MANUALE DI ISTRUZIONI - Italiano

Accessorio di sicurezza per massimo livello, serie 231-1 + 800.

Codici: 231-11Y-0Z regolatore di livello con autodiagnosi
800-000-5W sonda di sicurezza

Grazie per aver acquistato un regolatore serie 231-1 e una sonda serie 800.
Vi preghiamo di leggere attentamente questo manuale, prima dell'uso, e di conservarlo per futura consultazione.

1 - Descrizione

Il regolatore di livello con autodiagnosi serie **231-1** e la sonda di sicurezza serie **800**, costituiscono insieme un accessorio di sicurezza limitatore, in categoria IV per caldaie industriali e generatori di vapore in genere.
Abbinamenti diversi fanno decadere la certificazione PED.

L'accessorio è conforme alle seguenti Direttive Europee:

Direttiva Bassa Tensione	2014/35/UE
Direttiva Compatibilità Elettromagnetica	2014/30/UE
Direttiva Attrezzature a Pressione	2014/68/UE
Norme applicate:	EN 12953-9
	IEC 61508

Grazie alla particolare costruzione meccanica della sonda e all'impiego di un circuito elettronico specifico, il dispositivo è in grado di rilevare con sicurezza la presenza di acqua all'interno di una caldaia.
Il principio di misura è di tipo conduttivo.
Due contatti di allarme indipendenti segnalano:

- acqua sopra il livello stabilito (massimo livello)
- perdita di isolamento all'interno della sonda
- situazione di guasto all'interno del dispositivo (autodiagnosi)
- interruzione del collegamento tra la sonda e il dispositivo

Il reset del regolatore è stato concepito in modo automatico; qualora fosse richiesto un reset manuale, questo dovrà essere realizzato attraverso circuiti esterni.

Nei confronti della norma EN 12953-6 (TRD 604) relativamente ai ns. dispositivi di sicurezza, possiamo affermare che essi soddisfano i requisiti per quanto riguarda gli accessori limitatori di massimo livello per acqua.

2 - Caratteristiche tecniche del regolatore 231-1

- alimentazione: dipende dal codice di ordinazione:

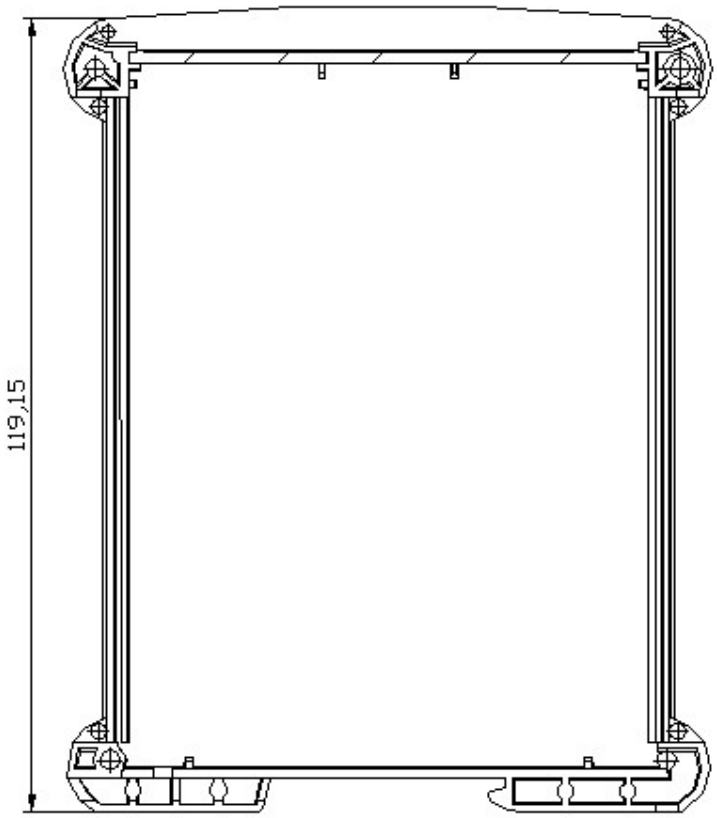
Z=8	→	110 ÷ 230 VAC +10% -15%
Z=9	→	24VAC +10% -15% / 24VDC +10% -15%

