Note

This manual must be carefully read by those who have or will have the responsibility for the operation or maintenance of this product. The product may not perform as designed if it is not used and maintained in accordance with the manufacturer’s instructions.

The warranties made by Simtronics with respect to the product are voided if the product is not used and maintained as described in this manual.

Please read the general warnings in chapter 3.

© Simtronics ASA, all rights reserved.

Revision index

<table>
<thead>
<tr>
<th>Revision index</th>
<th>Short Description of the Content</th>
<th>Date of issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rev. 0</td>
<td>Preliminary Version</td>
<td>30/08/2010</td>
</tr>
</tbody>
</table>

© Simtronics ASA, all rights reserved.
Table of contents

0. PRELIMINARY INFORMATION ................................................................. 5
   0.1. Important notes .................................................................................. 5
   0.2. Symbology ....................................................................................... 5
   0.3. Glossary of technical terms ............................................................... 6

1. SAFETY LIFECYCLE ........................................................................ 10
   1.1. Purpose of the safety ........................................................................ 10
   1.2. Safety Management System ............................................................. 10
   1.3. Phases of the safety lifecycle ............................................................. 11
   1.4. Functional Safety Assessment .......................................................... 12
   1.5. SIL - Safety integrity level ................................................................ 12
   1.6. Methods for assessing the reliability of a subsystem ....................... 15
   1.7. Hardware architecture ..................................................................... 15
   1.8. Average probability of failure of a function on demand ................. 16
   1.9. Procedure for calculating the PFD .................................................. 16
   1.10. Classification of the subsystems ...................................................... 18

2. REMARKS ON THE MSMX SYSTEM ......................................... 20
   2.1. Characteristics of the MSMX system ............................................... 20
       2.1.1. Safety Applications .................................................................... 21
   2.2. Hardware configurations ................................................................. 22
       2.2.1. Detection of the failures .............................................................. 23
       2.2.2. Failures of the central unit ......................................................... 23
       2.2.3. Rack controllers failures ............................................................... 23
       2.2.4. Failures of the digital input modules .......................................... 24
       2.2.5. Failures of the analogue input modules ...................................... 24
       2.2.6. Failures of the digital output modules ....................................... 25
       2.2.7. Failures of the power supply unit .............................................. 25
       2.2.8. Failsafe of the safety related outputs ......................................... 26
   2.3. Development of the application program ........................................ 26
       2.3.1. Modifications to the application program ................................. 26
       2.3.2. Protection of the application program ....................................... 27
       2.3.3. Manual forcing of the outputs .................................................... 27
   2.4. Environmental requirements .......................................................... 27
       2.4.1. Climate conditions ..................................................................... 27
       2.4.2. Mechanical conditions ............................................................... 28
       2.4.3. Electromagnetic compatibility conditions EMC ....................... 28
       2.4.4. Requirements of the power supply units .................................... 29
       2.4.5. Interaction with the communication devices ............................ 29
   2.5. Proof Test ....................................................................................... 30
   2.6. Lifetime of the product .................................................................. 30
   2.7. Calculating the PFD ...................................................................... 32

3. Warnings ............................................................................................ 37
   3.1. Ownership and confidentiality ......................................................... 37
   3.2. Liability ......................................................................................... 37

4. Warranty ............................................................................................ 37

5. Certifications and standards ............................................................... 37
6. Contact details ..................................................................................................................... 39
0. PRELIMINARY INFORMATION

0.1. Important notes

Notes on how to use this manual
This manual consists of two parts. The first part (chapter 1) provides a general description of the main concepts related to functional safety. The second part (chapter 2) provides all the recommendations and measures to be adopted when using the MSMX for safety applications.

Safety precautions
- In order to ensure that the system performs the required safety functions properly, make sure that the precautions included in this manual are respected. The manufacturing company is not responsible with respect to safety if the system users do not observe the directions included in this manual before using the system.
- In order to ensure the suitable level of protection, the MSMX system must only be used as described in this manual and in the user and maintenance manual. (ST-048-IT)
- Only use components approved by SIMTRONICS. Do not modify the product in any way without the consent by the manufacturer.

0.2. Symbology

Some symbols are used in this manual to draw the attention on some aspects of particular importance. This section defines the meaning.

CAUTION
This symbol identifies the instructions that must be followed to prevent physical damages to objects or to the operator.

WARNING
This symbol identifies the instructions that must be followed to prevent system’s failures.

IMPORTANT
This symbol identifies important information required to understand the meaning of an operation.
0.3. **Glossary of technical terms**

**Architecture**
Specific configuration of hardware and software elements in a system

**β**
Beta factor (common cause factor); measurement of the percentage of failures having a common cause.

**CAT [Category]**
Classification of the “safety related parts” of a control system with respect to their resistance to failures and their behaviour in failure conditions, as well as if it is possible to identify the failure and how reliable the components and the system are.

**DC Diagnostic coverage**
Measurement of the actual diagnostic ability: it can be defined as the relationship between the “failure rate” of the dangerous failures identified and that of all the dangerous failures.

**E/E/PE Electrical/electronic/ programmable electronic**
Based on electric (E) and/or electronic (E) and/or programmable electronic (PE) system.

**Failure**
A device inability to perform a desired function.

**Fault**
State of a device characterized by the inability to perform a desired function, excluding the inability to perform it during preventive maintenance or other planned activities or activities due to a lack of external resources.

**Functional Safety**
Functional safety is the part of the overall safety – resulting from a system or an equipment – that works properly in response to one or more logical inputs. In this case, it is the part related to the process and to the basic process control system (BPCS), depending on the proper operation of the safety instrumented system (SIS) and of the other protection levels [independent]

**HFT Hardware Fault Tolerance**
It indicates the number N of simultaneous faults for which a N+1 fault can cause a loss of the safety function; it basically defines the redundancy degree of the system.

**IEC 61508**
Published in 1998 –2000, this is an international standard defining the general approach for all the activities of the Life Cycle of safety for E/E/PES systems used to perform safety functions. This standard offers a method for the development of the safety requirements specification, as well as introducing and using the safety integrity layers (SIL), and is particularly important for manufacturers and suppliers of components of Instrumental Safety Systems. IEC 61508 is also based on the concept of Safety Life Cycle, in order to provide a systematic analysis of the phases of a SIS system, to be performed over the time span that goes from the general conception of the functional safety project to the disposal of the SIS system. The safety life cycle is used as the base for achieving the compliance with the IEC 61508 and IEC 61511 standards.
It consists of 12 phases, the most important ones being the following:
- General conception of the project
- Risk analysis
- Allocation of the safety functions to the independent protection layers
- Design of the SIS (instrument system for the implementation of the safety functions)
- Test of the HW and SW components before installation
- Installation
- Maintenance
- Modifications
- Disposal

**IPL Independent Protection Layer**
An independent protection layer is any independent device that reduces risks by means of control, prevention or mitigation. An explosion-proof design, a PSV, a SIS, a warning system, a F&G system, but also an emergency plan or procedure can be an IPL.

**Mission time (T_m)**
Period of time that cover the whole life cycle of a SRP/CS.

**MTBF Mean time between failures**
It indicates the mean time between failures. It is a quality parameter that can be applied to mechanical, electric and electronic devices as well as to software applications. The MTBF value defines the time expected between one failure and the following one;

**MTTF Mean time to dangerous failure**
Expected time during which one channel is free from dangerous failures.

**MTTR Mean time to restore**
Mean time necessary for the safety systems to be restored, measured as the time that elapses from the failure appearance to the moment when it is completely repaired.

**PL Performance level**
This level specifies the ability of the parts of a control system to perform a safety function in specific conditions.

**PL Required performance level**
Performance level (PL) that allows to achieve a required risk reduction for each safety function.

