Instruction manual
Safety level switch
High level
Series 231 (AUX)

MMT srl
www.mmtitalia.com
Capralba (CR) - Italy
[5-2025]

Series 231 Instruction Manual (AUX)

Index

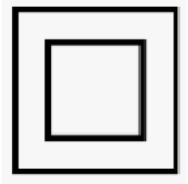
231 INSTRUCTION MANUAL - English

Safety accessory for minimum level, series 231 + 800.

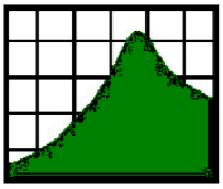
1 - Caption of used symbols

Warning. Read carefully the user manual and carefully follow the instructions of this paragraph.

Danger. Terminal block live during operation. Risk of serious injury due to electric shock.



Device with a
double insulation on the
supply voltage



M.M.T. srl ® logo

2 - Codes

Main product code:

231-X10-YZ SIL2/SIL3 conductivity self-testing level switch

Matched product codes:

800-000-5W safety probe

Optional codes:

999-230-00 option for auxiliary service relay

999-200-01 option for greater sensitivity (0.5÷20µS/cm)

Thank you for purchasing this **231** series level switch and an **800** series probe.
Before using the device, please read this manual carefully and keep it in a safe place for future use.

3 - Description

The electronic self testing conductivity level switch series **231 together** with the safety probe series **800** are a limiting safety accessory device in the IV category for industrial boilers and steam generators.
Different combinations invalidate the PED certification.

They are compliant to the following European Directives:

Low Voltage Directive	2014/35/UE
EMC Directive	2014/30/UE
PED Directive	2014/68/UE.
Applied norms:	EN 12953-9
	IEC 61508

Given the particular mechanical construction of the probe and the use of a specific electronic circuit, the device can safely measure water presence inside a boiler. The measure is conductive.
Two independent alarm contacts signal:

- water above the established level (maximum level)
- isolation loss inside the probe
- failure situation inside the device (by self-testing)
- wiring break between the probe and the device

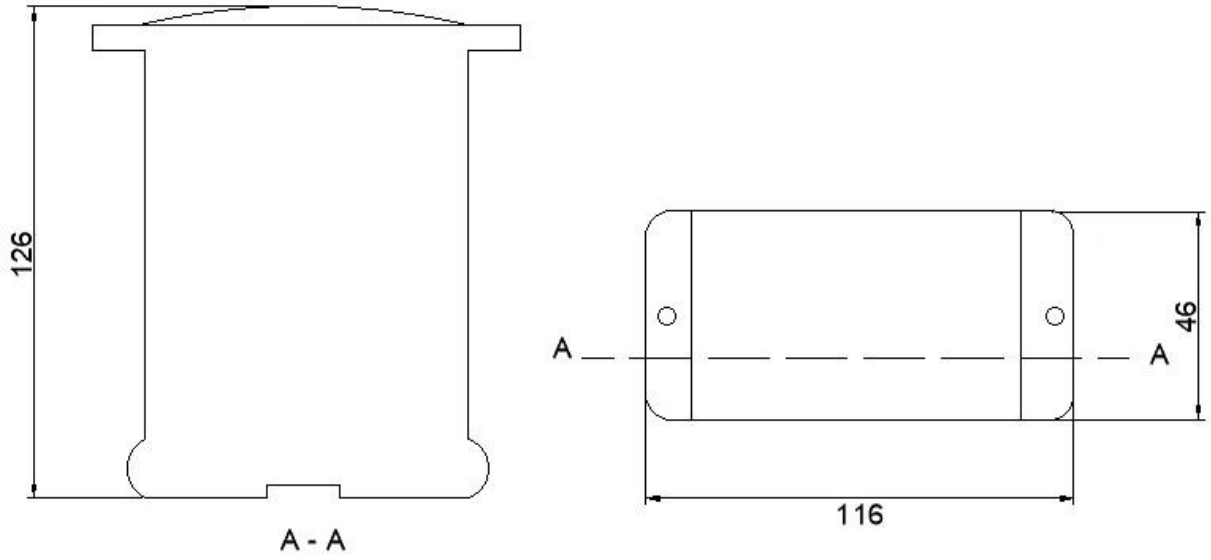
The reset of the level switch is automatic.
If manual reset is required, this must be obtained out by external circuitry.

In accordance with EN 12953-6 standard (TRD 604), our safety accessories comply with the regulation for the high water level limiter.

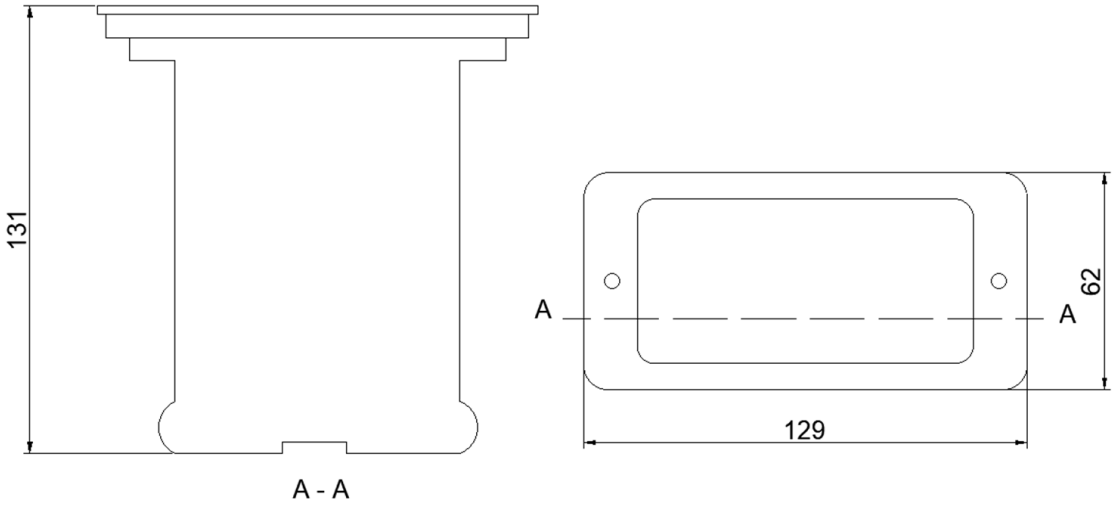
4 - Technical characteristics of the level switch series 231 (code 231-X10-YZ)

- SIL level depends on **X** character of ordering code:
X=1 → SIL2
X=2 → SIL3
- The version depends on **Y** character of ordering code:
Y=0 → DIN
X=1 → FP (=Front Panel)
- The power supply voltage depends on **Z** character of ordering code:
Z=8 → 230Vac [110-230 Vac]
Z=9 → 24Vac [20.4-26.4 Vac] / 24Vdc [20.4-26.4 Vdc]
- Overvoltage category: II
- Pollution degree = 2
- Frequency: 50-60 Hz (for AC versions)
- IP code: IP10. The level switch must always be inserted in an electrical panel with adequate protection for the environment of use (IP54 recommended)
- Power absorption: 5 VA
- Working environment temperature: 0°C ÷ 55 °C
- Maximum working altitude: 2000 m.a.s.l.
- Maximum relative humidity: 80%, at T=31°C. Linear derating till 50% at T=40°C.
- electronically controlled by 1 microcontroller (SIL2); 2 microcontrollers (SIL3)
- double conductivity measurement circuit, with a compensation electrode
- output: 2 exchange-independent relays contacts, 230V - 2,5A - AC1 (resistive load), 10 million operations when unloaded; 260000 operations when loaded
- positive safety, burner-break circuit
- conductivity: >10μS/cm (special version on request)
- maximum voltage on the electrode = 0.81 V_RMS AC at 78 Hz, with no DC component

- **DIN** version mechanical dimension (mm):



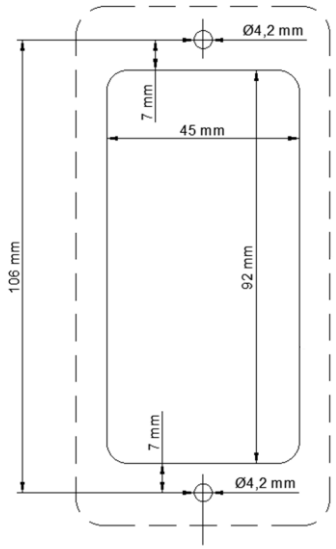
- **FP** version mechanical dimension (mm):



The level switch can be installed on the panel door of the cabinet, using the provided accessory kit, which includes a rubber gasket, a frame and 2 fixing screws.

It is provided also a plastic clip, in order to possibly use the mounting DIN rail.

