XPSMF60/XPSMF40

Safety Manual

03/2017

33003792.05

www.schneider-electric.com

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

Table of Contents

Safety Information

Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

About the Book

At a Glance

Document Scope

This manual contains information for proper application of the safety-related XPSMF60/XPSMF40 automation devices.

Knowledge about the regulations and the proper application of the safety information contained in this manual by qualified personnel are prerequisites for the safety-related installation, start-up, operation, and use of the XPSMF60/XPSMF40 automation devices.

Validity Note

The safety-related XPSMF60/XPSMF40 programmable controllers (programmable electronic systems, PES) are tested and certified by TÜV for functional safety in accordance to and the standards listed below:

- TÜV Rheinland Industrie Service GmbH
  Automation, Functional Safety
  Am Grauen Stein
  51105 Köln
- Test report No. 968/EZ 236.04/12 (XPSMF40)
  Test report No. 968/EZ 217.02/12 (XPSMF60)
- International standards:
  - IEC 61508, part 1-7: 2000
  - IEC 61511, part 1-3: 2004
  - EN 12067-2: 2004, EN 298: 2003, EN 230: 2005
  - NFPA 85: 2011
  - EN / IEC 61131-2: 2007
  - EN 61000-6-2: 2007
  - EN 54-2: 1997 + AC:1999 + A1:2006+ A1:2007, NFPA 72: 2010
    (XPSMF40 is only compliant to this standard if suited remote I/O modules are used.)
  - EN / ISO 13849-1: 2008 + AC:2009 Performance level e

- EN / IEC 62061: 2005 + AC: 2010
- EN 50156-1: 2004
- NFPA 86: 2011
- EN 50130-4: 1989 + A1: 1989 +A2: 2003 + Corr. 2003

The chapter *Test Conditions, page 133* contains a detailed listing of all applied environment and EMC tests.

All devices are labelled with the CE sign.

To program the XPSMF60/XPSMF40 devices, a PADT (programmer unit, PC) running the programming tool XPSMFWIN and the program languages function block diagram (FBD) and sequential function chart (SFC) in accordance to IEC 61131-3 is used. This software assists the user in creating safety-related programs and operation of the PES.

The technical characteristics of the devices described in this document also appear online. To access this information online:

Step	Action
1	Go to the Schneider Electric home page *www.schneider-electric.com*.
2	In the **Search** box type the reference of a product or the name of a product range. ● Do not include blank spaces in the reference or product range. ● To get information on grouping similar modules, use asterisks (*).
3	If you entered a reference, go to the **Product Datasheets** search results and click on the reference that interests you. If you entered the name of a product range, go to the **Product Ranges** search results and click on the product range that interests you.
4	If more than one reference appears in the **Products** search results, click on the reference that interests you.
5	Depending on the size of your screen, you may need to scroll down to see the data sheet.
6	To save or print a data sheet as a .pdf file, click **Download XXX product datasheet**.

The characteristics that are presented in this manual should be the same as those characteristics that appear online. In line with our policy of constant improvement, we may revise content over time to improve clarity and accuracy. If you see a difference between the manual and online information, use the online information as your reference.

Related Documents

Title of Documentation	Reference Number
Safety Suite V1 Installation Instruction	33003529
XPSMF60 Hardware Manual	33003387
XPSMF40 Hardware Manual	33003363
XPSMFWIN Software Manual	33003788

You can download these technical publications and other technical information from our website at http://www.schneider-electric.com/en/download

Product Related Information

Knowledge about the regulations and the proper application of the safety information contained in this manual by qualified personnel are prerequisites for the safety-related installation, start-up, operation, and use of the XPSMF60/XPSMF40 automation devices.

In case of unqualified interventions into the automation devices, de-activating or bypassing safety functions, or if advices of this manual are neglected (causing disturbances or impairments of safety functions), severe personal injuries, property or environmental damage may occur for which Schneider cannot take liability.

XPSMF60/XPSMF40 automation devices are developed, manufactured and tested according to the relevant safety standards. They must only be used for the applications described in the instructions with the specified environmental conditions, and only connected with approved external devices.

Chapter 1
Introduction

Overview

This chapter gives a general overview of the XPSMF60/XPSMF40 Safety Manual.

What Is in This Chapter?

This chapter contains the following sections:

Section 1.1
Safety

Overview

This section gives a general overview about safety.

What Is in This Section?

This section contains the following topics:

Safety

Overview

The programmable controllers are designed for use in the deenergize to trip mode, i. e. the peripherals and the function of the controller interprets a deenergized state as a safe state.

In the event of a fault, the input and output signals revert to a voltage-free or current-free state to ensure a safe operation.

PFD and PFH

PFD and PFH calculations have been carried out for the XPSMF60/XPSMF40 systems in accordance to IEC 61508.

IEC 61508-1 sets a PFD of 10^{-4} to 10^{-3} and a PFH of 10^{-8} to 10^{-7} per hour for SIL 3.

Controller (PES)

For the controller (PES), 15 % of the limit value is assumed from the standard for PFD and PFH.

This results in limit values of $1.5 * 10^{-4}$ per hour (for the PFD section of the controller) and $1.5 * 10^{-8}$ per hour (for the PFH section).

XPSMF60/XPSMF40

The interval for the repeat test for XPSMF60/XPSMF40 systems is set to 10 years, 3 years for relay output modules of the XPSMF60 (Off-line Proof Test, see IEC 61508-4, *paragraph 3.8.5*).

The safety functions, consisting of a safety-related loop (input, processing module, output and communication between XPSMF60/XPSMF40 systems) fulfil the above requirements whichever way they are combined. The remote I/O modules also fulfill these requirements.

NOTE: Further information is available on request.

Deenergize to Trip Mode / Energize to Trip Mode

Overview

The programmable controllers are designed for use in the deenergize to trip mode.

XPSMF60/XPSMF40 System

The XPSMF60/XPSMF40 systems are certificated for process controllers, safety systems, burner systems and machine controllers.

A system operating according to the deenergize to trip mode does not need energy to perform its safety function.

In the event of a fault, the input and output signals revert to voltage-free or current-free states to ensure safe operation.

The XPSMF60/XPSMF40 controllers can also be used in energize to trip mode applications. A system operating according to the energize to trip mode needs energy, for example electrical or pneumatic energy, to perform its safety function.

Therefore XPSMF60/XPSMF40 system were tested and certificated according to EN54 and NFPA72 for use in fire alarm systems and fire extinguish systems. In these systems it is necessary that on demand the active state is used for controlling the danger (further details see *General, page 129*).

NOTE: XPSMF40 is only compliant if suited remote I/O modules are used.

Section 1.2
Safety Requirements

Overview

The following safety requirements must be followed when using the safety-related PES of the XPSMF60/XPSMF40 system.

What Is in This Section?

This section contains the following topics:

Hardware Configuration

Product Independent Requirements

- For proper safety-related operation, only the specified hardware and software components should be used. The permitted hardware modules and software components are listed in the *Revision List of Devices and Firmware of XPSMF60/XPSMF40-Systems of Schneider Electric GmbH / HIMA Paul Hildebrandt GmbH + Co KG, Certificate-No. 968/EZ 217.00/06* as well as in the *EC Type Examination Certificate Reg.-No.: 01/205/5234/12 for XPSMF60 and Reg.-No.; 01/205/5233/12 for XPSMF40*. The valid versions are contained in the version list, which is maintained together with the approval authority.
- The specified operating conditions (see *Test Conditions, page 133*) regarding EMC, mechanical, chemical and climatic influences must be followed.
- Hardware modules and software components that are not fail safe (but which do not cause any reactions) can be used to process non-safe signals. They cannot, however, be used to carry out safety-related tasks.
- The deenergize to trip mode should be used in all external safety circuits connected to the system.

Product Dependent Requirements

- Only equipment that can be safely isolated from the mains should be connected to the system.
- The safe electrical isolation of the power supply must take place in the 24 V supply. Only PELV or SELV power supplies may be used.

Programming

Product Independent Requirements

- In the case of safety-relevant applications, ensure that the safety-relevant system variables are correctly configured.
- Particular attention should be paid to the system configuration, the maximum cycle time and the safety time.

Product Dependent Requirements

Requirements for using the programming system:

- The XPSMFWIN tool must be used for programming purposes.
- After the application has been created, check that the compilation was successfully carried out by manually compiling twice and comparing the CRCs.
- The correct conversion of the specification of the application should be validated and verified. A comprehensive test of the logic must be carried out.
- This procedure must be repeated each time a modification is made to the application.
- The error response of the system (when a fault occurs in the fail-safe input/output modules) must be determined by the application program according to the plant-specific safety aspects.

Communication

Total Response

When safety-related communication is used between different devices, ensure that the total response time of the system does not exceed the fault tolerance time. The basis for calculations listed in *Safety-Related Communication (Peer-to-Peer), page 121* should be used.

Safety-Related Data

At present it is not permitted to transfer safety-related data using public networks (e.g. the internet).

Protection Against Manipulation

If the data is to be transferred across company/factory networks, care must be taken (via administrative or technical means) to ensure that sufficient protection is provided against manipulation (e.g. using a firewall to keep the safety-relevant part of the network separate from other networks).

Serial Interfaces

At this stage, the serial interfaces should only be used for non-safety-related purposes.

Safe Electrical Isolation

Only devices that have safe electrical isolation should be connected to the communication interfaces.

Special Operating Modes

Maintenance Override

When using *Maintenance Override*, the most recent version of the *Maintenance Override* document of TÜV Rheinland and TÜV Product Service should be followed (see *General Information on Forcing, page 91*).

Access Protection

If necessary, the operator must consult the acceptance department responsible for the application to determine the administrative measures required to provide access protection to the systems.

Safety Times

Overview

Individual errors, which can lead to a dangerous operating state, are detected by the self-test devices and within the safety time, will lead the controller to defined error responses which transfer the faulty components into a safe state.

Fault Tolerance Time

The fault tolerance time (FTZ) is a characteristic of the process and it describes the period of time in which the process can receive faulty signals without a dangerous situation arising. A dangerous situation can arise if a fault is present for longer time than the FTZ.

(FTZ, see DIN VDE 0801, appendix A1 2.5.3)

Safety Time (of PES)

The safety time is the time in which the PES (in RUN state) must react after an internal error has occurred.

In terms of the actual process, the safety time is the maximum amount of time within which the safety system must respond to the outputs when the input signals change (response time).

In case of the controllers, times in the region of 20... 50,000 ms can be achieved.

Multi-Fault Occurrence Time ()

The occurrence time for multiple faults is the period of time within which the probability of multiple faults occurring (which, when combined, are critical with regard to safety) is sufficiently small.

The multi-fault occurrence time is defined as 24 hours in the operating system.

Response Time

The maximum response time of cyclic XPSMF60/XPSMF40 controllers is twice the cycle time of these systems, but only if there is no delay caused by parameterization or logic of the application program.

The cycle time of a controller involves the following important operations:

- reading the inputs
- processing the application program
- writing the outputs
- process data communication
- carrying out test routines

In addition, in the worst case scenario for the whole system, the switching times of the inputs/outputs should be taken into account.

Watchdog Time

The watchdog time is specified as the time in the menu for setting the PES attributes. It is the maximum permitted duration of a RUN cycle (cycle time). If the cycle time exceeds the specified watchdog time, the CPU goes into ERROR STOP.

The CPU watchdog time must be set between 2 ms and ½ * safety time of the PES.

The maximum value permitted is 5,000 ms.

Default settings: XPSMF60/XPSMF40 50 ms.

Offline Proof-Test

Overview

The offline proof-test recognizes dangerous concealed faults that would affect the safe function of the plant.

XPSMF60/XPSMF40 safety systems have to be subjected to an offline proof test in intervals of 10 years.

For relay modules, the proof test for the relays has to be carried out in intervals defined for the respective plant.

Execution of the Offline Proof Test

The execution of the offline proof test depends on the configuration of the plant (EUC = equipment under control), which risk potential it has, and which standards for operation are applied and form the bases for the approval by the test authority in charge.

According to the standards IEC 61508 1-7, IEC 61511 1-3, EN/IEC 62061, and VDI/VDE 2180 sheet 1 to 4, in case of safety-related systems the operating company has to arrange for proof tests.

Periodic Proof Testing

The XPSMF60/XPSMF40 can be proof tested by exercising the full safety loop.

In practice the input and output field devices have a more frequent proof test interval (e.g., every 6 or 12 months) than the XPSMF60/XPSMF40. If the end-user tests the complete safety loop because of the field devices then the XPSMF60/XPSMF40 is automatically included in these tests. No additional periodic tests are required for the XPSMF60/XPSMF40.

If the proof test of the field devices does not include the XPSMF60/XPSMF40 then the PES needs to be tested as a minimum once in 10 years. This can be done by executing a reset of the XPSMF60/XPSMF40.

