

## Commissioning, maintenance and safety manual



# CAL40

# SIL2 / SIL3



Change content	Date	Index
Initial release	30/06/21	0
minors correction	13/07/21	1



LOREME 12, rue des Potiers d'Etain Actipole BORN Y - B.P. 35014 - 57071 METZ CEDEX 3  
Phone 03.87.76.32.51 - Telefax 03.87.76.32.52  
Contact: Commercial@Loreme.fr - Technique@Loreme.fr  
Download manual at: [www.loreme.fr](http://www.loreme.fr)

writing : DP  
checking : KR  
Approved : PH

# Summary

<b>1 Introduction</b>	<b>E3</b>
<b>1.1 General information</b>	<b>E3</b>
<b>1.2 Functions and intended uses</b>	<b>E3</b>
<b>1.3 Standards and Guidelines</b>	<b>E3</b>
<b>1.4 Information manufacturer</b>	<b>E3</b>
<b>2 Safety function and safety state</b>	<b>E4</b>
<b>2.1 Safety function</b>	<b>E4</b>
<b>2.2 Safety fallback position</b>	<b>E4</b>
<b>3 Safety Recommendation</b>	<b>E4</b>
<b>3.1 Interfaces</b>	<b>E4</b>
<b>3.2 Configuration / Calibration</b>	<b>E4</b>
<b>3.3 Useful lifetime</b>	<b>E4</b>
<b>4 Installation, commissioning and replacement</b>	<b>E5</b>
<b>4.1 Device description</b>	<b>E5</b>
<b>4.2 Electrical connection</b>	<b>E6</b>
<b>4.3 Internal synoptic</b>	<b>E6</b>
<b>5 Commissioning and periodic proof</b>	<b>E7</b>
<b>5.1 Control steps</b>	<b>E7</b>
<b>5.2 proof interval</b>	<b>E7</b>
<b>SIL2 compliance Declaration</b>	<b>E8</b>
<b>FMEA</b>	<b>E9-10</b>
<b>Appendix 1: Using data from the FMEA and further information on temperature sensors.</b>	<b>E11</b>
<b>Appendix 2: Terms and definitions.</b>	<b>E12</b>
<b>Appendix 3: EMC consideration</b>	<b>E13</b>

## 1 Introduction

### 1.1 General Information

This manual contains necessary information for product integration to ensure the functional safety of related loops. All the failure modes and the HFT of the module are specified in the FMEA analysis referenced AMDEC CAL40 Rev2.xls

Other documents:

- Technical datasheet CAL40
- EMC conformity declaration CAL40
- FMEA analysis CAL40 rev2

The mentioned documents are available on [www.loreme.fr](http://www.loreme.fr)

The assembly, installation, commissioning and maintenance can only be performed by trained personnel qualified and have read and understood the instructions in this manual.

When it is not possible to correct the defects, the equipment must be decommissioned, precaution must be taken to protect against accidental use. Only the manufacturer can bring the product to be repaired.

Failure to follow advice given in this manual can cause a deterioration in security features, and damage to property, environment or people.

### 1.2 Functions and intended uses

The transmitter CAL40 provides measurement of input signals coming from PT100, Pt1000 temperature sensors or potentiometer and the retransmission of information on 4-20mA analog output current.

The devices are designed, manufactured and tested according to security rules. They should be used only for the purposes described and in compliance with environmental conditions contained in the data sheet: [http://www.loreme.fr/fichtech/CAL40\\_eng.pdf](http://www.loreme.fr/fichtech/CAL40_eng.pdf)

### 1.3 Standards and Guidelines

The devices are evaluated according to the standards listed below:

- Functional safety according to IEC 61508, 2000 edition:  
Standard for functional safety of electrical / electronic / programmable electronic .

The evaluation of the material was performed by "*failure modes and effects analysis*" (IEC 60812 - Issue 2 - 2006) to determine the device safe failure fraction (SFF)

The FMEA is based on (IEC 62380-2004) Reliability data handbook. Universal model for reliability prediction of electronics components, PCBs and equipment

### 1.4 Manufacturer information

LOREME SAS  
12, rue des potiers d'étain 57071 Actipole Metz Borny  
[www.loreme.fr](http://www.loreme.fr)

## 2 Safety function and safety state

### 2.1 Safety function

The safety function of the device is completed, as long as the 4-20mA output current reproduce the temperature input measurement with a tolerance of + / -2%.