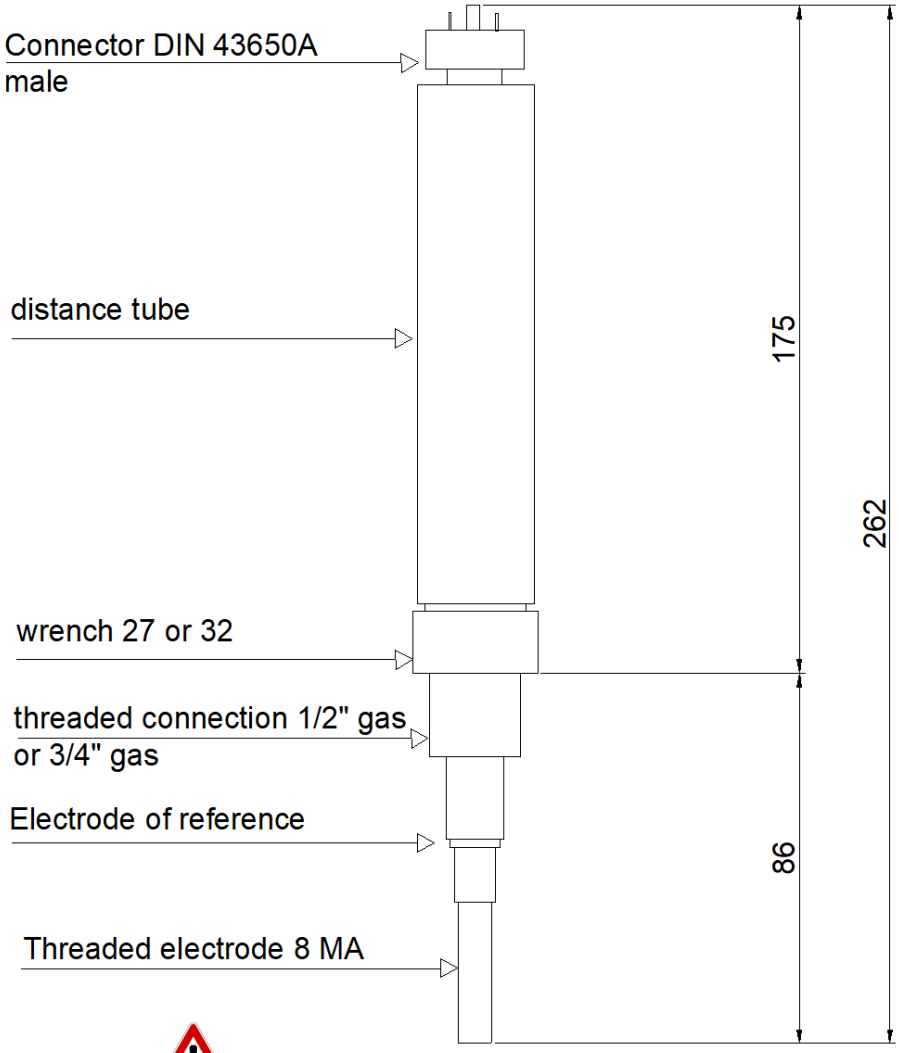
For door mounting, use the following drilling and cutout template.



Dotted lines represent the outline of the device.
Solid lines represent the size of the hole.
Note: in case of mounting of multiple level-switch next to each other, keep a separation between each of at least 20 mm.

5 - Technical characteristics of the 800 probe (code 800-000-5W)

- The threaded connection depends on **W** character of ordering code:
W=0 → ½" gas
W=1 → ¾" gas
- PS = 32 bar (on the electrode)
- TS = 239 °C (on the electrode)
- electric connection: DIN 43650 male IP65
- stainless steel body, with PTFE insulation
- mechanical dimension (mm):



6 - General Safety information

Safe use of the product depends on correct installation. All necessary operations and interventions on this product must be performed by a qualified technician, according to the operating instructions.

Qualified technicians are people that have:

- knowledge on electrical engineering
- knowledge on electric safety regulations
- knowledge of accidents prevention

It is important to follow general instructions, safety installation procedures and safety regulations for thermal and electric plants, and use all the tools and safety equipments properly.

The product has been designed and produced to withstand the conditions encountered during normal use.

The use of the product for any other purpose, or failing its proper installation, or not following the instructions, can cause damage to the product, can invalidate its CE marking, and can cause serious injuries or fatality, to people, to things and to environment.

The level probe and the level switch are only a part of the safety chain.

To complete the safety chain, additional devices are required, as wirings, relays, bells, lamps, actuation devices.

The chain has to be designed and built to be fail-safe.

In case of fire in the environment, or seismic events or adverse atmospheric events (wind), the correct working of the safety accessory is no longer guaranteed.

In these cases, the power supply must be immediately removed from the safety accessory, and the probe, the level switch and the cable between them, must be checked by qualified staff.

Only after having verified that the accessory is not damaged, can power supply be reconnected.

6.1 Probe

All the operations on the probe must always be done exclusively by a qualified technician.

The operations on the probe must always be done when the boiler is not pressurized, and cold.

Remember that a boiler can remain at high temperature also for a long time after depressurization.

Contact the manufacturer of the boiler for information about the water alarm level.

Consider carefully, that in some cases, the water level in the boiler can be different from the external indicator.

The electrode **must** to be positioned at least 14 mm far from the protection tube (if present), or from the sides of the boiler (PED).

Do not install the probe in the open air without a suitable protection against atmospheric agents.

The vent and drain holes must always be free and clear, and never covered.

6.2 Level switch

Always entrust all the operations on the level switch exclusively to a qualified technician.

Operations on the level switch must always be performed when the power supply is shut off, because dangerous voltages may be present inside the level switch.

Before performing any operation or test on the safety accessory, the technician must be electrostatically discharged to avoid damaging the equipment.

The power supply must be protected against the risk of short circuits or overcurrent by a suitable system according to the construction standard of the electric cabinet and plant, to enable easy maintenance, service, and repair.

7 - Installation

On the probe label there is "with electronic switch □ 230 / □ 231". Please tick using a permanent marker the appropriate level switch code used with the probe, in order to identify the set used once the system is installed.

7.1 - Mechanical assembly of the probe

The probe series 800 must be mounted vertically in the boiler.

The height for high-level alarm is at the lower end of the electrode, which therefore must be cut to the necessary length.

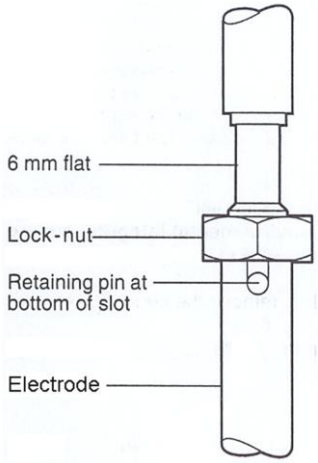
In order to correctly cut the electrode, please follow the following procedure:

1. The lower end of the electrode is an internally threaded cylinder, with a small hole on one side. The probe and the electrode must be screwed together, then fixed with the retaining pin and lock-nut.
2. Use a 6mm spanner on the probe flats, in order to prevent probe rotation.
3. Screw the lock-nut completely onto the probe, but do not tighten it in this phase.

WARNING: the threaded end of the probe must not be allowed to rotate in the body of the probe, otherwise damage of the internal wiring could take place.

4. Screw the electrode onto the probe until the hole of the probe aligns up with the bottom end of the slot in the electrode (see image below).

5.



5. Holding up the assembly, insert the retaining pin until its protrusions from both sides of the electrode are symmetric.
6. Tighten the lock-nut onto the electrode (with torque 4 ÷ 7 Nm); these operations prevent the unscrewing and loosening of the electrode.
7. Cut the electrode to the desired length using a fine hacksaw.
8. Smooth the end of the electrode.

The probe with electrode can now be assembled permanently on the boiler.

Interpose the usual copper gaskets.

The electric contact between the thread of the probe and the body boiler must be secure; a bad contact can cause the malfunction of the level switch.