**PFD Probability of failure on demand**
Probability of failure upon demand of the function

**PFD_{avg} Average probability of failure on demand**
Average probability of failure upon request of the function

**PFH Probability of failure per hour**
Probability of failures per hour

**PFHD Probability of dangerous failure per hour**
Probability of dangerous failures per hour

**Redundancy**
The duplication of the means required to perform a required function
**Residual risk**
The risk that remains after the protective and preventive measures have been adopted.

**Risk**
Combination of the probabilities of appearance of a danger and its seriousness.

**Risk analysis**
Combination of the specifications of the limits of the machine, identification of the limits of the machine, identification of the dangers and estimate of the risks.

**Risk assessment**
The global process for analysing and evaluating the risks.

**Risk evaluation**
Evaluation on the basis of the risk analysis if the targets of the risk analysis have been achieved.

**Safety**
Safety is defined as the freedom from an unacceptable risk for the personnel, the community and the environment.

**Functional safety**
Part of the safety that depends on the proper operation of the safety related system [E/E/PE system], or other external risk reduction or safety system technologies.

**SFF Safe Failure Fraction**
It indicates the percentage of safe failures or identified dangerous failures. It is complementary to the previous indexes as – for high SIL levels – it is necessary that the failures are safe or detectable, as well as the least probable possible.

\[
SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_T}
\]

- \(\lambda_S\) is the probability of a non-dangerous failure.
- \(\lambda_{DD}\) is the probability of a detected dangerous failure.
- \(\lambda_T\) is the total failure probability

**Safety Function**
A safety function is a function that must be implemented by a safety instrumented system [SIS] and other protection layers [independent] to achieve or take the process back to safety, with respect to a specific dangerous event (in case one or more pre-defined conditions are no more met).

**SIF Safety Instrumented Function**
A safety instrumented function is a safety function [protection or control] that, with a specific safety integrity level [SIL], must be performed by a safety instrumented system [SIS] within a specified time.
SIS Safety Instrumented System
The safety instrumented system (SIS) defines an instrumented system for the implementation of one or more safety instrumented functions (SIF). It consists of a combination of one or more:
- sensors (e.g. transmitters);
- E/E/PE logic solvers, where: E = Electric (e.g. electromechanical relays) E = Electronic (e.g., solid state logics) PE = Programmable Electronic (e.g. PLC TMR), including I/O modules, user interface and power supply units:
- final elements (e.g. solenoids and RBV);

Safety Integrity
Probability that a SIS or any of its subsystems appropriately perform the safety control function under any condition.

Safety Lifecycle
The safety lifecycle includes all the activities that are necessary for the implementation of one or more safety instrumented functions (SIF), to be performed during the time span that starts from the general conception of the functional safety project and ends with the disposal of the SIS.

SRS Safety Requirements Specification
The safety requirements specification is the specification that includes all the requirements of the safety functions, which must be performed by the SIS and the other IPL.

Safety-related system
A system is defined as Safety Related when it is able to perform the safety functions that are necessary to implement a safety condition.

SIL Safety Integrity Level
The safety integrity level is the discrete number indicating the probability that a SIS appropriately performs a safety instrumented function within a specified time. The SIL is fixed for each independent safety instrumented function included in the SIS, not for the whole SIS. It is expressed by a number from 1 to 4, where the safety integrity level 4 is the highest and the safety integrity level 1 is the lowest.

Subsystem
Integrable part of the system architecture of a SIS, where the failure of each subsystem can lead to a failure of the safety control function.

Test rate $r_i$
Frequency of the automatic tests performed to detect failures in a SIS; reciprocal value of the "diagnostic test interval" 

$T_i$
Time interval between the periodic tests in a safety system.

Validation
Confirmation – by means of an examination [test, analysis] – that a “SIS” performs the requirements of the functional safety of a specific application.

Verification
Confirmation – by means of an examination [test, analysis] – that a SIS, its subsystems or each element of the subsystem perform the requirements of the relevant specifications.
1. SAFETY LIFECYCLE

The IEC 61508 standard requires using the safety lifecycle to achieve the functional safety. This paragraph provides some general directions related to safety, with particular focus on the aspects related to the System integration process. These principles can be perfectly applied to all the systems [safety-related], including the MSMX system.

1.1. Purpose of the safety

The systems of the MSMX series have been designed and certified to be used for safety applications. In this kind of systems, it is necessary to define and respect the requirements related to the system project, system construction, validation tests, installation, commissioning, operation, maintenance and disposal. This manual aims to define the requirements that must be respected during the phases of the lifecycle of the safety related systems, in order to ensure that the required safety targets are achieved and maintained over time. The MSMX system is certified by an independent body (TÜV Rheinland) and complies with the requirements of the IEC61508 SIL2, in single configuration with double CPU and SIL3 in duplex configuration. The content of this manual has been checked by the external certification body and represents the requirements that must be met to achieve a safety related system that can be certified up to SIL3.

1.2. Safety Management System

The safety management system defines all the technical activities that are necessary for the functional safety. In many cases, the management of safety and quality can be integrated into a single set of procedures. For this reason, it is recommended that the system integrator operates in compliance with the ISO9000 standards. The safety management shall include:

- a statement on the policy and strategies being used to achieve functional safety.
- a planning of the procedures related to safety, thus defining the different phases of the safety lifecycle, the measures and techniques to be adopted for each phase and identifying the people in charge of the performance of the necessary activities.
- Definition of the registers that must be produced and their management, including the revisions control system. The procedure for checking the amendments must include a register for the amendment requests, the analysis of the impact of the required amendments and the approval of the amendments. The guidelines for checking the amendments must be clearly defined.
- The key aspects of the development phase must be clearly identified and must include information on the version, e.g. system safety requirements, detailed plans of the project, source code of the application software, test plan, test procedures with the relevant results.
- Measures able to ensure that the staff has the skills that are necessary to perform the planned activities.
1.3. Phases of the safety lifecycle

The safety lifecycle includes all the activities that are necessary for the implementation of one or more safety instrumented functions (SIF), to be performed during the time span that starts from the general conception of the functional safety project and ends with the disposal of the safety instrumented system (SIS). It consists of the following phases:

- Definition of the purpose
- Specification of the functional requirements of the system
- Specification of the safety requirements of the system
- Design of the system
- Development of the software
- Manufacturing of the system
- Integration of the system
- Validation of the safety of the system
- Installation and commissioning of the system
- Procedures for the operation and maintenance of the system
- Modifications to the system
- Disposal of the system

Each phase of the lifecycle must include input data, output data and verification activities. The figure below shows a scheme of the safety lifecycle, as described in the IEC61508 standard.
1.4. Functional Safety Assessment
The functional safety assessment process aims to verify the effective implementation of the system functional safety only with respect to the safety functions, in order to verify that it was
designed, produced and installed in accordance with the relevant safety requirements. The assessment must be performed for all the required safety functions. It will take into consideration all the effects of the failures and errors occurred both inside and outside the system, as well as the failures due to procedure misapplications. The assessment shall be performed by a team of people not involved in the project. At least one functional safety assessment must be performed before any potential damage can occur, e.g. before start-up.