The operation range of the output signal goes from 3.8 mA to 20.5 mA

### 2.2 Safety fallback position

The safety fallback state is defined by output current outside the range of 3.6 mA to 21mA.

- Either an output current <3.6 mA
- Either an output current > 21 mA

The application should always be configured to detect the current value out of range (<3.6 mA -> 21 mA) and considered "faulty".

Thus, in the FMEA study, this condition is not considered dangerous.

The reaction time for all safety functions is <200 ms.

## 3 Safety Recommendation

### 3.1 Interfaces

The device has the following interfaces.

- safety interfaces: analog input measurement, analog output
- not safety interfaces : no

### 3.2 Configuration / Calibration

No hardware configuration is needed, the calibration is only possible by factory return .  
No changes should be made to the device

### 3.3 Useful lifetime

Although a constant failure rate is assumed by the probabilistic estimation, that it applies only to the useful lifetime of components.  
Beyond this lifetime, the probability of failure is increasing significantly with time.  
The useful lifetime is very dependent components themselves and operating conditions such as temperature, particularly (Electrolytic capacitors are very sensitive to temperature).

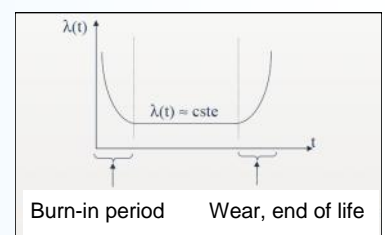
This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior of electronic components.  
Therefore, the validity of this calculation is limited to the useful life of each component.  
It is assumed that early failures are detected for a very high percentage during the burn in and the installation period, assuming a constant failure rate during the useful life remains valid.  
according to IEC 61508-2, a useful lifetime based on the feedback, must be considered.  
Experience has shown that the useful lifetime is between 15 and 20 years, and may be higher if there are no components with reduced lifetime in security function.  
(Such as electrolytic capacitors, relays, flash memory, opto coupler) and if the ambient temperature is well below 60 °C.

#### Note:

The useful lifetime corresponds to constant random failure rate of the device.  
The effective lifetime may be higher.

user must ensure that the device is no longer necessary for the security before its disposal.

Evolution of failure rate



## 4 Installation, commissioning and replacement

Operating capacity and current error reporting should be checked during commissioning (validation) see section: "**commissioning and periodic proof**" and at appropriate intervals recommended in paragraph: "**proof interval**" Any device that does not satisfy the commissioning control must be replaced.