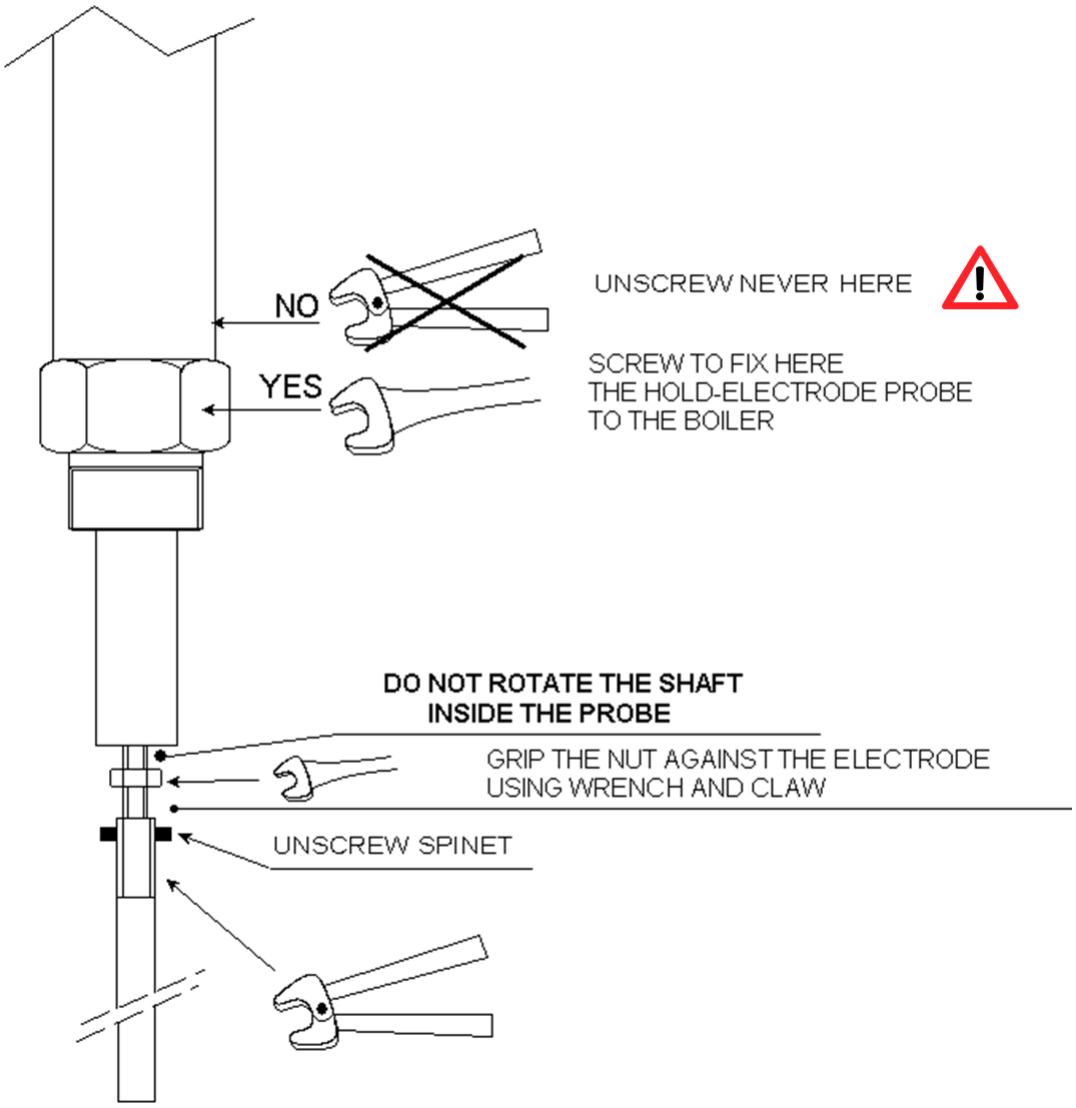
To work properly, the probe series 800 does not need to be assembled inside a pipe; however to reduce the effects of the level fluctuations, of foam or of turbulence, a suitable pipe can be used.

The pipe must present some holes in its body, to allow the free circulation of water and cleaning and to prevent deposit formation; the diameter of these holes must be larger than 20 mm and smaller than 1/3 of the internal diameter of the pipe itself. These holes will be positioned in the lower part and in the high part of the pipe itself.

The minimum distance between the measure electrode and boiler sides, or between other internal parts of the boiler and the pipe, must be higher than 14 mm (PED).

Each pipe can be used for not more than one probe series 800.

Follow the instructions reported in the following drawing.



7.2 - Level switch installation

The level switch must always be inserted in a suitable industrial electric cabinet, with appropriate protection from the environment, or in a fireproof enclosure; IP54 code is recommended.

Provide a resettable disconnector nearby the device to be able to remove the voltage when carrying out operations on it.

Provide a 100mA (T) fuse on the power supply.

Provide a protection device against overcurrents on the realys (2.5A max).

Use, for the power supply, (N/L or 0V/+24V) cables with a section of 0.75÷1.25mm^2.

For the connections, use cable suitable for high temperatures, ≥ 65°C.

Before operating on the 6 terminal blocks related to the 2 relays, ensure the voltage have been removed from those terminal blocks.

For **DIN** version

The level switch must be placed inside the electric cabinet, using the suitable DIN rail hook (see §4).

Should there be more than one level switch in the same electric cabinet, ensure at least 20 mm spacing between them, for air circulation.

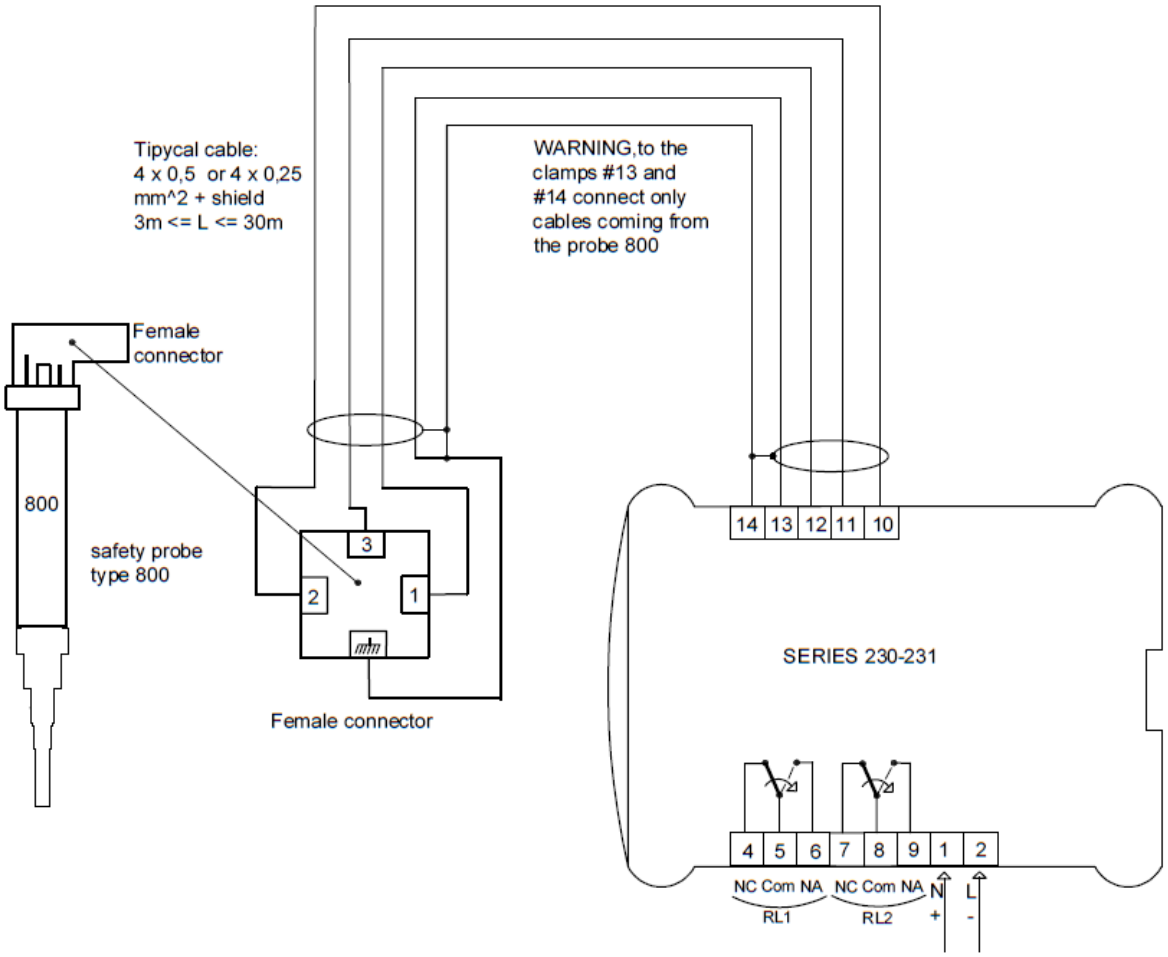
For **FP** version

The level switch can be installed on the panel door of the cabinet, using the provided accessory kit, which includes a rubber gasket, a frame and 2 fixing crews (see §4).

Should there be more than one level switch in the same electric cabinet, ensure at least 20 mm spacing between them for air circulation.

WARNING: danger! during the operation, the terminal block of the level switch may be at a dangerous voltage and danger of electric shock. The operations on the level switch must always be done with the power supply turned off; see also §6.

For the electric wiring, refer to the following diagrams.



7.3 - Electric power supply

Before powering the device, verify that the power supply voltage corresponds to the power supply indicated on the label.

Ensure that, when supplying the level switch, the front green LED labelled "PW" is ON.