In case there are periodic proof test requirements for specific modules then the end-user should refer to the data sheets of these modules.

Chapter 2
Central Functions

Overview

The device types XPSMF40 are compact systems, which cannot be modified.

Type XPSMF60 controllers are modular systems; up to six I/O modules can be inserted inside a controller with a power supply module and a central processing module.

What Is in This Chapter?

This chapter contains the following topics:

Power Supplies

Overview

A power supply module is only available with XPSMF60. In the case of compact devices, this function is integrated into the system and cannot be viewed in a modular way.

The power supply module PS 01 (for XPSMF60) or the integrated function converts the 24 V system supply voltage to 3.3 V and 5 V (use for internal I/O bus).

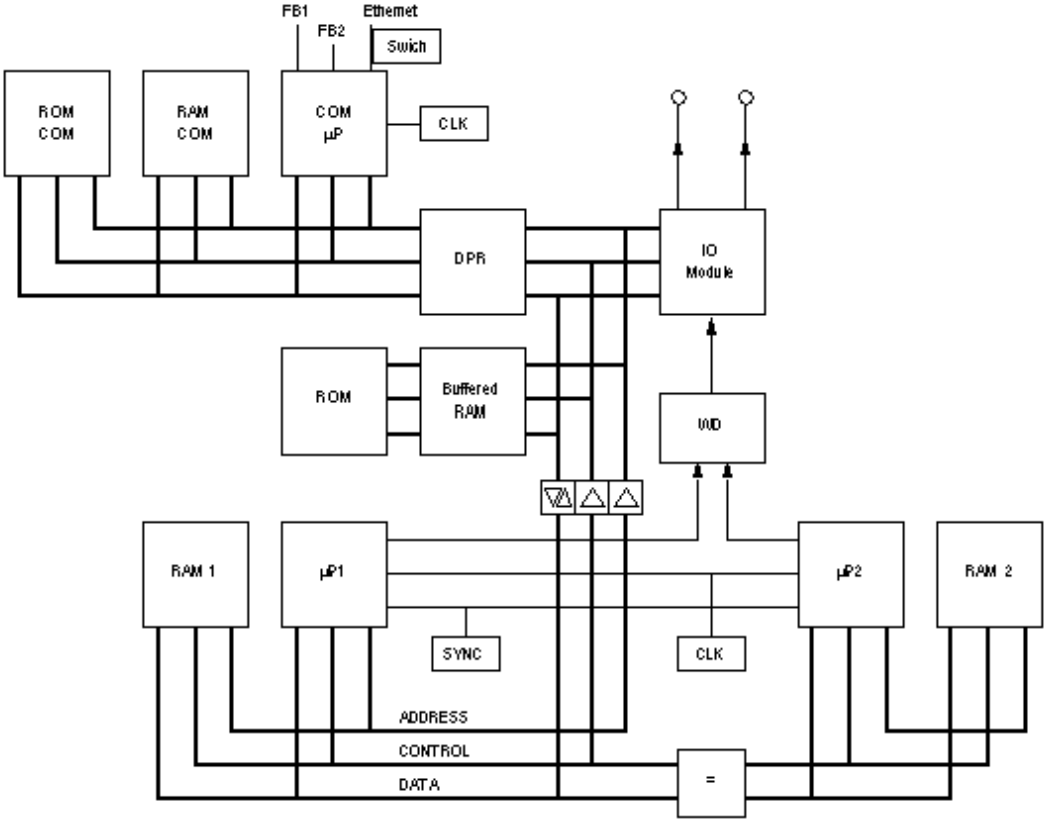
Functional Description of the Central Section

Overview

The central module (example) consists of the following function blocks.

Representation

Function blocks, using CPU01 of XPSMF60 as an example



Central Module Attributes

Attributes of the central module CPU01 of XPSMF60:

- Two synchronous microprocessors (µP1 and µP2)
- Each microprocessor has its own RAM memory
- Testable hardware comparators for all external accesses of both microprocessors
- In the event of an error the watchdog is set to a safe state
- Flash EPROMs of program memories for operating systems and application programs, suitable for at least 100,000 storage cycles
- Data memory in NVRAM
- Multiplexer for connecting I/O bus, Dual Port RAM (DPR)
- Backup supply (goldcap) for date/time
- Communication processor for field bus and Ethernet connections
- Interface for data transfer between XPSMF60/XPSMF40 devices and the PADT, based on Ethernet
- Optional interface(s) for data exchange via field bus
- Signaling of system status via LEDs
- I/O bus logic for connection to I/O modules
- Safe watchdog (WD)
- Power supply monitoring, testable (3.3 V / 5 V system voltages)

Self Tests

Overview

The most important self-test routines of the safety-related central modules of the controllers and the coupling to the I/O tier are listed below.

Microprocessor Test

The following are tested:

- all commands and addressing modes used
- the writability of the flags and the commands generated by them
- the writability and crosstalk of the registers

Test of the Memory Areas

The operating system, application program, constants and parameters as well as the variable data are saved in both processor areas in each central module and are tested by a hardware comparator.

Protected Memory Areas

The operating system, application program and parameter areas are each stored in a memory. They are protected by write protection and a CRC test.

RAM Test

The modifiable RAM areas, in particular stuck-at and crosstalk, are tested with a write and read test.

Watchdog Test

The watchdog signal switches off if it is not triggered from both CPUs within a defined time window and also if the test of the hardware comparator fails. A separate test determines whether the watchdog signal is able to switch off.

Test of the I/O Bus Inside the Controller

The connection between the CPU and the associated inputs and outputs (I/O modules) is tested.

Reactions to Faults in the CPU

A central hardware comparator permanently checks whether the data in microprocessor system 1 is identical to the data in microprocessor system 2. If it is not identical or if the central test routines return a negative result, the controller automatically goes into ERROR STOP and the watchdog signal is switched off. This means that input signals are no longer processed and the outputs switch to the deenergized switched off state.

If such a fault occurs for the first time, the controller is restarted (reboot). If a further internal fault occurs within the first minute after start-up, the controller enters the STOP/INVALID CONFIGURATION state and will remain in this state.

Error Diagnosis

Overview

All XPSMF60 modules have an LED to indicate errors in the event of faults in the module or the external wiring. This facilitates a quick fault diagnosis of a module that has been signaled as faulty.

XPSMF Systems

Due to the fact that XPSMF40 systems are compact systems, these fault displays are grouped together as a group fault signal.

In addition, an evaluation of various system signals can take place in the application with status displays of the inputs/outputs or of the CPU.

Fault signaling only takes place if the fault does not prevent communication with the CPU, i. e. the CPU is still able to evaluate the signals.

The error codes of all input and output signals and those for the system signals can be evaluated via the logic of the application program.

An extensive diagnostic record of system performance and faults detected are stored in the diagnostic memory of the CPU and the COM. The record can be read out via the PADT, even after a system fault.

Details about the analysis of diagnosis messages see *System Manual Compact Systems or System Manual Modular System XPSMF60, chapter Diagnosis.*

Chapter 3
Inputs

Overview

This chapter describes the inputs.

What Is in This Chapter?

This chapter contains the following sections:

Section 3.1
Overview

Hardware Overview

Modular XPSMF60 Controller

Digital inputs

Module	Quantity	Safety-Related	Non-Interacting	Electrically Isolated
XPSMF DIO241601	24	+	+	+
XPSMF DI3201 (with Line Control Configurable)	32	+	+	+
XPSMF DI2401 (110 V)	24	+	+	+

Analog inputs

Module	Quantity	Safety-Related	Non-Interacting	Electrically Isolated
Counter 24bit: XPSMF CIO2401	2	+	+	+
Analog Inputs: XPSMF AI801	8	+	+	+

+ Applicable
- Not applicable

XPSMF40 Controller

System Section	Quantity	Safety-Related	Non-Interacting	Electrically Isolated
Digital Inputs	24	+	+	-

+ Applicable
- Not applicable

Section 3.2
General

General Information on Inputs

Overview

Safety-related inputs can be used for both safety-related and non-safety-related signals.

Status Signals

Apart from the diagnostic LEDs of the modules, the controllers also send status signals to the application program, which can be evaluated. I/O errors stored in the diagnostic memory can be read using XPSMFWIN.

Cyclic Self-Tests

Safety-related input modules are automatically subject to stringent cyclic self-tests during operation. These test routines are TÜV tested and monitor the safe functioning of the relevant module.

Fault Information

In the event of a fault, a 0-signal is sent to the application program. Detailed fault information will be also generated in any case. This fault information can be evaluated in the application program by reading the error codes.

Non-Safety-Related Signals

For a few component failures, which do not impinge on safety, no diagnostic information is generated.

Section 3.3
Safety of Sensors, Encoders and Transmitters

Safety Requirements

Overview

In a safety-related application, both the PES and the sensors connected to it must meet the safety requirements (SIL).

SIL

The safety-related sensors, encoders and transmitters with the required SIL can be connected to the PES inputs. If there are no sensors, encoders and transmitters with the specific SIL, they can also be connected. However the application program must then handle the logic and monitoring of the signals.

Information on how to achieve the required SIL is contained, for example in *IEC 61511-1 standard, Paragraph 11.4*.

Section 3.4
Safety-Related Digital Inputs

Overview

The points listed below apply to both digital input channels of XPSMF60 modules and digital input channels of all compact systems XPSMF40 (unless stated otherwise).

What Is in This Section?

This section contains the following topics:

General

Overview

The digital inputs are read once per cycle and saved internally; cyclic tests are carried out to assure their function safety.

Input Signals

Input signals, which are present for shorter time than the time between two samplings (i. e. shorter than a cycle time), are possibly not recorded.

Test Routines

Input Signals

The online test routines check whether the input channels, regardless of the pending input signals, are able to connect both signal levels (L and H signals). This test is carried out each time the input signals are read.

Reaction in the Event of a Fault

Overview

If the test routines detect a fault in the digital inputs, a 0-signal is processed in the application program for the defective channel according to the deenergize to trip mode. The LED ERR on the module of the XPSMF60 or the LED FAU on the XPSMF40 is then activated.

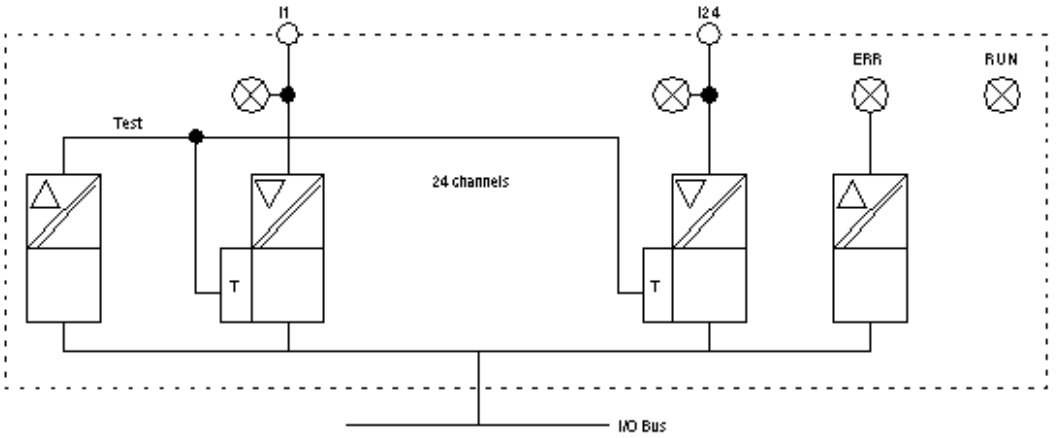
Error Code

In addition to the signal value of the channel, the relevant error code must be taken into account in the application program. The error code gives you the ability to provide fault handling in the application program and to diagnose the external wiring.