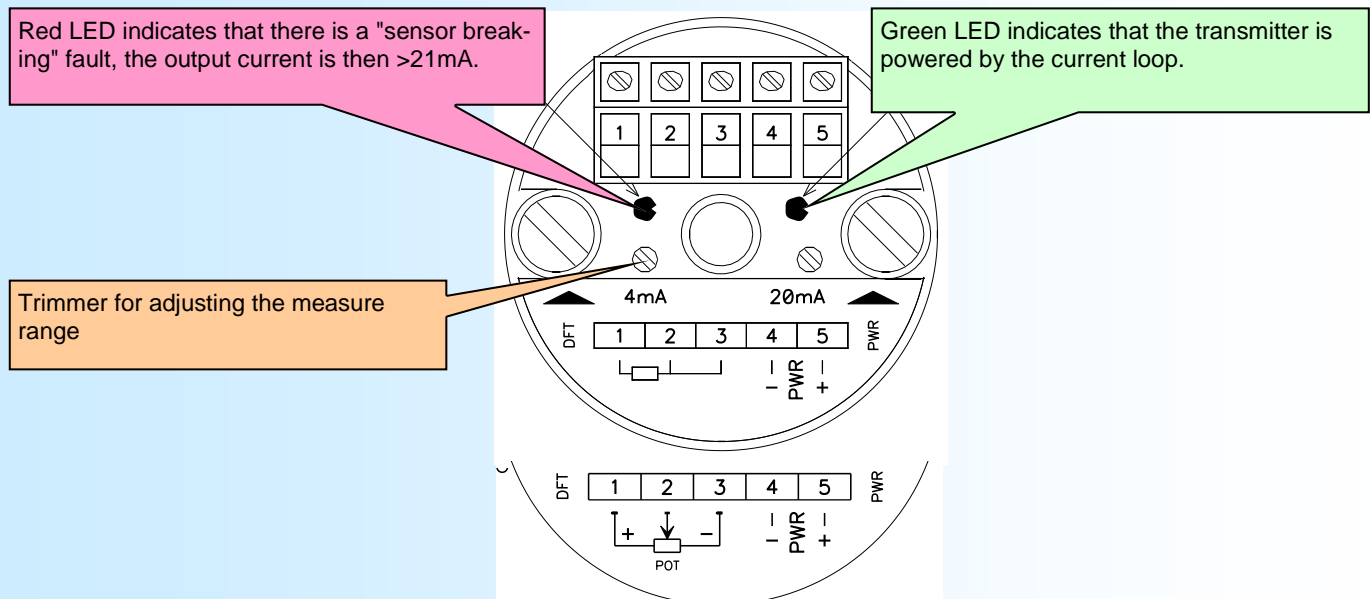
**WARNING!**

No user maintenance should be conducted, a defective device must be replaced by a new device of the same type. For a repair return or recalibration, it is very important that all types of equipment failures are reported to allow the company to take corrective action to prevent systematic errors.

### 4.1 Front panel description

Convention:

- The green LED indicate correct operation.
- The red LED indicate a warning or a defect.



# Analog transmitter for sensor head mounting Pt100, potentiometer, current loop powered

CAL40

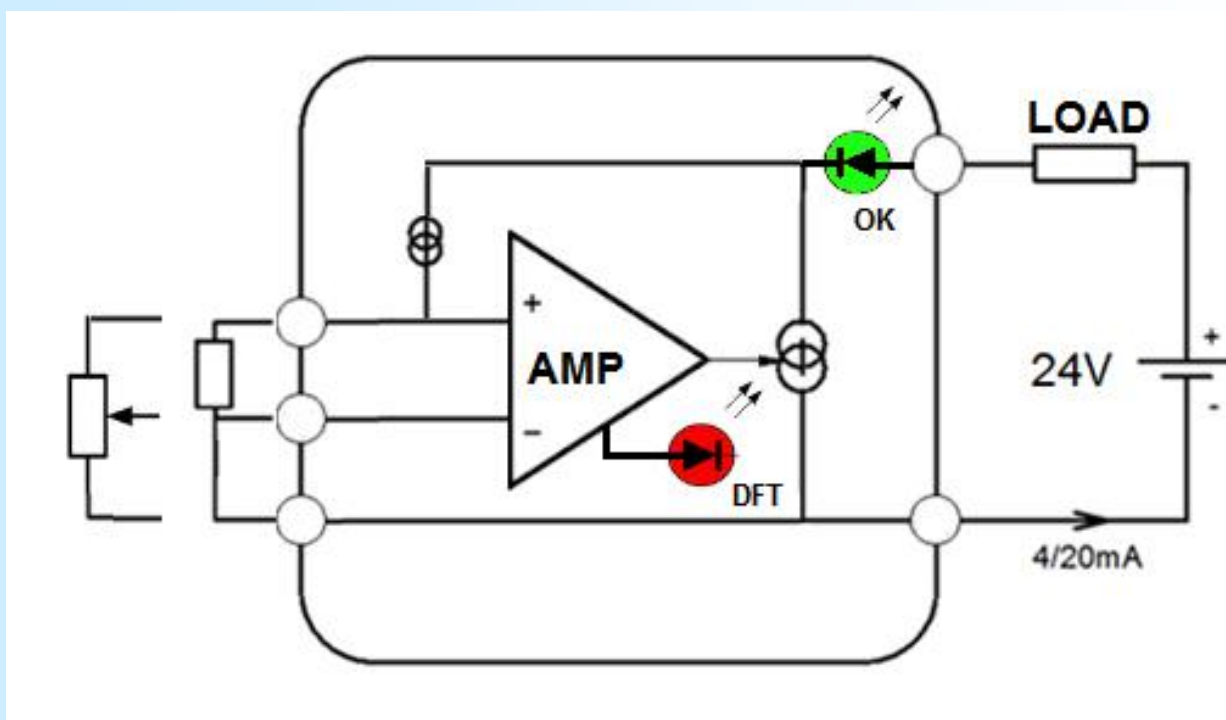


## 4.2 Electrical connection

\* **Device Power supply:** terminal 5 + and terminal 4 - , The device is powered by the 4-20mA current loop.