7.3.1 - Electric power supply for 230V-AC version

Connect terminals 1-2 to the 230VAC line (1=Neutral; 2=Line)

7.3.2 - Electric power supply 24V

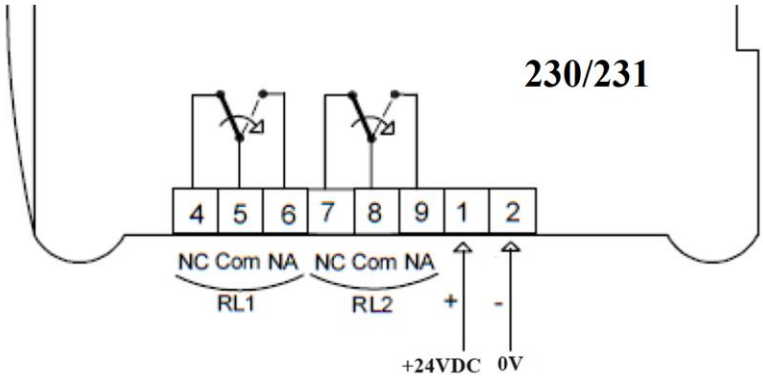
For 24V electric power supply refer to the following indications.

In all our 230/231 level switches, for a regular functionality, 0V pin of supply is electrically connected to the ground of the boiler.

Therefore it is mandatory to observe some indications about the **possible** connection to ground of the external power supply.

7.3.2.1 - Power supply 24V-DC

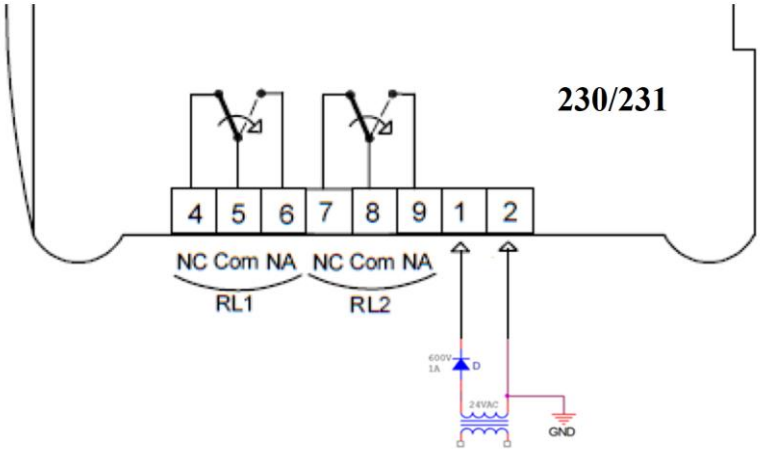
For 24V-DC supply, **only** the 0V pin can be connected, if required, to ground.
Follow the connection diagram below.



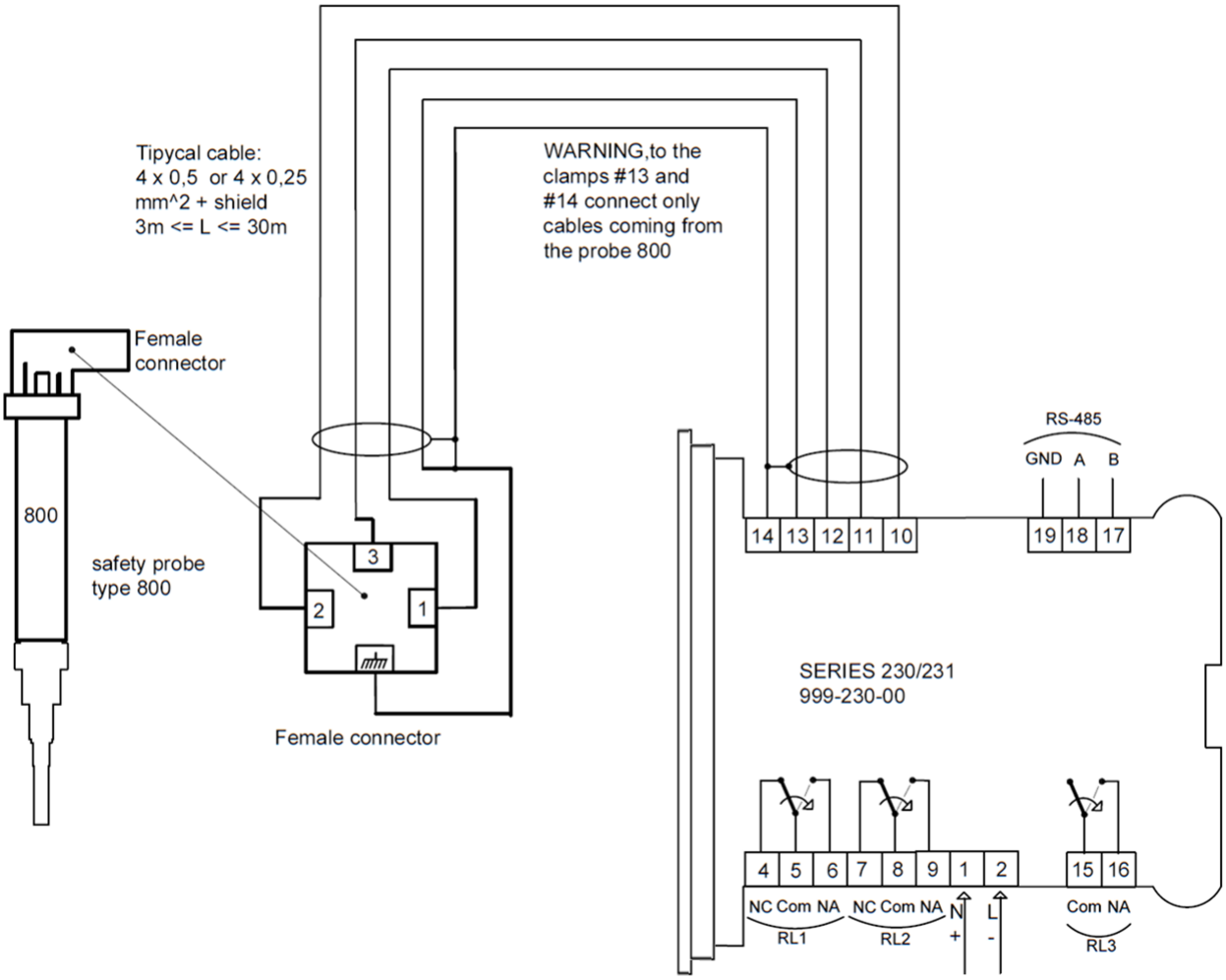
7.3.2.2 - Power supply 24V-AC

For 24V-AC supply, neither of the two pins of the secondary of the supply transformer should be connected to ground, in general.

Should a connection to ground of one of the two pins be required anyway, it is necessary to interpose a diode (600V/1A) **in series to the other pin**, as reported in the connection diagram below:

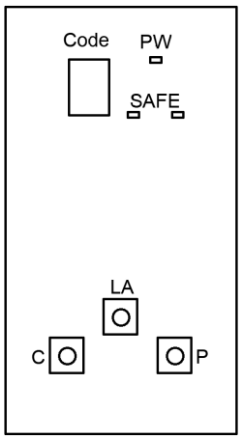


7.4 - Wiring diagram for option 999-230-00 only



7.5 - Push buttons usage

There are available 3 push buttons in the lower part of the front panel.
For the **DIN** version, access is permitted by lifting the transparent swinging front panel.
For the **FP** version, access is directly via the front label.
Their function is as follows.



- LA (Last Allarm): when kept pressed, the display shows the latest alarm code since the last time the level switch was powered. At power on, this code is “0” by default.
- P (probe): when kept pressed, the connection between probe and level switch is interrupted.
After a few seconds its displayed alarm “2”.

- C (cable): when kept pressed, a second connection between probe and level switch is interrupted. After a few seconds its displayed alarm “F”.

7.6 - Wiring between probe and level switch (terminal block 10-11-12-13-14)

For the wiring between the probe and the level switch, use a 4 x 0,25 mm^2 or 4 x 0,50 mm^2 screened cable; the cable has to be suitable for the temperature of the environment in which it is used, particularly when near the boiler. The maximum length of the cable is 30 m.

As shown in the drawing above (§7.2), wire the cable end with a DIN female connector, supplied with the probe (spare code 999-027-00), to ensure the wiring is securely connected with the head of the probe.

The cable screen works as a functional ground, not as a protective earth (PE).

Connect the cable screen as in the scheme above (see §7.2).

Do not connect to earth pins #13 and #14 of the level switch, otherwise this could create undesired earth loops, which may reduce the performance of the level switch, and potentially damage it.

7.7 - User’s wiring (terminal block 4-5-6 and 7-8-9)

The level switch has 2 independent output contacts in exchange, which can be used to control the boiler burner and to signal alarm.

The contacts are closed when there is no alarm; or open when there is alarm (positive safety).

A recommended diagram is show in the §7.2.

Should there be inductive loads, contact commutation may produce voltage spikes that may influence the operation of the measurement and control systems.

