# Commissioning, maintenance and safety manual


## CAL150-8

SIL2

SIL3

| Following of document | Date | Index |
|---|---|---|
| Initial version | 22/06/21 | 00 |
| | | |
| | | |
| | | |
| | | |

**LOREME 12, rue des Potiers d'Etain Actipole BORNY - B.P. 35014 - 57071 METZ**
**Phone 03.87.76.32.51 - Fax 03.87.76.32.52**
**Contact: Commercial@Loreme.fr - Technique@Loreme.fr**
**Download manual on: www.loreme.fr**

***writing : PD***
***verified : KR***
***Approved : PH***

# Summary




LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr

## 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 and the HFT of the module are specified in the FMEA analysis referenced AMDEC CAL150-8 rev0.xls

**Other relevant documents**: - Technical datasheet CAL150-8
- UE conformity declaration CAL150-8
- FMEA analysis AMDEC CAL150-8 rev0

The mentioned documents are available on 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 signal isolator CAL150-8 provides isolation and duplication of analog current 4 ....20mA.
an auxiliary power supply for a loop powered sensor is available.

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/CAL150-8_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 relative to electronic safety.

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

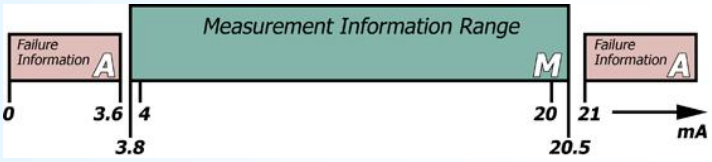
LOREME SAS
12, rue des potiers d'étain 57071 Actipole Metz Borny
www.loreme.fr

## 2 Safety function and safety state

### 2.1 Safety function

The safety function of the device is completed, as long as the outputs reproduce the input current (4 ... 20 mA) with a tolerance of +/- 1%.
The operation range of the output signal goes from 3.8 mA to 20.5 mA

### 2.2 Safety fallback position (according to NAMUR NE 43)




The safety fallback state is defined by an 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 < 20 ms.

## 3 Safety Recommendation

### 3.1 Interfaces

The device has the following interfaces.

• safety interfaces: input 1...8, output 1...8

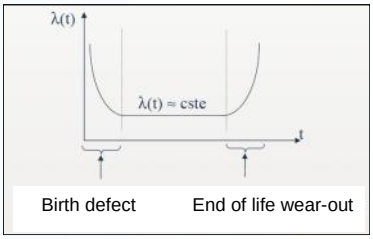
• not safety interfaces : no

### 3.2 Configuration / Calibration

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

### 3.3 Useful lifetime

Evolution of failure rate




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.


LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr

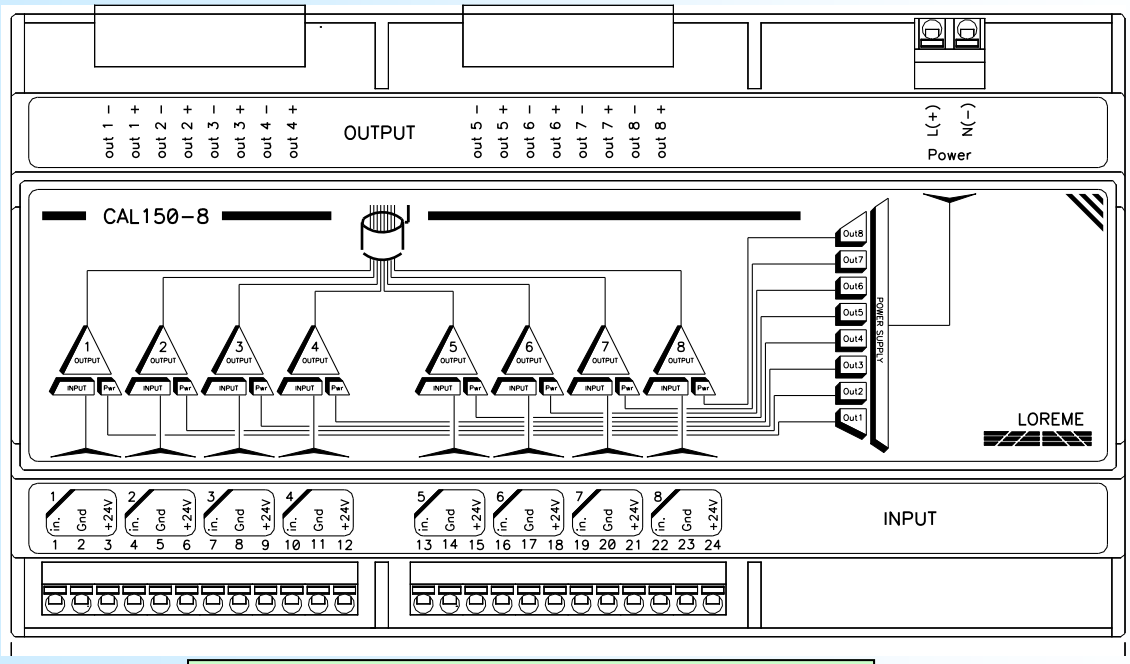
**4 Installation, commissioning and replacement**

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 a 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.