\* **Input measure:**  
Terminals 1, 2, 3 : wiring of PT100 sensor or potentiometer

## 4.3 Internal synoptic





## 5 Commissioning and periodic proof

The periodic test procedure is defined by LOREME and must be followed by the end user to ensure and guarantee the SIL level over time.

Periodic testing should be performed following the procedure defined below and at the intervals defined under paragraph " **proof interval** "

### 5.1 control steps

Periodic proof allows detection of possible product internal failure and loop calibration. environmental conditions and a minimum heating time of 5 minutes must be respected.

Complete test of transmitter and output Loop control (the system is unavailable during the test)

1. If necessary, bypass the security system and / or take appropriate provision to ensure safety during the test.
2. Disconnect the input sensor  
=> the transmitter should be in security. "Breaking sensor" condition, current >21mA.
3. Connect a *simulator\** in measure input. The transmitter should be in "out of alarm" condition
4. Simulated the temperature value for an output current of 4mA. Check if output current reaches this value at +/- 2%.
5. Simulated the temperature value for an output current of 20mA. Check if output current reaches this value at +/- 2%.
6. Simulated the temperature value for an output current of 12mA. Check if output current reaches this value at +/- 2%.
7. Disconnect the *simulator\**.
8. Connect the input sensor. Check if transmitter is in "out of alarm" condition.
9. After testing, the results should be documented and archived.

Any device that does not satisfy the control needs to be replaced.

\* *the temperature simulator must be calibrated (according to the state of the art and practice)*

### 5.2 proof interval

According table 2 from CEI 61508-1 the PFDavg ,for systems operating in low demand mode, must be between  $\geq 10^{-3}$  and  $<10^{-2}$  for SIL2 safety functions and between  $\geq 10^{-4}$  and  $<10^{-3}$  for SIL3 safety functions .

$\lambda f$	$\lambda$ dangerous = PFH	SFF (Safe Failure Fraction)	DC (Diagnosis coverage)
221 FIT	16 FIT	94 %	92.6 %

temperature conditions 25°C

### PFDavg value depending proof interval

T[Proof] = 1 year	T[Proof] = 5 years	T[Proof] = 10 years	T[Proof] = 20 years
PFDavg=7E <sup>-05</sup>	PFDavg=3.5E <sup>-04</sup>	PFDavg=7E <sup>-04</sup>	PFDavg=1.4E <sup>-03</sup>

approximation :  $PFD_{avg} = \lambda_{dangerous} \times T[Proof] / 2$  (error caused by approximation < 3%)

Fields marked in green means that the calculated values of PFDavg are within the limits allowed for SIL 3

Summary:

fault probability  $PFD = 7 E^{-5} \times T_{proof}$  [year]

either for :  $T_{proof} = 10$  years 7 % from SIF

Remarks :

- Test intervals should be determined according to the PFDavg required .

- The SFF , PFDavg and PFH must be determined for the entire safety instrumented function (SIF) ensuring that the " out of range current values" are detected at system level and they actually lead to the safety position.

<h1 style="margin: 0;">DECLARATION OF CONFORMITY</h1>		<p><b>REV1</b> <b>Page 1/1</b></p>
---	--	--

The LOREME society declare under our sole responsibility, that the following product:

<p>Designation: <b>Analog transmitter for head mounting PT100, PT1000 or potentiometer inputs</b></p> <p>Type: <b>CAL40</b></p> <p>Revision : 2 <span style="float: right;">date : 06/12/1995</span></p>
--

Can be used for functional safety applications up to SIL3 according to standard IEC61508-2: 2000 respecting the safety instructions specified in the safety manual .

The assessment of the safety critical and dangerous random errors lead to the following parameters :

device with type A components , Hardware fault tolerance HFT = 0 values for the converter only (worst case)

$\lambda_f$	$\lambda$ dangerous = PFH	SFF (1)	DC	PFD <sub>avg</sub> T[Proof] = 1 year	PFH
221 FIT <sub>(2)</sub>	16 FIT <sub>(2)</sub>	94 %	92.6%	7.0E <sup>-05</sup>	1.6E <sup>-08</sup> 1/h

(1) according to FMEA CAL40 rev2 established with "ALD MTBF calculator" : <http://www.aldservice.com/>

(2) FIT = Failure rate (1/h)

The safety manual gives the failure probabilities of associated sensors (Pt100 and thermocouple) to allow the evaluation of a complete loop.