1.5. SIL - Safety integrity level
The safety integrity level is the discrete number indicating the probability that a SIS appropriately performs a safety instrumented function within a specified time. The SIL is fixed for each independent safety instrumented function included in the SIS, not for the whole SIS. It is expressed by a number from 1 to 4, where the safety integrity level 4 is the highest and the safety integrity level 1 is the lowest. Basically, the SIL is a quantitative measure of the “availability” of a given protection function and allows the designer to reduce the risk of a dangerous situation and to quantify its reduction. The SIL value quantifies the extent to which the user can expect the function to be available and, in case of failure, that this happens in a safe way. With respect to general protection functions, the OLF guideline reports the following SIL requirements:

<table>
<thead>
<tr>
<th>Protection Function</th>
<th>SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch for Emergency Shut Down (ESD)</td>
<td>2</td>
</tr>
<tr>
<td>Blow down with opening of Blow Down valve</td>
<td>2</td>
</tr>
<tr>
<td>Sump isolation or sump shut down</td>
<td>3</td>
</tr>
<tr>
<td>Riser isolation</td>
<td>2</td>
</tr>
<tr>
<td>Gas detection</td>
<td>2</td>
</tr>
<tr>
<td>Electric insulation activated by signal-related logics deriving from the Fire&amp;Gas system</td>
<td>2</td>
</tr>
<tr>
<td>Activation of extinguishing gas or water system</td>
<td>2</td>
</tr>
</tbody>
</table>

Tab. 1: SIL requirements for some protection functions

The IEC 61508 standard defines four levels for the Safety Integrity Level (from SIL1 to SIL4); each of them defines a quantitative measure of the necessary risk reduction and thus the reliability degree that shall be achieved by the system to ensure such reduction. This is a general level, which can be applied to all the safety related systems regardless of the application (transports, production...). The standard covers all the phases of the safety system, from the design phase to the operation and maintenance phase and to disposal, and can be applied to all the safety systems in which at least one of the components includes electric, electronic or electronic programmable devices. The standard does not define the SIL to be achieved with respect to the specific application: this operation must be performed by means of a risk analysis on the technical system taken into consideration and an assessment of the acceptable risk, as a combination of danger level and probability. It is also important to remember that the SIL is related to the specific safety function, not to the whole system or its components. Within a given system, there will be several safety functions; each of them is related to a specific danger and shall be assigned with a specific SIL. The combination of all the components (not the components considered one by one) of each safety system shall comply with the SIL classification to be achieved.
Risk consequence:
C1: minor injuries to a person or minor damages to the environment
C2: major and irreversible injuries to one or more people, death of one person. Major/temporary damages to the environment
C3: death of several people and major damages to the environment
C4: catastrophic consequences, many deaths

Frequency and time of exposition to the dangerous area:
F1: rare or frequent exposition
F2: frequent or permanent exposition

Damage avoidability:
P1: possible in some circumstances
P2: almost impossible

Risk probability:
W1: very low
W2: low
W3: relatively high
Tables 1 and 2 show the requirements for the fault tolerance of a safety device when used in combination with equipment of Group I or II.

### Tab. 2: Requirements of Safety Integrity Level and fault tolerance of a safety device controlling potential ignition sources in equipment Group I

<table>
<thead>
<tr>
<th>Hazardous area</th>
<th>2</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>-1&lt;sup&gt;a&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault tolerance of EUC</td>
<td>-</td>
<td>0&lt;sup&gt;b&lt;/sup&gt;</td>
<td>1&lt;sup&gt;c&lt;/sup&gt;</td>
<td>-</td>
<td>0&lt;sup&gt;e&lt;/sup&gt;</td>
</tr>
<tr>
<td>Fault tolerance of the safety device</td>
<td>-</td>
<td>0&lt;sup&gt;b&lt;/sup&gt;</td>
<td>1&lt;sup&gt;c&lt;/sup&gt;</td>
<td>-</td>
<td>0&lt;sup&gt;e&lt;/sup&gt;</td>
</tr>
<tr>
<td>Safety Integrity Level of the safety device</td>
<td>SIL 1</td>
<td>SIL 2</td>
<td>SIL 1</td>
<td>SIL 2</td>
<td></td>
</tr>
<tr>
<td>Category of the combined equipment</td>
<td>M1</td>
<td>M2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<sup>a</sup> “-1” indicates that the EUC performs a source of ignition in normal mode of operation (e.g., general purpose equipment which may not comply with the relevant standards EN 60079-0, EN 61241-0 or contains relays, fuses, switching contacts, etc.).

<sup>b</sup> “0” indicates that one single fault may cause the safety device to fail.

<sup>c</sup> “1” indicates that two faults may cause the safety device to fail, e.g. in case the safety device is seen as redundant.

<sup>d</sup> According to EN 61508 series.

<sup>e</sup> The appropriate category definitions and conformity assessment procedures relating to the category are defined in Directive 94/9/EC.

NOTE: Specific features regarding the construction, manufacturing and operation of equipment of Category 1 can be found in Directive 94/9/EC.

### Tab. 3: Requirements of Safety Integrity Level and fault tolerance of a safety device controlling potential ignition sources in equipment Group II

<table>
<thead>
<tr>
<th>Hazardous areas</th>
<th>Zone 20</th>
<th>Zone 21</th>
<th>Zone 22</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault tolerance of EUC</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Fault tolerance of the safety device</td>
<td>-</td>
<td>0&lt;sup&gt;b&lt;/sup&gt;</td>
<td>1&lt;sup&gt;c&lt;/sup&gt;</td>
</tr>
<tr>
<td>Safety Integrity Level of the safety device</td>
<td>-</td>
<td>SIL 1</td>
<td>SIL 2</td>
</tr>
<tr>
<td>Category of the combined equipment</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

<sup>a</sup> “-1” indicates that the EUC performs a source of ignition in normal mode of operation (e.g., general purpose equipment which may not comply with the relevant standards EN 60079-0, EN 61241-0 or contains relays, fuses, switching contacts, etc.).

<sup>b</sup> “0” indicates that the EUC is assessed as safe in normal operation in zone 2/22 without a safety device, (e.g. conforms to protection type EEx n)

<sup>c</sup> “0” indicates that one single fault may cause the safety device to fail.

<sup>d</sup> “1” indicates that two faults may cause the safety device to fail, e.g. in case the safety device is seen as redundant.

<sup>e</sup> According to EN 61508 series.

NOTE: Specific features regarding the construction, manufacturing and operation of equipment of Category 1 can be found in Directive 94/9/EC.
1.6. Methods for assessing the reliability of a subsystem

The FMEA technique is a method used to analyse the failure or fault modes of a process, product or system. The acronym stands for **Failure modes and effects analysis**. It is basically used only to select applications and industries where failures are particularly costly. The main benefit was to have a qualitative assessment of the safety of a system, to define the unacceptable failure modes, to identify any potential improvement of the project, to plan the maintenance activities and to help understand the system behaviour in the presence of failures. The FMECA technique [**Failure Mode, Effects, And Criticality Analysis**] is an extension of FMEA. In addition to the basic FMEA, it includes the criticality analysis that is used to define the probabilities of the failure modes considered according to the seriousness of the consequences. The result highlights the failure modes that have the highest probability to occur combined with the highest seriousness of the consequences, allowing to direct the design revision efforts toward the greatest benefit.

The FMEDA technique [**Failure Modes, Effects and Diagnostic Analysis**] adds two kinds of information with respect to the FMEA analysis. The first additional piece of information refers to the quantitative analysis of the failures (percentage of failures and distribution of the failure modes) of all the components that are being analysed; the second additional piece of information refers to ability of a system or subsystem to detect any internal failures by means of automatic diagnostic systems. This is crucial to implement and maintain the reliability in complex systems and systems than need to fully perform their functions in some circumstances such as the request of an emergency shut down in the ESD systems. Therefore, it is important to quantify the automatic diagnostic ability of a system or subsystem. The IEC 61508 standard officially accepts the FMEDA technique and many IEC 61508 certification bodies use the FMEDA results to verify the safety level achieved for each application. In the field of functional safety, standardized failure modes have been defined to help facilitate the implementation of the FMEDA and to interpret its results. The use of FMEDA in IEC61508 is focused on the definition of the two measurements of **Safety Integrity**: the **Dangerous Undetected Failure Rate** and a measurement standard known as **Safe Failure Fraction**, SFF. This datum represents the non-dangerous failure percentage detected by the system.