Under the hinging front face:
For each channel, a green LED pass through by the output current (indicates current flow). Light off when using "test" terminals.

The "test" terminals allow to connect a miliameter to check the current without opening loop.

### 4.2 Electrical connection

* **Device power supply :** between terminal Pwr (L)+ and Pwr (N) - ; the module is insensitive to power polarity
The polarity is given as a guide for the implementation of schemes (device working with AC or DC supply).

*** Output 1:** - mirror of input 1. Active output (device supplied the output current): Terminal Out1 + and Out1 -
*** Output 2:** - mirror of input 2. Active output (device supplied the output current): Terminal Out2 + and Out2 -
**....** **....** **....**
*** Output 8:** - mirror of input 8. Active output (device supplied the output current): Terminal Out8 + and Out8 -

**WARNING !**
*Do not wire loop with its own power supply on the active output otherwise the device can be damaged .*
*Do not exceed the technical specifications to ensure output safe operation, the output load resistance must be between 0 ohms and 600 ohms.*

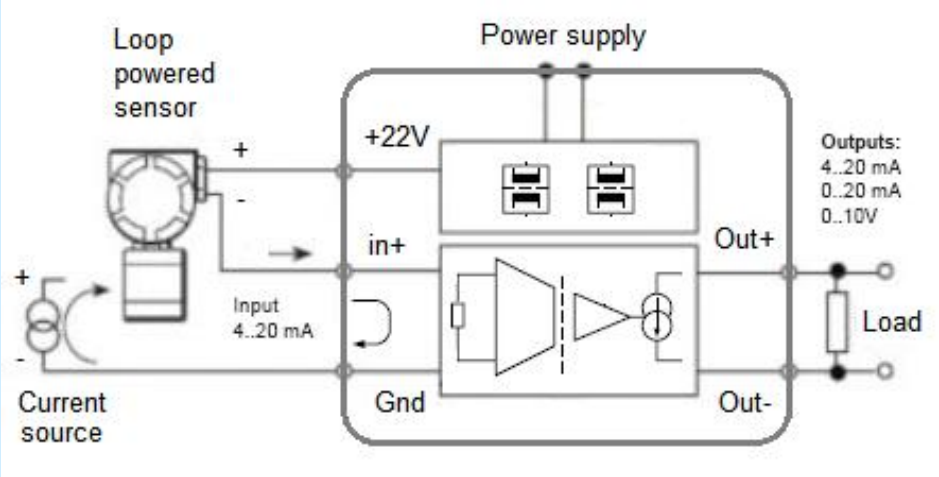
**Input wiring :**
In 4/20mA passive current input : between terminal in + and GND (for active transmitter)
In 4/20mA loop with transmitter supply : between terminal +24V and in + (for loop powered transmitter)

*** Input 1:** two operating mode are available ( active mode or passive mode)
*- Passive input mode (the input transmitter should supply current) : terminal 1 (+) and terminal 2 (-)*
*- Active input mode (The device supply the input transmitter) : terminal 3 (+) and terminal 1 (-)*

*** Input 2:** two operating mode are available ( active mode or passive mode)
*- Passive input mode (the input transmitter should supply current) : terminal 4 (+) and terminal 5 (-)*
*- Active input mode (The device supply the input transmitter) : terminal 6 (+) and terminal 1 (-)*
*Is it the same for other channel.*

**WARNING !**
*- Do not short the sensor power supply otherwise the device can be damaged*

### 4.3 Internal synoptic





LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr

## 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.

Isolator test and complete 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 current input transmitter.
3. Using a *current simulator** , set the input current of channel 1 to high alarm value (≥ 21.0 mA).
4. Raise the front cover of device. With the TEST terminals and a milliammeter, check if output current have this value within +/- 1%. (the green LED of each output is light off when the milliammeter is connected)
5. Set the input current to the low alarm value (≤ 3.6 mA)
6. Check if the output current reaches this value within +/-1%
7. Set the input current to a median value (= 12 mA)
8. Check if the output signal reaches this value at +/-1% (linearity and transfer function check)
9. Do the same test with the other channels.
10. Remove the *simulator**, close the front panel and connect the transmitter input .
11. Remove the bypass on the safety controller system or return to a normal operating condition
12. After testing, the results should be documented and archived.

