes: 3 (x, y, z). Traverse rate: 1 oct/min in operation.
IEC 60068-2-27	Environmental testing – Part 2: Tests – Test. Ea: shock.	Half sine shock. 2 shocks per 3 axes (6 in total). Maximum acceleration: 15 G. Shock duration: 11 ms. Safety Manager in operation.

Safety Manager fault detection and response

3

Introduction

The goal of fault detection and response is to detect and isolate any single fault that affects the safety of the process under control, within a time frame that is acceptable for the process.

Note:

There is always a diagnostic alarm available upon detection of a fault.

Diagnostic Test Interval

The Diagnostic Test interval (DTI) is the time in which detection and isolation of faults takes place. The DTI must be set to a value that is acceptable for the process, such as the Process Safety Time (PST). These values can be obtained from hazard analysis reports.

FR state

The Fault Reaction (FR) state of each IO point is the predetermined state or action the point assumes in case of faults.

- For normally energized safety related applications, like ESD applications, the required predefined safe fault reaction state is de-energized or `Low`.
- For normally de-energized safety related applications, like FGS applications, the required predefined safe fault reaction state for inputs is energized or `High` / `Top Scale`.

Repair timer

Note:

The repair timer setting must be based on a hardware reliability analysis which includes MTTR figures.

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.

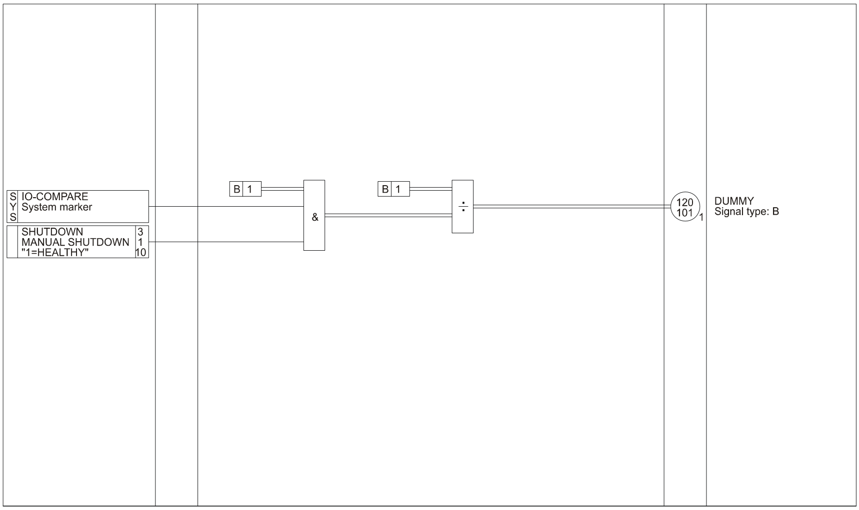
To prevent such a scenario to develop, the system starts a repair timer if a secondary means becomes vulnerable to faults. Once started, this configurable timer counts down until the fault is repaired. If the timer is allowed to reach zero, the Control Processor halts.

Shutdown at assertion of Safety Manager alarm markers

If the normal system response of Safety Manager is not enough when Safety Manager detects a fault and more stringent system response is required, the Safety Manager alarm markers can be used to shut down the system via the application.

Figure 5 on page 21 shows an example of how to shut down the system in case of an IO compare error. An additional manual shutdown input is provided by which the operator can initiate a shutdown by hand.

Figure 5 Diagram to shut down system in case of output compare error



If an IO compare error is detected or a manual shutdown is initiated, a divide-by-zero is forced and Safety Manager shuts down. Other alarm markers can be used in a similar way.

Note:

A manual shutdown can also be realized via the shutdown (SD) input of the SM Controller.

With aid of the SD input a tested, hard wired connection can be used. The SD input is accessible via the SD loop connector at the back of the CP chassis.

Breaking the SD loop causes all outputs to be de-activated!

SM Controller faults

Below topics provide an overview of detected Controller faults and the Controller response to these faults.

QPP faults

Table 4 on page 22 provides an overview of faults that the Controller detects related to the QPP and the response to these faults.

Table 4 Controller response to QPP faults

QPP faults		**Non redundant Controller response**	**Redundant Controller response**	
related to	**diagnostics report includes**		**CP$_{X(faulty)}$**	**CP$_{Y (not faulty)}$**
temperature monitoring (set points user configurable)	high alarm or low alarm	none -continue	none -continue	
	high-high alarm or low-low alarm	halt Controller	halt CP	none -continue
	1 sensor faulty and temp. more than 3 degrees from shutdown limits	none -continue	none -continue	
	1 sensor faulty and temp. less than 3 degrees from shutdown limits	halt Controller	halt CP	none -continue
Memory	QPP memory	halt Controller	halt CP	none -continue
Execution	execution time out of range / failure	halt Controller	halt CP	none -continue
	error on logical sheet		halt Controller	
Watchdog	output shorted	halt Controller	halt CP	none -continue
	de-energized watchdog line for redundant outputs	halt Controller	halt CP	none -continue
	de-energized watchdog line for non-redundant outputs	halt Controller	de-energize non redundant outputs, *continue* operation on redundant outputs	
Watchdog	faulty	halt Controller	halt CP	none -continue
Bus drivers				
Internal link				
QPP module				
secondary switch-off	faulty	halt Controller	halt CP	none -continue

Table 4 Controller response to QPP faults *(continued)*

QPP faults		Non redundant Controller response	Redundant Controller response	
related to	**diagnostics report includes**		**CP$_{X\text{(faulty)}}$**	**CP$_{Y\text{ (not faulty)}}$**
repair timer (user configurable)	running	none -continue	none -continue	
	expired	halt Controller	halt CP	none -continue
software	corrupted	halt Controller	halt CP	none -continue
intervention	QPP key switch to `IDLE` position	halt Controller	halt CP	none -continue
	Spurious watchdog interrupt			
	safe state initiated			
	SD input de-energized		halt Controller	
synchronization	QPP	n.a.	halt CP	none -continue
	system software		halted CP does not start	none -continue
	base timer		halt CP	none -continue
	IO compare error		apply FR state	
time sync (user configurable)	source unavailable	switch to other source	switch to other source	
internal communication		n.a.	halt CP	none -continue

USI faults

Table 5 on page 24 provides an overview of detected faults in relation to the USI and the response to these faults.