Metz : 31/10/2017

Signed on behalf of LOREME ; M. Dominique Curulla



## FMEA Details

**Context**

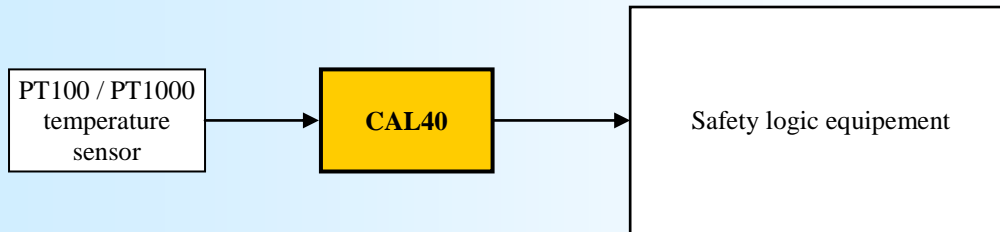
This document details the Failure Mode and Effects Analysis (FMEA) of CAL40 device of society LOREME. Besides the characterization of the information necessary for safe operation (especially for availability calculations and constitution of stock of spare parts), this study can meet the requirements of IEC-61508 standard for identifying and quantifying dangerous failures of the component, allowing to interact with the design to avoid or reduce these risks.

**Circumstances of the analysis**

This study was conducted in order to verify the ability of the transmitter CAL40 to be used in SIL3 applications.

**Scope of analysis**

The component concerned includes an electronics component assembly dedicated to the acquisition of input signals from temperature sensors and return an analog 4-20mA current in output. Typically, a converter is interfaced between a sensor and protection equipment, referred to as "logical security equipment"



**Characterization of the component**

The transmitter CAL40 is a type « A » subsystem [CEI61508-2-§ 7.4.3.1.2] :  
 The components failure modes necessary for achieving the safety function are well defined.  
 The transmitter behavior in fault conditions is fully determined.  
 The device has a feedback in many security applications.

**Safe failure**

[CEI61508-4-§3,6.8] Safe failure : Failure that has no potential to put the safety system in a dangerous state or unable to perform its function.  
 A safe failure is a failure that is not hazardous. Also known as secure failure.

**SFF** [CEI61508-2-§7.4.3.1.1-d] Safe failure fraction is the ratio of the sum of safe failure rate  $\lambda_S$  plus the dangerous detected failure rate  $\lambda_{DD}$  of the subsystem to the total failure rate of the subsystem (sum of safe failure  $\lambda_S$  and hazardous failure  $\lambda_D$  ).

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D}$$

**Dangerous Failure:**

[CEI61508-4-§3,6.7] Failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state.

## Functional Analysis

The transmitter consists of:  
an power supply stage  
an analog digital converter input stage  
an input stage  
and an output stage

## Definition of the feared event

For **CAL40** transmitter, the feared event ( the dangerous failure, as defined in the previous section) is to provide an erroneous output current.

Either an output current of more than 2% compared to input current

Either an blocked output current at value such it cannot take a safety fallback value:  
output current blocked within 3.6mA and 21mA

## Definition of the failsafe state

The failsafe state is defined by an output current out of range ( $\leq 3.6\text{mA}$  or  $\geq 21\text{mA}$ ).

The application "Safety logic equipment" should always be configured to detect any current  $< 3.6\text{mA}$  or  $> 21\text{mA}$  and considered them as "faulty".

Therefore, in the FMEA study, this state is considered safe.

## Study assumptions

The failure rate of the components are considered constant throughout the life of the system.

The evaluation of safety features of the module involves a number of assumptions:

Only the hardware aspect is covered.

Only catalectic failures are taken into account : Clear failures, sudden and unpredictable.

Are not considered, the defects that may be due to:

- design errors,
  - to defects in production batch,
  - the environment (electrical interference, temperature cycling, vibration)
  - human errors in operation or maintenance
- (precautions are taken to avoid them: such as range value checks, consistency of Hardware ...)

only simple failures are handled. Solder defects, which are usually due to a lack of quality

detectable after manufacturing by a specific burn-in, are not taken into account.

All specific aspects related to the power up phase are not covered.