The user will have to use appropriate protection against discharge, depending on the load connected to the contacts themselves, in accordance with EN 12953-9, item 4.4.3.4.

7.8 - User’s wiring (terminal board 15-16) for option 999-230-00 only

Is available a auxiliary service contact (COM-NO) (100mA - 24V/AC-DC).

The contact switches with the same logic of the 2 main relays:

It is **closed** in case of No Alarm.

It is **open** in case of Alarm.

8 - Operation

The level switch continuously measures two different electric resistances: the first between the “measure” electrode and the ground of the boiler; the second between the “reference” electrode and the ground of the boiler.

Analysing the values of these two resistances, the device is able to determine if there is water in contact with the “measure” electrode or if the probe has a loss of insulation.

The device also performs periodically internal diagnostic tests to verify its functionality in ohmic measurements on the “measure” electrode and on the “reference” electrode; and to verify the wiring integrity.

Analysis of all measurements leads to the determination of the status of the system: if the level switch recognizes one of the possible alarm conditions, it automatically goes into safe alarm mode.

Since the system is a positive safety device, in normal working conditions the 2 internal relays are ON, both the front red LED labelled "Safe" is ON and the 8-segment displays show '0 '.

In alarm condition, the relays open, the front red led go OFF, the display shows a different code that corresponds to the particular situation of alarm; the two change-over contacts interrupt the safety chain.

In case water presence at the measuring electrode (alarm code 1), the level-switch de-energizes relays opening their contacts in about 8 seconds.

List of alarm codes with the corresponding situation for version 231:

Code	Situation
0	no alarm (normal situation); no water presence at high level
1	water presence at high level
2	interrupted wire or no communication with probe
3	anomalous operation
4	too high resistance of the connection cable
6	interrupted wire or no communication with probe
7-9	anomalous operation
8	water presence on the “reference” electrode
C	test of the internal 100 ohms resistor outside the proper range
F	interrupted wire or no communication with probe
H	anomalous operation signaled by the diagnostic microcontroller (SIL3 version only)

8.1 - Possible solutions to failure

Alarm codes 1	Verify that the level of the water is indeed above the maximum required. If the level is below, and alarm continues, verify the connection between the level switch and the probe, the integrity of the probe, and of the electrode.
Alarm codes 2, 6, F	Verify the connection between the level switch and the probe; if it has been performed as from scheme at §7.2, and the situation of alarm remains, it means that there is a broken connection.
Alarm codes 3, 7, 9, C, H	Possible failure inside the level switch, related to self testing. The alarm must switch off within 10 seconds. If the alarm remains, the regulator must be replaced.
Alarm code 4	Verify the connection between probe and level switch. The wire is too long or its resistance is too high.
Alarm code 8	Verify that the conductivity of the water in the boiler is in the range of conductivity of the level switch used (see its label); if it is out of range, it is necessary to replace the level switch with a suitable one (appropriate for the conductivity of the water). If conductivity is in the range, remove the probe from the boiler (see §6), and verify that there are no deposits or dirt on the probe. If there are no deposit or dirt on the probe, an infiltration could have taken place inside the probe; in this case the probe must be replaced.

If, after the above troubleshooting, the alarm condition remains, or different situations arise, it will be necessary to replace the whole safety accessory (level switch + probe), and contact our technical service.

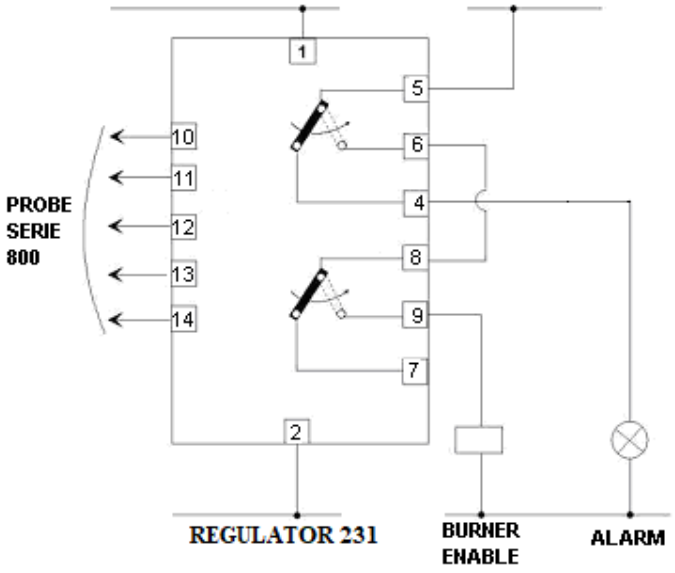
It is possible to manually verify some important functionalities of the level switch.
Refer to §7.5.
These tests must be performed only by qualified technical staff (see §6).

Warning: consider carefully that during these manual tests, an alarm is intentionally produced and the boiler will stop. Take all the necessary safety precautions to ensure there are no risks for the boiler, for the people, or for the environment.
Before performing any operation or test on the safety accessory, is manadtiry to electrostatic discharge ourselves, in order not to damage the accessory.

If there is a lockout circuit with manual reset, the operator will have to restart the boiler.
If at least one of the 2 manual tests is not carried out successfully, as described above, it means that the level switch does not work correctly and must therefore be replaced or repaired, according to the operational and installation procedures.

8.2 - Connection of the switch to the burner enable signal

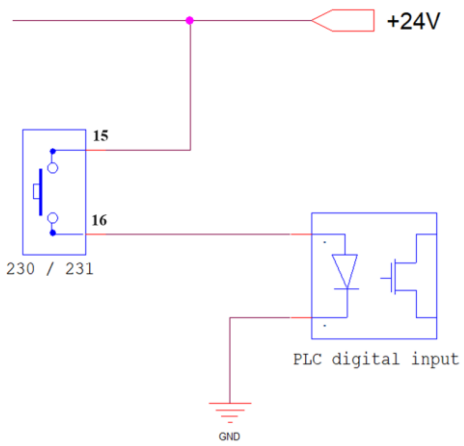
The switch must be connected to the burner enable signal using the following drawing: the two N.O. relays contacts must be connected in order to obtain a series that gives the enable signal to the burner.



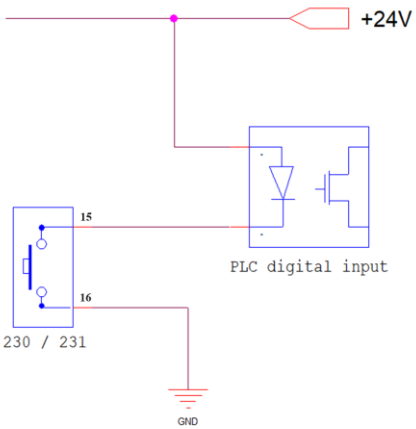
It is optionally possible to use one of the two N.C. contacts of the relays to power an alarm signal. Warning: the voltage of the alarm signal must be the same of the voltage used for the burner enable signal.

8.3 - Example of connection for option 999-230-00 only

Two typical wiring diagrams are as follow, for connection to Digital Input board of plc.



PNP



NPN

9 - Maintenance

The level switch does not require particular maintenance or service.
The probe must be cleaned and inspected at least once a year.
For aggressive water, periodically verify the "measure" electrode; clean it with an abrasive paper (always operate when the boiler is not pressurized and cold, see §6).

To avoid compromising the safety of the device, perform diagnostic tests at least once a year.
Check the correct operation of the device by performing the tests as described in §7.5 and manually simulating a possible alarm condition (e.g. by disconnecting the connector) and verifying the response of the device itself.
After maintenance reassemble everything following the instructions from point §7 of this instruction manual.

10 - Disposal

Only entrust this operation to qualified staff.
The unusable equipment parts must be disposed of using proper means, to guarantee safety.