A fault in the USI also means that the communication channels of that USI are down.

Table 5 Controller response to USI faults

USI faults		Non redundant Controller response	Redundant Controller response	
related to	**diagnostics report includes**		**CP$_{X(\text{ faulty})}$**	**CP$_{Y\text{ (not faulty)}}$**
Memory	USI module	apply FR state to affected COM & FSC inputs	use values from CP$_Y$ for affected COM & FSC inputs.*	none
Execution				
communication	USI module			
module faulty	USI module			
synchronization	system software			
software	corrupted			

* If values are not available via CP$_Y$ apply FR state to affected COM & FSC inputs.

BKM faults

Table 6 on page 24 provides an overview of faults that can be detected in relation to the BKM and the response to these faults.

Table 6 Controller response to BKM faults

BKM faults		Non redundant Controller response	Redundant Controller response	
related to	**diagnostics report includes**		**CP$_{X(\text{ faulty})}$**	**CP$_{Y\text{ (not faulty)}}$**
key switch	input compare error (reset key switch)	none -continue	none -continue	
	input compare error (force key switch)			
module faulty	BKM module	none -continue	none -continue	
battery	faulty / low	none -continue	none -continue	
	lifetime expired			
	transport switch			

PSU faults

Table 7 on page 25 provides an overview of faults that can be detected in relation to the PSU and the response to these faults.

Table 7 Controller response to PSU faults

PSU faults		**Non redundant Controller response**	**Redundant Controller response**	
related to	**diagnostics report includes**		**CP$_{X(faulty)}$**	**CP$_{Y (not faulty)}$**
Voltage monitoring	spurious watchdog interrupt	halt Controller	halt CP	none -continue
module faulty	PSU module			

Communication faults

Note

Please note that a fault in the communication links may be caused by USI modules.

Table 9 on page 27 provides an overview of faults that can be detected in relation to communication and the response to these faults.

Table 8 Controller response to communication faults

communication faults		**Non redundant communication or "shared CP" Controller response***	**Redundant communication Controller response**	
Related to	**Diagnostic message reports**		**CP$_{X(faulty)}$**	**CP$_{Y(not faulty}$**
broken link wrong protocol assigned time-out	communication fault	apply FR state to COM & FSC inputs of that channel if channel belongs to active clock source, switch to other clock source	continue communication via healthy link**	none -continue
too many data requests	USI module faulty	apply FR state to COM & FSC inputs of that USI	use values from CP$_{Y}$ for affected COM and FSC inputs***	
data mismatch between inputs**** (SafeNet redundant)	compare error	n.a.	apply FR state	
data mismatch between inputs**** (redundant Experion or Modbus)		n.a.	values received by CP2 prevail.	

* If the Controller is redundant, both CP channels respond the same.

** If no healthy link remains, apply FR state to the `COM` and `FSC` inputs allocated to that channel and/or switch to other clock source.

*** If values are not available via CP_Y apply FR state to affected `COM` and `FSC` inputs.

**** Inputs as in communication inputs of this SM Controller.

Communication time-out

If no communication with the external device is established within a predefined time frame a communication time-out is generated.

A communication time-out always results in a communication failure. Communication time-outs can be configured by the user.

If a device is connected to Safety Manager via a redundant communication link, the fault detection applies to each link separately resulting in single-fault tolerant communication.

SM IO faults

Tip:

For more information on repair timer settings or fault reaction states as referred to in these topics, see “Introduction” on page 19.

These topics provide an overview of detected IO faults and the Controller response to these faults.

Digital input faults

Table 9 on page 27 provides an overview of faults that can be detected in relation to digital inputs and the response to these faults.

Table 9 Controller response to digital input faults

Digital input faults		**Non redundant input**	**Redundant input, Controller response**	
Related to	**Diagnostic message reports**	**Controller response****	**CP_X (faulty input)**	**CP_Y (healthy input)**
digital input loop** (line monitored)	lead breakage	apply FR state	apply FR state	
	short circuit			
loop power**	power output to sensors shorted	apply FR state	use values from CP_Y***	none -continue
channel	module faulty	apply FR state	use values from CP_Y***	none -continue
module	module faulty	apply FR state	use values from CP_Y***	none -continue
compare****	input compare error	apply FR state	apply FR state	

* If the Controller is redundant, both CPs respond the same.

** This fault is usually caused by an anomaly in the field, *not* by a defect of an input module.

*** If values are not available via CP_Y apply FR state to affected inputs.

**** Occurs when detecting a difference in the input values persists for more than 2 application cycli.

Analog input faults

Table 10 on page 28 provides an overview of faults that can be detected in relation to analog inputs and the response to these faults.

Table 10 Controller response to analog input faults

Analog input faults		Non redundant input	Redundant input, Controller response	
Related to	**Diagnostic message reports**	**Controller response***	**CP_X (faulty input)**	**CP_Y (healthy input)**
analog input value	below low transmitter alarm level per range	none- continue for 0-20mA, 0-10V	none- continue for 0-20mA, 0-10V	
		bottom scale for 4-20mA, 2-10V	bottom scale for 4-20mA, 2-10V	
	above high transmitter alarm level all ranges	none- continue	none- continue	
loop power (SAI-1620m)	External voltage monitoring fault	none- continue	none- continue	
channel	module faulty	apply FR state	use values from CP_Y**	none- continue
module	module faulty	apply FR state	use values from CP_Y***	none- continue
	Internal power down			
compare***	input compare error	apply FR state	apply FR state	

* If the Controller is redundant, both CPs respond the same.

** If values are not available via CP_Y apply FR state to affected inputs.

*** Occurs when detecting a deviation of >2% in the input values persists for more than 2 application cycles.

Digital output faults

Table 11 on page 28 provides an overview of faults that can be detected in relation to digital outputs and the response to these faults.