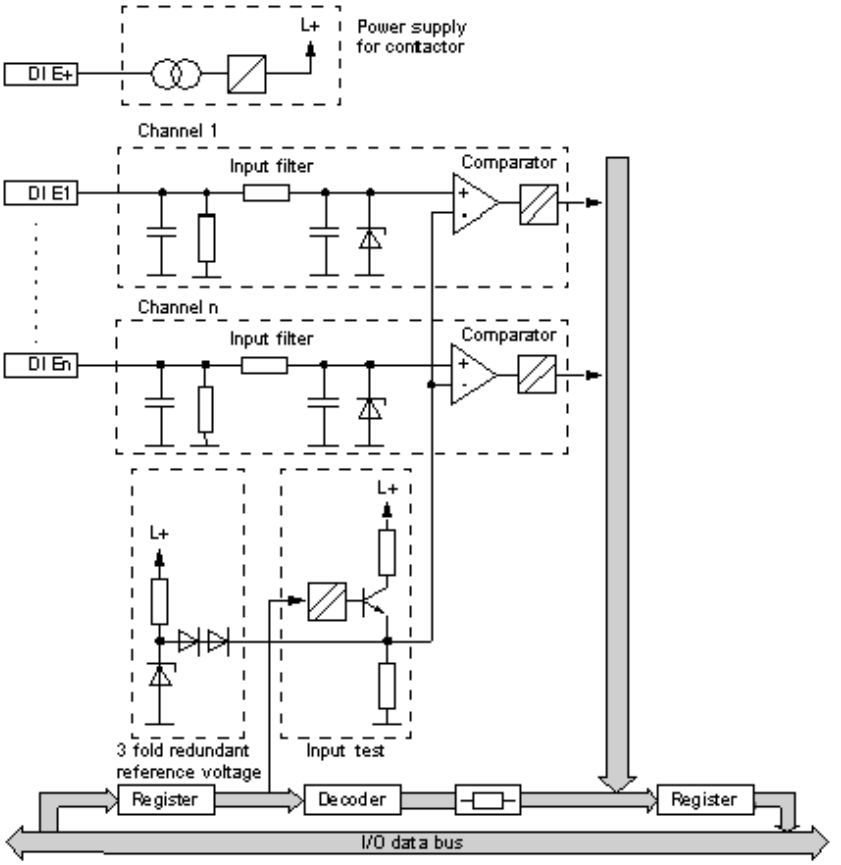
Diagram of the Digital Inputs

Representation

View of the functions, using the XPSMF DIO241601 module as an example



View of the functions of safety-related digital inputs XPSMF40



Surge on Digital Inputs

Overview

In the case of digital inputs, an EN 61000-4-5 surge impulse can be read as a shorttime high signal (caused by the fast cycle time of the XPSMF60/XPSMF40 systems).

To avoid errors of this type, one of the following measures must be taken in respect to the applications:

- Installation of shielded input lines to prevent the effects of surges in the system,
- Fault masking in the application program: A signal must be present for at least two cycles before it is evaluated.

NOTE: Proper EMC design techniques will allow the designer of the safety system to achieve the maximum performance by using the minimum response time of the safety PLC.

Parameterizable Digital Inputs

Overview

The digital inputs of the XPSMF35 control module operate according to the principle of analog inputs, but set to digital values by parameterization of operating points.

For parameterizable digital inputs the test routines and safety functions for analog inputs apply as mentioned in *Test Routines, page 50*.

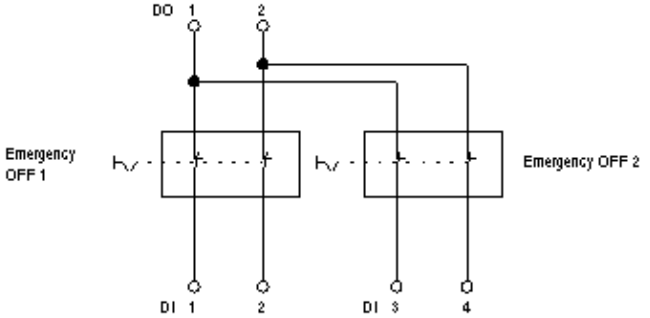
Line Control

Overview

Line Control is a short-circuit and line break monitoring system, for example, of EMERGENCY STOP devices, which can be configured on XPSMF60/XPSMF40 systems with digital inputs (not with parameterizable digital inputs, see chapter *Parameterizable Digital Inputs, page 44*).

Line Control

In addition, digital outputs DO are connected to the digital inputs DI of the same system, as shown below (example):



Emergency OFF switches according to standard, e. g EN 60947-5-1, EN 60947-5-5

Pulsed Outputs

The controller pulses the digital outputs to detect the line short-circuits and open-circuits to the digital inputs. To do so, configure the DO[01].Value system signal in ELOP II Factory. The variables for the pulsed outputs must begin with channel 1 and reside in direct sequence, one after the other (*see system signals in corresponding manuals*):

The LED ERR on the front plate of the module XPSMF60 or the LED FAU of the XPSMF40 flashes, the inputs are set to 0 and an error code (which can be evaluated) is generated when the following faults occur:

- short-circuit between two parallel lines,
- change of two lines (e.g. DO 2 to DI 3),
- earth fault on one of the lines (only with earthed reference pole),
- line break or opening of the contacts, i. e. when one of the Emergency OFF switches (displayed figure in section *Line Control, page 45*) is pressed, the LED flashes and the fault code is generated.

Section 3.5
Safety-Related Analog Inputs

Overview

This section describes the safety-related analog inputs.

What Is in This Section?

This section contains the following topics:

General

Overview

The input signals in the analog input channels are converted to an `Integer` value. The application program can then use this value.

The safety-related accuracy is the guaranteed accuracy of the analog input without error reaction of the module. This value should be taken into account when the safety functions are configured.

XPSMF60 Controller

The following input values are available:

Input Channels AI 801	Measuring Method	Current, Voltage	Range of Values in the Application		Safety Accuracy
			FS1000[1)]	FS2000[1)]	
8	unipolar	-10...+10 V	-1000...1000	-2000...2000	1%
8	unipolar	0...20 mA	0...1000[3)]	0...2000[3)]	1%
8	unipolar	0...20 mA	0...500[2)]	0...1000[2)]	4%
4	bipolar	-10...+10 V	-1000...1000	-2000...2000	1%

1) Specified via device type selection (XPSMF60)
2) With external shunt 250 Ω
3) With external shunt 500 Ω (accuracy 0.05%, P 1W)

XPSMFAI801

The module XPSMF AI801 from the XPSMF60 can be configured in the application program for use with eight unipolar or four bipolar functions. However, the mixing of functions on a module is not permitted.

The analog inputs of the XPSMF60 module XPSMF AI801 operate with voltage measurement.

Measurement

In the case of an open-circuit fault (there is no line monitoring in the system), any input signals will be received on the high-resistance inputs. The value resulting from this fluctuating input voltage is not reliable; with voltage inputs, the channels must be terminated with a 10 kΩ resistor. The output impedance of the source should be taken into account.

To measure a current, the shunt is connected in parallel to an input; the 10 kΩ is then not required.

If input channels are not used, the measurement input must be connected to the reference potential. Negative influences (fluctuating input voltages) on other channels in case of a line break are avoided.

For the unused input channel the corresponding signal AI[0x]. Used has to be set to the default value FALSE or 0 in XPSMFWIN Hardware Management. By this the channel is decommissioned in the application program, i.e. no signals of this channel are available within the logic.

Test Routines

Overview

The analog values are processed in parallel via two multiplexers and two analog/digital converters with 12-bit resolution and the results are compared. In addition, test values are connected to digital/analog converters and converted back to digital values, which are then compared with the specified value.

Errors

When an error is detected, the input is set to 0 for further processing by the application program, and the error state is set.

Reaction in the Event of a Fault

Overview

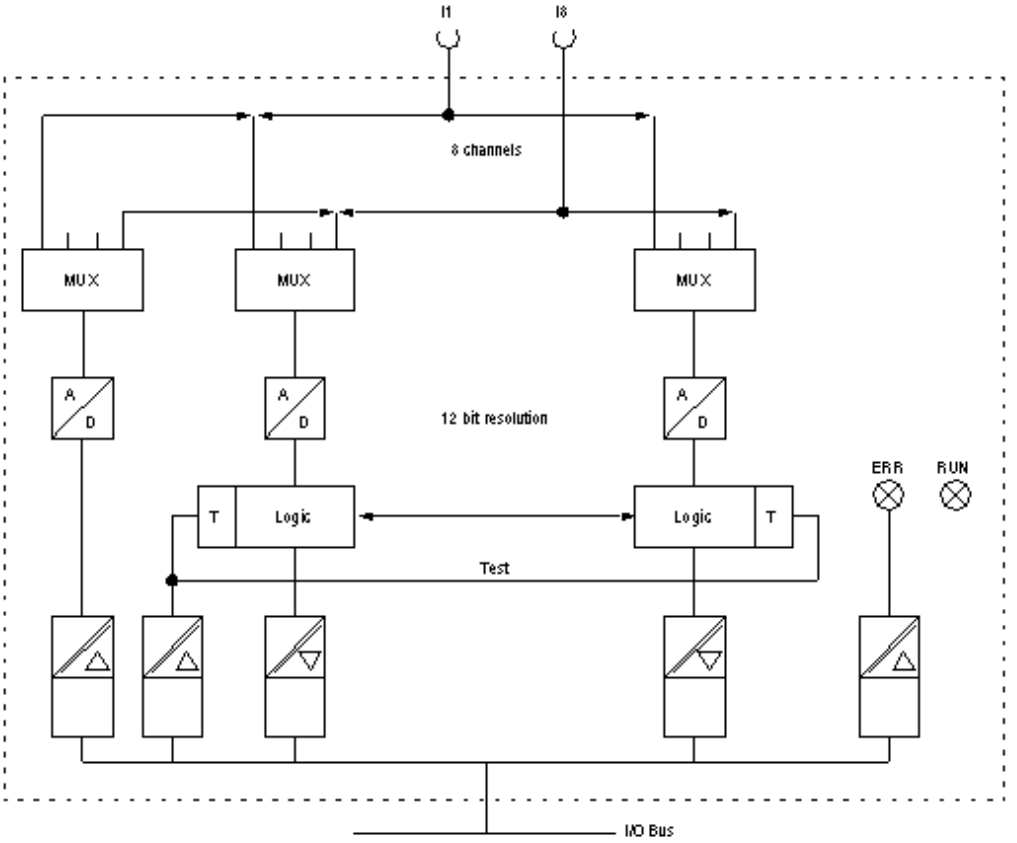
If there are channel faults in the analog inputs, the error code of the corresponding channel is set to a value > 0. If the entire module is faulty the error code for the module is set to a value > 0. The LED ERR is activated in both cases.

The analog input value must be interlocked with this status information (error code of analog inputs) within the application program. In case of a value > 0 a safety-related reaction must be programmed.

Diagram of the Analog Inputs

Representation

View of the functions, using input module XPSMF AI801 as an example



Section 3.6
Safety-Related Counters

Overview

The points listed below apply to XPSMF60 counter modules.

What Is in This Section?

This section contains the following topics:

General

Overview

Depending on the configuration, the counter module can be operated in the application program as a high-speed up or down counter with 24-bit resolution or as a decoder in Gray code.

Counter Module

If used as a high-speed up or down counter the pulse input and count direction input signals are required in the application. A reset only takes place in the application program.

The XPSMF60 counter module has 4 or 8-bit encoder resolution. A reset is possible.

The interconnection of two independent 4-bit inputs to an 8-bit input can only be carried out via the application program. A switching option for this purpose is not planned.

The encoder function monitors the change of the bit pattern on the input channels. The bit patterns on the inputs are transferred directly to the application program. The display on the PADT is in the form of a decimal number (*Counter[0x].Value*) that corresponds to the bit pattern.

Depending on the application, this number (which corresponds to the Gray Code bit pattern) can be converted into, for example, the corresponding decimal value.

Reaction in the Event of a Fault

Overview

If a fault is detected in the counter section of the module, a status bit is set for evaluation in the application program. Additionally the relevant error code can be taken there into consideration. The LED ERR on the module is activated.

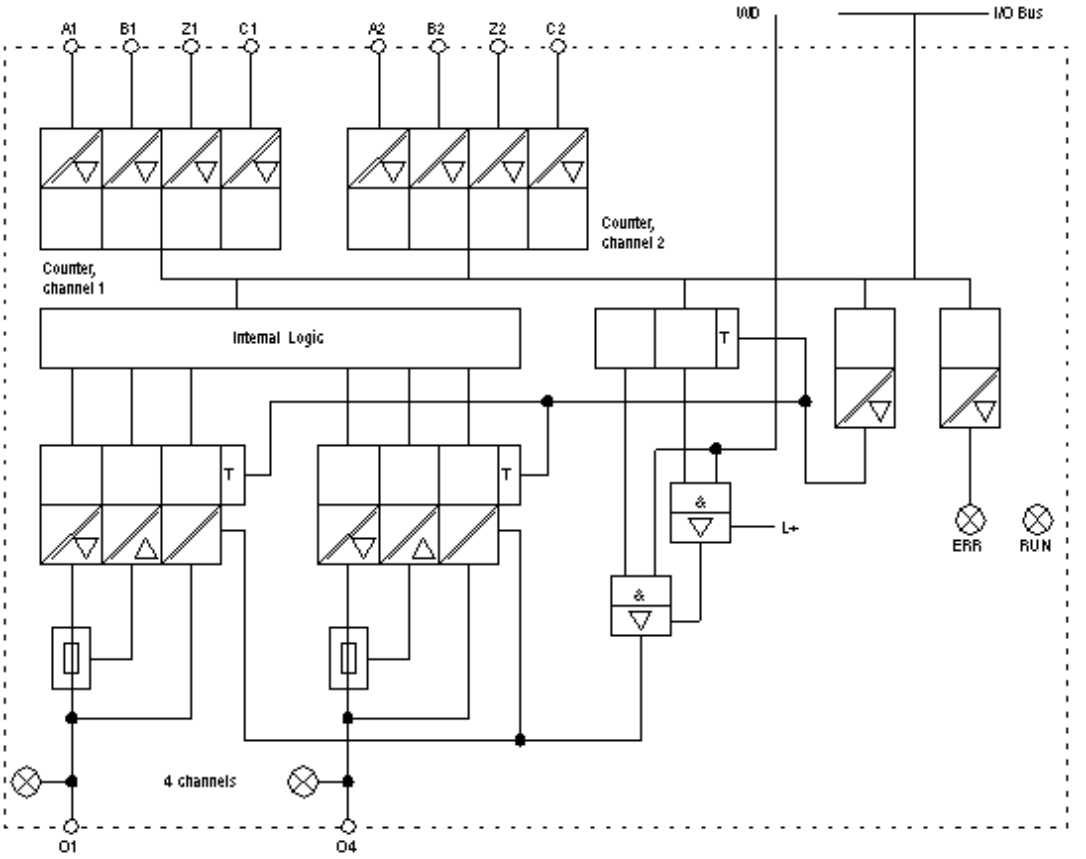
Errors

The error code enables you to provide additional fault handling in the application program.

