Commissioning and safety manual

INP101
INP101V

SIL2

LOREME 12, rue des Potiers d'Etain Actipole BORNY - B.P. 35014 - 57071 METZ CEDEX 3
Phone 03.87.76.32.51
Contact us: Commercial@Loreme.fr - Technique@Loreme.fr
Download manual on : www.loreme.fr

REV 2-18/10/19

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 CNL40ig rev2.XLS (the CNL40ig is the embedded transmitter in INP101)

Other documents:
- Technical datasheet INP101
- EMC conformity declaration INP101 (available in the EMC section of this manual)
- FMEA analysis CNL40igH (converter embedded in INP101)
- configuration handbook INP101

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 INP101 transmitter provides temperature measurement from PT100 or thermocouple and retransmission as an analog signal 4 ... 20 mA with or without Hart protocol, and signal isolation.

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/INP101_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

Programmable isolated transmitter for PT100 and thermocouple sensors head mounting with display

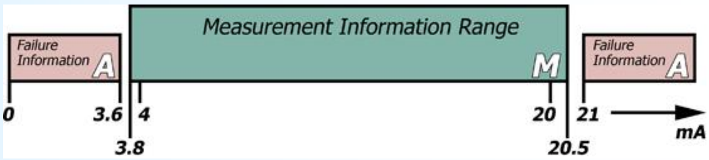
2 Safety function and safety state

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 + / -2%. The operation range of the output signal goes from 3.8 mA to 20.5 mA

2.2 Safety fallback position (according NAMUR NE 43)

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 the safety functions is <200 ms.

WARNING! the burn out value is freely programmable, on CNL40ig, it is up to the installer to verify compatibility with process safety (factory burn out value is programmed at : 21 mA)

3 Safety Recommendation

3.1 Interfaces

The device has the following interfaces :

- safety interfaces : temperature input, analog output

- not safety interfaces : HART communication (diagnostic and configuration), serial link RS232 (device configuration)

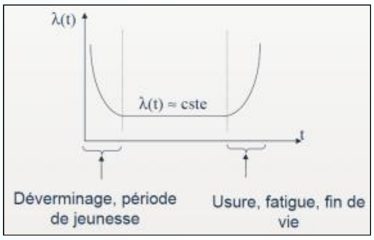
HART communication is not relevant for functional safety, loss of communication is considered as detected by the application, therefore, in the FMEA study, this condition is considered as non-hazardous.

3.2 Configuration / Calibration

the device configuration is required to define the operating mode (sensor type, measurement range, burn out value) 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 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

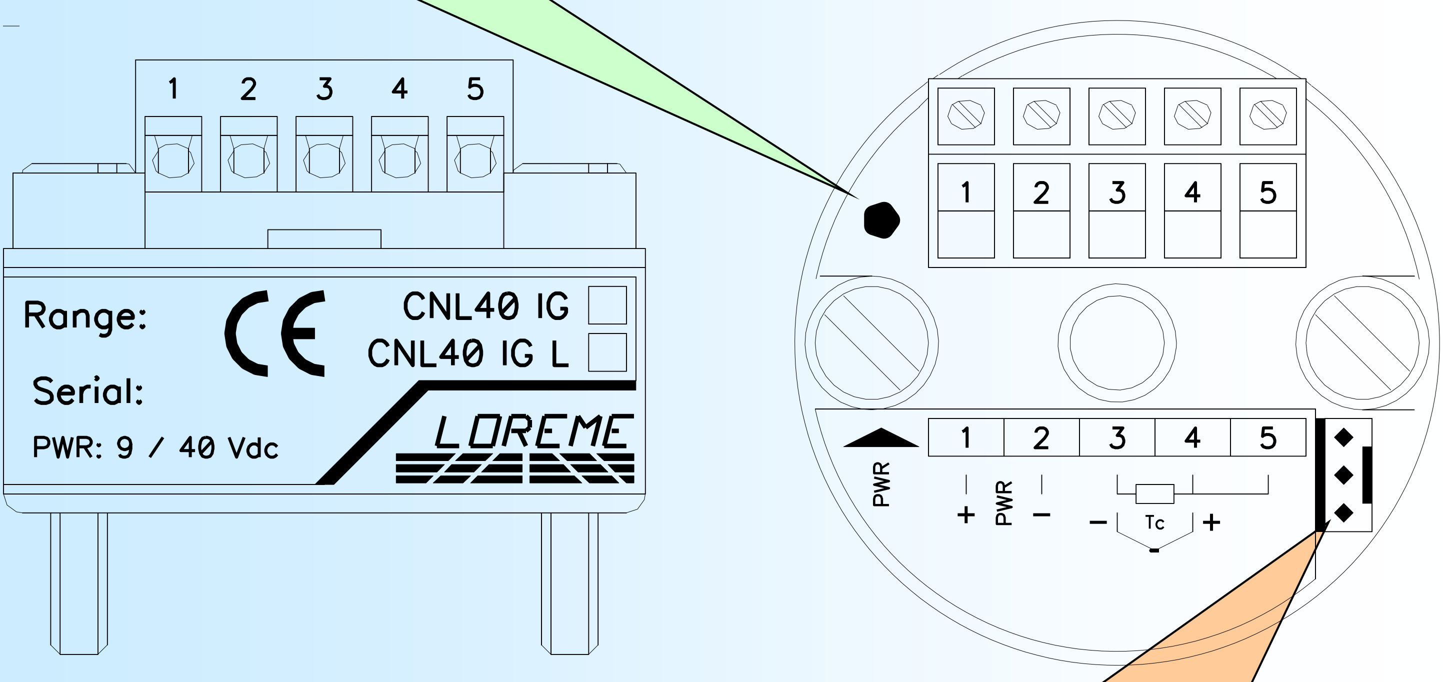
4 Installation, commissioning and replacement