Table 11 Controller response to digital output faults

Digital output faults		Non redundant output	Redundant output, Controller response	
Related to	**Diagnostic message reports**	**Controller response***	**CP_X (faulty output)**	**CP_Y (healthy output)**
digital output loop** (line monitored) default voting	current detected	Apply FR state	apply FR state	

Table 11 Controller response to digital output faults *(continued)*

Digital output faults		**Non redundant output**	**Redundant output, Controller response**	
Related to	**Diagnostic message reports**	**Controller response***	**CP_X (faulty output)**	**CP_Y (healthy output)**
digital output loop** (line monitored) 1oo2D voting	current detected	De-energize shorted output(s).	de-energize shorted output(s).	
digital output loop** (line monitored)	open loop	none -continue	none -continue	
digital output loop** (other)	short circuit detected	De-energize shorted output(s).	de-energize shorted output(s).	
loop power***	external power down	none -continue	none -continue	
channel fault (line monitored) FR state = `Low`	module faulty	De-energize outputs on module & start repair timer	De-energize outputs on module & start repair timer	
channel fault (other) FR state = `Low`	module faulty	De-energize outputs on module & start repair timer	De-energize outputs on module & start repair timer	none -continue
channel fault Other FR states	module faulty	none -continue	none -continue	
module fault FR state = `Low`	module faulty	De-energize outputs on module & start repair timer	De-energize outputs on module & start repair timer	none -continue
module fault Other FR states	module faulty	none -continue	none -continue	
compare****	output compare error	apply FR state	apply FR state	

* If the Controller is redundant, both CPs respond the same.

** This fault is usually caused by an anomaly in the field, *not* by a defect of an output module.

*** When this anomaly occurs on all modules in a watchdog group or a power group, it is *not* a defect of the output module.

**** Occurs when detecting a difference in the output values of a redundant SM Controller.

Analog output faults

Table 12 on page 30 provides an overview of faults that can be detected in relation to analog outputs and the response to these faults.

Table 12 Controller response to analog output faults

Analog output faults		**Non redundant output**	**Redundant output, Controller response**	
Related to	**Diagnostic message reports**	**Controller response**[*]	**CP_X (faulty output)**	**CP_Y (healthy output)**
analog output	calculation error	halt Controller	halt Controller	
analog output loop	open loop	De-energize outputs on module & start repair timer	none -continue	
channel fault FR state = `0 mA`	module faulty	De-energize outputs on module & start repair timer	De-energize outputs on module & start repair timer	none -continue
channel fault Other FR states	module faulty	none -continue	none -continue	
module fault FR state = `0 mA`	module faulty	De-energize outputs on module & start repair timer	De-energize outputs on module & start repair timer	none -continue
module fault Other FR states	module faulty	none -continue	none -continue	
compare[**]	output compare error	Apply FR state	Apply FR state	

[*] If the Controller is redundant, both CPs respond the same.

[**] Occurs when detecting a difference in the output values of a redundant SM Controller.

IO compare errors and system response

Note

Because of the high level of self-testing and fault-handling by Safety Manager, the actual occurrence of a compare error is very unlikely.

For proper operation both Control Processors of a redundant system must have identical IO values at the beginning and at the end of each application cycle.

An IO compare error is generated as soon as the Controller detects a difference between the IO values of CP1 and CP2.

The Controller responds towards IO compare errors by applying the fault reaction state to the faulty IO.

Note

A Controller does not automatically shut-down upon detection of IO compare error.

Table 13 on page 31 shows the relation between Input and output compare faults, alarm markers and Controller response.

Table 13 Controller response to IO compare faults

IO compare error			
Related to	**redundancy**	**Occurs when detecting**	**Controller response**
digital inputs	N.A.	a persisting difference for more than 2 application cycles	apply FR state
analog inputs	N.A.	a deviation of >2% for more than 2 application cycles.	
digital outputs	N.A.	a difference between outputs	
analog outputs	N.A.		

Compare error detection and synchronization

Input compare errors

Input compare error detection applies to all hardware inputs.

Differences in the input status read should be momentary. Persisting differences could be the result of detected hardware faults. In that case, the faulty input channel is reported in the diagnostics, and both Control Processors use the process value read from the healthy input channel.

A persisting difference in status of an input while no faults are detected at the accessory hardware channels leads to an input compare error.

Output compare errors

An output compare error applies to all hardware outputs.

In configurations with a redundant Controller, both Control Processors will continuously have an identical application status, resulting in identical process outputs.

An output compare error is detected if there is a difference between the Control Processors with respect to:

- the calculated application output values for hardware outputs (AO/DO) or communication outputs (DO, BO) to another Safety Manager.
- the actual application values sent to hardware outputs (AO/DO) or communication outputs (DO, BO) to another Safety Manager.

If outputs are no longer synchronized an Output Compare error is generated.

Input synchronization algorithm

In configurations with a redundant Controller, the process inputs are scanned every application program cycle by both Control Processors.

Each Control Processor executes the application cycle independently of the other. It is therefore essential that they use identical values for the process inputs.

There is no problem if the process inputs are stable. However, if an input value changes when the Control Processors read the value, both Control Processors could read a different value. In such cases, an identical input value in the Controller is obtained via input synchronization.

If inputs are no longer synchronized, the signal value freezes to the last known synchronized state and a synchronization timer -equal to two application cycles- is started. This state is maintained until:

- a synchronized state is obtained or
- the synchronization timer runs out.

If a synchronized state is not achieved within two application cycles the fault reaction is activated and an Input Compare error is generated.

If a synchronized state is achieved within two application cycles the synchronization timer is reset.

Synchronization algorithms are used for digital and analog inputs.

Digital input synchronization

A digital input compare error is detected if the inputs of both Control Processors are stable but different (for example Control Processor 1 continuously ‘0’, Control Processor 2 continuously ‘1’), for the duration of two application cycles.

The input compare error detection algorithm puts the following demands on the dynamic nature of the digital process inputs:

1. If an input state changes, it must become stable again within two application cycles.
2. The frequency of continuously changing inputs must be less than two application cycles.

