Commissioning, maintenance and safety manual

RPL34HiG

Change content	Date	Index
Initial release	18/06/21	0

LOREME 12, rue des Potiers d'Etain Actipole BORNY - 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

Writing : DP
Checking : 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 modes and the HFT of the module are specified in the FMEA analysis referenced:
AMDEC RPL34HiG rev0.XLS

Other documents:
- Technical datasheet RPL34HiG
- EMC conformity declaration RPL34HiG rev0
- FMEA analysis RPL34HiG rev0
- configuration handbook RPL34HiG rev0.x

The mentioned documents are available on www.loreme.fr

The assembly, installation, commissioning and maintenance can only be performed by trained personnel qualified who 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 protection relay RPL34HiG is used for monitoring voltage or current needing a high level of isolation. It provide the monitoring (detection of overvoltage, undervoltage, overcurrent, undercurrent, loss or defect of current shunt).
The information transmit is made by free potential contacts.

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/RPL34HiG_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
FRANCE
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 threshold detection stay in +/- 2% tolerance of initial setting and the breaking of external current shunt detection function is not altered.

2.2 Safety fallback position

The failsafe state is defined by the opening of N.O contacts.
The application should always be configured to detect the opening of contact output and considered "faulty ".
Thus, in the FMEA study, this condition is considered as **"not dangerous"**.
The reaction time for all the safety functions is <300 ms.

3 Safety Recommendation

3.1 Interfaces

The device has the following interfaces :

• safety interfaces : analog input, relay output

• not safety interfaces or auxiliary: pushbutton interface, display, serial link RS232 (device configuration)

3.2 Configuration / Calibration

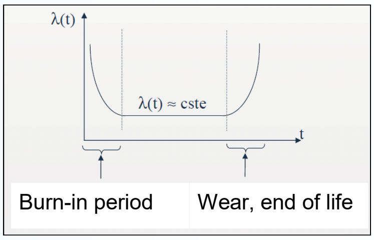
Any re-calibration needed. Only the threshold value should be setting.
Refer to the configuration handbook.
the calibration is only possible by factory return, no changes should be made to the device.

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 of components themselves
and operating conditions particularly the temperature,
(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.

failure rate evolution



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.

