Commissioning and safety manual

CNL35L
DNL35L

SIL2

Safety Integrity Level
SIL2
IEC 61508 / IEC 61511

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

REV 2-18/10/19

Summary

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 CNL35L rev2.XLS

Other documents:
- Technical datasheet CNL35L
- EMC conformity declaration CNL35L rev2
- FMEA analysis CNL35L rev2
- configuration handbook CNL35L rev2.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 CNL35L transmitter provide the conversion and isolation of analog signal or temperature measurement. The information transmit is made by analog signal like 4..20mA or 0..10V.
In option the product allows a threshold detection with 4 internal relays.

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/CNL35L_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

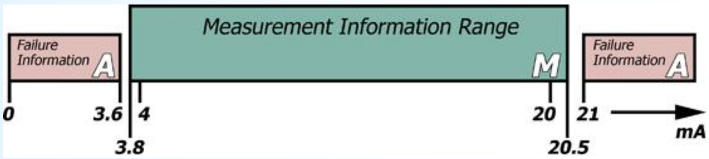
LOREME SAS
12, rue des potiers d'étain 57071 Actipole Metz Borny
FRANCE
www.loreme.fr

2 Safety function and safety state

2.1 Safety function

The safety function of the device is completed, as long as the 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, and the threshold detection function is not altered.

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 CNL35L, 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 : analog input, analog output, relay output

- not safety interfaces : pushbutton interface, display, serial link RS232 (device configuration)

If the device have the optional display, pushbutton interface, the local configuration access must be invalidated (by the RS232 link) for the SIL2 applications.

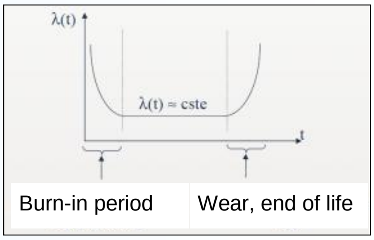
3.2 Configuration / Calibration

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 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.
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.

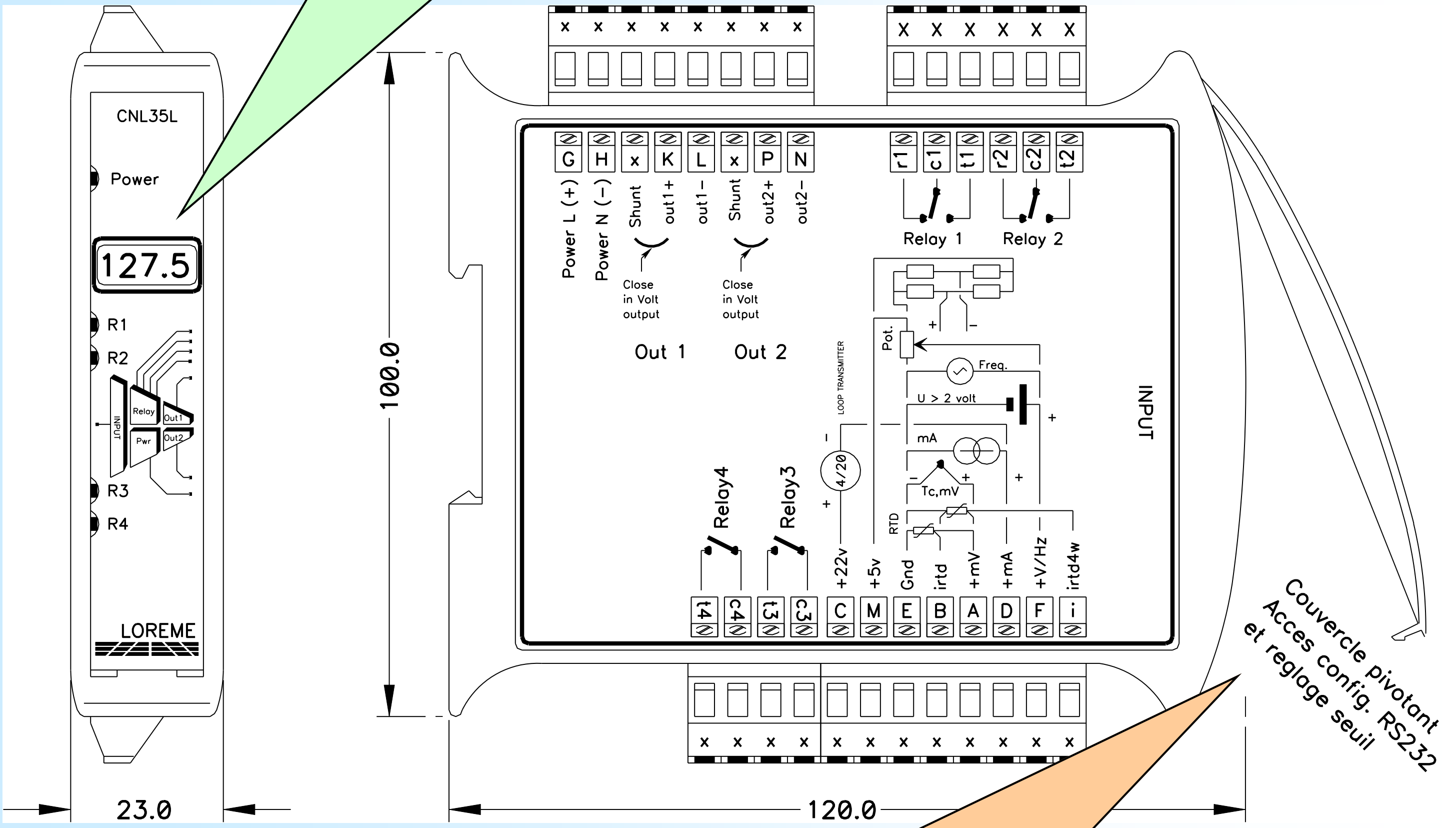
4 Installation, commissioning and replacement

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

The display and the Led indicators are not included in the safety function. The access to configuration by push buttons must be inhibited in SIL2 application.



RS232 link behind the cover, allows access to configuration mode (use only the communication cable provided by LOREME)
Warning : In configuration mode, the output current is frozen (stop of measure function during the configuration)
For safety reasons, the CNL35L quit the configuration mode and return in measure mode after 2 minutes of inactivity.

Only the RS232 configuration must be available to prevent malfunction due to local access to configuration by someone who's not qualified.
(for device with display option)

4.2 Electrical connection and configuration

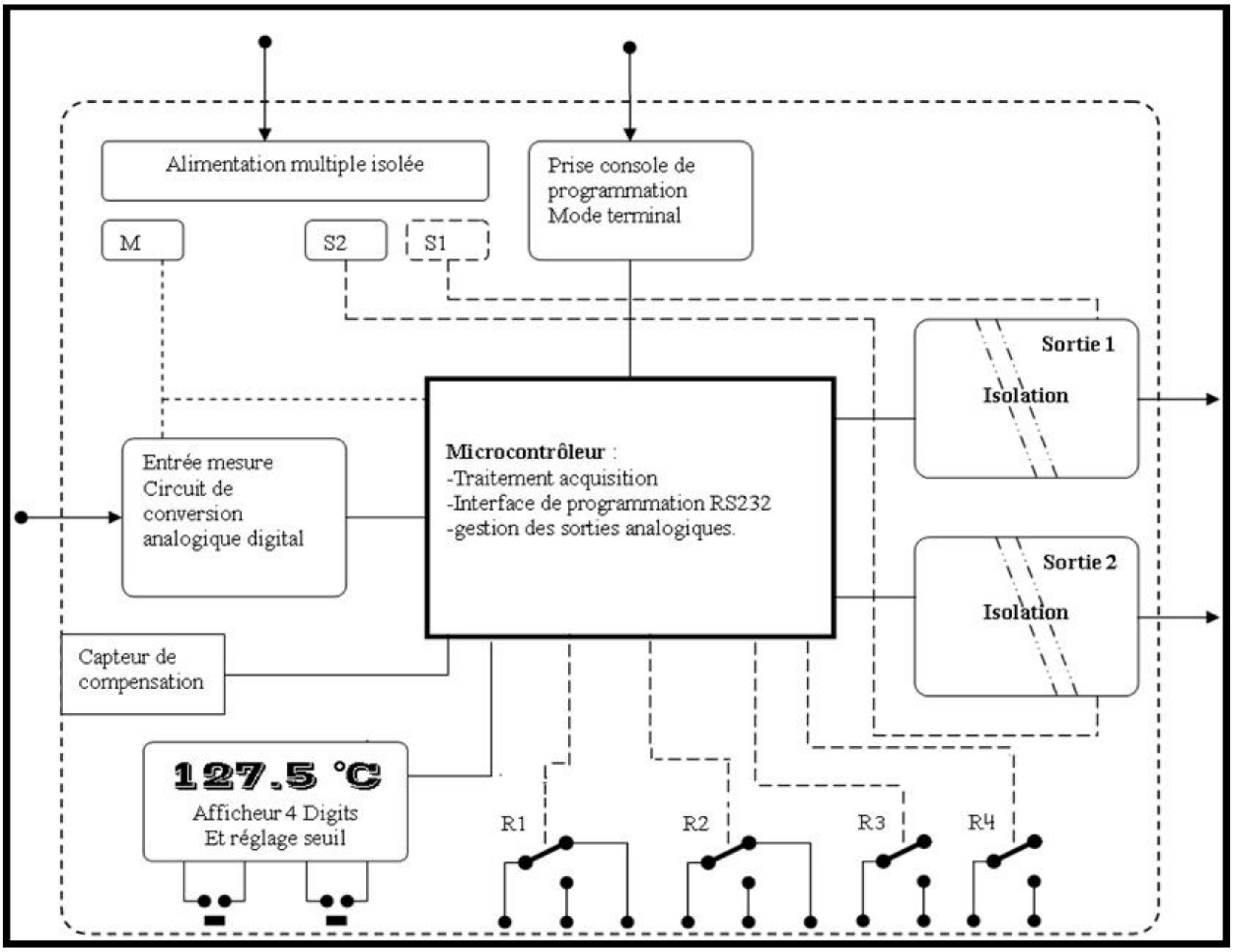
This information are complementary to the handbook manual

- The device is not sensitive to the power supply polarity. The power supply may be DC or AC
- For a remote thermocouple, take care of using compensation cable or extension cable with the same type of thermocouple and with good polarity. (it may cause error or drift of temperature measure)
- For a remote PT100 probe, take care of using cable with 3 or 4 wire with same section to have a good line compensation.
- For the current (mA) input, check the loop calculation (load) to prevent a saturation of input signal.
- Ensure the right choice of sensor type input in configuration.
- Check if the temperature range in device and in plc are the same.
- The burn out value (Sensor break detection) of the analog output must be programmed <3.6mA or ≥ to 21mA (21mA factory)
- The relay contact 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 of the analog output it is necessary to have:
- respect the voltage range of power supply
- respect the maximum load in loop current with 10% margin
Be careful, exceeding 4 ... 20mA loop load ,can prevent the output current to reach the burn out or max value. It may saturate in the measurement range , and place the system in a dangerous state.

4.3 Typical connection


Alimentation multiple isolée
Prise console de programmation Mode terminal
M
S2
S1
Sortie 1
Isolation
Microcontrôleur :
-Traitement acquisition
-Interface de programmation RS232
-gestion des sorties analogiques.
Entrée mesure Circuit de conversion analogique digital
Sortie 2
Isolation
Capteur de compensation
127.5 °C
Afficheur 4 Digits
Et réglage seuil
-
-
R1
R2
R3
R4

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 or the input signal
5. verify that the output current goes into burn out value (≤ 3.6mA or ≥ 21mA)
   (this functionality is available only for sensor input and 4..20mA input)
6. Connect a simulator* at the input of the converter
7. Simulate the appropriate 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 + / -0.15% near
8. Check the threshold detection (if option relay)
9. Disconnect the simulator and reconnect the sensor to the converter input
   (check that the output current is in the measurement range)
10. Remove milliammeter and close the output loop (green LED must light)
11. 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 $\geq 10^{-3}$ and $<10^{-2}$ for SIL2 safety functions and between $\geq 10^{-4}$ and $<10^{-3}$ for SIL3 safety functions.

λ safe detected	λ dangerous detected	λ safe undetected	λ dangerous undetected = PFH	**SFF**
198 FIT	11 FIT	13 FIT	16 FIT	93.3% (without relay)
192 FIT	11 FIT	13 FIT	22 FIT	90.75% (with relay)

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=$9.60E^{-05}$	**PFD**avg=$4.80E^{-04}$	**PFD**avg=$9.60E^{-04}$	**PFD**avg=$1.9E^{-03}$

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 = 9.20 E^{-5} x Tproof [years]

either for Tproof = 10 years, 10 % 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

SIL 2
Safety Integrity Level
IEC 61508 / IEC 61511

REV1
Page 1/1

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

Designation: **Programmable analog signal transmitter**

Type: **CNL35L**

Revision : 2 date : 25/06/2015

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 year**	**PFH**
192 FIT$_{(2)}$	11 FIT$_{(2)}$	13 FIT$_{(2)}$	22 FIT$_{(2)}$	90.75%	9.60E^{-05}	2.2E^{-08} 1/h

(1) according to FMEA CNL35L 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 : 25/06/2015

Signed on behalf of LOREME ; M. Dominique Curulla

FMEA Details

Context

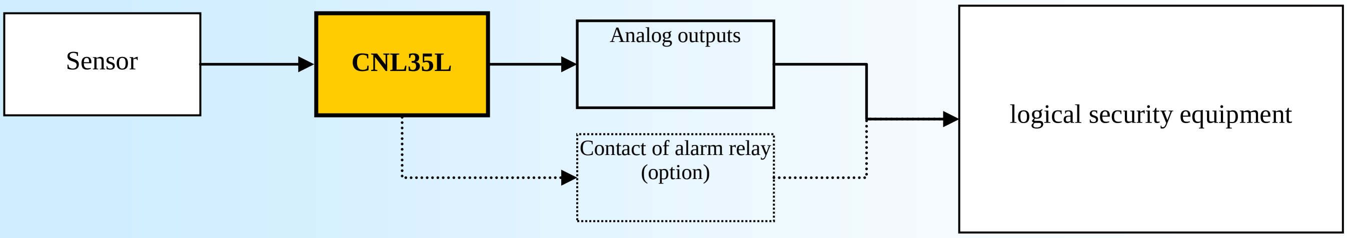
This document details the Failure Mode and Effects Analysis (FMEA) of CNL35L component of society LOREME. Besides the characterization of the information necessary for safe operation (especially for availability calculations and constitution of stock of spare parts), this study can meet the requirements 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 CNL35L 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 sensors in order to reconstitute an analog output signal (4 .. 20 mA) with or without alarm relay.
Typically, a converter is interfaced between a sensor and protection equipment, referred to as "logical security equipment"



Characterization of the component

The CNL35L 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 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 transmitter consists of:
an input stage , analog digital converter
an isolation stage (ADC power and signal transmission)
a microcontroller (linearization, temperature compensation, signal scaling and alarms functions)
an isolated stage (signal transmission)
an output stage (current amplifier)
and alarms relays

Definition of the feared event

For CNL35L 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.
or the impossibility to transmit an alarm.

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 CNL35L 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.
(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 : 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 CNL35L converter are available in document : **AMDEC CNL35L rev2.XLS** (on request)

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
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. 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