Diagram of Counters

Representation

View of the functions, counter module XPSMF CIO2401 as an example



Section 3.7
Check List for Safety-Related Inputs

Check List

Overview

We recommend that the check list below is used during the configuration, programming and commissioning of safety-related inputs. It can be used as a planning document, and at the same time proves that the planning has been carefully carried out.

Requirements Check List

As part of the configuring or commissioning phases, a separate requirements check list can also be compiled for each of the safety-related input channels installed in the system. This ensures that all the requirements are noted in a clear, comprehensive manner. It also enables documentation regarding the connection of external wiring to the application program to be produced.

Representation

Safety Manual XPSMF60/XPSMF40 Check list for configuring, programming and commissioning				
Company				
Location				
Loop				
Safety-related inputs for XPSMF60/XPSMF40				
No.	**Repuirements**	**Yes**	**No**	**Remarks**
1	Is this a safety-related input?			
2	Is the fault display processed in the application program? [VALUE=0] and [ERRORCODE≠0]			
3	Is this an analog input?			
4	unipolar 0...+/-10 VDC			
5	unipolar 0...20 mA			
6	bipolar +/-10 VDC			
7	Voltage input terminated or failure caused by line break can be excluded?			

Safety Manual XPSMF60/XPSMF40 Check list for configuring, programming and commissioning				
8	Do the sensor areas match the channel configuration?			
9	Are the unused analog inputs short-circuited?			
10	Are the releases (AI[0x].Used) for the concerning inputs parameterized?			
11	Is this input a counter input?			
12	Function: Pulse counter?			
13	Function: Decoder (Gray code)?			
14	Is a safety-related encoder/sensor provided for this input?			

Chapter 4
Outputs

Overview

This chapter describes the outputs.

What Is in This Chapter?

This chapter contains the following sections:

Section 4.1
Overview

Hardware Overview

Modular XPSMF60 Controller

Digital outputs

Module	Quantity	Safety-Related	Electrically Isolated
XPSMF CIO2401	4	+	+
XPSMF DIO241601 (Configurable for Line Control)	16	+	+

Others

Module	Quantity	Safety-Related	Electrically Isolated
XPSMF DO801 (with Relay Contacts)	8	+	+
XPSMF AO801 (Analog Outputs)	8	+	+

+ Applicable
- Not applicable

XPSMF40 Controller

System section	Quantity	Safety-Related	Electrically Isolated
Digital Outputs	24	+	-
Pulsed Outputs	8	-	-

+ Applicable
- Not applicable

Section 4.2
General

General Information on Outputs

Overview

The safety-related output modules are written once every cycle, the output signals are read back and compared with the specified output data.

The safe state of the outputs is the 0 value or an open relay contact.

Testable Switches

Three testable switches are integrated in series into the safety-related output channels. This enables the independent second disconnection path (required for safety reasons) to be integrated into the output module.

Safety Shutdown Mechanism

This integrated safety shutdown mechanism disconnects all the channels of the malfunctioning output module (deenergized state).

WD Signal

Besides that the WD (watchdog) signal of the CPU is the second possibility of the safety shutdown: With loss of the WD signal the system is immediately transferred into the safe state.

This function is only effective for all digital outputs and relay outputs of the controller.

Error Code

The relevant error code enables the user to provide additional fault reactions in the application program.

Section 4.3
Safety Related Digital Outputs

Overview

The points listed below apply to both digital output channels of XPSMF60 modules and digital output channels of the compact device XPSMF40. The relay modules are excluded in both cases, unless specified otherwise.

What Is in This Section?

This section contains the following topics:

Test Routines for Digital Outputs

Overview

The modules are automatically tested during operation.

Test-Functions

The main test functions are

- Read back of the output signal of the switching amplifier. The switching threshold for a read-back 0-signal is 2 V. The diodes used prevent a feed back of signals
- Checking the integrated redundant safety shutdown
- A shutdown test of the outputs is carried out within the MEZ for a max of 200 µs. The minimum time between two tests is ≥ 20 s.

The operating voltage of the entire system is monitored, deenergizing all outputs at an undervoltage of < 13 V.

Reaction in the Event of a Fault

Overview

If a faulty 1-signal is detected, the concerning output of the module is set to a deenergized 0 state via the safety switches.

In case of a module fault all outputs are switched off. Both faults are also indicated via the LED ERR on the module of the XPSMF60 or the LED FAU at the XPSMF40.

External Short-Circuit or Overload Performance

Overview

If the output is short-circuited to L- or an overload, it is still possible to carry out tests on the module. A safety shutdown is not required.

Consumption Monitored

The total current consumption of the module is monitored. If the threshold is exceeded, all the channels of the output module are set to the safe 0 state.

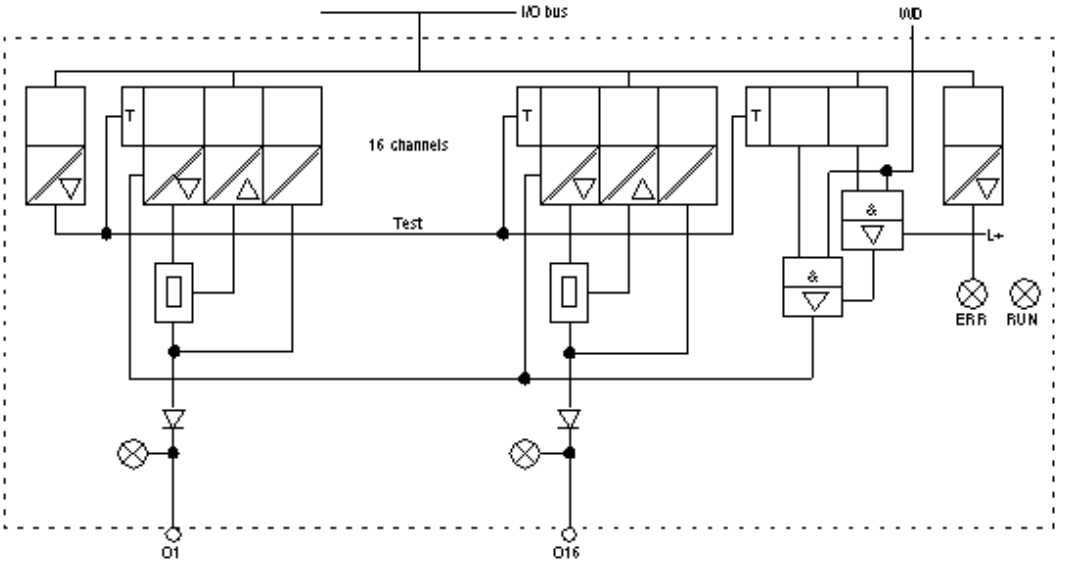
Re-Connection

In this state the outputs are cyclically checked (in periods of several seconds) if the overload is still present. At a normal state the outputs are connected again to the load.

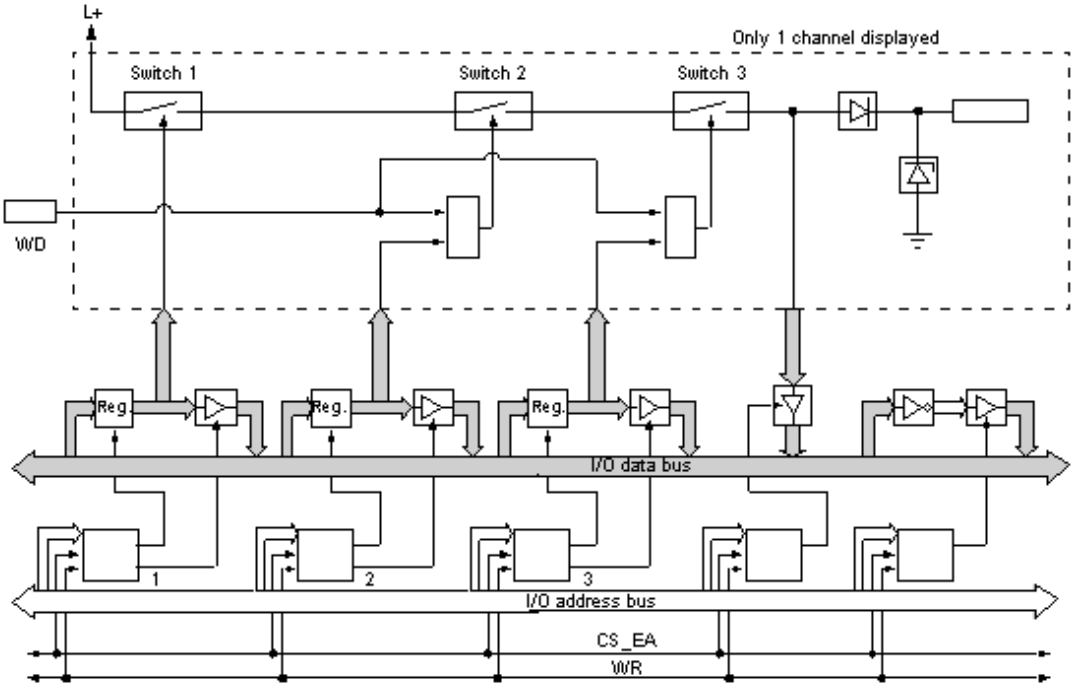
Diagram of the Digital Outputs

Representation

View of the functions, using the XPSMF DIO241601 module as an example



View of the functions of safety-related digital outputs of the XPSMF40



Line Control

Overview

Safety-related digital outputs can be cycled with the safety-related digital inputs of the same system (but not with parameterizable digital inputs, see chapter *Parameterizable Digital Inputs, page 44*). This enables short-circuit or line break monitoring to be carried out, for example, with EMERGENCY STOP devices according to PL/e Cat. 4 as specified in EN ISO 13849 (see *Line Control, page 45*).

⚠ CAUTION

IMPROPER RELAY OUTPUT USAGE

Relay outputs cannot be used as pulsed outputs.

Failure to follow these instructions can result in injury or equipment damage.

⚠ CAUTION

IMPROPER PULSED OUTPUT USAGE

Pulsed outputs must not be used as safety-related outputs, e.g. for control of safety-related actuators!

Failure to follow these instructions can result in injury or equipment damage.

Section 4.4
Relay Outputs

Overview

This section describes the properties for relay outputs.

What Is in This Section?

This section contains the following topics:

Test Routines for Relay Outputs

Overview

The modules are automatically tested during operation.

Test-Functions

The main test functions are

- read back of the output signals of the switching amplifiers before the relays
- testing the switching of the relays with positively guided contacts
- testing the integrated redundant safety shutdown

The operating voltage of the entire system is monitored, deenergizing all outputs at an undervoltage of < 13 V.

Safety Relays

At the module XPSMF DO801 module, the outputs are equipped with three safety relays: two relays with positively guided contacts and one standard type relay. So the outputs can be used for safety shutdowns.