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 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

Yellow LED is traversed by the output current, indicates that the output loop is closed and powered.
(current flow)
turns off when opening the output loop
allows a quick visual check of smooth operation.



3-pin header (RS232) to enter in configuration
(use only the supplied cable by LOREME for this purpose)
Attention: configuration mode freezes the output current
(no measurement during setup)
For security reasons the converter leaves automatically setup mode after 2 minutes of inactivity and returns to measurement mode.

4.2 Electrical connection and configuration

*** power supply and analog output :** terminal 1+ and terminal 2 -
The device is protected against reverse polarity of power supply

*** Input** : two configurations are possible, PT100 and thermocouple
- Connection for Thermocouple input : Tc+ terminal 4 ; Tc- terminal 3
- Connection for 3 wires RTD (PT100) input : white wire terminal: 3 ; two red wire on terminal 4 and 5

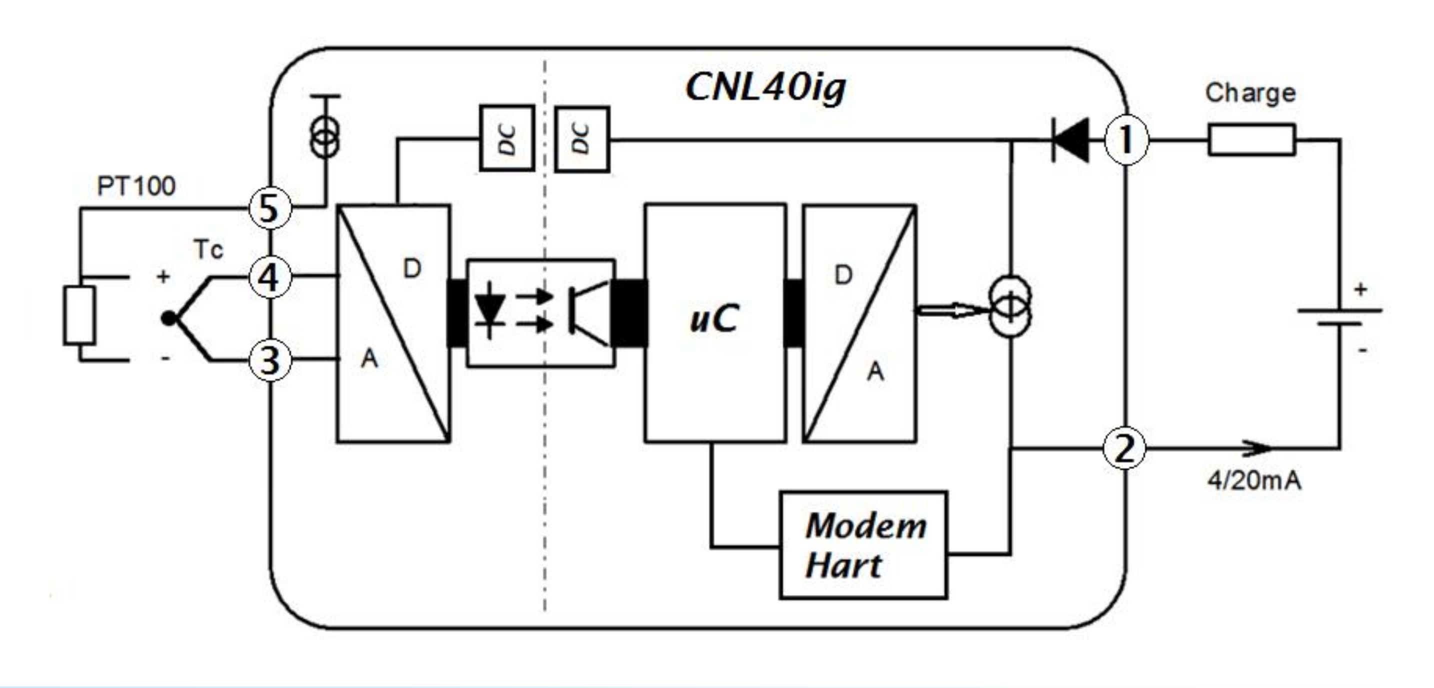
Notes:
- For remote thermocouple, make sure that the extension is made with compensation cable of the same type as the thermocouple, with respect to the cable polarity.
- For a remote Pt100 sensor, make sure the extension cable used has 3 conductors with same cross section to ensure the best line compensation.
- Ensure the proper choice of sensor type in the configuration.
- the temperature range programmed into the controller and the converter must be identical.
- the burn out value (Sensor break detection) of the analog output must be programmed <3.6mA at or> = to 21mA (21mA factory)