Analog input synchronization

For analog inputs, the synchronized value is the mean value of the input values. An input compare error is detected if the input values differ more than 2% of the full scale for the duration of the configured Diagnostic Test Interval.

The input compare error detection algorithm puts the following demands on the dynamic nature of the analog process inputs:

1. For inputs allocated on a redundant module (type SAI-0410 or SAI-1620m), the slope steepness must be less than 125 mA/s.
2. For inputs allocated on a non-redundant module (type SAI-1620m), the slope steepness must be less than 20 mA/s

.

⚠ **Caution**

Analog input compare errors may, for example, occur when calibrating smart transmitters using hand-held terminals. Refer to the *Troubleshooting and Maintenance Guide* for details on calibrating smart transmitters that are connected to Safety Manager analog inputs.

Calculation errors

⚠ **Caution**

Safety Manager stops if a calculation error occurs.

Calculation errors may occur in the application program.

Calculation errors occur if:

- The calculated value of an analog output is outside the specified range.
- The square root of a negative number is taken.
- A logarithm function is loaded with a negative value or zero
- A divide-by-zero occurs.
- An overflow occurs during a calculation.
- The value for a counter is outside the specified range.

Calculation errors reflect an incorrect design of the application program for the intended function. Once a calculation error occurs for a specific process point, a correct result of successive calculations based on this point cannot be guaranteed.

Guidelines on how to avoid calculation errors in the Safety Manager application are presented below.

Preventing calculation errors

Calculation errors can be prevented as follows:

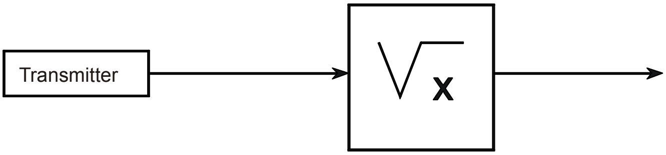
- Overall process design.
- Inclusion of Safety Manager diagnostic data.
- Validation of signals in the Functional Logic Diagrams (FLDs).
- Exception handling during the actual calculation.

Prevention by design

In line with good software engineering practice, as promoted by IEC 61508, calculation errors should be avoided by design. This means that an application should be designed in such a way that the operands of a symbol in the FLDs can never get an invalid value. The design approach starts with making sure that input values as obtained from the process remain within a predefined range. This approach ensures that the derived values are also valid for successive operations.

Sometimes, however, it cannot be guaranteed that an input value remains within a predefined range which is valid for all functions. For example, a signal derived from a reverse-acting, non-linear 4-20 mA transmitter which has been configured for a zero top scale in the application domain could become negative if the transmitter fails and delivers a signal beyond 20 mA. If the signal is then linearized through a square-root function, a system stop occurs (square root of negative number).

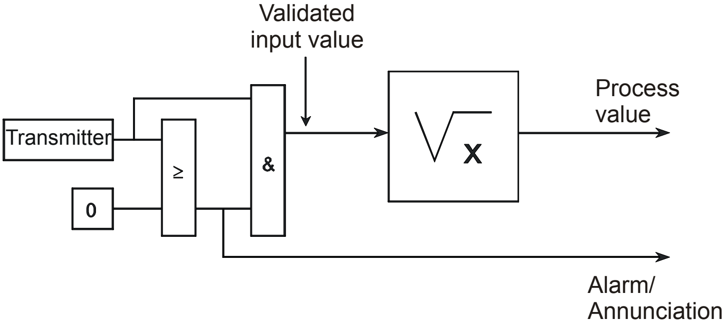
Figure 6 Intended square-root function



Preventive measures

If a valid input value cannot be guaranteed, preventive measures must be built into the design. A comparison function can be used as an indicator that the transmitter value has left its normal operational band and that the calculation should not be done. The alarm signal is used to implement a corrective action and to indicate the exception to the operator (see Figure 7 on page 35).

Figure 7 Square-root function with validated input value



If diagnostics are not available (e.g. for 0-20 mA transmitters), it is necessary to implement range checking in the application. The result of the range check is again used for the implementation of corrective actions.

Tip

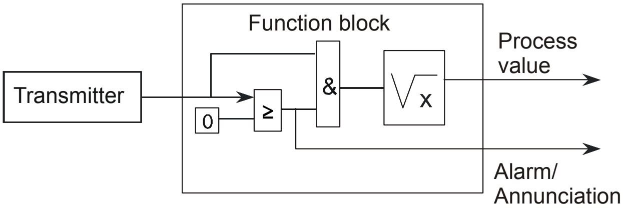
Range checking is also useful to define the boundaries of analog outputs 0(4)-20mA, thus preventing a system shutdown due to driving values that exceed the boundaries.

An important advantage of input validation is that it can be implemented for input values of which the validity cannot be guaranteed. Furthermore, the invalid input can be exactly identified. This allows the implementation of effective correction strategies of only the affected part of the process.

Common function block

A last option is to create a common function block, e.g. square root. The function block validates the operand(s) and only performs the intended function if the operands are valid. Otherwise a predefined value is returned. An additional function block output should be provided which indicates if the calculation result is valid or not. This output signal can be used for the implementation of corrective actions in the application (see Figure 8 on page 36).

Figure 8 Square-root function with validity check in function block



Safety Manager special functions

4

Unit shutdown

Process units

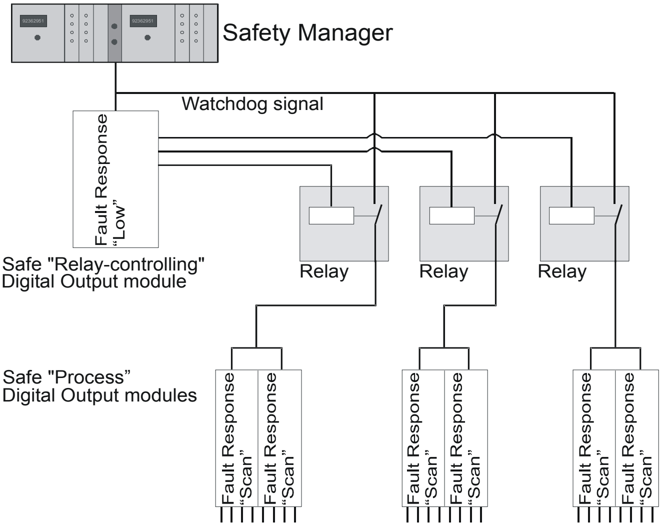
If a process can be divided into independent process units, the overall process availability can be increased by a separate shutdown of the units within Safety Manager. In this way, whenever a fault is detected in the hardware of a process unit, only the affected unit needs to be shut down, while the other parts of the process remain unaffected.