Any device that does not satisfy the control needs to be replaced.
** The current generator and the milliammeter 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 ≥ $10^{-3}$ and <$10^{-2}$ for SIL2 safety functions and between ≥ $10^{-4}$ and <$10^{-3}$ for SIL3 safety functions .

| **λf** | λ dangerous = PFH | **SFF** (safe failure fraction) | **DC** (diagnostic coverage) |
|---|---|---|---|
| 263 FIT | 1.8 FIT | 99.4 % | 88.8 % |

temperature conditions 30°C

**PFD**avg **value depending proof interval**

| **T**[Proof] **= 1 year** | **T**[Proof] **= 5 years** | **T**[Proof] **= 10 years** | **T**[Proof] **= 20 years** |
|---|---|---|---|
| **PFD**avg=7.88E$^{-06}$ | **PFD**avg=3.94E$^{-05}$ | **PFD**avg=7.88E$^{-05}$ | **PFD**avg=1.57E$^{-04}$ |

approximation : PFDavg = λdangerous x 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 = 7.88 $E^{-6}$ x Tproof [year]

either for : Tproof = 10 years 8 % from SIF and for Tproof = 20 years 16 % from SIF in SIL3

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.

# *DECLARATION OF CONFORMITY*

**REV1**
**Page 1/1**

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

Designation: **8 channels signal isolator / splitter**

Type: **CAL150-8**

Revision : 0 date : 17/02/2014

***Can be used for functional safety application 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 failure give the following values:***

***Device with type A components, hardware fault tolerance HFT = 0***

| λf | λ dangerous = PFH | SFF (1) | DC | PFDavg T[Proof] = 1 year | PFH |
|---|---|---|---|---|---|
| 263 $FIT_{(2)}$ | 1.8 $FIT_{(2)}$ | 99.4 % | 88.8% | $7.9E^{-06}$ | $1.8E^{-09}$ 1/h |

***(1)*** ***according to AMDEC CAL150-8 rev0*** *created with "ALD MTBF calculator" : http://www.aldservice.com/ Standard : CEI 62380 2004-08*

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

Metz, the : 16/03/2021

Signed on behalf of LOREME; M. Dominique Curulla

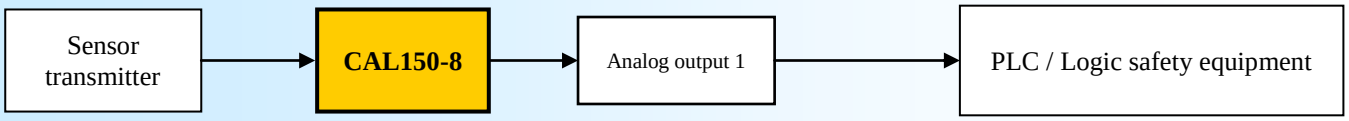

LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr

# FMEA summary

***Overview***
This document summarizes the results of the Failure Modes, and Effects Analysis (FMEA) of the isolator CAL150-8 from LOREME manufacturer.
In addition to the characterization of information required for the operational safety ( especially for the availability and storage of spares parts ), this study fulfils the requirement of IEC-61508 by indentify and quantify the dangerous failures of the component, thus allowing to interact on design for reduce this risks.

***Purpose of analysis***
This study was made in order to verify the suitability of the isolator CAL150-8 to be used in SIL2 or SIL3 safety applications.

***Scope of analysis***
The dedicate device embedded a set of electronic components for acquiring a 4-20mA current input signal from a transmitter and reproducing an analog output signal (4-20mA), image of input.
Generally, an isolator is taking place between a transmitter and a protective equipment, designated as "Logic Safety Equipment"




***Specification of device***
The isolator CAL150-8 is a subsystem of type "A" according to [CEI61508-2-§ 7.4.3.1.2] :
The failure modes of components required for the safety function are well defined.
The behaviour of the converter in fault conditions is fully defined.
The converter benefits from a experience feedback in many safety application.

***Safe failure***
[CEI61508-4-§3,6.8] Failure that does not have the potential to put the safety system in a dangerous or fail to function state. A safe failure it is not dangerous failure.

***SFF***
[CEI61508-2-§7.4.3.1.1-d] The Safe Failure Fraction is the proportion of non-hazardous failures. It describe the fraction in percent of safe failures λS and detected dangerous failures λDD related to the total failure rate (sum of safe failures λS and dangerous failures λD).

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

***Dangerous failure***
[CEI61508-4-§3,6.7] Also designated as unsafe failures. It is failures that have the potential to put the safety system in a dangerous or fail to function state.