WARNING!

Do not exceed the specifications of the data sheet,
to ensure safe operation of the analog output it is necessary to have:
- an auxiliary voltage supply range between 15 volts and 40 volts
- maximum load in the loop, calculated so that the residual voltage across the converter is 15V for a loop current of 21 mA.

Be careful, exceeding 4 ... 20mA loop load ,can prevent the output current to reach the burn out value it may saturate in the measurement range , and place the system in a dangerous state.

4.3 Typical connection



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.

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. Insert a milliammeter* in the output loop
4. disconnect the sensor (Pt100 or thermocouple)
5. verify that the output current goes into burn out value (<= 3.6mA or> = 21mA)
6. Connect a simulator* at the input of the converter (Pt100 or thermocouple) in place of the sensor
7. Simulate the appropriate temperature values across the converter (on 5 points : 0%, 25%, 50%, 75%, 100%) and check that the output current (4..8..12..16..20mA) is proportional to the input to + / -2% near
8. Disconnect the simulator and reconnect the sensor to the converter input (check that the output current is in the measurement range)
9. Remove milliammeter and close the output loop (green LED must light)
10. After testing, the results should be documented and archived.

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

*note *: milliammeter, and the simulator must be calibrated on a regular basis for this test (depending on the state of the art and best 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 detected	λ dangerous detected	λ safe undetected	λ dangerous undetected = PFH	SFF
420 FIT	0 FIT	17 FIT	21 FIT	95.4%

temperature conditions : 30°C

PFDavg **value depending proof interval**

T[Proof] **= 1 an**	**T**[Proof] **= 5 ans**	**T**[Proof] **= 10 ans**	**T**[Proof] **= 20 ans**
PFDavg=9.20E^{-05}	**PFD**avg=4.60E^{-04}	**PFD**avg=9.20E^{-04}	**PFD**avg=1.8E^{-03}

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 SIL2

summary :

Probability of default: PFD = 9.20 E^{-5} x Tproof [years]

either for Tproof = 5 years, 50 % 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.

EC DECLARATION OF CONFORMITY

REV8
Page 1/1

With requirements of directive 2004/108/CE "Electromagnetic Compatibility"
And requirements of directive 2006/95/CE "LOW VOLTAGE"

We declare under our sole responsibility, that the following product:

Designation: **Loop powered smart temperature transmitter**

Type: **INP101** with CNL40igH embedded

Revision : 2 date : 16/12/2008

Complies with the following harmonized generic or specific standards:

GENERIC STANDARDS:	tested	STANDARDS:	
Low Voltage Directive 2006/95/EC.			
	X	EN 61010-1	Safety requirements for electrical equipment for measurement, control, and laboratory use
NF EN 61000-6-4 March 2007 **Electromagnetic compatibility (EMC)** **Part 6-4 : generic standards - Emission standard for industrial environments**			
	X	EN 55011 Class A	Radiated emission and induced emission on alternative current power supply
NF EN 61000-6-2 January 2006 **Electromagnetic compatibility (EMC)** **Part 6-2 : generic standards** **Immunity for industrial environments**			
	X	EN 61000-4-2	Electrostatic discharges.
	X	EN 61000-4-4	Burst.
	X	EN 61000-4-5	Surge 1,2/50 (5/20) µs.
	X	EN 61000-4-8	Power frequency magnetic field.
	na	EN 61000-4-11	Voltage dips and short voltage interruptions.
	X	EN 61000-4-3	RF AM electromagnetic field.
	X	EN 61000-4-6	Common mode RF AM.

Metz : 16/12/2008

Signed on behalf of LOREME ; M. Dominique Curulla

Year of affixing the CE marking : 2008

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

Appendix 1: EMC consideration

1) Introduction:

In order to satisfy its policy of Electromagnetic compatibility, based on the EU Directive 89/336/EC,
LOREME company takes into account the standards relative to this directive early in the design of each product.
All tests performed on devices designed to work in industrial environment, are compliant to EN 50081-2 and EN 50082-2 in order to establish the EMC compliance certificate. The devices being in some typical configurations during the test, it is impossible to guarantee results in all possible configurations.

To ensure optimum operation of each device ,it would be judicious to comply with several recommendations of use.

2) Recommendations:

2.1) General information:

- Comply with the mounting recommendations (mounting direction, devices spacing ...) specified in the datasheet.
- Follow the recommendations of use (temperature range, protection) specified in the datasheet.
- Avoid dust and excessive moisture, corrosive gases, sources of heat.
- Avoid disturbed environments and disruptive phenomena.
- If possible, group together the instrumentation devices in a zone separated from the power and relay circuits.
- Avoid close proximity with remote switches for high power, contactors, relays, SCR ,...
- Do not approach within two feet of a device with a walkie-talkie (5 W output power), because it creates a electromagnetic field with an intensity greater than 10 V / M for a distance of less than 50 cm.

2.2) Power supply:

- Observe the characteristics specified in the datasheet (Voltage and frequency tolerance).
- It is preferable that the power comes from a system with section switches equipped with fuses for instrumentation components, and the supply line is the most direct route possible from the section switch. Avoid using this power supply to control relays, contactors, solenoid valves, …
- If the power circuit is heavily disturbed by SCR switching , motor, inverter, ... it may be necessary to install an isolation transformer specifically for instrumentation and connecting the screen to ground.
- It is also important that the installation has a good grounding, and preferable that the voltage compared to neutral does not exceed 1V, and the ground resistance less than 6 ohms.
- If the installation is located near high frequency generators or arc welding, it is preferable to mount adequate power line filter.

2.3) Inputs / Outputs:

- In harsh conditions, it is advisable to use sheathed twisted cables whose ground braid will be grounded at on 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 minimize the lengths of data cables.

DECLARATION OF CONFORMITY

Safety Integrity Level SIL 2 IEC 61508 / IEC 61511

REV1
Page 1/1

We declare under our sole responsibility, that the following product:

Designation: **Loop powered smart temperature transmitter**

Type: **INP101** with CNL40igH embedded

Revision : 2 date : 16/12/2008

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 detected	**λ** dangerous detected	λ safe undetected	λ dangerous undetected = PFH	**SFF (1)**	**PFD**avg **T**[Proof] **= 1 an**	**PFH**
420 FIT$_{(2)}$	0 FIT$_{(2)}$	17 FIT$_{(2)}$	21 FIT$_{(2)}$	95.4%	$9.20E^{-05}$	$2.1E^{-08}$ 1/h

(1) according to FMEA CNL40igH 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 : 11/07/14

Signed on behalf of LOREME ; M. Dominique Curulla

INP101 transmitter with CNL40igH rev2 converter

FMEA Details

Context

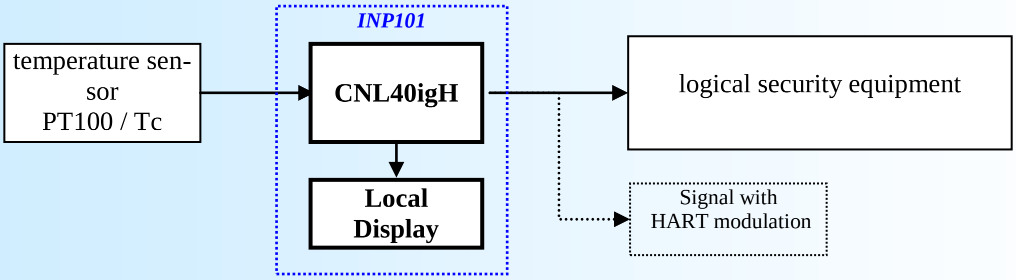
This document details the Failure Mode and Effects Analysis (FMEA) of CNL40igH component of society LOREME. Besides the characterization of the information necessary for safe operation (especially for availability calculations and constitution of stock of spare parts), this study can meet the requirements 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 CNL40igH converter to be used in SIL2 applications.

Scope of analysis

The component concerned includes an electronics component assembly dedicated to the acquisition of input signals from temperature sensors in order to reconstitute an analog output signal (4 .. 20 mA) with or without HART communication. Typically, a converter is interfaced between a sensor and protection equipment, referred to as "logical security equipment"



Characterization of the component
The CNL40igH converter 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 converter 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 (total safe failure rate of a subsystem plus the dangerous detected failure rate of the subsystem) to the total failure rate of the subsystem.

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

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 input stage , analog digital converter
an isolation stage (ADC power and signal transmission)
a microcontroller (linearization, signal scaling and Hart communication)
an output stage (current amplifier)
and a modulator / demodulator for Hart signal

Definition of the feared event

For CNL40igH converter, the feared event (the dangerous failure, as defined in the previous section) is the emission of erroneous output current :
Either erroneous output current of more than 2% compared to the process demand.
Either an output current, blocked at a value such that it can not take a failsafe value :
output current locked in a range> 3.6 mA or <21mA.

Definition of the failsafe state

The failsafe state is defined by an output current out of the range of 3.6 mA….. 21mA.
Either an output current = <3.6 mA
Either an output current >= 21 mA
The burn out value of CNL40igH converter will necessarily be programmed for one of these values.
The application of the "logical Safety Equipment" program must absolutely be set to detect any current value out of range (=< 3,6 mA et >= 21 mA) and considered as "Invalids".
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.
Only catalectic failures are taken into account : Frank 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 CNL40IGH converter
for a temperature around of the components of 30 ° C: (2 following pages)

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

Programmable isolated transmitter for PT100 and thermocouple sensors head mounting with display

LOREME

AMDEC CNL40ig rev2

Etabli avec "ALD MTBF calculator" : http://www.aldservice.com/

Count	RefDes	Pattern-Name	Value	selon IEC6-2380 λf (fit)	type	répartition ratio	λf (fit)	λf = 1/MTBF: λfd: λsd	λfd: λdd	λfnd: λsnd	λfnd: λdnd	effet
1	XC174	1206	0	0,02	co	100%	0,020	0,020				repli sortie > 21 mA
1	73	1206	1M 1% 50ppm	0,21	co	40%	0,084			0,084		drift sortie < 2%
					drift	60%	0,126			0,126		drift sortie < 2%
4	76	1206	1u X7R	0,21	co	30%	0,063			0,063		sans influence découplage vref
					cc	70%	0,147	0,147				repli sortie > 21 mA (vref=0)
	163	1206	1u X7R	0,21	co	30%	0,063			0,063		sans influence découplage modem hart
					cc	70%	0,147	0,147				plus de communication Hart
	XC169	1206	1u X7R	0,21	co	30%	0,063			0,063		plus de passe bas ligne
					cc	70%	0,147	0,147				plus de mesure de ligne (err < 2%)
	XC171	1206	1u X7R	0,21	co	30%	0,063			0,063		plus de passe bas entrée
					cc	70%	0,147				0,147	en tc non detecté / en pt rupture capteur
1	XC172	1206	2k5 1% 50ppm	0,02	co	40%	0,008				0,008	en tc non detecté / en pt rupture capteur
					drift	60%	0,012				0,012	dérive mesure (référence)
3	96	1206	2n2 NPO	0,07	co	10%	0,007			0,007		perte filtre reception Hart
					cc	70%	0,049	0,049				plus de communication Hart
					drift	20%	0,014			0,014		altération filtre Hart
	97	1206	2n2 NPO	0,07	co	10%	0,007	0,007				plus de communication Hart
					cc	70%	0,049	0,049				plus de communication Hart
					drift	20%	0,014			0,014		altération filtre Hart
	100	1206	2n2 NPO	0,07	co	10%	0,007			0,007		pas de filtre HF boucle 4..20 mA
					cc	70%	0,049	0,049				courant sortie > 21 mA (court circuit)
					drift	20%	0,014			0,014		sans influence
2	XC170	1206	5k 1% 50ppm	0,02	co	40%	0,008	0,008				repli sortie > 21 mA rupture capteur
					drift	60%	0,012			0,012		sans influence
	XC177	1206	5k 1% 50ppm	0,02	co	40%	0,008				0,008	mesure flottante
					drift	60%	0,012			0,012		sans influence
2	84	1206	7k5 1% 50ppm	0,02	co	40%	0,008	0,008				repli sortie < 3.6 mA
					drift	60%	0,012				0,012	dérive sortie
	XC166	1206	7k5 1% 50ppm	0,02	co	40%	0,008	0,008				rupture en PT / sans influence en tc
					drift	60%	0,012				0,012	dérive en pt / sans influence en tc
3	74	1206	10k 1% 50ppm	0,02	co	40%	0,008	0,008				repli sortie < 3.6 mA
					drift	60%	0,012				0,012	dérive sortie
	79	1206	10k 1% 50ppm	0,02	co	40%	0,008	0,008				plus de configuration RS232
					drift	60%	0,012			0,012		sans influence
	95	1206	10k 1% 50ppm	0,02	co	40%	0,008	0,008				plus de communication Hart
					drift	60%	0,012			0,012		sans influence
1	81	1206	10M 1% 100ppm	0,02	co	40%	0,008				0,008	plus de détection rupture tc
					drift	60%	0,012			0,012		sans influence
1	99	1206	23.7 1% 50ppm	0,02	co	40%	0,008	0,008				repli sortie < 3.6 mA
					drift	60%	0,012			0,012		dérive < 2%
1	83	1206	47u X7R	0,21	co	30%	0,063			0,063		plus de découplage uC
					cc	70%	0,147	0,147				repli sortie < 3.6 mA
2	67	1206	50k 1% 50ppm	0,02	co	40%	0,008	0,008				rupture capteur (ref à 0)
					drift	60%	0,012				0,012	dérive mesure (référence)
	78	1206	50k 1% 50ppm	0,02	co	40%	0,008	0,008				risque altération com RS232
					drift	60%	0,012			0,012		sans influence
4	77	1206	100n X7R	0,21	co	30%	0,063				0,063	ondulation courant de sortie
					cc	70%	0,147	0,147				repli sortie < 3.6 mA
	103	1206	100n X7R	0,21	co	30%	0,063			0,063		plus de decouplage AD
					cc	70%	0,147	0,147				rupture capteur AD plus alimenté
	105	1206	100n X7R	0,21	co	30%	0,063			0,063		plus de découplage XTR116
					cc	70%	0,147	0,147				courant sortie > 21 mA (court circuit)

AMDEC CNL40ig rev2

				selon IEC6-2380		répartition		λf = 1/MTBF				
								λfd		λfnd		
Count	RefDes	Pattern-Name	Value	λf (fit)	type	ratio	λf (fit)	λsd	λdd	λsnd	λdnd	effet
	107	1206	100n X7R	0,21	co	30%	0,063	0,063				plus de découplage ref modem Hart, perte com
					cc	70%	0,147	0,147				plus de tension de ref modem Hart, perte com
2	98	1206	250k 1% 50ppm	0,02	co	40%	0,008	0,008				perte polarisation entrée modem hart, perte com
					drift	60%	0,012			0,012		sans influence
	106	1206	250k 1% 50ppm	0,02	co	40%	0,008	0,008				perte polarisation entrée modem hart, perte com
					drift	60%	0,012			0,012		sans influence
1	XC183	1206	500 1% 50ppm	0,02	co	40%	0,008	0,008				plus d'alimentation etage d'entrée rupture capteur
					drift	60%	0,012			0,012		sans influence
1	8	DC/DC 1W	LME1212S	286,00	co	50%	143,000	143,000				plus d'alimentation etage d'entrée rupture capteur
					cc	50%	143,000	143,000				plus d'alimentation etage d'entrée rupture capteur
1	13	LEDC-MSDUAL	LED	2,00	co	20%	0,400				0,400	risque dépassement charge en sortie
					cc	80%	1,600	1,600				plus d'alimentation etage d'entrée rupture capteur
1	2	MSOP10	LTC2402	37,00	out gnd	50%	18,500	18,500				rupture capteur plus de signal AD
					out vcc	50%	18,500	18,500				rupture capteur plus de signal AD
1	16	QFN20 0.65	DS8500	2,00	out gnd	50%	1,000	1,000				plus de communication Hart
					out vcc	50%	1,000	1,000				plus de communication Hart
1	1	QUARTZ HC49 CMS	3.6864 Mhz	5,00	cc	50%	2,500	2,500				plus de communication Hart
					co	50%	2,500	2,500				plus de communication Hart
1	6	SC70	TMP05	37,00	out gnd	33%	12,210	12,210				plus de t° de comensation
					out vcc	33%	12,210	12,210				plus de t° de comensation
						34%	12,580				12,580	dérive mesure erreur compensation
1	75	SO8	385 2v5	15,00	co	50%	7,500				7,500	dérive mesure alim AD non défini
					cc	50%	7,500	7,500				rupture capteur AD plus alimenté
1	18	SO8	ADuM1100A	12,00	out gnd	50%	6,000	6,000				rupture capteur plus de signal AD
					out vcc	50%	6,000	6,000				rupture capteur plus de signal AD
1	69	SO8	XTR116	19,00	out gnd	50%	9,500	9,500				repli sortie > 21 mA
					out vcc	50%	9,500	9,500				repli sortie < 3.6 mA
2	148	SOD8	4148	10,00	co	20%	2,000	2,000				repli sortie < 3.6 mA (ouverture boucle)
					cc	80%	8,000			8,000		sans influence, plus de protection inversion polarité
	149	SOD8	4148	10,00	co	20%	2,000	2,000				plus d'alimentation modem Hart, perte com
					cc	80%	8,000			8,000		tension modem Hart hors spécifications
1	5	SSOP28-0.65	16F886	20,00	outgnd	50%	10,000	10,000				repli sortie < 3.6 mA
					out vcc	50%	10,000	10,000				repli sortie > 21 mA
								420,029	0,000	16,827	20,774	
			somme fit :	457,63			457,63	(verif)		SFF=	95,46%	
			MTBF =	2 185 171	Hrs					DC=	91,78%	

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

Appendix 2:
Using FMEA data and Additional information about temperature sensors.

The CNL40igH 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
4 wires Pt100 in low stress environment	500
4 wires Pt100 in high stress environment	10000

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
4 wires Pt100 in low stress environment	50
4 wires Pt100 in high stress environment	1000

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 (2,3,4 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.

Certification to a Safety Integrity Level

The International Electrotechnical Commission's (IEC) standard IEC 61508, defines SIL using requirements grouped into two broad categories: hardware safety integrity and systematic safety integrity.
A device or system must meet the requirements for both categories to achieve a given SIL.
The SIL requirements for hardware safety integrity are based on a probabilistic analysis of the device. To achieve a given SIL, the device must meet targets for the maximum probability of dangerous failure and a minimum Safe Failure Fraction. The concept of 'dangerous failure' must be rigorously defined for the system in question, normally in the form of requirement constraints whose integrity is verified throughout system development. The actual targets required vary depending on the likelihood of a demand, the complexity of the device (s), and types of redundancy used.
PFD (Probability of Failure on Demand) and RRF (Risk Reduction Factor) of low demand operation for different SILs as defined in IEC EN 61508 are as follows:

SIL	PFD	RRF
1	0.1-0.01	10-100
2	0.01-0.001	100-1000
3	0.001-0.0001	1000-10,000
4	0.0001-0.00001	10,000-100,000

For continuous operation, these change to the following.

SIL	PFD	RRF
1	0.00001-0.000001	100,000-1,000,000
2	0.000001-0.0000001	1,000,000-10,000,000
3	0.0000001-0.00000001	10,000,000-100,000,000
4	0.00000001-0.000000001	100,000,000-1,000,000,000

Hazards of a control system must be identified then analyzed through risk analysis. Mitigation of these risks continues until their overall contribution to the hazard are considered acceptable. The tolerable level of these risks is specified as a safety requirement in the form of a target 'probability of a dangerous failure' in a given period of time, stated as a discrete SIL level.

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

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