Configuration of unit shutdown (watchdog grouping)

This subsection covers the required configuration, application programming and wiring to achieve shutdown per process unit.

Figure 9 on page 38 shows a standard wiring diagram for unit shutdown of three separate process units.

Figure 9 Wiring diagram for unit shutdown



For each process unit, a relay is used to connect the watchdog signal of the unit output to the process Safety Manager watchdog. The relays are controlled via outputs of Safety Manager: the unit shutdown outputs. In normal operation, all relays are activated. If a fault is detected in a process unit, the corresponding relay is deactivated, which results in a shutdown of the relevant unit.

The unit relays must meet the requirements of DIN VDE 0116, part 8.7.4.5 and 8.7.4.6 of October 1989, i.e.:

1. Mechanical reliability > $3 * 10^6$ switches.
2. Contacts protected (for example fuses, series resistors, etc.) at 0.6 ∗ nominal contact current.
3. Electrical reliability > $2.5 * 10^5$ switches.

Tip

The relay output FTA TSRO-0824 complies to these requirements.

Unit shutdown outputs

The unit shutdown outputs must:

- Be allocated on safe modules (such as a SDO-0824 or SDOL-0424 module)
- Have their `fault reaction state` set to `Low`.
  This guarantees that Safety Manager directs the process to its safe state if a fault occurs which affects this output.
- Have set the `power-up status` of the unit shutdown output to `ON`.
  This allows a correct start-up of Safety Manager with activated unit relays.

For optimal availability it is recommended that unit shutdown outputs are allocated to redundant output modules.

Process outputs (safety related)

The process outputs must be allocated to a Safety Manager output module of the type:

• SDO-0824	Safety-related digital output module (24 Vdc, 0.55 A, 8 channels)
• SAO-0220m	Safety-related analog output module (0(4)-20 mA, 2 channels)
• SDO-04110	Safety-related digital output module (110 Vdc, 0.32 A, 4 channels)
• SDO-0448	Safety-related digital output module (48 Vdc, 0.75 A, 4 channels)
• SDO-0424	Safety-related digital output module (24 Vdc, 2 A, 4 channels)
• SDOL-0424	Safety-related loop-monitored digital output module (24 Vdc, 1 A, 4 channels)
• SDOL-0448	Safety-related loop-monitored digital output module (48 Vdc, 0.5A, 4 channels

To allow the programming of the response via the application, the fault reaction of these outputs must be set to `Appl`. This disables the automatic response of Safety Manager in case a fault occurs at safety-related output modules.

Application programming

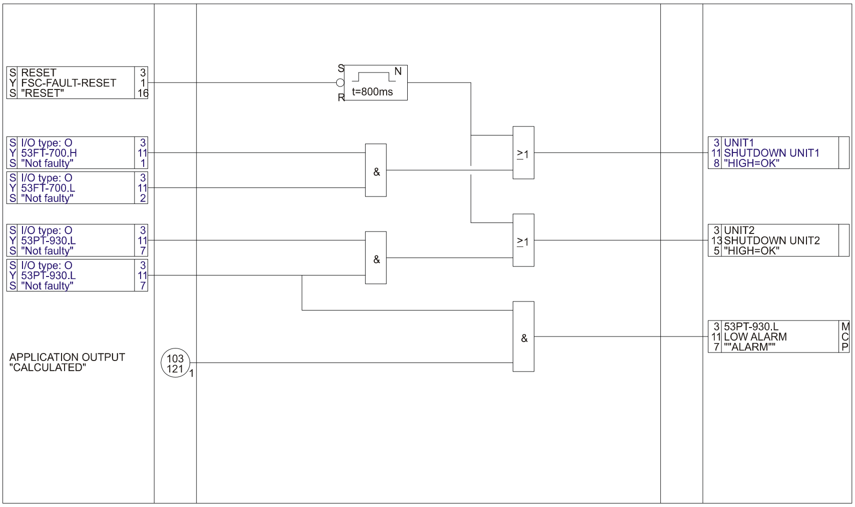
To realize unit shutdown in the functional logic diagrams, all diagnostic inputs related to output modules of each process unit are connected to an AND gate.

Figure 10 on page 40 shows how the output signal of the AND gate is connected to the unit shutdown.

As long as all diagnostic inputs are “healthy”, they are `High`, the unit shutdown output is `High` and the unit relay is activated (relay contact closed).

If a diagnostic input of an output channel in the unit becomes “unhealthy”, the corresponding unit shutdown output becomes `Low` and the unit relay is deactivated (relay contact open).

Figure 10 Functional logic diagram of unit shutdown



A defective output channel can be switched-off in accordance with the normal Safety Manager response for safety-related signals. To switch off a defective output channel, the calculated application output and the channel diagnostic input must be supplied to the output channel via an AND gate.

The Safety Manager `FaultReset` alarm marker is connected to all unit shutdown outputs via an OR gate. When an error is detected and repaired in a unit, the unit may be restarted using the `FaultReset` alarm marker.

The minimum and maximum time the unit output is enabled by the `FaultReset` is limited to ensure that the `FaultReset` is detected by the output. The pulse length (typically set at 800 ms) may not exceed the Diagnostic Test Interval.

On-line modification

Tip:

Detailed information about On-line modification can be found in *On-line Modification Guide*

Introduction

On-line modification (OLM) is a Safety Manager option which allows you to modify the application software, embedded system software and the Safety Manager hardware configuration of systems with a redundant Controller while the system remains operational.