## Failure rate

Below the rate of basic component failures of **CAL40** transmitter are available on document :

[AMDEC CAL40 rev2.XLS](#).

establish with " ALD MTBF calculator " according : MIL-HDBK-217F Notice 2 Electronic Reliability Prediction.

**Using FMEA data and Additional information about temperature sensors.**

The measure converter connected to a temperature sensor in a temperature probe becomes an assembly. Therefore, when using the results of the FMEA in a SIL assessment, the failure rate of the sensors (Pt100 or thermocouple) must be taken into account for the calculation of the safety instrumented function (SIF)

Below are the summary of failure modes and frequencies for PT100 and thermocouples depending on the type of connection and the environment in which they are used.

**Typical failure rates of thermocouples and PT100 with extension cable (remote sensor)**

sensor type and process conditions	failure rate (FIT)
thermocouple in low stress environment	1000
thermocouple in high stress environment	20000
2 or 3 wires Pt100 in low stress environment	475
2 or 3 wires Pt100 in high stress environment	9500

**Typical failure rates of thermocouples and PT100 without extension cable (sensor with included transmitter)**

sensor type and process conditions	failure rate (FIT)
thermocouple in low stress environment	100
thermocouple in high stress environment	2000
2 or 3 wires Pt100 in low stress environment	48
2 or 3 wires Pt100 in high stress environment	960

**Typical distribution of failure mode for thermocouples**

Failure mode	With extension cable	Direct connection without extension
open circuit	90%	95%
short circuit	5%	4%
drift *	5%	1%

\* the drift phenomenon of the thermocouples is essentially due to aging

**Typical distribution of failure mode for PT100**

Failure mode	With extension cable	Direct connection without extension
open circuit	78%	79%
short circuit	2%	3%
drift	20%	18%

The failure rate distribution depends slightly of the type of pt100 connection (2,3 wires)

stress conditions are: strong vibrations on the process and or frequent temperature cycles, these events that cause substrate cracks and broken welds on the connecting cables.

# Analog transmitter for sensor head mounting Pt100, potentiometer, current loop powered

CAL40



## Terms and definitions

The International Electrotechnical Commission's (IEC) standard IEC 61508 defines SIL. The SIL notions are repeated in standard derivative of IEC61508 like IEC61511 related to instrumented system (SIS) for process and the IEC 62061 related to the system with programmable electronic for machines. To achieve a safety application, first evaluate the risk (dangerousness, frequency of occurrence), to define the level of safety: the SIL level.

SIL defines the reliability level of SIS. There are two methods to calculate SIL, depending on whether the security system is operating in low demand or whether it operates continuously or at high load. There are 4 levels of SIL (SIL1 to SIL4). More than SIL level is high, more the availability of safety system is high.

For the safety system operating in low demand, we talk about probability of failure on demand  $PFD_{avg}$  in a 10 years period. Following the relationship between the SIL and the  $PFD_{avg}$

SIL 4 :  $PFD_{avg}$  between  $10^{-5}$  and  $10^{-4}$

SIL 3 :  $PFD_{avg}$  between  $10^{-4}$  and  $10^{-3}$

SIL 2 :  $PFD_{avg}$  between  $10^{-3}$  and  $10^{-2}$

SIL 1 :  $PFD_{avg}$  between  $10^{-2}$  and  $10^{-1}$

For the safety system operating in high load demand or in continuous operation, we talk about probability of dangerous failure per hour PFF. Following the relationship between the SIL and the PFF

SIL 4 : PFF between  $10^{-9}$  and  $10^{-8}$

SIL 3 : PFF between  $10^{-8}$  and  $10^{-7}$

SIL 2 : PFF between  $10^{-7}$  and  $10^{-6}$

SIL 1 : PFF between  $10^{-6}$  and  $10^{-5}$

## SIL levels scale :

SIL *	Mode of operations		Risk reduction factor
	Low demand PFD**	High demand PFH***	
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$	10 000 to 100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$	1 000 to 10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$	100 to 1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$	10 to 100