11 - Accessories

Included
-connector DIN 43650A female cod. 999-027-00, as end part of the wire between the probe and the level switch
-copper gasket
- frame, rubber gasket, fixing screws for mounting on the door

Optional:
- electrode: 10 mm diameter, 500 mm in length (cod. 999-800-05)
- electrode: 10 mm diameter, 1000 mm in length (cod. 999-800-10)

12 SAFETY MANUAL – SIL2

Safety Level Controller 230-1/231-1 + probe 800 up to SIL 2 in single (1oo1) module/probe configuration

Summary

12.1 Manufacturer Information

M . M . T . s.r.l.
26010 CAPRALBA (CR) - ITALY
Via degli Artigiani, 56
tel. 0373 450595
fax. 0373 450728
www.mmtitalia.com
e-mail: info@mmtitalia.com

12.2 Equipment identification and ordering code

Ordering codes:

- 230-110-YZ low level safety controller with diagnostic

Code	Characteristics	Power supply
230-110-19	Conductivity>10 µS/cm	24Vac/dc.
230-110-18	Conductivity>10 µS/cm	230Vac
230-112-09	Conductivity>10 µS/cm	24Vac/dc
230-112-08	Conductivity>10 µS/cm	230Vac

- 231-110-YZ high level safety controller with diagnostic

Code	Characteristics	Power supply
231-110-19	Conductivity>10 µS/cm	24Vac/dc
231-110-18	Conductivity>10 µS/cm	230Vac
231-112-09	Conductivity>10 µS/cm	24Vac/dc
231-112-08	Conductivity>10 µS/cm	230Vac

- 800-000-5W Level probe

Code	Temperature	Pressure	Thread
800-000-50	239°C	32 bar	½ inch
800-000-51	239°C	32 bar	¾ inch

12.3 Introduction

12.3.1 Scope

This manual is the “SIL Safety manual” of the device in the scope of the document.
This manual contains information for application of the device in functional safety related loops.
This manual must be read in full and definitely understood before installation of the equipment.
A copy of his manual must be stored and preserved and used in conjunction with the equipment for all useful life of the equipment itself.
The corresponding relevant documents including data sheets, installation, operating and maintenance instructions, CE Declaration of Conformity and all applicable Certificates/Reports must be used in conjunction with this document.
The documents aforementioned are available from MMT Srl.
Only trained and qualified personnel and operators shall be involved in mounting, commissioning, operating, maintenance and dismounting of any devices may be included in the safety loop.
Installation related faults fixing is admitted acting on external features of the equipment; if fixing is not successful, the devices must be taken out of service and action taken to protect against accidental use.
Faulty devices shall be delivered to and only be repaired directly by the original manufacturer.

De-activating or bypassing safety functions causing impairment of safety functions may cause injuries to property, environment or persons for which MMT Srl will not be liable.
Failure in application of advice given in this manual causing impairment of safety functions may cause injuries to property, environment or persons for which MMT Srl will not be liable.

12.3.2 Intended Use

The equipment must only be used for the applications described in the instructions and with specified environmental conditions, and only in conjunction with approved external devices.

The device monitors levels of conductive fluids: low level (type 230-1), or high level (type 231-1) leads to trip of the output (de-energized output relays).

The device provides alarm and shutdown functions associated with level control of fluids.

The device is equipped with a three level self-diagnostic.

The first level diagnostic detects a probe loss of insulation.

The second level diagnostic detects the probe/regulator wire breakage.

The third level diagnostic detects a generic fault in the circuitry affecting the safety function.

The output counts two independent relays.

During an error condition the outputs de-energize (fail-safe).

During a loss of power the outputs de-energize (fail–safe).

If not otherwise arranged, the chain involved in the safety integrated system must be fail-safe.

The single module including one Safety Level Controller type 230-1 or 231-1 + one probe type 800 is suitable for use in safety related control loop of systematic capability and level of integrity up to SIL2.

12.3.3 Relevant Standards and Directives

12.3.3.1 Device specific standards and directives

The devices are developed, manufactured and tested according to the relevant safety standards and applicable Directives.

Standards

• Pressure equipment: EN 12953-9 edition 2007 : Standard for Shell boilers - Part 9: Requirements for limiting devices of the boiler and accessories.

• Electromagnetic compatibility: EN 61326-2-3 edition 2006: Standard for electrical equipment for measurement, control and laboratory use - EMC requirements -- Part 2-3: Particular requirements - Test configuration, operational conditions and performance criteria for transducers with integrated or remote signal conditioning.

• Functional safety IEC 61508 part 1,2,3,4,5,6,7 edition 2010:Standard for functional safety of electrical/electronic/programmable electronic safety-related systems (product manufacturer).

Directives

- Low voltage Directive 2014/35/EU.

- Electro Magnetic Compatibility 2014/30/EU.
- Pressure equipment Directive 2014/68/EU.

12.3.3.2. System specific standards and directives

• Functional safety IEC 61511 part 1,2,3, edition 2003:
Standard of functional safety: safety instrumented systems for the process industry sector (user).

12.4 Planning

12.4.1 System constraint and SIL loop determination

12.4.1.1 Low Demand Mode

The demand rate for the safety loop including the Safety Level Controller 230-1/231-1 + probe 800 is assumed to be performed on demand only, in order to transfer the EUC (steam boiler, hot water boiler) into a specified safe state, and the frequency of demands is assumed to be no greater than one per year (low demand mode).

12.4.1.2 SIL assessment of the safety loop

The relevant safety parameters to be verified in order to are:

- the PFDavg value (average Probability of Failure on Demand) and
- Tproof (proof test interval that has a direct impact on the PFDavg) and
- the SFF value (Safe Failure Fraction) and
- the HFT architecture (Hardware Fault Tolerance architecture)

12.4.1.3 Special consideration on (SFF) Safe Failure Fraction

The safe failure fraction is the measure of residual ratio of unsafe failures against the total failure rate amount.

SFF = (λs +λdd) / λtot = 1- λdu / λtot

The safe failure fraction is only relevant if determined for elements or (sub)systems in a complete safety loop.

The device under consideration is intended to be a part of a safety loop and, according to the chosen safety chain can be or cannot be a complete element or subsystem, depending on the (sub)system it is included in.

Contact MMT experts in case of any doubts on SFF calculation constraints.

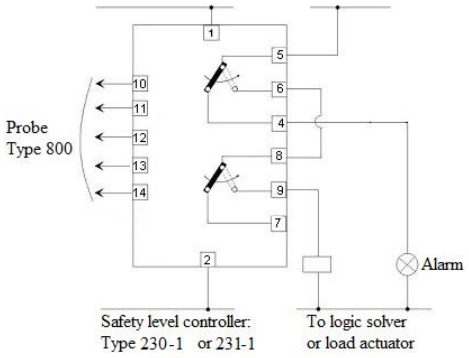
12.5 Assumptions

12.5.1 Configuration

The following assumptions have been made during the FMEDA analysis:

- The input is generated by the probe 800

- The output safety function includes the series of the contacts of the two internal relays according to the following example:



- The safe status of the EUC (steam boiler, hot water boiler) must be chosen considering that the safe state for the Safety Level Controller 230-1/231-1 + probe 800 is “de-energized relay”; decide for expected safe status of relay contacts accordingly.
- All three diagnostic levels are activated.
- The device can claim less than 15% of the total failure budget for a SIL2 safety loop.
- For a SIL2 application operating in Low Demand Mode the total PFDavg value of the SIF (Safety Instrumented Function) should be smaller than 10^{-2}, hence the maximum allowed PFDavg value is $1{,}5x10^{-3}$.
- Failure rate of components is based on the Siemens SN29500 data base.
- Failure rates are constant, wear out mechanisms are not included.
- External power supply failure rates are not included; the Safety Level Controller 230-1/231-1 + probe 800 is nevertheless a “fail safe” device leading to a safe status the relay output when a loss of power is handled.
- The safety-related device couple is considered to be of type B components with a Hardware Fault Tolerance of 0.
- It is assumed that the appearance of an error (relay output in safe state) would be repaired within 7 hours (e. g. remove device burnout).
- It is assumed that the indication of an error (relay output in safe state) would be detected within 1 hour by the logic solver.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed Classification of MIL-HNBK-217F.
- The required installation environment must be comparable to IEC 60654-1 Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40 ºC. For a higher average temperature up to 55 ºC, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed. Contact MMT in case of installation in harsh environment.
- During removal of the device for maintenance or repairing, the safety function must be guaranteed by the substitution with an identical device.

12.6 Safety Function and Safe State

The safe state is defined as the outputs being de-energized. The output status depends on the user free choice of the contact (Normally Open o Normally Closed) in the de-energized status.

12.7 Reaction Time

The reaction time for the safety function, on demand, is <3s.
The reaction time to diagnose any generic fault in: probe or wiring or regulator is <60s

12.8 Characteristic Safety Values

Safety Integrity related parameter	**Values, description**
Assessment type	FMEDA Assessment and V-model development
Device type	Complex, B
Operation mode	Low Demand Mode
Hardware fault Tolerance (HFT)	0
Architecture	1oo1D
Systematic Capability	2
SIL eligibility	SIL 2 (up to 1 Years Proof Test)
PFD Budget	Up to 15% of the SIS budget
Safety function	One channel, double relay output (series connection on charge to the user) de-energized on detection of: - Low liquid level on probe (type 230-1) - High liquid level on probe (type 231-1) or on detection of the following failures: - probe loss of insulation. - probe/conditioner wire breakage. - generic fault in the circuitry affecting the safety function.
MTTR	8 Hours (including alarm detection and restoration)
λdu	55,26 FIT
λdd	1841,9 FIT
λs	4296,0 FIT
SFF	99,11 %
PFD_{avg}, T_{proof} = 1 Year (8760 Hours)	$2,57x10^{-04}$(SIL2)
PFD_{avg}, T_{proof} = 2 Year (17520 Hours)	$4,99x10^{-04}$(SIL2)
PFD_{avg}, T_{proof} = 5 Year (43800 Hours)	$1,23x10^{-03}$(SIL2)
Response Time	< 3 Sec

NOTE:
1 "Not part" failures are not counted in the FMEDA and therefore do not contribute to the safety integrity determination according to IEC61508:2010. Such failures do not affect system reliability or safety and shall not be included in spurious trip calculation.
2 The failure rates listed in this report do not include failures due to wear out of any components.
3 Safe Failure Fraction shall be calculated on (Sub)system level
4 FIT = failure in time -> FIT x ($1x10^{-9}$) = Number of failures per hour

12.9 Life Time

A constant failure rate is assumed by the probabilistic estimation provided that the useful life time of components is not exceeded.
This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.
Early failures are cleaned by means of the burn-in procedure actuated by MMT for every piece produced and therefore the assumption of a constant failure rate during the useful life time is valid if the useful lifetime is not exceeded.
Experience has shown that the useful life time often lies within a range period of about 10 years with adequate maintenance and considering a maximum probe substitution period not exceeding 5 Years.