During the on-line modification, the changes are implemented in the Control Processors one by one. While one Control Processor is being modified, the other Control Processor continues safeguarding the process.

The engineer executing the OLM is guided through the OLM procedure step by step by **Controller Management** which is integrated in the Safety Builder.

Compatibility check

During the modification, Safety Manager performs a compatibility check of the application-related data, to guarantee a safe changeover from the existing configuration to the new configuration. The system reports *all* application changes in a detailed report in the Extended Diagnostics.

The user is expected to verify each reported change before starting up the system.

When modifications are implemented in an application, only a functional logic test of the modified functions is required by, for example, TUV. This must be done when the final verification of the implemented changes is obtained via the built-in sheet difference report in Controller Management diagnostics.

Safety Manager networks

If a system has been integrated into a Safety Manager communication network (SafeNet), it performs a compatibility check for all connected systems.

If it detects inconsistencies or if the check of a specific system cannot be completed for some reason, an error message is generated in the extended diagnostics. In case such an error occurs, no data will be exchanged with that system. The communication can only be established after a successful completion of the compatibility check by any of the Safety Managers that can communicate with each other, initiated via a QPP reset.

SafeNet communication

Safety Managers can be connected together to form safety-related networks. The protocol used for this network is called SafeNet.

SafeNet is available to Safety Managers for:

- Distributed processing
- Sharing safe data for joint SIS related tasks.
- SIL3, TUV approved, communication.
- Remote load

Networks

Attention:

USIs running 3rd party protocols may be vulnerable to communication overflow, causing USI outages and communication shutdown.

If communication overflow is a potential risk, we recommend to allocate all SafeNet links on dedicated USIs (not running vulnerable 3rd party protocols).

Data that is transferred between Safety Managers is represented in function logic diagrams as IO symbols with the location `FSC`. Points with location `FSC` can be of type DI or DO (markers), BI or BO (registers), and may be configured for safe and non-safe functions.

Protocol versus response time

The response time between Node ID and logical Peer ID depends on:

- the application program cycle time of the Node ID and Peer ID system in the logical link.
- the delay caused by the data layer protocol of the physical links.

Response time and time-out time are related.

The minimum time-out depends on the system application cycle and the type of communication link.

The time-out time you set must be larger than the maximum response time.

The response time to a communication request highly depends on the actual states of both Node ID and Peer ID system at the time of the request.

The maximum response time equals the sum of:

- the application cycle time of the Node ID plus
- the application cycle time of the Peer ID plus
- the expected communication delay.

The Node ID periodically sends data to the Peer ID systems and initiates a request for data from the Peer IDs. A *correct* answer must be provided for within the time-out period; when not received in time, the link is regarded faulty.

A new data transmission and request for a Peer ID are initiated after the Peer ID reply to the previous request has been received. This could be equal to the time-out time, but usually it is shorter.

SafeNet time-out time

All systems within the network monitor the operation of a communication link by means of a time-out.

- The time-out can be set for each individual logical link and must be chosen such that it stays within the Process Safety Time (PST) for the Safety Instrumented Functions (SIFs) involved.
- The time-out time set must be at least 2x the calculated response time.

Ethernet communication

When communicating via Ethernet you should be aware of the following:

- “Ethernet communication risks” on page 43
- “Ethernet bandwidth and response time calculation” on page 44

Ethernet communication risks

Attention:

USIs running 3rd party protocols may be vulnerable to communication overflow, causing USI outages and communication shutdown.

If communication overflow is a potential risk, we recommend to allocate all SafeNet links on dedicated USIs (not running vulnerable 3rd party protocols).

When devices communicate via an Ethernet based local area network (LAN), their information is contained and sent in packets. This is no different when using SafeNet through Ethernet. However, Ethernet has far less timing restrictions and, when sending SafeNet packets together with other application packets, some packets may suffer critical delay or get lost if a network gets congested.

Packet losses and network congestion may occur if e.g.:

- several devices start transmitting packets at the same time and/or,
- a single device generates a peak in network traffic,

Attention:

1. Risks are involved when using SafeNet on an *insecure, open or shared* Ethernet, where downtime, delays, loss and/or access to packets can be caused by other devices on the LAN.
   Such risks can be caused by office computers, network printers, servers and open access points (such as wifi access points, WAN routers, etc.)
2. Viruses and applications such as MSN Messenger may affect SafeNet reliability when active on the same Ethernet.

When the Ethernet is dedicated to a single Safenet, issues do not take place:

- No single SafeNet configuration can cause a 100MB Ethernet to operate at its maximum capacity (Safety Builder checks this in the configuration stage).

Packets are vulnerable to modifications or alterations when accessed by external systems: Applications running on these systems could (deliberately or via a virus infection) intercept, delay and/or alter packets.

Ethernet bandwidth and response time calculation

Please consult the release notes issued with your Safety Builder software for ways to determine bandwidth and response time.

Conventional serial communication

Please consult the release notes issued with your Safety Builder software for ways to determine bandwidth and response time.

Reset

The reset function is a means to allow Safety Manager to recover from an abnormal state. (Running fault free is the normal operating state.)

Safety related resets allow the recovery from all fault types whereas non safety related resets allow the recovery of non safety related faults only.

Safety related resets can be given via the reset key switch, via the ***Remote Reset*** button in Safety Builder (after enabling in the configuration) and by SM Controllers, initiating a safety related reset command via SafeNet.