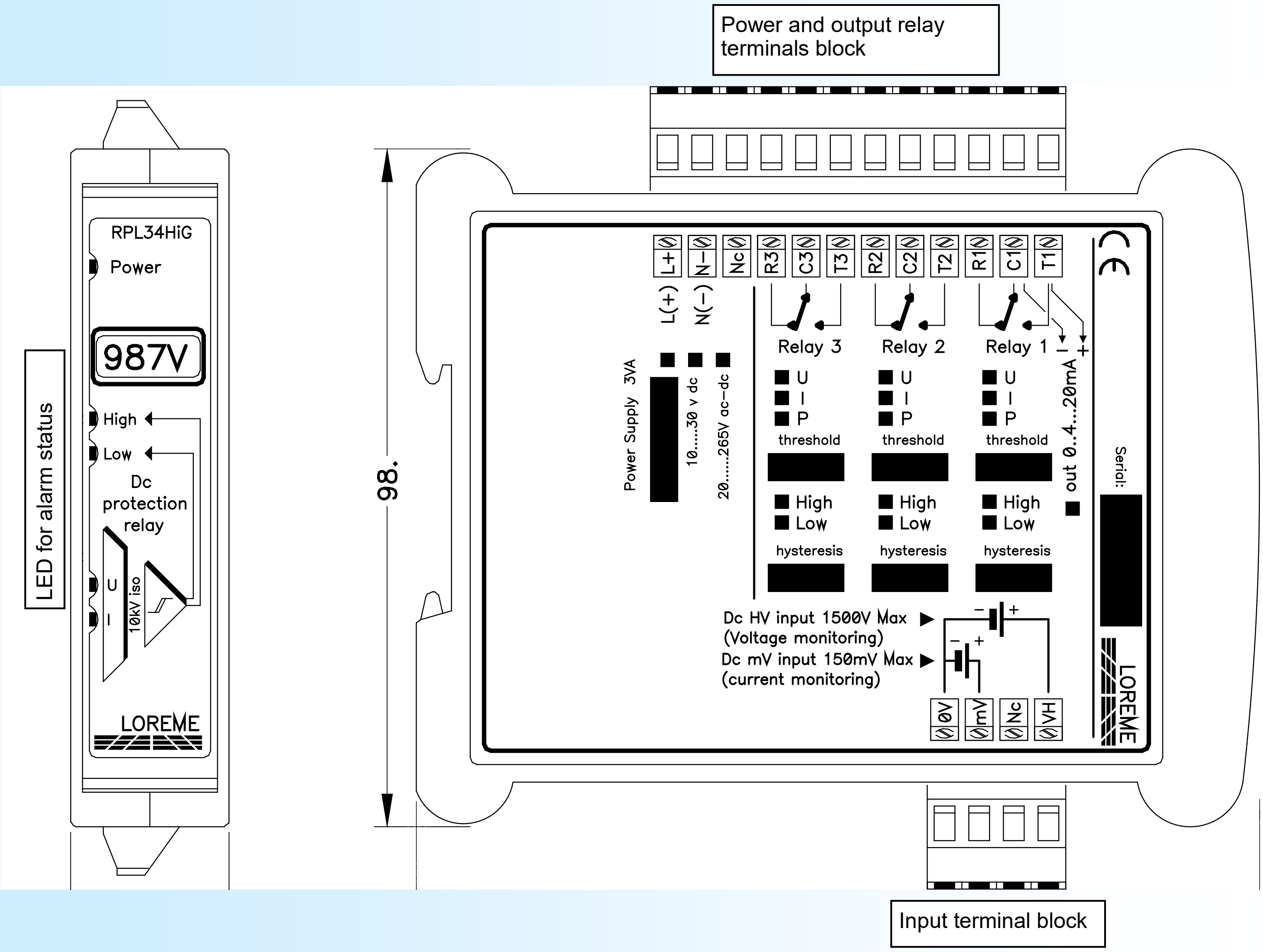
LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr

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 Device description



4.2 Electrical connection and configuration

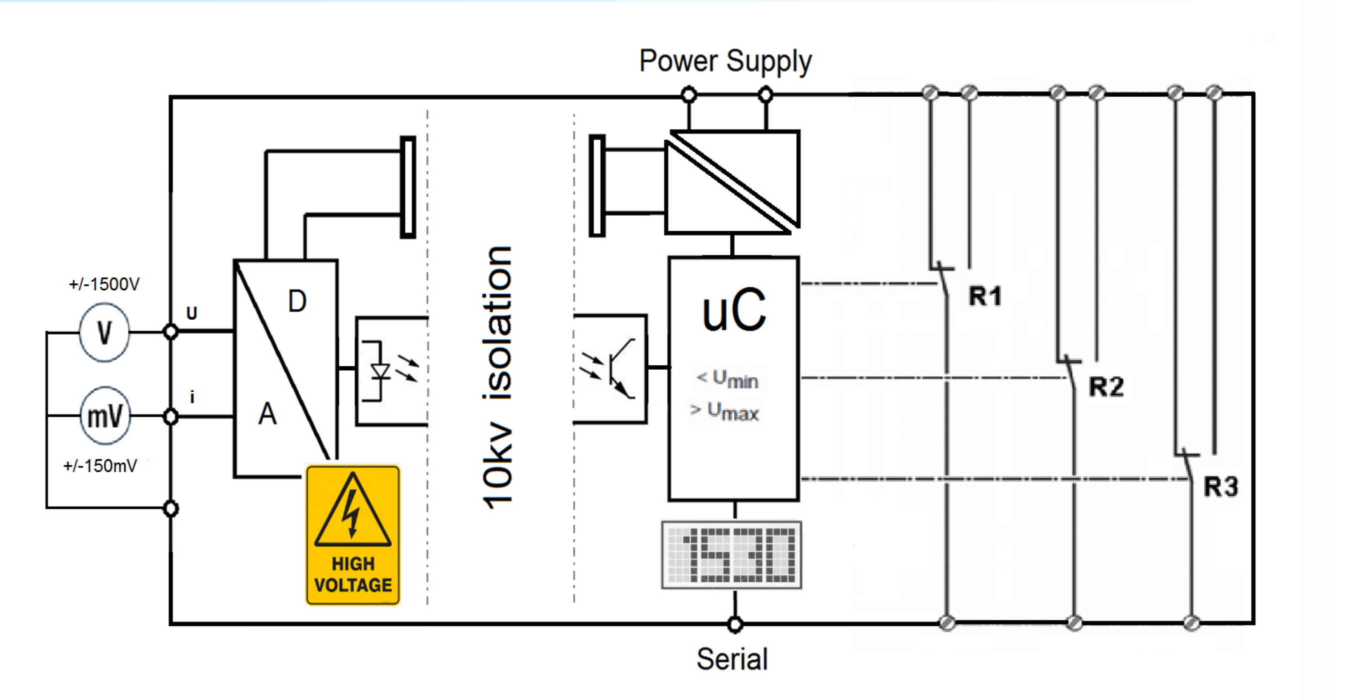
This information are complementary to the handbook manual