Reaction in the Event of a Fault

Overview

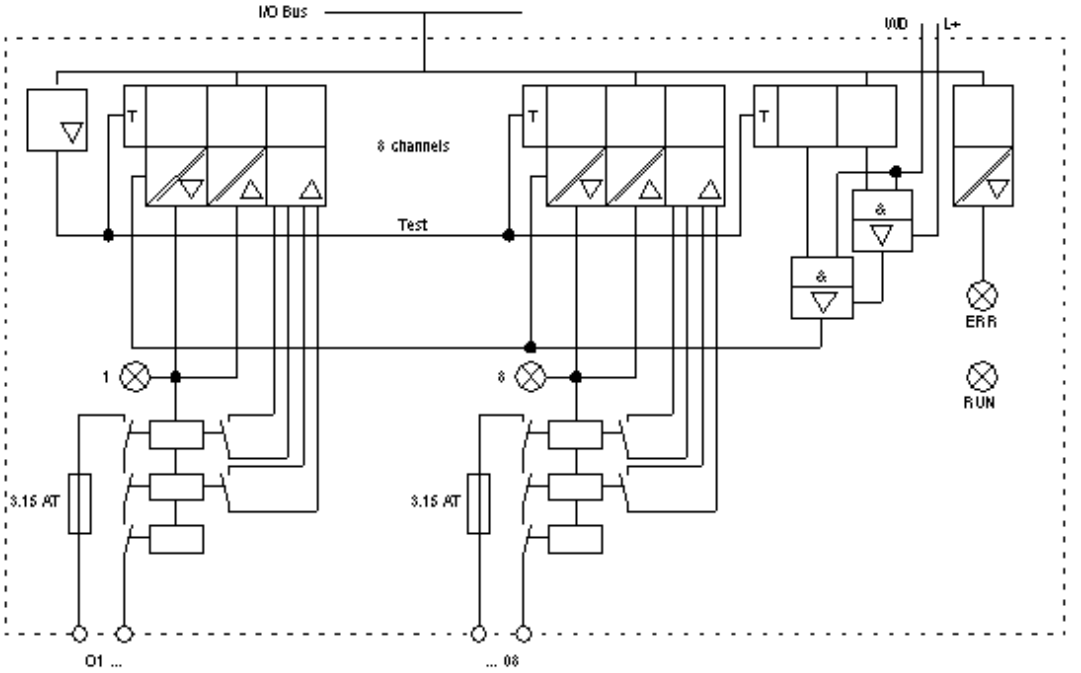
If a faulty 1-signal is detected, the concerning output of the module is set to a safe, de-energized 0 state via the safety switches.

In case of a module fault all outputs are switched off. Both faults are also indicated via the LED ERR on the module.

Diagram of the Relay Outputs

Representation

View of the functions, using the XPSMF DO801 module as an example



Section 4.5
Safety-Related Analog Outputs

Overview

This section describes the safety-related analog outputs.

What Is in This Section?

This section contains the following topics:

General

Overview

The intelligent module XPSMF AO801 has its own safety-related 1oo2 A/D microprocessor system with safe communication. The analog outputs are written once every cycle and the values saved internally. The module itself tests the function.

Voltage or Current Outputs

The safety-related analog output modules can be set to voltage or current outputs using the DIP switches (dual in-line package) on the module. Ensure that the settings correspond to how they are applied in the system and configured in the application program. Failure to do so leads to unpredictable module reaction.

⚠ CAUTION
IMPROPER DIP SWITCH SETTINGS Before installing the module in the system: Check the DIP switch settings on the module and their configuration in the application program! **Failure to follow these instructions can result in injury or equipment damage.**

Signal Values

Depending on the selection of the device type (FS1000, FS2000) via the resource of the XPSMF60 you have to consider different values for the signal AO 0x.Value in the logic to get equal output values.

Coupled Outputs

Respectively two analog outputs are DC coupled to each other (output 1 and 2, output 3 and 4, output 5 and 6, output 7 and 8).

Analog Output Circuits

The analog output circuits have current or voltage monitoring, read back and test channels (even for parallel output circuits), as well as two additional safety switches for the safe disconnection of the output circuits in the event of a fault. This ensures that the safe state is achieved (current output: 0 mA, voltage output: 0 V).

Test Routines

Overview

The module is automatically tested during operation.

Test-Functions

The main test functions are

- duplicated read back of the output signal,
- crosstalk test between the outputs,
- checking the integrated safety shutdown.

Reaction in the Event of a Fault

Overview

The output signals are read back once every cycle and compared with the internally saved output signals of the intelligent module.

If there is a discrepancy, the defective output channel is switched off via both safety switches, and the module error is signaled via the LED ERR on the module.

Response Time

The error code signal enables you to provide additional fault handling in the application program.

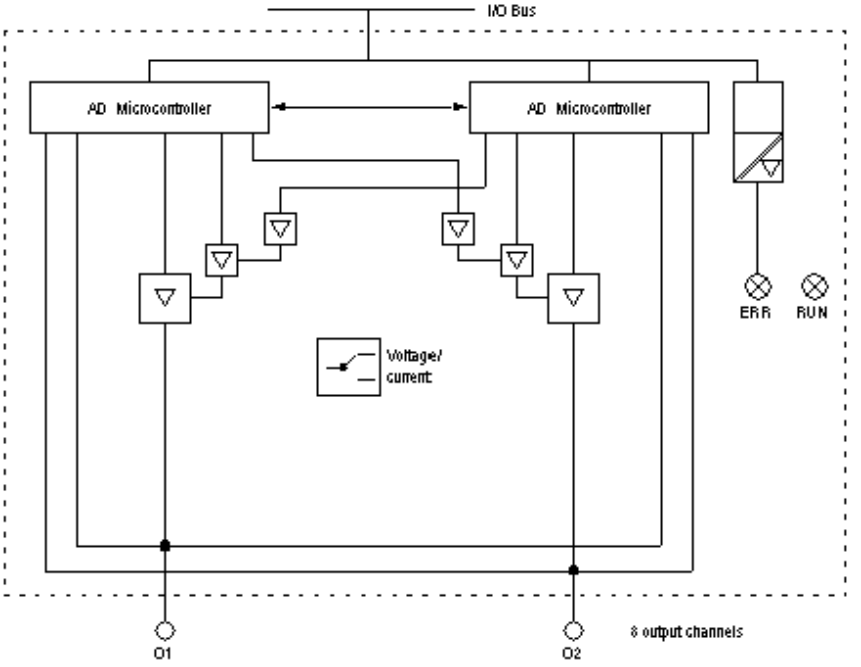
To obtain the worst case response time of the analog outputs, add twice the watchdog time ($2 \times WDT_{CPU}$) to twice the watchdog time of the AO-CPU ($2 \times WDT_{AO\text{-}C}$).

The worst case response time is shown in the data sheet.

Diagram of the Analog Outputs

Representation

View of the functions, using module XPSMF AO801 as an example



Section 4.6
Check List for Safety-Related Outputs

Check List

Overview

We recommend that the check list below be used during the configuring, programming and commissioning of safety-related outputs.

It can be used as a planning document, and at the same time proves that the planning has been carefully carried out.

Requirements Check List

A separate requirements check list for the configuration or commissioning can also be compiled for each of the safety-related output channels installed in the system. This ensures that all the requirements are noted in a clear, comprehensive manner. Documentation regarding the connection of external wiring to the application program could also be produced.

Representation

Safety Manual XPSMF60/XPSMF40 Check list for configuring, programming and commissioning				
Company				
Location				
Loop				
Safety-related outputs for XPSMF60/XPSMF40				
No.	**Requirement**	**Yes**	**No**	**Remarks**
1	Is this a safety-related output?			
2	Is the fault signal processed in the application program?			
3	Is this a digital output?			
4	Does the channel load correspond to the maximum permitted value?			
5	Does the module load correspond to the maximum permitted value?			
6	Are there RC circuits (free-running circuits) fitted to the actuators?			

Safety Manual XPSMF60/XPSMF40 Check list for configuring, programming and commissioning				
7	Has the actuator been connected according to the data sheet?(two-pole connection)			
8	Is this an analog output?			
9	Application of voltage output: DIP switch positions according to configuration in application program?			
10	Application of current output: DIP switch positions according to configuration in application program?			
11	Are unused analog current outputs short-circuited?			
12	Are the releases (AO[0x]).Used for the concerning outputs parameterized?			
13	Is a safety-related actuator provided for this output?			

Chapter 5
Software for XPSMF60/XPSMF40 Systems

Overview

This chapter gives an general overview about the software of XPSMF60/XPSMF40 Systems.

What Is in This Chapter?

This chapter contains the following sections:

Section 5.1
General

General Information on Software

Overview

The software for the safety-related programmable controllers of XPSMF60/XPSMF40 systems can be divided into the following blocks:

- operating system,
- application program,
- programming tool for XPSMFWIN (conform to IEC 61131-3).

The operating system is loaded into the CPU of the controller and should be used in the valid, TÜV-certified form required for safety-related applications.

XPSMFWIN

The application program is created with the XPSMFWIN programming software and contains the system-specific functions that the programmable controller needs to carry out. The XPSMFWIN system software is also used to configure and control operating system functions.

Code Generator

The application program is translated into machine code using the code generator. This machine code is transferred into the Flash EPROMs of the programmable controller via an Ethernet interface.

Section 5.2
Safety Aspects of the Operating System

General Information on Safety Aspects

Overview

Each approved operating system is marked accordingly. To be able to better distinguish between operating systems, the revision and CRC signature are given.

Operating Systems

The valid versions of the operating system (approved by the TÜV for safety-related programmable controllers) and the relevant signatures (CRCs) are subject to revision control and are documented in a list, which is drawn up in conjunction with the TÜV.

The running operating system version can only be read using the XPSMFWIN programming tool. You have to carry out a check (see *Check List, page 94*).

Section 5.3
Mode of Operation and Functions of the Operating System

General Information on Operation and Functions

Overview

The operating system executes the application program cyclically.

Basic Functions

The following functions are carried out in a very simplified form:

- reading the input data,
- processing the logic functions that have been programmed according to IEC 61131-3,
- writing the output data.

Important Functions

The following important functions are also performed:

- extensive self tests,
- I/O module tests during operation,
- data transfer,
- diagnosis.

Section 5.4
Safety Aspects of the Programming

Overview

This section describes the safety aspects of the programming.

What Is in This Section?

This section contains the following topics:

XPSMFWIN Safety Concept

Overview

The XPSMFWIN safety concept ensures that,

- the programming system (PADT) functions correctly,
- errors in the programming system can be detected,
- you operate the PADT correctly,
- errors on your part are detected.

During installation of the programming tool, a CRC check sum ensures the integrity of the program package on the way from the manufacturer to the user.

The programming tool executes a plausibility check in order to reduce potential errors during entry.

It is necessary to compile twice with consequent comparison of the created configuration CRCs (check sums). This helps to ensure the detection of falsifications of the application as a result of temporary malfunctions of the used PC. For details please refer to XPSFMFWIN Software Manual.

Due to the programming tool and the measures defined in this safety manual, the generation of a semantically and syntactically correct code that, however, still contains unknown systematic errors resulting from the code generation, is very unlikely.

Safety of the System

When a safety-related controller is commissioned for the first time or when the application program is modified, a comprehensive functional test has to be carried out to check the safety of the whole system.

Procedure

The following steps must be carried out to guarantee the safety of the system:

Step	Action
1	Compile the application program twice and compare the code versions (CRC).
2	Check correct implementation of the application using the data and signal flows.
3	Perform a comprehensive test of the logic by trial (see *Checking the Configuration and the Application Program, page 87*).

Checking the Configuration and the Application Program

Overview

To check that the application program is performing the specific safety functions, you have to generate suitable test cases to cover the requirements in the specification.

Independent Test

An independent test of each loop (consisting of input, logical combinations from an application point of view important, and output) is normally sufficient. XPSMFWIN and the measures described in this safety manual make it sufficiently unlikely that a semantically and syntactically correct code is produced that still contains unrecognized systematic errors from the code generation process.

Suitable Test

Suitable test cases should also be generated for the numerical evaluation of formulas. Equivalent class tests are the most appropriate, i.e. tests within defined ranges of values, on the limits or that use invalid values. The test cases must be chosen in a way that demonstrates the calculation is correct.

After a compilation of the XPSMFWIN programming tool, compare the REAL and LREAL defined initial values and the values in the Force Editor to detect any deviation. If there is any difference between the original value set and the value loaded into the controller, then the REAL and LREAL values must be forced to be identical to the original value set in the application.

Active Simulation

An active simulation with sources must be used, only so the correct wiring of the system sensors and actuators (also connected via communication with remote I/O modules) can be proven. This is also the only way of checking the system configuration.

This procedure should be used when first creating an application program and when carrying out any modifications to it.

Creating a Project Archive

Overview

When creating a project archive the following steps should be carried out in the specified order.