System response towards a safety related reset

The response to a safety related reset action depends on the QPP state of the Control Processor. The following QPP states make the Control Processor respond to a reset:

1. `Running`
   The Control Processor is running without faults.
   Initiating a reset will have no effect on the SM Controller state.
2. `Running with Flt`
   The Control Processor is running with faults.
   Initiating a reset will move the faults logged in the actual fault database to the historical fault database (clearing the actual faults database) and log the reset.
3. `CPReady` (after startup or after recovering from a fault)
   (Both Control Processors contain the same application.)
   Initiating a reset, with a QPP in `CPReady` and identical applications residing in CP1 and CP2, will start the application in the ready QPP.
4. `CPReady` (during an OLM procedure)
   (Both Control Processors contain different applications.)
   Initiating a reset with a QPP in `CPReady` and different applications in the Control Processors (OLM) will cause an application switch-over from the running Control Processor to the ready (idle) Control Processor.
5. `Halt with Flt` (during an OLM procedure)
   (Both Control Processors contain different applications.)
   The Control Processor was halted due to a fault detected during the OLM compatibility check procedure. Initiating a reset will clear the fault database, run a new diagnostic cycle and log the result in the fault database.
   a. The QPP remains in the `Halt with Flt` state if faults are detected during the diagnostic cycle;
   b. The QPP goes to the `CPReady` (during OLM) state if no faults are detected.

Special requirements for TUV-approved applications

5

General

Safety Manager can be used for processes which require, amongst others, TUV approval. The requirements for the safety applications are the following:

1. The maximum application cycle time is half the Process Safety Time. For example, the accepted Process Safety Time for a burner control system in accordance with TRD-411 for boilers > 30 kW (July 1985) Table 1, TRD-412 (July 1985) Table 1 and DIN 4788 (June 1977) Part 2 Chapter 3.2.3.2 1 is 1 second.

   This implies that the application cycle time must be 0.5 second or less. The application cycle time is monitored by the SM Controller and can be seen on the **System Information** screen of Controller Management.

   The application cycle time is limited to 2.3 seconds by the watchdog, resulting in a maximum typical cycle time of 2 seconds. The typical application cycle time can be calculated by the Safety Manager MTBF and Cycle time calculation tool. This tool is available via Honeywell SMS and includes:

   - cycle time estimation based upon amount of IO, DTI, application complexity and communication parameters,
   - MTBF calculation

2. If Safety Manager detects a fault in output hardware that is configured with Fault Reaction `Low` or `0mA`, it will de-energize the faulty output modules or instead de-energize all outputs. The de-energization of faulty output modules or all outputs is fully implemented in the software and cannot be influenced by the user (see also item 3).

   If an output module (configured with Fault Reaction `Low` or `0mA`) is detected faulty, the outputs of that output module are switched off and the repair timer is started. The Control Processor then verifies the switch-off.

   - If the switch-off is verified the faulty output module can be replaced without affecting the status of the Control Processor and the

SM Controller reset before the repair timer expires. This stops the repair timer.

- If the repair timer expires or the switch-off cannot be verified all outputs connected to the Control Processor that controls the faulty output module are de-energized via the watchdog functionality. If the faulty output is located in a non-redundant IO section, all non-redundant outputs of the SM Controller are de-energized. De-energization is only effected if safety-related outputs are allocated to the faulty module.

3. If Safety Manager detects a fault in its output hardware (configured with Fault Reaction `Low` or `0mA`, see item 2 above), the repair timer is started. When this timer expires, all outputs are de-energized via the watchdog functionality. This timer can be set to the following values:
   - Not used. The timer is not started so an output fault may be present in the system without further action.
   - 0 minutes. This results in immediate de-energization of all outputs in case of an output fault.
   - 0 hours to 2047 hours. This represents the interval time between the fault occurrence and automatic system shutdown.
4. If Safety Manager detects a fault in its input hardware (configured with Fault Reaction `Low`, `High`, `Bottom scale`, `Top scale`), the faulty input is set to its configured Fault Reaction state.
5. Analog outputs may not be used as part of a safety loop when the *`Test disabled`* check box in **IO properties** is selected.
6. Input points with location `COM` may only be used for non safety-related functions.
7. The watchdog functionality of Safety Manager contains a shutdown (SD) input. For normal operation, the SD input must be 24 Vdc. If the input is forced to 0 V, a Safety Manager shutdown and de-energization of the outputs take place, independent of the QPP.
8. For more details on IO wiring details, termination of IO signals and power supply distribution see *Hardware Reference*.
9. The Diagnostic Test Interval (DTI, the time in which all IO tests are executed) can be set for each SM Controller in the Controller Properties in the Network Configurator.
10. The repair timer can be set for each SM Controller in the Controller Properties in the Hardware Configurator.
11. The values of the voltage monitor analog input channels of the SAI-1620m modules must be checked in the application to ensure that they are within the transmitter power supply range of the transmitters connected to that analog input module.

12. To reduce the influence of disturbances on the power supply lines, all major metal parts (cabinet sidewalls, doors, 19-inch chassis, horizontal bus chassis and flaps, swing frames, etc.) must be properly grounded.
13. All power supply inputs (except 110/230 Vac) require a power supply filter directly fitted after the power supply input terminals.
14. Grounding of the power supplies of Safety Manager is only permitted for the 0 Vdc. Grounding of the +24 Vdc / +48 Vdc / +60 Vdc / +110 Vdc is not allowed because an earth fault results in an unsafe situation.
15. The wiring of the external power supply (24 Vdc) and the internal power supply (5 Vdc) must be physically separated. This can be realized by using separate ducts and a separate power supply distribution.
16. Do not use radio frequency transmitting equipment within a radius of 1 m (3 ft) of the system cabinet when the doors are opened.
17. Safety-related inputs require the use of tested input modules (SDI-1624, SDI-1648, SAI-1620mm, SAI-0410, or SDIL-1608) and safety-related input sensors (transmitters). If the input sensors (transmitters) are not safety related, multiple sensors (transmitters) must be used.
18. If Safety Manager operates without operator surveillance, some measures have to be taken. During the design and implementation stages of the safety system a reliability calculation analysis (the maximum time period in which inspection has to take place) has to be performed. Without operator surveillance the following measures have to be taken to comply with the safety integrity requirements:
    - Inspection of Safety Manager status if the Safety Manager application is fault free, at least once per determined time period.
    - Alarm indication of Safety Manager if a fault is detected and subsequent inspection of the Safety Manager status within the safety determined time period.
19. The operating conditions of Safety Manager shall not exceed the following ranges:)
    - Operating temperature: –5°C to 70°C (23°F to 158°F)
    - Relative humidity: 5% to 95%, non-condensing
    - Vibration: 1G (10-55-10 Hz)
    - Shock: 15 G (11 ms, 3 axes, both directions of the axe)
    - Supply voltage: 110 Vdc (+25% / –15%), 48 Vdc (+15% / –5%), 24 Vdc (+30% / –15%)

    For details refer to *Hardware Reference*.