- categoria di sovratensione: II
- grado di inquinamento = 2
- frequenza: 47/60 Hz
- grado di protezione: IP10; deve essere sempre inserito in un quadro elettrico con protezione adeguata all'ambiente di impiego (consigliato IP 54)
- consumo: 3 VA
- temperatura ambiente: 0°C ÷ 55 °C
- funzionamento elettronico, governato da microcontrollore

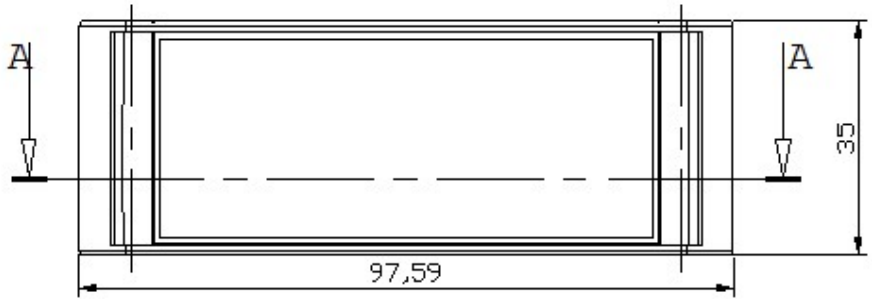
- doppio circuito di misura a conducibilità, con elettrodo di compensazione
- uscita a relè, 2 contatti in scambio indipendenti collegabili in cascata, 230V-2.5A-AC1 (carico resistivo); 10 milioni di manovre a vuoto e 260000 manovre a carico
- circuito di blocco bruciatore, a sicurezza positiva
- conducibilità:

Y=0	→	> 10 µS/cm
Y=2	→	0.5 ÷ 20 µS/cm

- Tensione max all'elettrodo: 0.81 V_RMS AC a 78 Hz senza componenti DC.
- dimensioni di ingombro (mm):