Creating a Project Archive

Step	Action
1	Print the application program to compare the logic with the requirements.
2	Compile the application program to generate the configuration CRC of the CPU.
3	Note the version of the configuration CRC from the CPU by checking the CRCs. This is done by selecting the controller in **Hardware Management**. The versions are displayed in the **About Configuration** context menu item. The following is relevant when specifying a version: ● *rootcpu.config* shows the safety-related configuration of the CPU, the configuration CRC of the CPU, ● *rootcom.config* shows the non-safety-related configuration of the COM, ● *root.config* shows the entire configuration including the remote I/O modules (CPU + COM).
4	Create an archive of the project on a data medium and make a note of ● names of the application programs ● configuration CRCs of the CPUs ● date (this does not replace your internal documentation requirements)

Possibility for Program and Configuration Identification

Overview

The application programs can be uniquely identified by the configuration CRCs from the *root.config*. The relevant archive can then be easily identified. The name given to an archive should contain the configuration CRCs of the *root.config*.

Compare Configuration

To ensure that the archive is not modified, compile the resource after recovery and then compare the configuration CRC of the *root.config* with the CRCs of the loaded configurations, which can be displayed using XPSMFWIN.

For monitoring you can check the menu **Resource → Check Consistency** in the Control Panel.

Section 5.5
Parameters of the Programmable Controller

Parameters of the Programmable Controller

Overview

The parameters listed below are defined by XPSMFWIN as permitted measures in the proper operation of the programmable controller, and designated as safety-related parameters.

Settings

The settings possible during safety-related operation are not linked to one specific requirement class; they must be agreed in conjunction with the approval authority for each application in which the programmable logic controller is used.

Parameters

Parameters of the programmable controller

Safety-Related Parameters	Safe Setting
Safety time in ms	process-dependent
Watchdog time in ms	Max. 50 % of safety time
Start/Restart	Reset/Off (in RUN only)
Force enable	Reset/Off
Force (single switch)	Reset/Off
Main enable switch (modifying the safety parameters)	Reset/Off (in RUN only)
Test mode	Reset/Off

Section 5.6
Forcing

General Information on Forcing

⚠ WARNING

FORCING HAZARD

Forcing is only permitted after consulting the approval authority responsible for the plant acceptance.

When forcing is being carried out, the person responsible must ensure that sufficient safety monitoring of the process is being performed through other technical and organizational measures.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Available Options with Forcing

The following options are available with forcing:

- Forcing can be prohibited on a configuration by configuration basis. The PES then accepts no more force values that are defined as user-specific. In this case, new force values can only be set after the controller has been enabled for forcing again.
- All the signals can be displayed using the Force Editor of the XPSMFWIN programming tool, for details refer to XPSFMFWIN Software Manual.
- In the Force Editor it can be checked which signals are actually forced.
- All forced signals can be deactivated again via the **Stop** command in the Force Editor of the XPSMFWIN programming tool. The individual force values and switches remain in the same state; this means that they become active again if the **Start** command is activated again.

Further Information

Refer to the online help of XPSMFWIN for further information regarding forcing.

NOTE: Force switches and force parameters are explained in *Forcing of Signals, page 113* in this manual.

Basic information on forcing can be found in the TÜV *Maintenance Override* document.

The document can be accessed on the following TÜV homepages:

- *http://tuvasi.com (TÜV Rheinland)*
- *http://www.tuv-fs.com (TÜV Cooperation Functional Safety)*

Section 5.7
Protection from Manipulation

General Information on Protection

Overview

Together with the relevant approval authority, the user must define, which measures are to be taken to provide protection from manipulation.

Protection Mechanisms

Protection mechanisms built into the PES and the XPSMFWIN programming system prevent unintentional or unapproved modifications to the safety system.

- A modification to the application program or the configuration generates a new CRC. These modifications can only be transferred to the PES via a download (during which the PES is in STOP).
- The operating options requires you to be logged into the PES.
- The XPSMFWIN programming tool requires a password to connect to the PES when you log on.
- The connection between the PADT and the PES is not required when in RUN mode.

Safety

The safety and application requirements regarding protection from manipulation should be observed. It is the responsibility of the operator to authorize staff and to take the necessary protective measures.

⚠ CAUTION
UNAUTHORIZED ACCESS HAZARD The password must be protected from unauthorized access. The default login and password settings must both be changed. **Failure to follow these instructions can result in injury or equipment damage.**

PES and PADT

PES data can only be accessed if the PADT in use has access to the XPSMFWIN programming tool and the currently running version of the application project (archive maintenance!).

The connection between the PADT and the PES is only required for downloading the application program or for reading the variables/signals. During normal operation the PADT is not required; disconnecting the PADT from the PES in normal operation provides protection from unauthorized access.

Section 5.8
Check List for the Creation of an Application Program

Check List

Overview

We recommend that the check list below is used in order to ensure safety aspects are observed during programming and before and after loading a new or modified program.

Representation

Safety Manual XPSMF60/XPSMF40 Check list for creation of an application program			
Company			
Location			
Project			
File/archive			
Checks	**Yes**	**No**	**Remarks**
With program creating / Before a modification			
Have the PES configuration and application program been created with safety in mind?			
Were programming guidelines used when creating the application program?			
Are functionally independent sections of the program encapsulated in functions and function blocks?			
Were only safe signals used for all safety functions?			
Does each safety-related signal source correctly (also via communication) reach the application program?			
Is each safety-related signal drain correctly (also via communication) written?			
After a modification - before loading			
Has a person not involved in the program creation carried out a check of the application program with regard to the mandatory system specifications?			
Has the result of the test been documented and released (date/signature)?			

Safety Manual XPSMF60/XPSMF40 **Check list for creation of an application program**			
Has the application program been compiled twice with a subsequent comparison of both the configuration CRCs produced?			
Has an archive of the entire project been made before loading the program into the PES?			
After a modification - after loading			
Have an adequate number of tests been carried out for all safety-relevant logical operations (including I/O) and for all mathematical operations?			
Has all the force information been reset before safety mode?			
Do the Enable switches correspond to the settings for the maximum/specified protection?			
Are the CPU operating system and the CRC official TÜV-approved versions?			

Chapter 6
Safety Aspects of the Application Program

Overview

This chapter describes the different safety aspects of the application program.

What Is in This Chapter?

This chapter contains the following sections:

Section 6.1
General Sequence

Programming Sequence

Overview

General sequence in the programming of the XPSMF60/XPSMF40 programmable controllers for safety-related applications:

- specification of the controller functions,
- writing the application program,
- compiling the application program with the C-Code generator,
- second compilation of the application program (both results (CRC) should be compared),
- generation of the program with no errors and program is executable,
- verification and validation.

You then can test the program, the PES can assume safe operation.

Section 6.2
Framework for Safety-Related Operation

Overview

This section describes the framework for safety-related operations.

What Is in This Section?

This section contains the following topics:

General

Overview

The application program is loaded with the XPSMFWIN programming software for PCs.

Main Features

The main features of the XPSMFWIN programming system are:

- input (function block editor), monitoring and documentation
- variables with symbolic names and data types (`BOOL`, `UINT`, etc.)
- assignment of the XPSMF60/XPSMF40 system controllers
- code generator (conversion of the application program into machine code)
- hardware configuration
- communication configuration

NOTE: Conditions, rules and explanations to the safety requirements see *Safety Requirements, page 17*.

Programming Basics

Overview

The task that the controller will perform should already exist in the form of a specification. The specification should be used to check whether its requirements have been correctly implemented in the program. The way in which the specification is presented depends on the task in hand.

Combinatorial Logic

Combinational logic can be:

- cause/effect diagram
- logic operation with functions and function blocks
- function blocks with specified characteristics

Sequential Controllers (Sequence Control)

Sequental controllers can be:

- verbal description of the enabling step conditions and of the actuators to be controlled
- flowcharts
- matrix or table showing the step enabling conditions and the actuators to be controlled
- definition of the ancillary constraints, e.g. operating states, EMERGENCY STOP, etc.

I/O Concept

The I/O concept for the system must contain an analysis of the field circuits, i.e. the types of sensors and actuators.

Sensors (Digital or Analog)

Sensor signals

- signal in normal operation (deenergize to trip mode with digital sensors, live-zero with analog sensors)
- signals in the event of a fault
- determining the required safety redundancies (1oo2, 2oo3) (see *Safety Requirements, page 36*)
- discrepancy monitoring and reaction

Actuators

Actuator positions

- position and activation during normal operation
- safe reaction/position in event of shutdown or power failure

Targets

Targets when writing the application program

- easy to understand
- easy to implement
- easy to modify
- easy to test

Signal and Variable Declaration

Variables

A variable is a substitution for a value within the program logic. The memory space with the stored value is symbolically addressed by the variable name. These symbolic names can have up to 256 characters. A variable is generated in the variable declaration of the program or the function block.

Signals

A signal is used as an allocation between the different areas of the entire control. The signal is generated in the signal editor and corresponds to the global layer of a `VAR_EXTERNAL` if the relation was set up.

Symbolic Names

The use of symbolic names as opposed to physical addresses has two distinct advantages for you:

- The system designations of inputs and outputs can be used in the application program.
- Changes to how signals are assigned to input and output channels have no effect on the application program.
- After a cold start, variables with no user-defined initial value are set to the default value 0 or FALSE.
- Variables with invalid source, e.g., due to a hardware fault in a physical input, adopt the configured initial value.

Assignment to the I/O Level

Overview

When the value of a variable shall be allocated to an I/O channel, an identically named signal must be generated in the signal editor of the Hardware management.

Then the signal is dragged (per drag and drop) to the variable list of the program and to the channel list of the I/O module.

The required test routines for safety-related I/O modules or I/O channels are carried out automatically by the operating system.

Assignement of Signals to I/O Channels

To assign a signal to an I/O channel, proceed as follows:

Step	Action
1	In the Signal Editor located in the Hardware Management define a signal.
2	Drag the signal onto the program's variable declaration. VAR_EXTERNAL is automatically created.
3	Drag the signal onto the channel list associated with the I/O module.
4	In the user program, evaluate the error code and program a safety-related reaction.

The system is assigned to an I/O channel.

NOTE: The system signal name for the error code depends on the I/O channel type.

Types of Variables

Overview

Depending on the program organization unit (POU) - program, function block or function - various types of variables can be defined.

Types of Variables

The following table provides an overview:

Variable Type	Program	Function Block	Function	Use
VAR	+ (CONST)	+ (CONST)	+ (CONST)	Local variable
VAR_INPUT	-	+	+	Input variable
VAR_OUTPUT	-	+	+	Output variable
VAR_EXTERNAL	+ (CONST, RETAIN*)	+ (CONST, RETAIN*)	-	External to / from other POU or higher global level
VAR_GLOBAL	+ (CONST)	-	-	Global to / from other POU

+ Can be used.
- Can not be used.
CONST Constants that cannot be modified by the application program (e. g. switching point).
RETAIN Buffered value at warm start, initial value at cold start.
***** Only if signal.

Main Features

The main feature is the inclusion of functions in function blocks that you create yourself and functions derived from standard functions. This enables a program to be clearly structured into modules (functions, function blocks). Each module can be seen as a separate entity, and a large, complex function can also be created by connecting modules together to form a larger module or program.

Functions of the Application Program

Overview

The programming is not subject to any hardware restrictions. The application program functions can be programmed as required.

Programming

When programming, the deenergize to trip mode must be kept in mind with physical inputs and outputs. Only components complying with IEC 61131-3 and their relevant functional requirements are used within the logic.

- The physical inputs and outputs generally operate according to the deenergize to trip mode, i.e. their safe state is 0.
- The application program contains appropriate logical and/or arithmetic functions irrespective of the deenergize to trip mode of the physical inputs and outputs.
- The logic should be designed and documented in a clear manner so that errors can easily be located. This includes the use of function charts.
- Negation can be used as required.
- Fault signals from inputs/outputs or from logic modules must be evaluated by the programmer.

System Parameters of the CPU

Overview

The parameters listed below determine the performance of the controller during operation and are specified in the resource attributes.

The permitted operations for the safe operation of the controller are set here using the programming tool (PADT) and the safety-related parameters are specified.

System Parameters

System parameters of the CPU

Switch	Function	Default Value	Setting for Safe Operation
Main Enable	Following switches/parameters can be modified during operation (= RUN) with the PADT	ON	OFF*
Autostart	Automatic start after power ON of the CPU	OFF	ON/OFF**
Start/Restart allowed	Cold start, warm start or hot start by PADT in RUN or STOP mode	ON	OFF*
Loading allowed	Load release for an application program	ON	ON
Test Mode allowed	Test Mode allowed or forbidden. At Test Mode the program execution will be frozen or stopped. The outputs remain actuated and the program execution can be done in single cycle steps.	OFF	OFF
Change Variables in OLT allowed	Values of variables can be displayed and set in the online test (OLT) fields	OFF	OFF***
Forcing allowed	Input or activation of values for signals are permitted, regardless of the current value of the process/logic signal	OFF	Determined by approval authority
Stop on Force timeout	STOP of CPU after force time is exceeded	ON	Determined by approval authority

* In RUN mode only changing the value to OFF is possible.
** The application will determine whether it is set to ON or OFF.
*** In RUN mode only changing the value to ON is possible.