    The operating temperature is measured in Safety Manager. This temperature is higher than the temperature outside the cabinet, which results in a lower ambient temperature for the cabinet. Depending on the internal dissipation in the cabinet and the ventilation, a temperature difference of 25°C (77°F) is allowed, which results in a maximum ambient temperature of 45°C (113°F). To minimize the temperature difference, forced ventilation with one or more fans may be required. By using the temperature pre-alarm setpoints, an alarm can be given if the internal temperature is too high.

20. The storage conditions of the Safety Manager hardware modules shall not exceed the following ranges:

    Storage temperature: –40 to +85°C (–40 to 185°F).

21. If modifications have been made to the application program in the SM Controller or the visualization

22. Most modifications made to the application programs require the application program to be loaded into the SM Controller. Some modifications, such as renaming tag numbers, can be completed without loading.

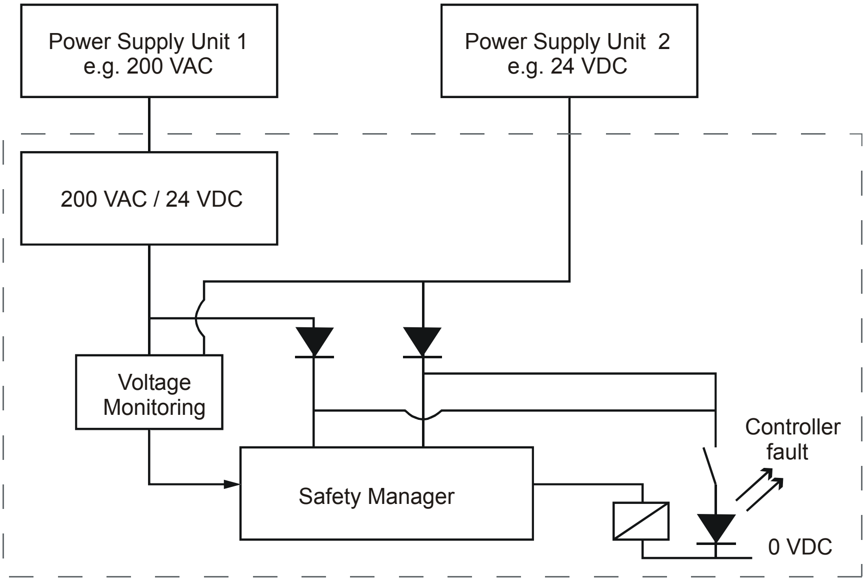
    It is mandatory that, after verification and approval of *any type* of application modification, proper configuration management is applied to make sure that all that all stations and backup systems that may have an instance of this application program get updated to the modified version.

F&G applications

Fire and Gas (F&G) applications have the following additional requirements:

1. Each visual indication (alarm, override or test, failure) shall have its own dedicated digital output. This digital output may be a hardware output or a communication output, e.g. to a DCS system. Override and test status may be combined in one visual indication. Alphanumeric displays are not supported.
2. Redundant power supplies must be connected to Safety Manager in such a way that the redundant power supplies do not fail at the same time, e.g. by using different primary power sources (e.g. 220 Vac mains and a 24 Vdc from a battery backup). Detection of power supply failure (e.g. via a voltage-monitoring module) shall be part of the system design.

Figure 11 Power supply



3. Faults in the Fire & Gas detection system are indicated visually. This indication must also be active if the Fire & Gas detection system has been switched off. This can be set up as shown in Figure 11 on page 51, using a normally de-energized relay, or via a visual indication in a DCS display which is activated if the communication to the Fire & Gas detection system fails. The protected side of the fuses are connected to a voltage-monitoring device to detect blown fuses.

4. The field instruments, including panel instruments such as (key) switches, which are used in conjunction with Safety Manager, must meet the requirements of the applicable parts of the EN-54 standard. Visual and audible indications shall be as defined in paragraph 3.2 of EN-54 part 2.
5. Field inputs must have loop-monitoring to detect short-circuits and open loops. Input module types that can be used are: SAI-0410, SAI-1620m and SDIL-1608.

   Field outputs must also have loop-monitoring. Output module type that can be used: SDOL-0424.
6. The Fire & Gas detection system shall have earth leakage monitoring/detection facilities.
7. Remote display of alarms, failures etc. may only be given via interconnection of Safety Manager systems using the communication option between Safety Manager systems or via hard wired outputs with loop-monitoring via the SDOL-0424 digital output modules. Communication and loop monitoring failures must be alarmed.
8. Safety Manager is only the basis for an EN-54 compliant application. The responsibility for a full EN-54 compliant application lies with the person(s) responsible for configuring and application programming of Safety Manager. The requirements of EN-54 which must be met by the application can be found in section 9, which references the requirements that must be fulfilled in the application.
9. For details on the requirements of the mechanical construction (cabinet, indications, horns) refer to “EN-54 part 2 paragraph 3.2.”

Fax Transmittal **Fax Number: +31 (0)73 6219 125**

Reader Comments

To: Honeywell Safety Management Systems, attn. Technical Documentation Group

From: Name: Date:

Title:

Company:

Address:

City: State: Zip:

Telephone: Fax:

Safety Manager Safety Manual, Release 131, Issue 4, 10 July 2008

Comments:

You may also call the Technical Documentation Group at +31 (0)73 6273 273,
email Honeywell SMS at sms-info@honeywell.com, or write to:

Honeywell Process Solutions
Safety Management Systems
P.O. box 116
5201 AC ‘s-Hertogenbosch
The Netherlands

Safety Manager
User documentation

Honeywell

Honeywell Process Solutions
Safety Management Systems
Rietveldenweg 32a
5222 AR ‘s-Hertogenbosch
The Netherlands