\* Safety integrity level

\*\* Probability of Failure on low Demand

\*\*\* Probability of a dangerous Failure per Hour

## Abbreviation

## Description

<b>HFT</b>	Hardware Fault Tolerance, capability of a functional unit to continue the execution of the demanded function when faults or anomalies exist.
<b>MTBF</b>	Mean interval between two failures
<b>MTTR</b>	Mean interval between the occurrence of the failure in a device or system and its repair
<b>PFD</b>	Likelihood of dangerous safety function failures occurring on demand
<b><math>PFD_{avg}</math></b>	Average likelihood of dangerous safety function failures occurring on demand
<b>SIL</b>	Safety Integrity Level, the international standard IEC 61508 defines four discrete safety integrity levels (SIL1 to SIL4). Each level corresponds to a specific probability range with respect to the failure of a safety function. The higher the integrity level of the safety-related system, the lower the likelihood of the demanded safety functions not occurring.
<b>SFF</b>	Safe Failure Fraction, the proportion of failures without the potential to put the safety-related system into a dangerous or impermissible functional state.
<b>TProof</b>	In accordance with IEC 61508-4, chapter 3.5.8, TProof is defined as the periodic testing to expose errors in a safety-related system.
<b>XooY</b>	Classification and description of the safety-related system with respect to redundancy and the selection procedure used. "Y" indicates how often the safety function is carried out (redundancy). "X" determines how many channels must work properly.
<b><math>\lambda_{sd}</math> und <math>\lambda_{su}</math></b>	$\lambda_{sd}$ Safe detected + $\lambda_{su}$ Safe undetected Safe failure (IEC 61508-4, chapter 3.6.8): A safe failure is present when the measuring system switches to the defined safe state or the fault signaling mode without the process demanding it.
<b><math>\lambda_{dd}</math> + <math>\lambda_{du}</math></b>	$\lambda_{dd}$ Dangerous detected + $\lambda_{du}$ Dangerous undetected Unsafe failure (IEC 61508-4, chapter 3.6.7): Generally a dangerous failure occurs if the measuring system switches into a dangerous or functionally inoperable condition.
<b><math>\lambda_{du}</math></b>	$\lambda_{du}$ Dangerous undetected A dangerous undetected failure occurs if the measuring system does not switch into a safe



## EMC Consideration

### 1) Introduction

To meet its policy concerning EMC, based on the Community directives **2014/30/EU** & **2014/35/EU**, the LOREME company takes into account the standards relative to this directives from the very start of the conception of each product.

The set of tests performed on the devices, designed to work in an industrial environment, are made in accordance with **IEC 61000-6-4** and **IEC 61000-6-2** standards in order to establish the EU declaration of conformity. The devices being in certain typical configurations during the tests, it is impossible to guarantee the results in every possible configurations. To ensure optimum operation of each device, it would be judicious to comply with several recommendations of use.

### 2) Recommendations of use

#### 2.1 ) General remarks

- Comply with the recommendations of assembly indicated in the technical sheet (direction of assembly, spacing between the devices, ...).
- Comply with the recommendations of use indicated in the technical sheet (temperature range, protection index).
- Avoid dust and excessive humidity, corrosive gas, considerable sources of heat.
- Avoid disturbed environments and disruptive phenomena or elements.
- If possible, group together the instrumentation devices in a zone separated from the power and relay circuits.
- Avoid the direct proximity with considerable power distance switches, contactors, relays, thyristor power groups, ...
- Do not get closer within fifty centimeters of a device with a transmitter (walkie-talkie) of a power of 5 W, because the latter can create a field with an intensity higher than 10 V/M for a distance fewer than 50 cm.

#### 2.2 ) Power supply

- Comply with the features indicated in the technical sheet (power supply voltage, frequency, allowance of the values, stability, variations ...).
- It is better that the power supply should come from a system with section switches equipped with fuses for the instrumentation element and that the power supply line be the most direct possible from the section switch.
- Avoid using this power supply for the control of relays, of contactors, of electrogates, ...
- If the switching of thyristor statical groups, of engines, of speed variator, ... causes strong interferences on the power supply circuit, it would be necessary to put an insulation transformer especially intended for instrumentation linking the screen to earth.
- It is also important that the installation should have a good earth system and it is better that the voltage in relation to the neutral should not exceed 1V, and the resistance be inferior to 6 ohms.
- If the installation is near high frequency generators or installations of arc welding, it is better to put suitable section filters.

#### 2.3 ) Inputs / Outputs

- In harsh conditions, it is advisable to use sheathed and twisted cables whose ground braid will be linked to the earth at a single point.
- It is advisable to separate the input / output lines from the power supply lines in order to avoid the coupling phenomena.
- It is also advisable to limit the lengths of data cables as much as possible.