***Functional analysis***

The isolator/splitter consist of :
an power stage
and for each channel:
an analog input stage
an isolation stage (signal transmission)
and an output stage (current amplifier)

***Dreaded event definition***

For the isolator **CAL150-8,** the dreaded event (i.e the dangerous failure as defined in the previous section) it's to supply an wrong output current :
Either an erroneous output current of more than 1% compared to the process demand,
either an output current, blocked to a value, such as it is not possible to have a security fallback state : output current blocked in the range >3.6mA or <21mA. Therefore in the impossibility to transmitting an alarm.

***Security fallback definition***

The security fallback state is defined with an output current out of the range 3.6mA - 21mA.
Either an output current =< 3.6 mA
Either an output current >= 21mA
The application program of the "Logic safety equipment" shall be configured to detect all current values out of range (=< 3.6mA and >= 21mA) and considered them as "invalidate".
Thereby, in the FMEA analysis, this state is considered as a not dangerous state.

***Study hypotheses***

The failure rate of component are considered as constant for the all system life time.
The evaluation of the safety features of a device involves a number of assumptions:

Only the catalectic failures are taken in account : straight, sudden, or unpredictable failures.
Are not considered the failures that could be due to:
- design errors
- batch defect in production
- environment (electrical interference, temperature cycles, vibrations)
- human errors in operation or maintenance

Precautions are taken to avoid them: management of a L.O.F.C (List of manufacturing operation and control)
Only simple fault are handled. Welding defect, which are usually due to a lack of quality detectable at the end of production by a specific burn-in, are not taken into account.
All aspects of power-on specific features are not treated.

***Failure rate***

The simple failure rate for the components of the converter CAL150-8 are classified on the document:
AMDEC CAL150-8 rev0.XLS ( internal document not communicated for reasons of design confidentiality)

Created with "ALD MTBF calculator" according to the reliability reports :

- MIL-HDBK-217F Notice 2 Electronic Reliability Prediction et iec-tr-62380.e Reliability data handbook


LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr

## Term and definitions.

SIL stands for "Security Integrity Level", which is the level of integrity of security. The concept of SIL has been introduced in the IEC61508 standard and is incorporated in standards derived from IEC61508, such as the IEC61511 standard for safety instrumented systems (SIS) for processes and IEC62061 for safety systems with programmable electronics for machines.
When you want to make a security application, you have to start by assessing the risk (its dangerousness, its frequency of occurrence), which leads to defining the security requirements that we expect from the SIS. to say its SIL.
Ultimately, the SIL defines the level of reliability of the SIS. There are two ways to define the SIL, depending on whether the security system operates in low demand mode or if on the contrary it operates continuously or with high demand. There are 4 levels of SIL (rated SIL1 to SIL4) higher the SIL level, higher the availability of the security system.
For **Safety system operating in low demand mode**,
The failure measure is based on average Probability of dangerous Failure on Demand ( $PFD_{avg}$ ) with a 10 years period.
The relationship between SIL level and PFDavg are following:
SIL 4 : PFDavg from $10^{-5}$ to $10^{-4}$
SIL 3 : PFDavg from $10^{-4}$ to $10^{-3}$
SIL 2 : PFDavg from $10^{-3}$ to $10^{-2}$
SIL 1 : PFDavg from $10^{-2}$ to $10^{-1}$
For **Safety system operating in high demand mode,**
The failure measure is based on average Frequency of Dangerous failure per hour. relationship between level and PFH are following:
SIL 4 : PFH from $10^{-9}$ to $10^{-8}$
SIL 3 : PFH from $10^{-8}$ to $10^{-7}$
SIL 2 : PFH from $10^{-7}$ to $10^{-6}$
SIL 1 : PFH from $10^{-6}$ to $10^{-5}$

**SIL levels scale :**

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

**** Safety integrity level***
***** Probability of Failure on low Demand***
****** Probability of a dangerous Failure per Hour***

| Abbreviation | Description |
|---|---|
| **HFT** | Hardware Fault Tolerance, capability of a functional unit to continue the execution of the demanded function when faults or anomalies exist. |
| **MTBF** | Mean interval between two failures |
| **MTTR** | Mean interval between the occurrence of the failure in a device or system and its repair |
| **PFD** | Probability of a dangerous failure of a system on demand |
| **PFDavg** | Average of probability of dangerous failure of a system on demand |
| **SIL** | 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. |
| **SFF** | Safe Failure Fraction, the proportion of failures without the potential to put the safety-related system into a dangerous or impermissible functional state. |
| **TProof** | 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. |
| **XooY** | 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. |
| **λsd and λsu** | λsd Safe detected + λsu 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 with out the process demanding it. |
| **λdd and λdu** | λdd Dangerous detected + λdu 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. |
| **λdu** | λdu Dangerous undetected. A dangerous undetected failure occurs if the measuring system doesn't switch into a define safe state, or into an alarm signaling mode on process demand. |

# 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.


LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr