4-20 mA Current loop isolator and signal splitter
SIL3 / SIL2, HART transparency

LOREME

Commissioning and safety manual

CAL23DMA-S2

SIL2

SIL3

SIL
IEC 61508

LOREME 12, rue des Potiers d'Etain Actipole BORNY - B.P. 35014 - 57071 METZ CEDEX 3
Téléphone 03.87.76.32.51 - Télécopie 03.87.76.32.52
Nous contacter: Commercial@Loreme.fr - Technique@Loreme.fr
Manuel téléchargeable sur: www.loreme.fr

REV 2-18/10/19

Sommaire

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_CAL23DmA Revision A1

Other documents:
Technical datasheet CAL23DmA
- EMC conformity declaration CAL23DmA
- FMEA analysis CAL23DmA

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 transducer CAL23DmA-S2 provides isolation and duplication of analog current loop 4 ....20mA
It also allows the transmission of HART signals between input and output 1.
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/CAL23DmA_eng.pdf

1.3 Standards and Guidelines

The devices are evaluated according to the standards listed below:

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

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

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

1.4 Manufacturer information

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

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

The safety fallback state is defined by output current outside the range of 3.6 mA to 21mA.
- Either an output current <3.6 mA
- Either an output current> 21 mA

The application should always be configured to detect the current value out of range
(<3.6 mA -> 21 mA) and considered "faulty ".
Thus, in the FMEA study, this condition is not considered dangerous.

The reaction time for all safety functions is <30 ms.

3 Safety Recommendation

3.1 Interfaces

The device has the following interfaces.

- safety interfaces: input, output 1, output 2, simulation link (at rear the front panel)

- not safety interfaces : no

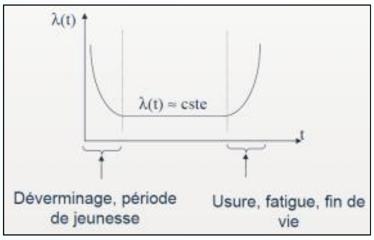
HART communication is not relevant for functional safety

3.2 Configuration / Calibration

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

3.3 Useful lifetime

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



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

Note:

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

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

4 Installation, commissioning and replacement

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

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

4.1 Front panel description

Convention:
- The green LED indicate correct operation.
- Red LED indicate a warning or a defect.

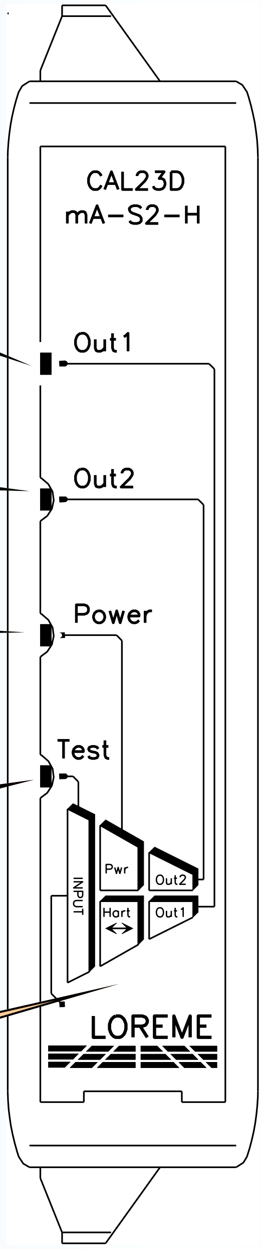
Output 1 current passes through the Green led and indicates that the output loop is closed. (Current flow) the green LED goes OFF when opening the output loop and when using test terminals located under the front panel

Output 2 current passes through the Green led and indicates that the output loop is closed. (Current flow) the green LED goes OFF when opening the output loop and when using test terminals located under the front panel

Green power supply LED indicates that the device is properly powered.
flashes when the power goes into protection.
(under voltage , thermal overload or short circuit)

Red "test" LED
indicates that the module is in simulation mode.
(Insertion of the jack underneath the front face)
the device transmits input current injected on the simulation cable.
(The led goes off when the simulation link is removed and the device return in normal operation)

Jack socket (simulation link) located under the front panel allows the switching in test mode for the periodic loop control.(Use only the cable provided by LOREME for this purpose)



4.2 Electrical connection

* Device power supply :between terminal K + and terminal L - , The module is insensitive to power polarity
The polarity is given as a guide for the implementation of schemes.

* Output 1: Two modes of operation are possible (active mode and loop powered mode)
- Active Mode (device supplied the output current) between terminal G + and terminal H -
- Loop powered mode (the device regulates the current of a loop with his own power supply) between terminal H + and terminal J -
(Loop powered output is protected against reverse polarity)
(Hart protocol transparency is ensured between the input and output 1)

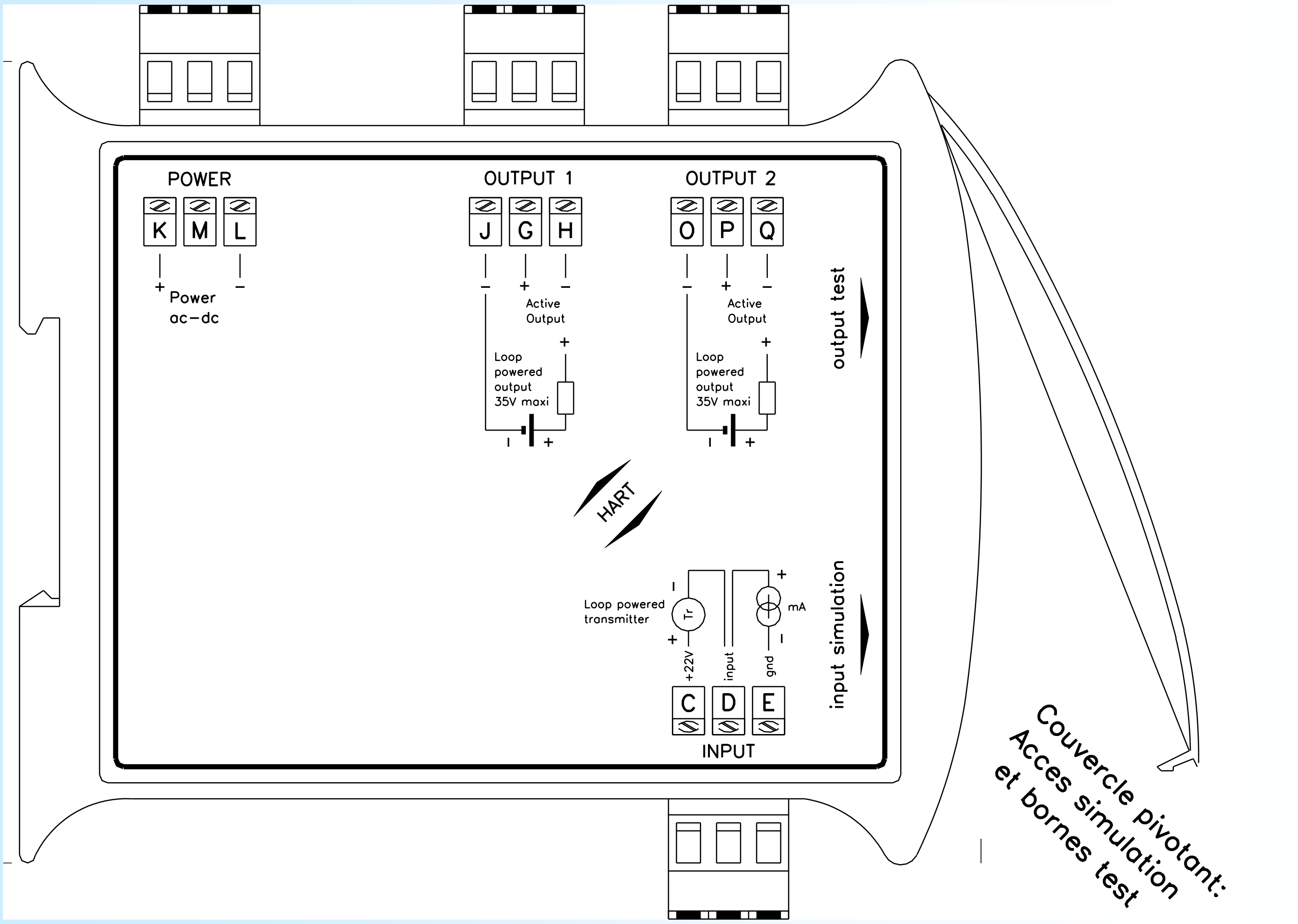
* Output 2: Two modes of operation are possible (active mode and loop powered mode)
- Active Mode (device supplied the output current) between terminal P + and terminal Q -
- Loop powered mode (the device regulates the current of a loop with his own power supply) between terminal Q+ and terminal O -
(Loop powered output is protected against reverse polarity)

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.
- In Loop powered mode , the output loop voltage must be between 10 volts and 35 volts
- In Active mode, the output load resistance must be between 0 ohms and 750 ohms.

Input : two modes of operation are possible (active mode and passive mode)
- passive input (the sensor must provide the device input current) Terminal D+ and Terminal E-
- active input (the device provides power supply to the input loop powered sensor) Terminal C (+22 V) and Terminal D -

WARNING !
- Do not short the sensor power supply (terminal C) otherwise the device can be damaged
- During a input simulation on the test jack (red LED 'test' on) the safety function of the unit is not maintained,
 (the unit does not repeat the signal from the input terminal, but the signal injected into the test lead.

4.3 Wiring



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. raise the front hood off the device
3. Using the jack cable and a simulator (current generator * Note 1) set the input current to high alarm value (≥ 21.0 mA).
   (The insertion of the jack must turn on the red LED "test")
4. Check if the current of each output reaches this value at +/-2%
5. Set the input current to the low alarm value (≤ 3.6 mA)
6. Check if the signal from each output reaches this value at +/-2%
7. Set the output current to a median value (= 12 mA)
8. Check if the signal from each output reaches this value at +/-2% (linearity check and the transfer function)
9. Remove the simulation link (red LED goes OFF "test"), close the front panel hood.
10. Remove the bypass on the safety controller system or return to a normal operating condition
11. After testing, the results should be documented and archived.

Any device that does not satisfy the control needs to be replaced.
Note 1: The current generator 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 .

λsafe	λdangerous = PFH	SFF
305 FIT	1.8 FIT	99.4%

temperature conditions 45°C

PFDavg **value depending proof interval**

T[Proof] **= 1 an**	**T**[Proof] **= 5 ans**	**T**[Proof] **= 10 ans**	**T**[Proof] **= 20 ans**
PFDavg=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.

Annex 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:

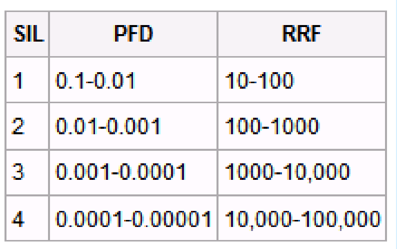
- Observe the characteristics specified in the datasheet (Voltage and frequency tolerance).
- It is preferable that the power comes from a system with section switches equipped with fuses for instrumentation components, and the supply line is the most direct route possible from the section switch. Avoid 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.

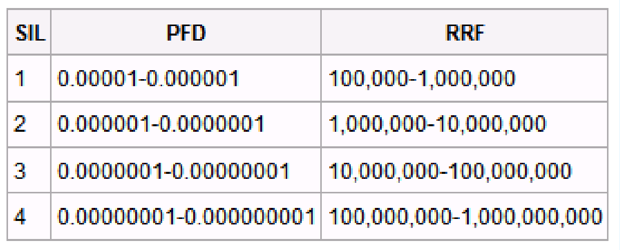
Certification to a Safety Integrity Level

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