NOTE: Additional switches and parameters can be specified for forcing (also see *Forcing of Signals, page 113*)

Locking the PES

Overview

Locking the PES, means that system functions and user access are blocked during operation. This means that the application program cannot be manipulated. The extent to which everything is blocked depends on the safety requirements regarding the use of the PES. However, it can also be determined in consultation with the approval authority responsible for the plant acceptance.

Locking a PES

The following procedure should be followed when locking a PES:

Step 1: The following values should be set on the controller and before compilation (see also *Code Generation, page 111*):

Switch	Value
Main Enable	TRUE
Forcing allowed	FALSE (depending on application)
Test Mode allowed	FALSE
Start/Restart allowed	TRUE
Loading allowed	TRUE
Autostart	TRUE/FALSE
Stop on Force Timeout	TRUE (depending on application)

Step 2: After loading and starting up, the following switches should be changed in the controller online in the order shown:

Switch	Value
Start/Restart allowed	FALSE
Loading allowed	FALSE
Main Enable	FALSE

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

The following switches can only be set to different values after consulting the approval authority.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Step 3: After consulting the approval authorithy switches should be changed:

Switch	Value
Forcing allowed	TRUE
Stop on force timeout	TRUE/FALSE
Start/Restart allowed	TRUE
Autostart	TRUE

Test Mode Never True

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

To ensure safe operation, never set the TEST MODE switch to TRUE.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Unlocking the PES

Overview

Unlocking the PES means the removal of the active blocks, i.e. so that work can be carried out on the controller. To unlock the PES (Main Enable to ON), the controller must be in STOP mode. Main enable cannot be activated when the controller is running (in RUN). It can, however, be deactivated in RUN mode.

Unlock the PES

To carry out another start after the CPU is initialized (following a power failure); the procedure below should be followed to unlock the PES:

Step	Action
1	Set Main Enable to TRUE.
2	Set Start/Restart allowed to TRUE.
3	Start the application program.

After having completed the changes of the controller, the PES should be locked again (see *Locking the PES, page 108*).

Code Generation

Overview

The code is generated after the application program has been fully entered and the inputs/outputs of the controller have been assigned. The configuration CRC of the *root.config* is also created at this time. It must be compiled twice and the configuration CRC must be identical in both compile cycles.

CPU Signature

This is the signature of the entire CPU and remote I/O modules configuration and is displayed as a hex code in 32-bit format. All components that can be configured or modified, i.e. logic, variables, switch settings, are included in it.

Loading and Starting the Application Program

Overview

The loading process of a XPSMF60/XPSMF40 system PES can only take place when the PES has already been set to STOP.

No Online Loading

Online loading is not possible at present.

Only One Program

Only one application program can be loaded into the relevant PES. The entire loading of the application program is monitored. The application program can then be started, i.e. the cyclic execution of routines begins.

Forcing of Signals

Overview

Forcing is the application of values to the signals irrespective of the current value of a signal from the connected process or the result of a logic operation. The signal may be assigned e.g. to inputs, outputs, or used for communication.

Force Switches and Parameters

The following table shows force switches and parameters:

Switch	**Function**	**Default Value**	**Setting for Safe Operation**	
Forcing allowed	Enable the forcing function	OFF	OFF/ON*	
Stop on Force Timeout	CPU stop after force time is exceeded	ON	ON	
Parameter	**Function**	**Default Value**	**Display**	
Forcing activated	Forcing active	OFF	OFF	ON
Remaining Force Time	Time limitation applied to the force value, time (in seconds)	0	0	Remaining Force Time or -1*

* Refer to the warnings below:

The switches **Forcing allowed** and **Stop on Force Timeout** cannot be changed during operation with a locked PES, i.e. this setting should already have been defined before locking the PES.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

The switch **Forcing allowed** must only be set after consulting the approval authority.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

NOTE: For forcing without time limit, the value -1 for the force time must be set.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Forcing without time limit is only admissible after consulting the approval authority for the plant.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

NOTE: The Forcing allowed switch enables central forcing via the CPU to be either permitted or forbidden.

CPU Switch

If CPU switch forcing allowed is...	Then...
set	• forcing is allowed. • the entered force values only become effective if the relevant force switch is set for the data source.
not set	• forcing is not possible (default setting). • entered force values remain in the system, but have no effect.

Stop on Force Timeout

After the force time has elapsed or by stopping the forcing, forcing is finished and the process value is activated again.

If Stop on Force Timeout is...	Then...
set	in the properties of the controller (see information field), the controller goes into STOP state after the force time and the process values are activated again.
not set	the controller is not stopped after the force time. Forcing is deactivated and the forced values (R-Force values) are exchanged by their process values.

This can result in unintentional reactions of the whole system.

With the **Stop** button in the Force Editor forcing will be stopped manually. In this case the controller remains in the state RUN, because the timeout time was not reached and the reaction **Stop on Force Timeout** was not set.

⚠ WARNING

UNINTENDED EQUIPMENT OPREATION

Forcing is only permitted after consulting the approval authority responsible for the plant acceptance.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Forcing

When forcing is being carried out, the person responsible must ensure that sufficient safety-related monitoring of the process is being carried through other technical and organizational measures.

The period during which forcing is applied can be limited. If the forcing time is exceeded, it can be specified whether the CPU will go into STOP or if the forcing value is no longer applicable and normal operation can be resumed. Exceeding the forcing time therefore always has an impact on the application program and so on the process.

Force Value

The force value is saved in the CPU. If the CPU is switched from RUN to STOP mode, forcing is deactivated to prevent the controller from being unintentionally started with active force signals.

Forcing Using Force Markers

Force markers are another way of forcing signals, e.g. for debugging purposes. Force markers are function blocks that can be used in the program to enable forcing of single signals. For details see the online help of XPSMFWIN.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Force markers are not influenced by the force switch settings.

Therefore, remove all force markers from the application program before putting it into safety-related operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Online Test

Overview

The function Online Test allows to use OLT fields within the logic for displaying and for setting of variables during operation of the controller.

CPU Switch

Change Variables in OLT allowed

Not Set	Set
Changing variables in Online Test is not possible.	Changing variables in Online Test is possible
If the switch **Changing Variables in OLT allowed** is switched off then values of signals/variables can only be displayed in OLT fields but not changed.	If the switch **Changing Variables in OLT allowed** is switched on then values of variables can be displayed and set in the OLT fields. The value set is only valid until a function in the logic overwrites it.

Further information about using OLT fields you can find under the index **OLT field** in the online help of XPSMFWIN Project management.

Program Documentation for Safety-Related Applications

Overview

The XPSMFWIN programming system enables project documentation to be automatically printed.

Main Types of Documentation

The main types of documentation are

- interface declaration
- list of signals
- logic
- description of data types
- configurations for system, modules and system parameters
- network configuration
- signal cross-reference list
- code generator information

Functional Acceptance

The documentation is part of the functional acceptance of a system requiring approval from an authority (e. g. TÜV). The functional acceptance only relates to the user functions, not to the safety-related modules and programmable controllers of the XPSMF60/XPSMF40 system that have already been type tested.

Acceptance by Test Authority

Overview

Schneider Electric recommends involving the test authority as soon as possible when designing a system that is subject to approval

This acceptance test only applies to the user functionality, but not to the safety-related modules and automation devices of the safety system that have already been approved.

Chapter 7
Communication Configuration

Overview

This chapter gives a general overview of the communication configuration.

What Is in This Chapter?

This chapter contains the following sections:

Section 7.1
Non-Safety-Related Communication

General

Overview

Besides with the physical input/output signals, signals can also be exchanged with another system via a data link. The variables required for this purpose are declared in the protocol area using the XPSMFWIN programming system.

Data can be exchanged in both read and write forms.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Do not use data imported from "non-safe sources" for the safety functions of the application program.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Depending on the device Modbus Slave, Modbus TCP and Profibus DP are available for non-safety-related communication.

Interfaces of the XPSMF40 Versions

XPSMF Version	Modbus Slave Interface	Profibus Slave Interface	Modbus TCP Server on SafeEthernet
4000	-	-	-
4002	-	-	+
4020	+	-	-
4022	+	-	+
4040	-	+	-
4042	-	+	+

+ XPSMF40 version has the interface
- XPSMF40 version does not have the interface

Section 7.2
Safety-Related Communication (Peer-to-Peer)

Overview

This section describes the safety-related communication.

What Is in This Section?

This section contains the following topics:

General

Overview

Safety-related communication via SafeEthernet is certified up to SIL 3.

Monitoring of a safety-related communication has to be configured in the Peer-to-Peer editor.

The `Receive TMO` monitoring time must also be specified. If no further imported signals are received within the specified time, the signals are set to their initial values (specified by the user) in the PES.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

`Receive TMO` is a safety-related parameter. The value of a signal must be present longer than `Receive TMO` or be monitored via Loop-Back, if each value has to be transferred.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Receive TMO

Overview

`Receive TMO` is the monitoring time on PES 1 during which a correct response must be received from PES 2.

NOTE: `Receive TMO` also applies in the reverse direction, i.e. from PES 2 to PES 1.

Safety-Related Communication

The `Receive TMO` (safety-related) is part of the `Worst Case Reaction Time TR` (see maximum response time, *Calculating the Maximum Response Time, page 125*). The `Receive TMO` must be calculated and entered via the Peer-to-Peer Editor.

If the communication partner does not receive a correct answer within the `Receive TMO` the safety-related communication is closed and all signals imported over this communication channel will be set to the initial values defined by you.

Requirements

The following requirement must be met for a network in which potential lost of data packages could occur:

`Receive TMO` = 2 * Response Time (minimum)

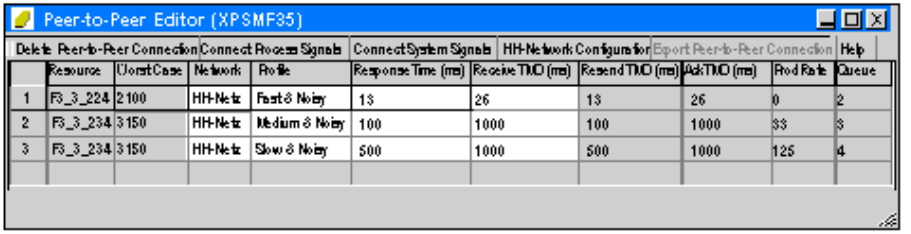
(Valid for profile Fast & Noisy)

If this requirement is...	Then...
met	the loss of at least one data packet can be tolerated without the Peer-to-Peer connection being dropped.
not met	the availability of a Peer-to-Peer connection can only be guaranteed in a network that is free of collisions and faults. However, this does not affect the safety of the CPU.

NOTE: The maximum permitted value for `Receive TMO` depends on the application process and is set in the Peer-to-Peer Editor together with the maximum expected Response time and the profile.

Representation

Example values for parameters of a Peer-to-Peer connection



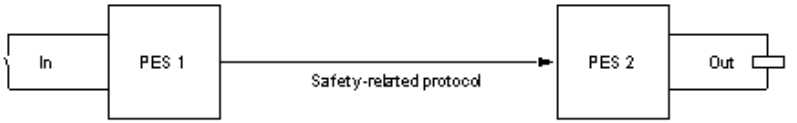
	Resource	Worst Case	Network	Profile	Response Time (ms)	Receive TMO (ms)	Resend TMO (ms)	Ack TMO (ms)	Prod Rate	Queue
1	F3_3_224	2100	HH-Netz	Fast & Noisy	13	26	13	26	0	2
2	F3_3_234	3150	HH-Netz	Medium & Noisy	100	1000	100	1000	33	3
3	F3_3_234	3150	HH-Netz	Slow & Noisy	500	1000	500	1000	125	4

Calculating the Maximum Response Time

Overview

The maximum `Response Time TR` (Worst Case) between changing a transmitter of PES 1 (In) and the response of the output of PES 2 (Out) can be calculated as follows.

Representation



$$T_R = t_1 + t_2 + t_3 + t_4$$

Symbol	Description
T_R	worst case
t_1	2 * watchdog time of PES 1
t_2	0 ms, if `Production Rate` = 0 (normal case), otherwise `Recive TMO` + watchdog time of PES 1
t_3	`ReceiveTMO`
t_4	2 * watchdog time of PES 2

The time T_R can be found in the Peer-to-Peer editor in the **Worst Case** column.

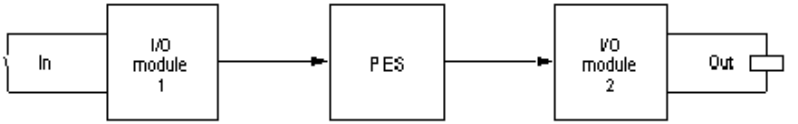
The maximum response time depends on the process and must be determined in conjunction with the acceptance authorities/department.