12.10 Installation and Commissioning

Installation must be executed by competent and qualified personnel and shall preserve the SIL level of the loop. Duringinstallation or replacement of the device the loop has to be shut down. Devices have to be replaced by the same type of devices.

12.11 Proof Test

12.11.1 Proof Test Procedure

According to IEC 61508-2 a recurring proof test shall be undertaken to reveal potential dangerous fails that are otherwise not detected by diagnostic test.
The functionality of the subsystem must be verified at periodic intervals depending on the applied PFDavg(1, 2 or 5 Years) in accordance with the data provided in this manual. See chapter 2.5.1 or chapter 2.5.2 according to the expected configuration.
It is under the responsibility of the operator to define the type of proof test and the interval time period (not exceeding the required intervals).
The full functionalities of the device must be tested:

- Trip of the device must be simulated to verify all relays commutate and all relay contacts change status (according to type 230-1 or type 231-1) when liquid level is measured by the probe over and below the expected threshold level. For example, for type 230-1 regulator, when water level goes under the threshold, it is always generated a specific error code (“1”).
- Trip of the device must be simulated to verify all relays commutate and all relay contacts change status by generating a dummy short circuit between the reference electrode of the probe and ground; it is always generated a specific error code (“8”).
- Trip of the device must be simulated to verify all relays commutate and all relay contacts change status by extracting the probe connector; it is always generated a specific error code (“F”).

The user can buy a version of the regulator (both for 230-1 and for 231-1) equipped with two additional features (a switch and a push button) with witch two of the above mentioned tests could be more easily carried out.
It is under the responsibility of the operator to put the plant in a safe status before operating the proof test.

12.12 Abbreviations

β	Beta common cause fraction
βd	Beta common cause fraction of the part of the system covered by the diagnostic
λ_{NE}	Failure rate of no effect failures
λ_{D}	Failure rate of dangerous failures
λ_{DU}	Failure rate of undetected dangerous failures
λ_{DD}	Failure rate of detected dangerous failures
λ_{S}	Failure rate of safe failures
λ_{SU}	Failure rate of undetected safe failures
λ_{SD}	Failure rate of detected safe failures
CL	Confidence Level
DC	Diagnostic Coverage factor
FSMS	Functional Safety Management System
FMEDA	Failure Mode Effect and Diagnostic Analysis
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
HFT	Hardware Fault Tolerance
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than one per year

13 - SAFETY MANUAL – SIL3

Safety Level Controller 230/231 + probe 800 up to SIL 3 in single (1oo1) module/probe configuration

Summary

13.1 Manufacturer Information

M . M . T . s.r.l.
26010 CAPRALBA (CR) - ITALY
Via degli Artigiani, 56
tel. 0373 450595
fax. 0373 450728
www.mmtitalia.com
e-mail: info@mmtitalia.com

13.2 Equipment identification and ordering code

Ordering codes:

- 230-210-YZ low level safety controller with diagnostic

Code	Characteristics	Power supply
230-210-19	Conductivity>10 µS/cm	24Vac/dc
230-210-18	Conductivity>10 µS/cm	230Vac
230-210-09	Conductivity>10 µS/cm	24Vac/dc
230-210-08	Conductivity>10 µS/cm	230Vac

- 231-210-YZ high level safety controller with diagnostic

Code	Characteristics	Power supply
231-210-19	Conductivity>10 µS/cm	24Vac/dc
231-210-18	Conductivity>10 µS/cm	230Vac
231-210-09	Conductivity>10 µS/cm	24Vac/dc
231-210-08	Conductivity>10 µS/cm	230Vac

- 800-000-5W Level probe

Code	Temperature	Pressure	Thread
800-000-50	239°C	33 bar	½ inch
800-000-51	239°C	33 bar	¾ inch

13.3 Introduction

13.3.1 Scope

This manual is the “SIL Safety manual” of the device in the scope of the document.

This manual contains information for application of the device in functional safety related loops.

This manual must be read in full and definitely understood before installation of the equipment.

A copy of his manual must be stored and preserved and used in conjunction with the equipment for all useful life of the equipment itself.

The corresponding relevant documents including data sheets, installation, operating and maintenance instructions, CE Declaration of Conformity and all applicable Certificates/Reports must be used in conjunction with this document.

The documents aforementioned are available from MMT Srl.

Only trained and qualified personnel and operators shall be involved in mounting, commissioning, operating, maintenance and dismounting of any devices may be included in the safety loop.

Installation related faults fixing is admitted acting on external features of the equipment; if fixing is not successful, the devices must be taken out of service and action taken to protect against accidental use.

Faulty devices shall be delivered to and only be repaired directly by the original manufacturer.

De-activating or bypassing safety functions causing impairment of safety functions may cause injuries to property, environment or persons for which MMT Srl will not be liable.

Failure in application of advice given in this manual causing impairment of safety functions may cause injuries to property, environment or persons for which MMT Srl will not be liable.

13.3.2 Intended Use

The equipment must only be used for the applications described in the instructions and with specified environmental conditions, and only in conjunction with approved external devices.

The device monitors levels of conductive fluids: low level (type 230), or high level (type 231) leads to trip of the output (de-energized output relays).

The device provides alarm and shutdown functions associated with level control of fluids.

The device is equipped with a three level self-diagnostic.

The first level diagnostic detects a probe loss of insulation.

The second level diagnostic detects the probe/regulator wire breakage.

The third level diagnostic detects a generic fault in the circuitry affecting the safety function.

The output counts two independent relays.

During an error condition the outputs de-energize (fail-safe).

During a loss of power the outputs de-energize (fail–safe).

If not otherwise arranged, the chain involved in the safety integrated system must be fail-safe.

The single module including one Safety Level Controller type 230 or 231 + one probe type 800 is suitable for use in safety related control loop of systematic capability and level of integrity up to SIL3.

13.3.3 Relevant Standards and Directives

13.3.3.1. Device specific standards and directives

The devices are developed, manufactured and tested according to the relevant safety standards and applicable Directives.

Standards

• Pressure equipment: EN 12953-9 edition 2007 : Standard for Shell boilers - Part 9: Requirements for limiting devices of the boiler and accessories.

• Electromagnetic compatibility: EN 61326-2-3 edition 2006: Standard for electrical equipment for measurement, control and laboratory use - EMC requirements -- Part 2-3: Particular requirements - Test configuration, operational conditions and performance criteria for transducers with integrated or remote signal conditioning.

• Functional safety IEC 61508 part 1,2,3,4,5,6,7 edition 2010:Standard for functional safety of electrical/electronic/programmable electronic safety-related systems (product manufacturer).

Directives

- Low voltage Directive 2014/35/EU.
- Electro Magnetic Compatibility 2014/30/EU.
- Pressure equipment Directive 2014/68/EU.

13.3.3.2. System specific standards and directives

• Functional safety IEC 61511 part 1,2,3, edition 2003:
Standard of functional safety: safety instrumented systems for the process industry sector (user).

13.4 Planning

13.4.1 System constraint and SIL loop determination

13.4.1.1 Low Demand Mode

The demand rate for the safety loop including the Safety Level Controller 230/231 + probe 800 is assumed to be performed on demand only, in order to transfer the EUC (steam boiler, hot water boiler) into a specified safe state, and the frequency of demands is assumed to be no greater than one per year (low demand mode).

13.4.1.2 SIL assessment of the safety loop

The relevant safety parameters to be verified in order to are:

- the PFDavg value (average Probability of Failure on Demand) and

- Tproof (proof test interval that has a direct impact on the PFDavg) and
- the SFF value (Safe Failure Fraction) and
- the HFT architecture (Hardware Fault Tolerance architecture)

13.4.1.3 Special consideration on (SFF) Safe Failure Fraction

The safe failure fraction is the measure of residual ratio of unsafe failures against the total failure rate amount.