- The device is not sensitive to the power supply polarity. The power supply may be DC or AC
- Be sure of setting of rating value (mV / A) for external current shunt in configuration.
- Ensure the right choice of alarm parameters in configuration.
- The relay contacts must be use in order to put the system in safety mode when device lost its power supply.

WARNING!

Do not exceed the specifications of the data sheet, to ensure safe operation it is necessary to respect the voltage range of power supply

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.
Environmental conditions and a minimum heating time of 5 minutes must be respected.

Transmitter 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. Inspect the device, no visible damage or contamination (oxidation)
3. disconnect the relay output and connect an *ohmmeter**, leaving the voltage and current input connected. The relay is closed, the green and red LED off, "out of alarm conditions"
4. Disconnect the current shunt. The relay is opened, the current alarm green LED is on and the low alarm red LED is on. "Current shunt breaking condition"
5. Disconnect the input voltage
6. Connect a simulator* at the voltage input of the protection relay.
7. Simulated the voltage to the threshold wishes.
  a) if device has never been adjusted, setting the threshold with pushbutton (check the correct selection and setting of threshold detection and the rating value for current shunt (mV / A))
  b) once the device setting, check the tripping point by varying the simulated temperature around this setpoint (the hysteresis is adjustable)
  c) during a periodic test, for a device already configured, a gap in the tripping point more than 2% should alert on a possible internal fault. It is then strongly recommended to replace the device.
8. doing the same test with current input (*simulator* connect to current input and simulated voltage (mV))
9. Disconnect the *simulator** and connect the input signal. check out the relay is in "out of alarm conditions".
10. Connect the output and ensure there is no faults on the safety system.
11. After the tests, the results must be documented and archived.

Any devices not satisfying the control need to be replaced
*note *: the temperature simulator and the ohmmeter must be regularly calibrated for this test (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.

λ safe	λ dangerous detected	λ dangerous undetected = PFH	**SFF** (Safe Failure Fraction)	**DC** (Diagnostic Coverage)
85 FIT	727 FIT	67 FIT	92.4 %	91.6 %

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=2.93E^{-04}	**PFD**avg=1.46E^{-03}	**PFD**avg=2.93E^{-03}	**PFD**avg=5.86E^{-03}

approximation : PFDavg = λdangerous undetected 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 SIL2
(using 10% of resources of the safety instrumented function, Tproof may be increased by using a larger fraction of SIF

summary :
Probability of default: PFD = 2.93 E^{-4} x Tproof [years]
either for Tproof = 5 years, 15 % of safety instrumented function in SIL2 category

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

SIL2 Safety Integrity Level IEC 61508 / IEC 61511

REV1
Page 1/1

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

Designation: **Protection relay for DC current and voltage with high isolation**

Type: **RPL34HiG**

Revision : 0 date : 15/02/2019

Can be used for functional safety applications up to SIL2 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 B components , Hardware fault tolerance HFT = 0
values for the converter only (worst case)