1.7. Hardware architecture

Several types of architecture are used to increase the availability and failure tolerance capacity of the safety systems. The choice of the architecture type depends on the safety level that you want to achieve. The addition of a redundancy does not always result in an increase in safety. The two figures below show the safe and dangerous failures percentages in the various architectures.

![Failure Rate vs Architecture](image-url)

**Fig. 3: Percentage of dangerous failures in the various architectures**
1.8. Average probability of failure of a function on demand

Every safety system consists of several subsystems (the sensor, the logic solver, the actuators) and each of these has its own reliability. According to the characteristics of the component, it is possible to decide if it can be part of a safety system with a specified SIL level.

\[ \text{PFDAVG/PFHAVG (Probability of Failure on Demand and Probability of Failure per Hour)} \]

\[ \text{PFDAVG} \] and \[ \text{PFHAVG} \] are the probabilities that the safety system fails to perform in case of need; in order to achieve high SIL levels, they should be as low as possible.

Where:

- \( \lambda_D \) percentage of dangerous failures.
- \( T_l \) time interval between two tests able to detect the failure.

The choice between the \( \text{PFDAVG} \) and \( \text{PFHAVG} \) indexes depends on the frequency of demand of operation of the safety function. For systems with low demand mode of operation the \( \text{PFDAVG} \) value is used, while the \( \text{PFHAVG} \) value is used for systems with high demand mode of operation.

The Fire&Gas systems usually fall into the first category.

1.9. Procedure for calculating the PFD

A safety-related system must be designed and developed in accordance with the defined safety specifications. For this reason, the hardware architecture requirements shall respect the requirements of the safety level that you intend to achieve. In order to calculate the safety integrity of a safety related system consisting of several elements, it is necessary to calculate the \( \text{PFD}_{\text{sys}} \) or \( \text{PFH}_{\text{sys}} \) values of the whole system, which can be achieved by the summing up the values of all the elements. The average probability of dangerous failures on demand for a safety function for E/E/PE safety-related systems is defined by calculating and combining the average probability of failure on demand of each of the subsystems that operate to implement a safety function.

\[ \text{PFD}_{\text{sys}} = \text{PFDS} + \text{PFDL} + \text{PFDFE} \]

Where: \( \text{PFDSYS} \) is the average probability of failure on demand of a safety function performed by a E/E/PE safety-related system. \( \text{PFDS} \) is the average probability of failure on demand with respect to the sensors.
**PFDL** is the average probability of failure on demand with respect to the logic solver

**PFDFE** is the average probability of failure on demand with respect to the final elements

In order to define the average probability of failure on demand for each of the subsystems, it is necessary to adopt the following procedures for each subsystem:

a) Drawing a flow-chart representing the components of the subsystems related to the sensors (Input), the logic solver and the final elements (Output). For example, the components related to the sensor subsystem can be sensors, barriers, and signal conditioning circuits; the components related to the logic solver subsystem can be the processor and scanning device; the components related to the final elements subsystem can be barriers and actuators.

b) Defining the time interval of the proof-test. (e.g. 1 year) and the necessary time to restore each failure after MTTR has occurred (e.g. 8 hours)

c) Defining the following information for each voted group in the subsystem:

- the architecture type (1oo1, 1oo2 etc)
- the diagnostic coverage of each channel (e.g., 60%)
- The failure rate (per hour), λ, of each channel (e.g., 5.0E-06)
- The common failure causes, β and βD, for interaction between the channels defined in the voted group (e.g., 2% and 1% respectively)

d) For each voted group, defining the average probability of failure on demand \((PFD_{AVG})\)

e) If the safety function depends on more than one voted group of sensors or actuators, the combined value of the average probability of failure on demand of the subsystems related to sensors or final elements, \(PFD_{so} \quad PFDFE\), is given by the following equations, where \(PFD_I\) and \(PFD_J\) indicate the average probability of failure on demand for each voted group of sensors and final elements

\[
PFD_s = \sum PFD_I \quad PFD_{FE} = \sum PFD_J
\]
1.10. Classification of the subsystems

It is possible to classify the safety subsystems in two groups: Type A and Type B. A subsystem belongs to type A if:

- The failure modes of all the elements are known
- The behaviour of the subsystem in case of failure can be defined
- A suitable number of data showing that the failure percentage is low is available

In short, they are simple subsystems such as valves, contactors, etc. A subsystem belongs to type B if:

- The failure mode of at least one element taken into consideration is not known
- The behaviour of the subsystem in case of failure cannot be fully defined
- A suitable number of data showing that the failure percentage is low is not available

These are complex subsystems, e.g. programmable logics. For this kind of systems, as they are partially unpredictable, the classification requirements are more pressing. In particular, with equal SFF values, they achieve a level less. The Fire&Gas systems as well as the MSMX-HS system belong to type B.

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Type A</th>
<th>Type B</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hardware failure tolerance</td>
<td>Hardware failure tolerance</td>
</tr>
<tr>
<td></td>
<td>0 failures</td>
<td>1 failure</td>
</tr>
<tr>
<td>&lt; 60 %</td>
<td>SIL 1</td>
<td>SIL 2</td>
</tr>
<tr>
<td>60 % - &lt; 90%</td>
<td>SIL 2</td>
<td>SIL 3</td>
</tr>
<tr>
<td>90 % - &lt; 99%</td>
<td>SIL 3</td>
<td>SIL 4</td>
</tr>
<tr>
<td>≥ 99 %</td>
<td>SIL 3</td>
<td>SIL 4</td>
</tr>
</tbody>
</table>

Tab. 4: Safe failure fraction and Hardware fault tolerance

**Hardware Fault Tolerance**

This parameter indicates the number N of failures for which an N+1Nth failure can cause a loss of the safety function.

<table>
<thead>
<tr>
<th>Safety Integrity Level (SIL)</th>
<th>Average Probability of Failure on Demand (PFD_{AVG})</th>
<th>Average Probability of Failure per Hour (PFH_{AVG})</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIL 4</td>
<td>$10^{-5} \leq x \leq 10^{-4}$</td>
<td>$10^{-9} \leq x \leq 10^{-8}$</td>
</tr>
<tr>
<td>SIL 3</td>
<td>$10^{-4} \leq x \leq 10^{-3}$</td>
<td>$10^{-8} \leq x \leq 10^{-7}$</td>
</tr>
<tr>
<td>SIL 2</td>
<td>$10^{-3} \leq x \leq 10^{-2}$</td>
<td>$10^{-7} \leq x \leq 10^{-6}$</td>
</tr>
<tr>
<td>SIL 1</td>
<td>$10^{-2} \leq x \leq 10^{-1}$</td>
<td>$10^{-6} \leq x \leq 10^{-5}$</td>
</tr>
</tbody>
</table>

Tab. 5: SIL and probability of failure on demand
Equations to define the PFD of a 1oo1 system

\[
PFD_{G,1oo1} = (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE}
\]

\[
= \lambda_D \cdot t_{CE}
\]

\[
= \lambda_{DU} \cdot \left(\frac{T_I}{2} + MTTR \right) + \lambda_{DD} \cdot \left(MTTR + \frac{T_D}{2} \right)
\]

Dove

\[
t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_I}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot \left(MTTR + \frac{T_D}{2} \right)
\]

Equations to define the PFD of a 1oo2 system

\[
PFD_{G,1oo2} = 2 \cdot \left(\left(1 - \beta_D\right) \cdot \lambda_{DD} + \left(1 - \beta\right) \cdot \lambda_{DU}\right)^2 \cdot t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot \left(MTTR + \frac{T_D}{2} \right) + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_I}{2} + MTTR\right)
\]

Dove

\[
t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_I}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot \left(MTTR + \frac{T_D}{2} \right)
\]

\[
t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_I}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot \left(MTTR + \frac{T_D}{3} \right)
\]

TI Proof test interval

TD Diagnostic interval (1h)
2. REMARKS ON THE MSMX SYSTEM
This chapter provides detailed remarks on the safety to be adopted for MSMX systems in safety applications.

2.1. Characteristics of the MSMX system
The MSMX system features a modular structure. The processing rack includes the central unit and a interface panel for the operator. Each central unit can be connected with up to 10 racks having up to 13 I/O modules, for an overall number of 130 modules. The I/O modules can be inserted into the racks without any kind of limit, according to the requirements of the system that need controlling.

Fig. 6 Architecture of the MSMX system
2.1.1. Safety Applications

In order to perform safety functions, it is necessary to use safety related I/O modules only, in single or duplex configuration.

It is also possible to use non safety related modules in safety systems, provided that they are not used to perform safety functions. The non safety related modules of the MSMX system do not affect the safety functions performed by the system.

<table>
<thead>
<tr>
<th>Part Number</th>
<th>Description of the module</th>
<th>Safety related</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSMX-F3002-1</td>
<td>Module with 8 controlled inputs</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F3002-2</td>
<td>Module with 8 controlled inputs that can be overloaded</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F4001-1</td>
<td>Module with 1 4-20mA analogical input</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F4001-2</td>
<td>Module with 1 4-20mA analogical input that can be overloaded</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F4002-1</td>
<td>Module with 2 4-20mA analogical inputs</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F4002-2</td>
<td>Module with 2 4-20mA analogical inputs that can be overloaded</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F4003-1</td>
<td>Module with 8 4-20mA analogical inputs</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F4003-2</td>
<td>Module with 8 4-20mA analogical inputs that can be overloaded</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F5001-1</td>
<td>Module with 8 500mA controlled outputs</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F5001-2</td>
<td>Module with 8 500mA controlled outputs that can be overloaded</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F5002-1</td>
<td>Module with 16 250mA non-controlled output</td>
<td>No</td>
</tr>
<tr>
<td>MSMX-F5003-1</td>
<td>Module with 8 250mA controlled outputs</td>
<td>No</td>
</tr>
<tr>
<td>MSMX-F5004-1</td>
<td>Module with 4 2A controlled outputs</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F5004-2</td>
<td>Module with 4 2A controlled outputs that can be overloaded</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F6001-1</td>
<td>Module with 8 outputs for the management of extinguishing systems</td>
<td>Yes</td>
</tr>
<tr>
<td>MSMX-F6002-1</td>
<td>Logic Module 100 flip/flop + 100 Timer</td>
<td>No</td>
</tr>
<tr>
<td>MSMX-F7002-1</td>
<td>Module for Loop control with ESP protocol</td>
<td>No</td>
</tr>
<tr>
<td>MSMX-F7006-1</td>
<td>Module ModBus RTU Master/Slave</td>
<td>No</td>
</tr>
<tr>
<td>MSMX-F7007-1</td>
<td>Module for Loop control with SSP protocol</td>
<td>No</td>
</tr>
</tbody>
</table>

Tab. 6: List of the I/O modules
2.2. **Hardware configurations**

The following hardware structures can be used for safety applications:

**Configuration 1**

This solution includes an overloaded central unit and single I/O modules.

```
<table>
<thead>
<tr>
<th>CPU-1</th>
<th>CPU-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input modules</td>
<td>Output modules</td>
</tr>
<tr>
<td>I/O bus</td>
<td>I/O bus</td>
</tr>
</tbody>
</table>
```

Fig. 7 Configuration 1

**Configuration 2**

This solution includes the central unit and the I/O modules in an overloaded configuration (duplex).

```
<table>
<thead>
<tr>
<th>CPU-1</th>
<th>CPU-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input modules</td>
<td>Output modules</td>
</tr>
<tr>
<td>I/O bus</td>
<td>I/O bus</td>
</tr>
</tbody>
</table>
```

Fig. 8 Configuration 2
The redundancy of the I/O modules increases the availability of the system. In the case of error or failure of a module, the latter is automatically put in safety mode (OFF) while the overloaded module continues to work.

2.2.1. Detection of the failures
The diagnostics on the MSMX system is regularly performed by means of hardware and software. The detected failures are clearly shown on the system display, providing the maintenance operator with clear information on the failure type and its causes. In the overloaded configurations (Type B), the other module continues to perform its functions without interrupting the safety functions. The replacement of the out-of-order module for all the modules of the MSMX system can be performed while the system is working (Hot plug), thus without the need to stop the system operation.

To replace the modules, please see the user and maintenance manual ST-048-IT. The user can define the system behaviour according to the failure types by means of the application program.

2.2.2. Failures of the central unit
The central unit of the MSMX systems for safety applications is always in the overloaded configuration (duplex). The two CPU modules exchange data continuously and compare the information received from the I/O modules; thus the detection of a failure is promptly shown on the diagnostic display. The detection of a failure on a CPU module causes the shutdown of the module. The other module continues to perform its functions without interrupting the safety functions performed by the system. In case of a failure that causes the shutdown of both modules (Power supply Undervoltage/Overvoltage), the safety related outputs are put in failsafe mode.

2.2.3. Rack controllers failures
The rack controllers are located in position 14 of each rack and perform the data exchange between the central unit and the I/O modules featured in the rack. The interruption of the communication links is detected by the firmware of the central unit and shown on the system display by the diagnostics. The architecture of the communication in single configuration includes two independent communication loops, one for each CPU module. For this reason, even if the modules are not overloaded, this structure is failure tolerant.
2.2.4. Failures of the digital input modules

The safety related digital input modules are equipped with a circuit that allows to simulate the opening and closing of each channel. During operation, each channel is constantly tested and if an error occurs on one channel, the latter is isolated from operation and put in failure mode by the central unit (channel shutdown). The application program allows defining the behaviour of the system logics according to the user’s requirements for this kind of failures.

![Digital inputs diagnostics](image)

2.2.5. Failures of the analogue input modules

The safety related analogue input modules are equipped with two different measurement circuits, one for each input channel. The two values are then compared and, in case of a difference between the two values, the channel is isolated from operation and put in the failure mode by the central unit (channel shutdown). The application program allows defining the behaviour of the system logics in accordance with the user’s requirements for this kind of failures.
2.2.6. Failures of the digital output modules

The safety related output modules have two driving semiconductors connected in series between them. During operation, the output channels are constantly tested by inverting the output status for a few hundreds of microseconds. If there is a difference between the status that has been set and the one read on the channel, the whole module is isolated from operation and the outputs are put in safety mode (Shutdown).

Fig. 10 Diagnostics of digital outputs

2.2.7. Failures of the power supply unit

The central unit promptly signals any kind of failure related to the power supply unit. In particular, the following types of failure are signalled:

- **PSU-1 Failure**: It indicates a failure of at least a power supply module or the complete lack of primary power supply.
- **PSU-2 Failure**: It indicates a failure of the batteries or of the charging module.

Moreover, during operation, the central units constantly check the value of the power supply voltages: main 25V and local 3.3V. If one of these two voltages is not included in the accepted range, a safety switch-off sequence is performed to put the whole system in safety mode. During such sequence, the following operations are performed:

- Activation of the general FAULT and SYSTEM FAULT outputs.
- Disabling of the general RUN output.
- Disabling of led RUN on CPU.
- Notification on display of the PANEL SHUT-OFF condition.
- Storage in the event history of the OPERATION END message.
- Sending of the OPERATION END message to the communication peripheral devices.

In this condition, the status of the outputs is frozen. In order to exit this situation, it is necessary to restart the system.