SFF = (λs +λdd) / λtot = 1- λdu / λtot

The safe failure fraction is only relevant if determined for elements or (sub)systems in a complete safety loop.

The device under consideration is intended to be a part of a safety loop and, according to the chosen safety chain can be or cannot be a complete element or subsystem, depending on the (sub)system it is included in.

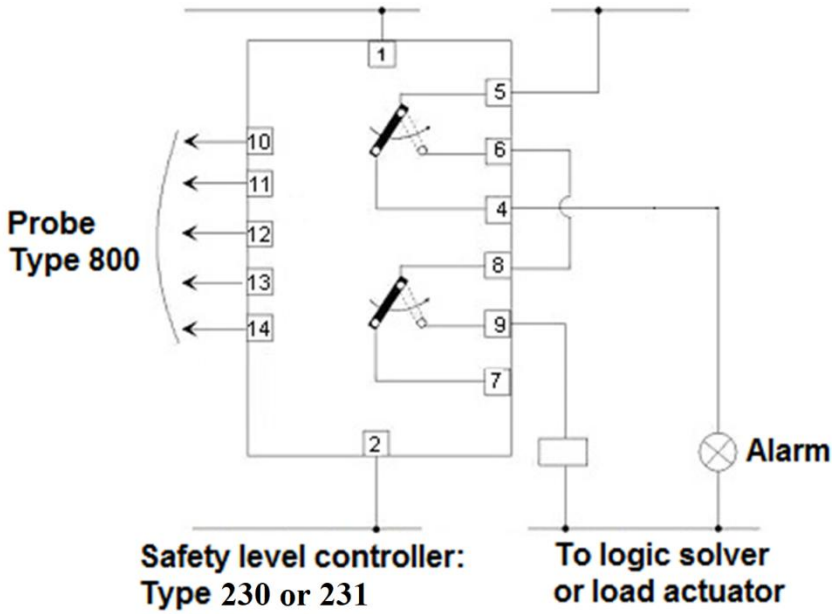
Contact MMT experts in case of any doubts on SFF calculation constraints.

13.5 Assumptions

13.5.1 Configuration

The following assumptions have been made during the FMEDA analysis:

- The input is generated by the probe 800
- The output safety function includes the series of the contacts of the two internal relays according to the following example:



- The safe status of the EUC (steam boiler, hot water boiler) must be chosen considering that the safe state for the Safety Level Controller 230/231 + probe 800 is “de-energized relay”; decide for expected safe status of relay contacts accordingly.

- All three diagnostic levels are activated.
- The device can claim less than 15% of the total failure budget for a SIL3 safety loop.
- For a SIL3 application operating in Low Demand Mode the total PFDavg value of the SIF (Safety Instrumented Function) should be smaller than 10^{-3}, hence the maximum allowed PFDavg value is $1{,}5x10^{-4}$.
- Failure rate of components is based on the Siemens SN29500 data base.
- Failure rates are constant, wear out mechanisms are not included.
- External power supply failure rates are not included; the Safety Level Controller 230/231 + probe 800 is nevertheless a “fail safe” device leading to a safe status the relay output when a loss of power is handled.
- The safety-related device couple is considered to be of type B components with a Hardware Fault Tolerance of 0.
- It is assumed that the appearance of an error (relay output in safe state) would be repaired within 7 hours (e. g. remove device burnout).
- It is assumed that the indication of an error (relay output in safe state) would be detected within 1 hour by the logic solver.
- The stress levels are average for an industrial environment and can be compared to the Ground Fixed Classification of MIL-HNBK-217F.
- The required installation environment must be comparable to IEC 60654-1 Class C (sheltered location) with temperature limits within the manufacturer's rating and an average temperature over a long period of time of 40 ºC. For a higher average temperature up to 55 ºC, the failure rates should be multiplied with an experience based factor of 2.5. A similar multiplier should be used if frequent temperature fluctuation must be assumed. Contact MMT in case of installation in harsh environment.
- During removal of the device for maintenance or repairing, the safety function must be guaranteed by the substitution with an identical device.

13.6 Safety Function and Safe State

The safe state is defined as the outputs being de-energized. The output status depends on the user free choice of the contact (Normally Open o Normally Closed) in the de-energized status.

13.7 Reaction Time

The reaction time for the safety function, on demand, is <3s.
The reaction time to diagnose any generic fault in: probe or wiring or regulator is <60s

13.8 Characteristic Safety Values

Safety Integrity related parameter	Values, description
Assessment type	FMEDA Assessment and V-model development
Device type	Complex, B
Operation mode	Low Demand Mode
Hardware fault Tolerance (HFT)	0
Architecture	1oo1D
Systematic Capability	3
SIL eligibility	SIL 3 (up to 1 Years Proof Test)
PFD Budget	Up to 15% of the SIS budget
Safety function	One channel, double relay output (series connection on charge to the user) de-energized on detection of: - Low liquid level on probe (type 230) - High liquid level on probe (type 231) or on detection of the following failures: - probe loss of insulation. - probe/conditioner wire breakage. - generic fault in the circuitry affecting the safety function.
MTTR	8 Hours (including alarm detection and restoration)
λdu	29,2 FIT
λdd	1868 FIT
λs	4296 FIT
SFF	99,5 %
PFD_{avg}, T_{proof} = 1 Year (8760 Hours)	$1,43x10^{-04}$(SIL3)
PFD_{avg}, T_{proof} = 2 Year (17520 Hours)	$2,71x10^{-04}$(SIL2)
PFD_{avg}, T_{proof} = 5 Year (43800 Hours)	$6,54x10^{-04}$(SIL2)
Response Time	< 3 Sec

NOTE:

5 "Not part" failures are not counted in the FMEDA and therefore do not contribute to the safety integrity determination according to IEC61508:2010. Such failures do not affect system reliability or safety and shall not be included in spurious trip calculation.
6 The failure rates listed in this report do not include failures due to wear out of any components.
7 Safe Failure Fraction shall be calculated on (Sub)system level
8 FIT = failure in time -> FIT x ($1x10^{-9}$) = Number of failures per hour

13.9 Life Time

A constant failure rate is assumed by the probabilistic estimation provided that the useful life time of components is not exceeded.
This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.
Early failures are cleaned by means of the burn-in procedure actuated by MMT for every piece produced and therefore the assumption of a constant failure rate during the useful life time is valid if the useful lifetime is not exceeded.
Experience has shown that the useful life time often lies within a range period of about 10 years with adequate maintenance and considering a maximum probe substitution period not exceeding 5 Years.

13.10 Installation and Commissioning

Installation must be executed by competent and qualified personnel and shall preserve the SIL level of the loop. During installation or replacement of the device the loop has to be shut down. Devices have to be replaced by the same type of devices.

13.11 Proof Test

13.11.1 Proof Test Procedure

According to IEC 61508-2 a recurring proof test shall be undertaken to reveal potential dangerous fails that are otherwise not detected by diagnostic test.

The functionality of the subsystem must be verified at periodic intervals depending on the applied PFDavg(1, 2 or 5 Years) in accordance with the data provided in this manual. See chapter 2.5.1 or chapter 2.5.2 according to the expected configuration.

It is under the responsibility of the operator to define the type of proof test and the interval time period (not exceeding the required intervals).

The full functionalities of the device must be tested:

- Trip of the device must be simulated to verify all relays commutate and all relay contacts change status (according to type 230 or type 231) when liquid level is measured by the probe over and below the expected threshold level. For example, for type 230 regulator, when water level goes under the threshold, it is always generated a specific error code (“1”).
- Trip of the device must be simulated to verify all relays commutate and all relay contacts change status by generating a dummy short circuit between the reference electrode of the probe and ground; it is always generated a specific error code (“8”).
- Trip of the device must be simulated to verify all relays commutate and all relay contacts change status by extracting the probe connector; it is always generated a specific error code (“F”).

The user can buy a version of the regulator (both for 230 and for 231) equipped with two additional features (a switch and a push button) with witch two of the above mentioned tests could be more easily carried out.

It is under the responsibility of the operator to put the plant in a safe status before operating the proof test.

13.12 Abbreviations

β	Beta common cause fraction
βd	Beta common cause fraction of the part of the system covered by the diagnostic
λ_{NE}	Failure rate of no effect failures
λ_{D}	Failure rate of dangerous failures
λ_{DU}	Failure rate of undetected dangerous failures
λ_{DD}	Failure rate of detected dangerous failures
λ_{S}	Failure rate of safe failures
λ_{SU}	Failure rate of undetected safe failures
λ_{SD}	Failure rate of detected safe failures
CL	Confidence Level
DC	Diagnostic Coverage factor
FSMS	Functional Safety Management System
FMEDA	Failure Mode Effect and Diagnostic Analysis
FIT	Failure In Time ($1x10^{-9}$ failures per hour)
HFT	Hardware Fault Tolerance
High demand mode	Mode, where the frequency of demands for operation made on a safety-related system is greater than one per year