λ safe	**λ** dangerous detected	λ dangerous undetected = PFH	**SFF (1)**	**DC**	**PFD**avg **T**[Proof] **= 1 an**	**PFH**
85 $FIT_{(2)}$	727 $FIT_{(2)}$	67 $FIT_{(2)}$	92.4 %	91.6%	$2.93E^{-05}$	$6.7E^{-08}$ 1/h

(1) according to FMEA RPL34HiG rev0 *established with "ALD MTBF calculator" : http://www.aldservice.com/*
(2) FIT = Failure rate (1/h)

Metz : 15/02/2019

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 Details

Context

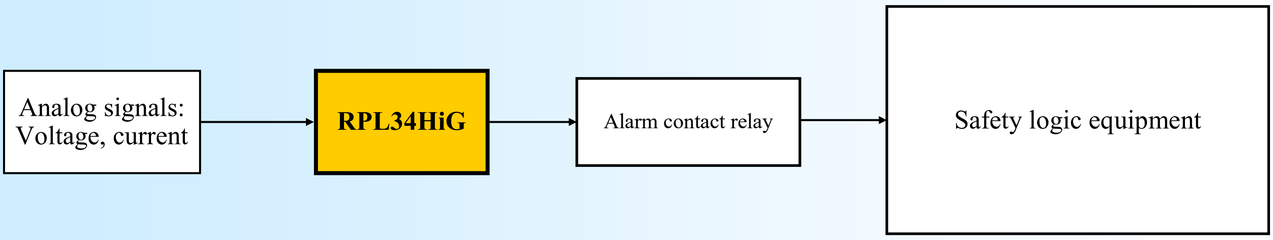
This document details the Failure Mode and Effects Analysis (FMEA) of RPL34Hig component of society LOREME. Besides the characterization of the information necessary for safe operation (especially for availability calculations and constitution of stock of spare parts), this study can meet the requirements 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 protection relay RPL34HiG to be used in SIL2 applications.

Scope of analysis

The component concerned includes an electronics component assembly dedicated to the acquisition of input signals like voltage and current from external current shunt and activate an alarm relay when a threshold is exceed.
Typically, a threshold detector is interfaced between a sensor and protection equipment, referred to as "logical security equipment"



Characterization of the component

The protection relay RPL34HiG is a type « B » 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 detector 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 λS plus the dangerous detected failure rate λDD of the subsystem to the total failure rate of the subsystem (sum of safe failure λS and hazardous failure λD).

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

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 threshold detector consists of:
an power supply stage
an analog digital converter input stage
a microcontroller (linearization, temperature compensation, signal scaling and alarms functions)
and alarms relays

Definition of the feared event

For the protection relay RPL34Hig, the feared event (the dangerous failure, as defined in the previous section) is the impossibility to transmit an alarm.

Definition of the failsafe state

The failsafe state is defined by the opening of N.O contacts.
The application should always be configured to detect the opening of contact output and considered "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. The aspect of dependability of the software is not discussed.
(the safety of software is taken to account during the development, checking, and validation phases of conception in quality procedure)
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 RPL34Hig are available in document : **AMDEC RPL34HiG rev0.XLS**

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

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

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 calculated SIL, depending on whether the security system is operating in low demand or whether it operates continuously or at high load. There are 4 level 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 : PFDavg between 10^{-5} and 10^{-4}
SIL 3 : PFDavg between 10^{-4} and 10^{-3}
SIL 2 : PFDavg between 10^{-3} and 10^{-2}
SIL 1 : PFDavg 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	PFD Low demand mode	PFH High demand or continuous mode	Risk reduction
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$	10 000 - 100 000
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$	1 000 - 10 000
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$	100 - 1 000
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$	10 - 100

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	Likelihood of dangerous safety function failures occurring on demand
PFDavg	Average likelihood of dangerous safety function failures occurring 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 und 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 without the process demanding it.
λdd +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 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.

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