Voltage accepted range 25V: \(18.5 - 32\text{Vdc}^1\)
Voltage accepted range 3.3V local: \(3.15 - 3.6\text{Vdc}^2\)

---

1 if the voltage is lower than 22.5 V and higher than 29.5, a warning condition is notified.

2 if the voltage is lower than 3.15 V, the function is performed by the external reset circuit.
2.2.8. Failsafe of the safety related outputs

The failsafe status of the safety related outputs is normally de-energized (de-energizing the output is necessary to perform the safety function). For this reason, all the safety related outputs must be configured to be energized during normal operation. In some applications, the energized status is required to perform the safety function.

This operation mode shall be used in the following cases only:
- The activation of the system is only a mitigation of a pre-existing risk, usually in Fire&Gas applications.
- The accidental activation of the system is dangerous for people, usually in gas-extinguishing systems.

2.3. Development of the application program

The application program is developed offline, on a personal computer in Windows environment, by means of the appropriate PR0-MSMX configuration program. For the production of the application program, please refer to the appropriate ST-015-IT manual. After developing the application program, it is necessary to perform a functional test to verify that the logics performed by the system comply with the specifications of the system. It is also possible to perform a preliminary simulation of the logics with the programming tool, offline.

The programming must be performed by skilled personnel that are qualified to operate on safety systems.

The functional test of a safety related application program is considered as 100% if:
- All the inputs have been tested in all the possible statuses
- All the outputs have been tested through the whole program
- All the logical paths have been tested
- All the timings have been checked
- The response timing of each safety loop have been checked
- All the combinations of the digital signals commutations – including the failure conditions – have been checked

2.3.1. Modifications to the application program

Before modifying the application program, it is necessary to:
- Analyse the impact to verify that the safety functions are not affected by the modification and to plan the tests to be performed for verification.
- Be sure to operate on the current version and not on previous versions. For this reason, we recommend downloading the application program from the system before performing the modification or checking online that the file on your PC and the resident file on the system are the same.
- Save the modified file with a different modification index.
- Keep track of the modifications to the application program.
- Test the modification on the system, according to the planning made during the analysis.
2.3.2. Protection of the application program

In order to keep the application program from being manipulated by unauthorized people, it is necessary to perform the protection of the program by means of the user code featured on the USB key supplied with the PR0-MSMX programming tool. After such operation, it will be possible to upload and download the application program only with the original USB key.

2.3.3. Manual forcing of the outputs

It is possible to perform a manual forcing of the outputs during the diagnostic cycle tests or the operation by means of the Iride supervision system. Such forcing is possible only with access level 4 (maintenance operator) from the diagnostic cycle or inserting the password from the Iride supervision system.

Before performing a manual forcing of the outputs, analyze the impact of the operation on the safety system and take any necessary and appropriate measures.

2.4. Environmental requirements

The environmental and installation conditions are a potential source of common failures. For this reason, it is important to ensure that the safety system and the related devices can be used in the intended environment.

2.4.1. Climate conditions

The following table shows the operating and storage climate conditions for the MSMX system. The climate conditions are referred to the system as a whole.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Accepted range</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating temperature</td>
<td>-5….+50°C</td>
<td>dry</td>
</tr>
<tr>
<td>Storage temperature</td>
<td>-40….+85°C</td>
<td>dry</td>
</tr>
<tr>
<td>Operating humidity</td>
<td>5….95% RH</td>
<td>No condensate</td>
</tr>
<tr>
<td>Storage humidity</td>
<td>5….95% RH</td>
<td>No condensate</td>
</tr>
</tbody>
</table>

Tab. 7 Climate conditions

Please note that the operating temperature inside an electronic device has an important impact on the duration of its operating lifetime. High operating temperatures and sudden temperature increases can significantly reduce the operating lifetime of electronic devices. For this reason, it is important that the operating conditions are included in the accepted range.

With storage temperatures under -30°C and above +60°C, it is necessary to remove the lithium battery featured on the central units (MSMX-U1002-1).
2.4.2. Mechanical conditions
The following table lists the types of mechanical tests that were performed on the MSMX system.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Test</th>
<th>Test levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 68-2-6</td>
<td>Vibration sinusoidal test (endurance)</td>
<td>Frequency range: 10...150Hz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acceleration amplitude: 0,5g</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of axis: 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of sweep cycles: 20 per axis</td>
</tr>
<tr>
<td>IEC 817</td>
<td>Impact test</td>
<td>Impact energy: 0,5J</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of impact per point: 3</td>
</tr>
</tbody>
</table>

Tab. 8 Mechanical conditions

2.4.3. Electromagnetic compatibility conditions EMC
The MSMX system was designed and tested to bear normal levels of radiated or conducted electromagnetic disturbances and electrostatic discharges. The following table lists the types of tests and the levels that were performed on the MSMX system.

<table>
<thead>
<tr>
<th>Basic Standard</th>
<th>Date</th>
<th>Title</th>
<th>Test Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN 61000-4-2</td>
<td>1995</td>
<td>Electrostatic discharge immunity test</td>
<td>6 kV contact discharge</td>
</tr>
<tr>
<td></td>
<td>1998</td>
<td></td>
<td>8 kV air discharge</td>
</tr>
<tr>
<td></td>
<td>2001</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EN 61000-4-3</td>
<td>1996</td>
<td>Radiated, radio-frequency, electromagnetic field immunity test</td>
<td>10 V/m 80 MHz...2 GHz, 80 % AM</td>
</tr>
<tr>
<td></td>
<td>1998</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2001</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EN 61000-4-4</td>
<td>1995</td>
<td>Electrical fast transients/bursts immunity test</td>
<td>2 kV power supply</td>
</tr>
<tr>
<td></td>
<td>2001</td>
<td></td>
<td>1 kV signal lines</td>
</tr>
<tr>
<td>EN 61000-4-5</td>
<td>1995</td>
<td>Surge immunity test</td>
<td>2 kV common mode</td>
</tr>
<tr>
<td></td>
<td>2001</td>
<td></td>
<td>1 kV differential mode</td>
</tr>
<tr>
<td>ENV 50141</td>
<td>1994</td>
<td>Conducted disturbances induced by radio-frequency fields immunity test</td>
<td>10 V, 150 kHz...80 MHz, AM</td>
</tr>
<tr>
<td>EN 61000-4-11</td>
<td>1994</td>
<td>Voltage dips, short interruptions and voltage variations immunity test</td>
<td>60% 200ms</td>
</tr>
<tr>
<td></td>
<td>2001</td>
<td></td>
<td>100% 100ms</td>
</tr>
</tbody>
</table>

Tab. 9 EMC Conditions

The electrical disturbances can vary highly according to the type of installation, the type of wiring and the distance from other types of devices. Therefore, it is important to make sure that the levels of electromagnetic disturbance do not exceed the ones listed in the table.
2.4.4. Requirements of the power supply units

An inappropriate design of the power supply units and their distribution represent a potential cause of common failures. For this reason, it is necessary to adopt the following measures:

- Only use power supply units that have been approved and certified by the manufacturer.
- Define the requirements of the power supply unit according to the power required, the batteries endurance and the supplied input voltage.
- Only use power suppliers in a 100% redundant condition.
- Define the distribution of power and, for each distribution, define the cable dimension and any protection devices (fuses, automatic switches).

Any connection to other devices (e.g., DCS, ESD, SCADA) shall be performed without reference to the power supply voltage, using galvanic-insulated interfaces.