Calculation of the Max. Response Time with Remote I/O Modules

Overview

The maximum response time T_R between changing a transmitter (In) of the first remote I/O module (e.g. XPSMF3 DIO20802) and the response of the output of the second remote I/O module (Out) can be calculated as follows:

Representation



Formular

$T_R = t_1 + t_2 + t_3 + t_4 +$	(input path)
$+ t_5 + t_6 + t_7$	(output path)

Symbol	Description
T_R	worst case
t_1	2 * watchdog time of remote I/O module 1
t_2	0 ms, if **Production Rate** = 0 (normal case), otherwise **ReceiveTMO** $_1$ + watchdog time of remote I/O module 1
t_3	ReceiveTMO$_1$
t_4	2 * watchdog time of PES
t_5	ReceiveTMO$_2$
t_6	0 ms, if **Production Rate** = 0 (normal case), otherwise **ReceiveTMO** $_2$ + watchdog time of PES
t_7	2 * watchdog time of remote I/O module 2

NOTE: Both remote I/O modules 1 and 2 can be identical. The times also apply if a PES is used in place of a remote I/O module.

Terms

Term	Description
ReceiveTMO	Monitoring time in PES 1 during which a valid reply must be received from PES 2. After the time has expired, the safety-related communication is closed.
$ReceiveTMO_1$	Remote I/O module 1 → PES
$ReceiveTMO_2$	PES → remote I/O module 2
Production Rate	Minimum time between two data transmissions
Watchdog Time	Maximum permitted duration of the RUN cycle of a PES
Worst Case	Maximum response time between the transfer of the signal change of a physical input (In) of a PES 1 and the change of the physical output (Out) of a PES 2.

The data are transferred using a safety-related protocol.

⚠ CAUTION

UNAUTHORIZED ACCESS

The operator must ensure that the Ethernet used for Peer-to-Peer communication is adequately protected from unauthorized access (i.e. by hackers). The nature and extent of the measures to be taken must be determined in conjunction with the approval authorities.

Failure to follow these instructions can result in injury or equipment damage.

Chapter 8
Use in Central Fire Alarm Systems

General

Overview

All XPSMF60 systems with analog inputs can be used for central fire alarm systems in accordance with DIN EN 54-2 and NFPA 72.

The application program must fulfill the functions laid down for central fire alarm systems according to the cited standards.

Maximum Cycle Time

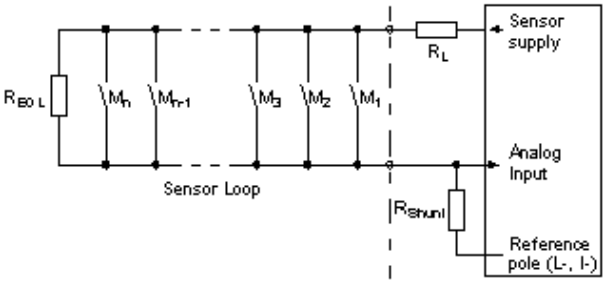
The required maximum cycle time of 10 seconds (DIN EN 54-2) for central fire alarm systems can easily be achieved with the systems as the cycle times of these systems can be measured in milliseconds. Similarly, the required 1 second safety time (if necessary) can also be easily achieved (error response time).

According to EN 54-2 the fire alarm system has to be in the fault report state within 100 seconds after the XPSMF60 system has received the fault report.

The fire alarms are connected using the energize to trip mode with line monitoring for the detection of short-circuits and line breaks. The digital and analog inputs can be used at the XPSMF AI801 analog input module.

Representation

Wiring of fire alarms



Symbol	Description
M	Fire alarm
R_{EOL}	Terminating resistor on the last sensor in the loop

Symbol	Description
R_L	Limitation of the maximum permitted current in the loop
R_{Shunt}	Measuring resistor

Resistance of R_{EOL}, R_L and R_{Shunt}

For the application, the resistance of R_{EOL}, R_L and R_{Shunt} should be calculated depending on the sensors being used and the number of sensors per alarm loop. The required data is contained in the relevant data sheet from the sensor manufacturer.

Line Break and Short-Circuit

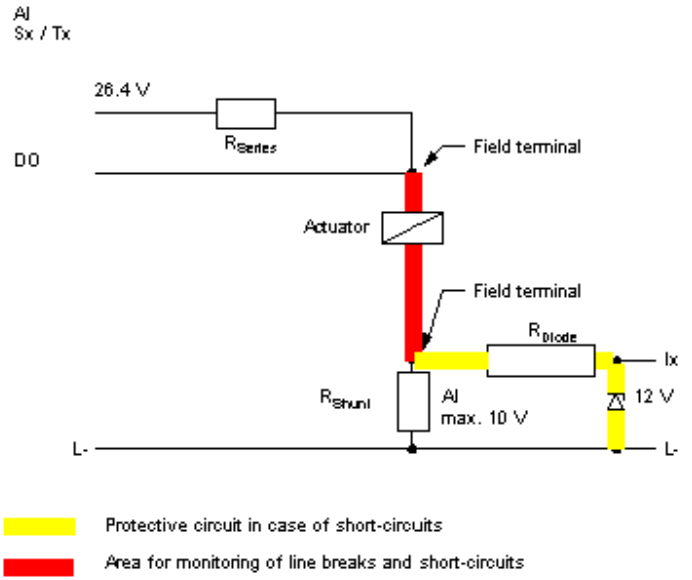
The alarm outputs, used for activating lamps, sirens, horns, etc., are operated using the energize to trip mode. These outputs must be monitored for line breaks and short-circuits. This can be done by feeding back the output signals directly from the actuator to the inputs.

The current in the actuator circuit should preferably be monitored via an analog input with an appropriate shunt. A series connection of zener diode and series protects the input against over-voltage in case of short-circuit.

For an explicit line break monitoring (at de-energized outputs DO) a transmitter supply additionally to the analog inputs is necessary (see scheme below).

Representation

Example for line break and short-circuit monitoring of digital outputs (actuator circuit)



Monitoring Short-Circuits

In chapter *Line Monitoring* of the *XPSMF35* you will find an example for monitoring short-circuit and line break of actuators via analog inputs.

Visual display systems, indicator light panels, LED displays, alphanumeric displays, audible alarms, etc. can all be controlled using an appropriate application program.

The routing of fault signals via input and output modules or to routing equipment must be carried out using the deenergize to trip mode.

Fire Alarms

Fire alarms can be transmitted from one XPSMF60 system to another using the Ethernet communications (OPC) standard available. Any breakdown in communications must be signaled.

XPSMF60 systems that are used as central fire alarm systems must have a redundant power supply. Precautions must also be taken against the power supply failing, i.e. using a battery-powered horn. There must be no interruption in operation when switching between the mains supply and the back-up supply. Voltage dips of up to 10 ms are permitted.

Signal Errors

When there is a fault in the system, the system signals specified in the application program are written by the operating system. This enables error signaling to be programmed to signal errors detected by the system. In the event of an error, safety-related inputs and outputs are switched off, i.e. 0-signals are applied to all the channels of faulty inputs and all the channels of faulty outputs are switched off.

Chapter 9
Test Conditions

Overview

This chapter gives a general overview of the test conditions.

What Is in This Chapter?

This chapter contains the following topics:

Standards and Common Conditions

Standards for EMC

The devices were developed in compliance with the requirements of the following standards for EMC, climate and environment.

IEC/EN 61131-2	Programmable Controllers, Part 2 Equipment Requirement and Tests
IEC/EN 61000-6-2	EMC Generic Standards, Part 6-2 Immunity for Industrial Environments
IEC/EN 61000-6-4	EMC Generic Emission Standard Industrial Environment

Common Conditions

For the use of the safety-related XPSMF60/XPSMF40 controller systems the following common conditions have to be met.

Protection class	Protection class II according to IEC/EN 61131-2
Pollution	Pollution degree II according to IEC/EN 61131-2
Altitude	< 2000 m
Enclosure	Standard: IP 20 If requested by the relevant application standards (e. g. EN 60204, EN 15849), the device must be installed in a required enclosure (e. g. IP 54).

Climatic Conditions

Important Test and Limit Values

The most important tests and limit values for climatic conditions are listed in the following table:

IEC/EN 61131-2 Chapter 6.3.4	Climatic Tests
	Temperature, operating: 0...60 °C (32...140 °F) (Test limits -10...+70 °C (14...158 °F))
	Storage Temperature: -40...85 °C (-40...185 °F)
6.3.4.2	Dry heat and cold withstand test: 70 °C / -25 °C (158 °F / -13 °F), 96 h, EUT power supply unconnected
6.3.4.3	Change of temperature, withstand and immunity test: -40 °C / 70 °C (-40 °F / 158 °F) and 0 °C / 55 °C (32 °F / 131 °F), EUT power supply unconnected
6.3.4.4	Cyclic damp heat withstand test: 25 °C / 55 °C (77 F / 131 °F), 95 % relative humidity, EUT power supply unconnected

Mechanical Conditions

Important Test and Limit Values

The most important tests and limit values for mechanical conditions are listed in the following table.

IEC/EN 61131-2 Chapter 6.3.5	Mechanical Tests
	Vibration test, operating: 5...9 Hz / 3.5 mm (0.137 in) 9...150 Hz / 1 g, EUT operating, 10 cycles per axis
6.3.5.2	Immunity shock test: 15 g, 11 ms, EUT operating, 2 cycles per axis, 3 shocks per axis (18 shocks)

EMC Conditions

Important Test and Limit Values

The most important tests and limit values for EMC conditions are listed in the following table:

IEC/EN 61131-2	Interference Immunity Tests	Criterion FS
IEC/EN 61000-4-2	ESD test: 6 kV contact, 8 kV air discharge	6 kV, 8 kV
IEC/EN 61000-4-3	RFI test (10 V/m): 80 MHz...2 GHz, 80 % AM RFI test (3 V/m): 2 GHz...3 GHz, 80 % AM: RFI test (20 V/m): 80 MHz...1 GHz, 80 % AM	– – 20 V/m
IEC/EN 61000-4-4	Burst test: 4 kV power supply lines 2 kV signal lines	 4 kV 2 kV
IEC/EN 61000-4-12	Damped oscillatory wave test: 2.5 kV L-, L+ / PE 1 kV L+ / L-	–

IEC/EN 61000-6-2	Interference Immunity Tests	Criterion FS
IEC/EN 61000-4-6	High frequency, asymmetrical: 10 V, 150 kHz...80 MHz, AM 20 V, ISM frequencies, 80 % AM	 10 V
IEC/EN 61000-4-3	900 MHz pulsed	–
IEC/EN 61000-4-5	Surge: power supply lines: 2 kV CM, 1 kV DM signal lines: 2 kV CM, AC I/O: 1 kV DM	 2 kV /1 kV 2 kV

Voltage Supply

Important Test and Limit Values

The most important tests and limit values for the voltage supply of the equipment are listed in the following table:

IEC/EN 61131-2 Chapter 6.3.7	Verification of DC Power Supply Characteristics
	The power supply must meet alternatively the following standards:IEC/EN 61131-2 or SELV (Safety Extra Low Voltage) or PELV (Protective Extra Low Voltage)
	The fusing of the XPSMF60/XPSMF40 devices must be in accordance to the statements of this manual
6.3.7.1.1	Voltage range test: 24 VDC, -20 %...+25 % (19.2 ...30.0 V)
6.3.7.2.1	Momentary interruption immunity test: DC, PS 2: 10 ms
6.3.7.4.1	Reversal of DC power supply polarity test.

Glossary

A

AI
analog input

AIO
analog input/output

AO
analog output

AWG
american wire gauge (wire diameter)

C

COM
communication module

CPU
central processing unit

CRC
cyclic redundance check

D

DI
digital input

DIO
digital input/output

DIP
dual in-line package, toggle switch with two possible positions (on/off or 1/0)

DO
digital output

E

EMC
electromagnetic compatibility

F

FB
field bus

FBD
functional block diagram

FTT
fault tolerance time

FTZ
see FTT.

H

H signal
high signal

I

IEC
international electrotechnical commission

L

L signal
low signal

M

MEZ
see MFOT.

MFOT
multi-fault occurrence time

O

OLE
object linking and embedding

OPC
OLE for Process Control

OSI Model
open system interconnection model

P

PADT (PC)
programming and debugging tool (according IEC 61131-3)

PELV
protective extra low voltage

PES
programmable electronic system

PFD
probability of failure on demand

PFH
probability of failure per hour

R

R
read

R/W
read/write

RC
requirement class

S

SELV
safety extra low voltage

SFC
sequential function chart

SIL
Safety Integrity Level (according to IEC 61508)

SNTP
Simple Network Time Protocol (REC 1769)

SRS
system-rack-slot

T

TMO
timeout

W

W
write

WD
watchdog

Index

R

S

T

V

W

X