2.4.5. Interaction with the communication devices

The MSMX system is equipped with a communication protocol that allows to interact with external supervision systems. If these communications are used only to report information to external devices, no particular safety-related measures are needed. On the other hand, if the external communication devices can affect the safety functions, it is necessary to adopt the following measures:

- Avoid that the data received from external devices affect the safety functions. E.g., trigger a shutdown sequence.
- Pay particular attention to the possibility of performing remote manual forcing on the actuators that perform safety functions.
- Make sure that the data received by the safety system comply with the technical specification related to the Host protocol for MSMX systems.
- If the communication is performed on Ethernet network with TCP/IP protocol, use precautions to avoid sending data packets to the MSMX system accidentally (e.g., using a Firewall)
- If the communication with other devices is performed through a serial port (RS232 or RS485), use a galvanic insulation between the two devices. (E.g., fibre optic or Current loop)
2.5. Proof Test

IEC 61508 requires that the final user of a safety related system regularly performs the proof test of the devices, within the time interval defined by the manufacturer. The purpose of the proof test is to detect any latent dangerous failure that may affect the safety functions of the system. With respect to MSMX safety systems, the proof test must be performed with time intervals of one year. The types of tests to be performed depend on the system type, the potential risk level and the applicable standards. The test plan must be authorized by the authority in charge. In MSMX systems, the proof test can be performed on the whole safety loop. Here are some types of test to be performed:

- Check all the failure conditions that affect the logics related to the safety functions in order to ensure that they are properly monitored by the system. (E.g., disconnect the batteries, disconnect the primary power supply voltage)
- Perform the test of digital inputs and outputs in order to check that the system properly responds to the status variations.
- Perform the calibration of the analogue inputs to ensure an accurate measurement of the values provided by the field devices.

In order to check the proper operation of the secondary CPU, it is recommended performing half proof test with the primary CPU and half proof test with the secondary CPU. In order to do this, it is necessary to perform half proof test on a CPU switchovers.

2.6. Lifetime of the product

Even if the probabilistic assessment method assumes a constant failure rate, this is applied only if the operating life of the components has not expired. After the operating life has expired, the result of the probabilistic calculation method is not significant because the failure probability increases significantly over time. The operating life mainly depends on the very component and its operating conditions, particularly temperature (e.g., the electrolytic capacitors can be very temperature-sensitive). This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behaviour of electronic components. Therefore, the PFDavg calculation is obviously valid only for the components that have this constant trend and the validity of the calculation is limited to the operating life of each component. It is assumed that the “infant mortality” failures are mainly detected during the installation period and, therefore, the assumption of a constant failure rate during the operating life of the product is valid. However, according to the 7.4.7.4 section of the IEC 61508-2 standard, it is necessary to assume an operating life value on the basis of experience.

Thanks to our experience, we can say that the average operating life of MSMX system is 10-13 years.
Failure rate trend of electronic components
### 2.7. Calculating the PFD

In case of systems configured in compliance with the IEC 61508 standard, the calculation of the PFD for the safety instrumented functions performed by the system is required. Table 10 show the PFD and SFF values for the safety related modules that are featured in the MSMX system.

<table>
<thead>
<tr>
<th></th>
<th>MSMX F3002</th>
<th>MSMX F4001</th>
<th>MSMX F4002</th>
<th>MSMX F4003</th>
<th>MSMX E2002</th>
<th>MSMX F6001</th>
<th>MSMX U1002</th>
<th>MSMX F5001</th>
<th>MSMX F5004</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \lambda ) ([/h])</td>
<td>6.04E-07</td>
<td>5.39E-07</td>
<td>7.52E-07</td>
<td>1.09E-06</td>
<td>4.85E-07</td>
<td>3.71E-07</td>
<td>6.28E-07</td>
<td>8.15E-07</td>
<td>6.46E-07</td>
</tr>
<tr>
<td>MTBF ([/Year])</td>
<td>189</td>
<td>212</td>
<td>152</td>
<td>104</td>
<td>235</td>
<td>308</td>
<td>181</td>
<td>140</td>
<td>177</td>
</tr>
<tr>
<td>Proof Test interval ([/Year])</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>MTTR ([/h])</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>( \beta_D )</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
</tr>
<tr>
<td>( \beta )</td>
<td>0.02</td>
<td>0.02</td>
<td>0.02</td>
<td>0.02</td>
<td>0.02</td>
<td>0.02</td>
<td>0.02</td>
<td>0.02</td>
<td>0.02</td>
</tr>
<tr>
<td>SFF</td>
<td>98.84%</td>
<td>95.37%</td>
<td>95.58%</td>
<td>99.27%</td>
<td>99.20%</td>
<td>98.77%</td>
<td>95.27%</td>
<td>97.81%</td>
<td>99.17%</td>
</tr>
<tr>
<td>PFDavg (1oo1D)</td>
<td>2.44E-05</td>
<td>7.23E-05</td>
<td>7.33E-05</td>
<td>1.87E-05</td>
<td>1.54E-05</td>
<td>1.52E-05</td>
<td>1.11E-04</td>
<td>5.23E-05</td>
<td>2.08E-05</td>
</tr>
<tr>
<td>PFDavg (1oo2D)</td>
<td>4.69E-07</td>
<td>1.44E-06</td>
<td>1.46E-06</td>
<td>3.46E-07</td>
<td>2.83E-07</td>
<td>2.87E-07</td>
<td>2.20E-06</td>
<td>1.08E-06</td>
<td>3.94E-07</td>
</tr>
<tr>
<td>SIL Capability in (1oo1D) configuration</td>
<td>SIL2</td>
<td>SIL2</td>
<td>SIL2</td>
<td>SIL3</td>
<td>SIL3</td>
<td>SIL2</td>
<td>SIL2</td>
<td>SIL2</td>
<td>SIL3</td>
</tr>
<tr>
<td>SIL Capability in (1oo2D) configuration</td>
<td>SIL3</td>
<td>SIL3</td>
<td>SIL3</td>
<td>SIL3</td>
<td>SIL3</td>
<td>SIL3</td>
<td>SIL3</td>
<td>SIL3</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

Tab. 10: Parameters for the SIL calculation
**Digital detection and control loop in single configuration (MSMX-LDR&C-M)**

![Diagram of single configuration]

<table>
<thead>
<tr>
<th>Module</th>
<th>Architecture</th>
<th>PFDavg</th>
<th>SFF</th>
<th>SIL Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSMX-F3002-1</td>
<td>1oo1D</td>
<td>2,44E-05</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
<tr>
<td>MSMX-E2002-1</td>
<td>1oo1D</td>
<td>1,54E-05</td>
<td>&gt;99%</td>
<td>3</td>
</tr>
<tr>
<td>MSMX-U1002-1</td>
<td>1oo2D</td>
<td>2,20E-06</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
<tr>
<td>MSMX-F5001-1</td>
<td>1oo1D</td>
<td>5,23E-05</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
<tr>
<td>Logic Solver subsystem</td>
<td>1oo1D</td>
<td>9,43E-05</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
</tbody>
</table>

**Digital detection and control loop in duplex configuration (MSMX-LDR&C-D)**

![Diagram of duplex configuration]

<table>
<thead>
<tr>
<th>Module</th>
<th>Architecture</th>
<th>PFDavg</th>
<th>SFF</th>
<th>SIL Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSMX-F3002-2</td>
<td>1oo2D</td>
<td>4,69E-07</td>
<td>&gt;90%</td>
<td>3</td>
</tr>
<tr>
<td>MSMX-E2002-1</td>
<td>1oo2D</td>
<td>2,83E-07</td>
<td>&gt;90%</td>
<td>3</td>
</tr>
<tr>
<td>MSMX-U1002-1</td>
<td>1oo2D</td>
<td>2,20E-06</td>
<td>&gt;90%</td>
<td>3</td>
</tr>
<tr>
<td>MSMX-F5001-2</td>
<td>1oo2D</td>
<td>1,08E-06</td>
<td>&gt;90%</td>
<td>3</td>
</tr>
<tr>
<td>Logic Solver subsystem</td>
<td>1oo2D</td>
<td>4,03E-06</td>
<td>&gt;90%</td>
<td>3</td>
</tr>
</tbody>
</table>
Analogue detection and control loop in single configuration [MSMX-LAR&C-M]

NB: Only one type of analog inputs card must be used for each safety loop

<table>
<thead>
<tr>
<th>Module</th>
<th>Architecture</th>
<th>PFDavg</th>
<th>SFF</th>
<th>SIL Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSMX-F4001-1</td>
<td>1oo1D</td>
<td>7.23E-05</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
<tr>
<td>MSMX-F4002-1</td>
<td>1oo1D</td>
<td>7.33E-05</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
<tr>
<td>MSMX-F4003-1</td>
<td>1oo1D</td>
<td>1.87E-05</td>
<td>&gt;99%</td>
<td>3</td>
</tr>
<tr>
<td>MSMX-E2002-1</td>
<td>1oo1D</td>
<td>1.54E-05</td>
<td>&gt;99%</td>
<td>3</td>
</tr>
<tr>
<td>MSMX-U1002-1</td>
<td>1oo1D</td>
<td>2.20E-06</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
<tr>
<td>MSMX-F5001-1</td>
<td>1oo1D</td>
<td>5.23E-05</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
</tbody>
</table>

Logic Solver subsystem with MSMX-F4001-1 card

<table>
<thead>
<tr>
<th>Module</th>
<th>Architecture</th>
<th>PFDavg</th>
<th>SFF</th>
<th>SIL Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic Solver subsystem with MSMX-F4001-1 card</td>
<td>1oo1D</td>
<td>1.42E-04</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
</tbody>
</table>

Logic Solver subsystem with MSMX-F4002-1 card

<table>
<thead>
<tr>
<th>Module</th>
<th>Architecture</th>
<th>PFDavg</th>
<th>SFF</th>
<th>SIL Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic Solver subsystem with MSMX-F4002-1 card</td>
<td>1oo1D</td>
<td>1.43E-04</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
</tbody>
</table>

Logic Solver subsystem with MSMX-F4003-1 card

<table>
<thead>
<tr>
<th>Module</th>
<th>Architecture</th>
<th>PFDavg</th>
<th>SFF</th>
<th>SIL Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic Solver subsystem with MSMX-F4003-1 card</td>
<td>1oo1D</td>
<td>8.86E-05</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
</tbody>
</table>
Analogue detection and control loop in duplex configuration (MSMX-LAR&C-D)

NB: Only one type of analog inputs card must be used for each safety loop
Extinction detection and control loop in single configuration (MSMX-LR&E-M)

![Diagram of extinction detection and control loop in single configuration]

<table>
<thead>
<tr>
<th>Module</th>
<th>Architecture</th>
<th>PFDavg</th>
<th>SFF</th>
<th>SIL Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSMX-F3002-1</td>
<td>1oo1D</td>
<td>2,44E-05</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
<tr>
<td>MSMX-F6001-1</td>
<td>1oo1D</td>
<td>1,52E-05</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
<tr>
<td>MSMX-E2002-1</td>
<td>1oo1D</td>
<td>1,54E-05</td>
<td>&gt;99%</td>
<td>3</td>
</tr>
<tr>
<td>MSMX-U1002-1</td>
<td>1oo2D</td>
<td>2,20E-06</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
<tr>
<td>MSMX-F5004-1</td>
<td>1oo1D</td>
<td>2,10E-05</td>
<td>&gt;99%</td>
<td>3</td>
</tr>
<tr>
<td>Logic Solver subsystem</td>
<td>1oo1D</td>
<td>7,82E-05</td>
<td>&gt;90%</td>
<td>2</td>
</tr>
</tbody>
</table>

Extinction detection and control loop in duplex configuration (MSMXLR&E-D)

![Diagram of extinction detection and control loop in duplex configuration]

<table>
<thead>
<tr>
<th>Module</th>
<th>Architecture</th>
<th>PFDavg</th>
<th>SFF</th>
<th>SIL Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSMX-F3002-2</td>
<td>1oo2D</td>
<td>4,69E-07</td>
<td>&gt;90%</td>
<td>3</td>
</tr>
<tr>
<td>MSMX-F6001-1</td>
<td>1oo2D</td>
<td>2,87E-07</td>
<td>&gt;90%</td>
<td>3</td>
</tr>
<tr>
<td>MSMX-E2002-1</td>
<td>1oo2D</td>
<td>2,83E-07</td>
<td>&gt;99%</td>
<td>3</td>
</tr>
<tr>
<td>MSMX-U1002-1</td>
<td>1oo2D</td>
<td>2,20E-06</td>
<td>&gt;90%</td>
<td>3</td>
</tr>
<tr>
<td>MSMX-F5004-2</td>
<td>1oo2D</td>
<td>3,94E-07</td>
<td>&gt;99%</td>
<td>3</td>
</tr>
<tr>
<td>Logic Solver subsystem</td>
<td>1oo2D</td>
<td>3,63E-06</td>
<td>&gt;90%</td>
<td>3</td>
</tr>
</tbody>
</table>
3. **WARNINGS**

This document is not contractual. The specifications may be modified without notice to improve the product, or to meet applicable standards.

3.1. **Ownership and confidentiality**

The information, design data, drawings and diagrams contained in this document remain the property of SIMTRONICS and are confidential.

The information contained in this document cannot be used, either partially or wholly, nor divulged or reproduced without the prior agreement of SIMTRONICS.

3.2. **Liability**

The liability of SIMTRONICS shall be limited to any direct prejudice resulting from failure on SIMTRONICS part to fulfil the contract. SIMTRONICS shall decline all liability for any indirect prejudice caused.

By explicit agreement between the parties, the term “indirect prejudice” shall refer in particular to any financial loss, moral damage, loss of profit, earnings, clients or order, or any action taken against the client by a third party.

Moreover, any damages due from SIMTRONICS for any reason whatsoever shall not exceed the tax-exclusive value of the contract, except in the event of an intentional or fraudulent offense on the part of SIMTRONICS.

Application of the equipment warranty is subject to compliance with the state of the art and the operating instructions contained in this manual.

The SIMTRONICS warranty shall not apply; furthermore SIMTRONICS declines all liability, for damage to equipment or harmful accidents caused by negligence, failure to supervise the equipment or failure to use the equipment in compliance with the applicable recommendations, standards and regulations stipulated in the present manual.

The SIMTRONICS warranty shall not apply to faults resulting either, from materials supplied by the Purchaser, from design imposed by the Purchaser, from servicing or maintenance carried out on SIMTRONICS equipment by a third party not explicitly authorized, or from the use of unsuitable storage conditions.

In order to guarantee correct operation of the system, any addition of equipment to the system or any modification of the installation must be validated by SIMTRONICS.

4. **WARRANTY**

The MultiSafe MX comes with a 5 year warranty on the product. The warranty covers correct function inside specified tolerances. Faulty detectors under warranty will be repaired or replaced.

5. **CERTIFICATIONS AND STANDARDS**

The MultiSafe MX has been certified according to:

- IMQ-certified to EN 54-2 and EN 54-4 (fire detection)
- IMQ-certified to CEI 79-2 (intruder alarm)
- CPD-certified to EN 12094-1 (fire extinguishing)
- TUV-certified to IEC61508 (functional safety) – SIL 2 & 3
6. CONTACT DETAILS

You will find an updated list of distributors on our web pages: www.simtronics-fg.com
Email address for general enquiries: mail@simtronics.no

Simtronics ASA
Kabelgaten 4 B, Økern Næringspark
PO Box 314, Økern, NO-0511 Oslo, Norway
Tel: +47 2264 5055

Simtronics SAS
792, av de la Fleuride
BP 11016, 13781 AUBAGNE CEDEX – FRANCE
Tel: +33 (0) 442 180 600