A–A

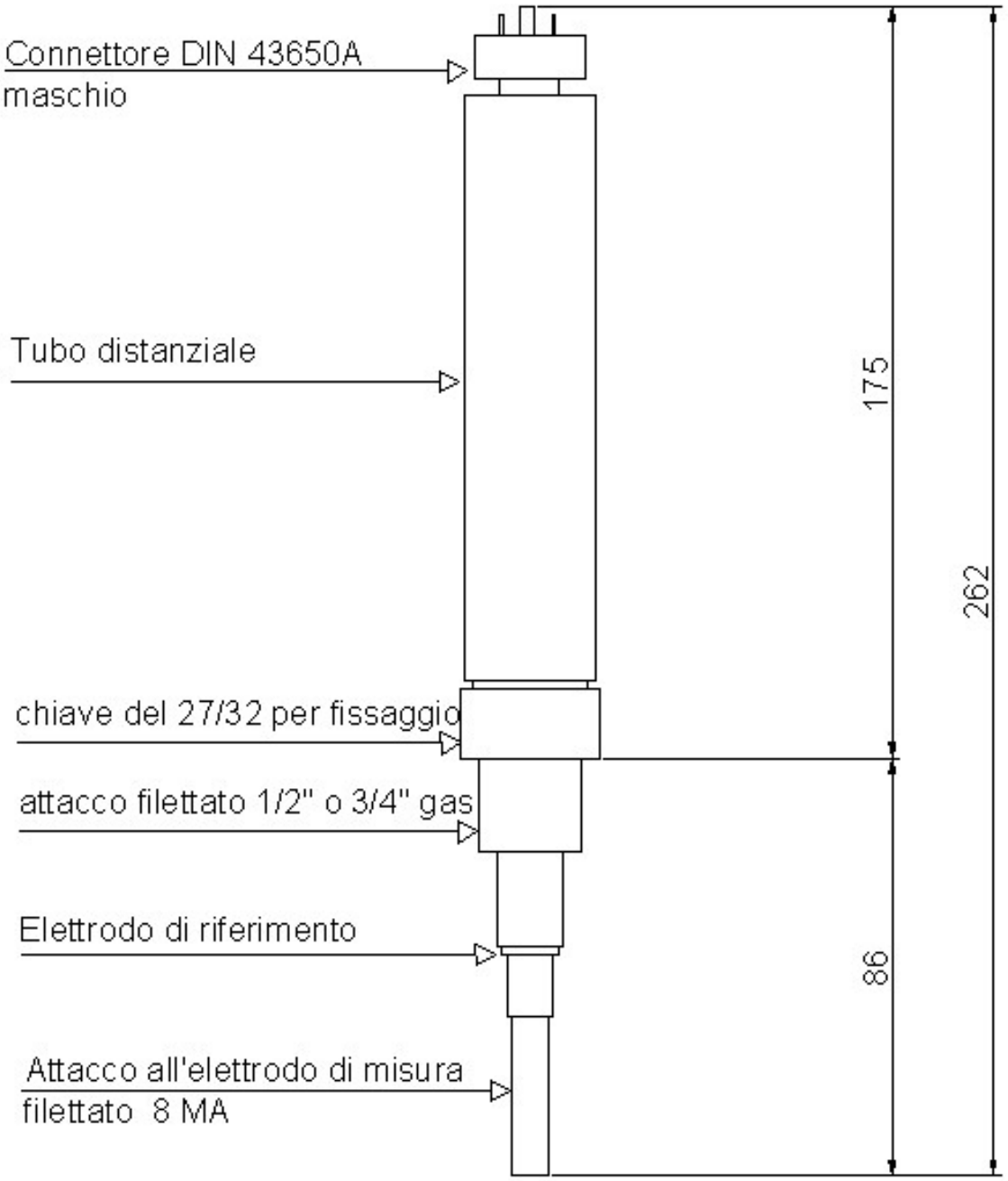


3 - Caratteristiche tecniche della sonda 800

- attacco al processo, in base al codice di ordinazione:

W=0	→	½" gas
W=1	→	¾" gas

- PS = 32 bar (all'elettrodo)
- TS = 239°C (all'elettrodo)
- connessione elettrica: DIN 43650A maschio IP65
- corpo inox anticorrosione con isolamento in teflon
- dimensioni di ingombro (mm):



4 - Avvertenze per la sicurezza

Operazioni sicure sul prodotto dipendono da una corretta installazione, uso e manutenzione da parte di personale qualificato, in accordo con le istruzioni operative.

Per personale qualificato si intendono persone che abbiano:

- preparazione e formazione elettrotecnica
- conoscenze del rispetto delle norme di sicurezza elettriche vigenti
- conoscenza di prevenzione infortuni.

E' importante seguire le istruzioni generali di installazione e sicurezza per gli impianti termici ed elettrici, come pure fare uso corretto di tutti gli strumenti per la sicurezza.

Il prodotto è stato studiato e prodotto per sopportare le condizioni incontrate durante un uso normale.

L'uso del prodotto per qualsiasi altro scopo, o la sua mancata installazione secondo queste istruzioni, può provocare danno al prodotto stesso, invalidarne la marcatura CE, e causare danni gravi, anche mortali, alle persone, alle proprietà e all'ambiente.

La sonda di livello e il regolatore sono solo una parte del sistema di sicurezza.

Per completarla, sono richiesti dispositivi addizionali, quali: cablaggi, relé, suonerie, lampade, organi di attuazione.

La catena deve essere progettata e realizzata a prova di guasto (fail-safe).

In caso di incendio nell'ambiente di impiego, di eventi sismici od eventi atmosferici avversi (vento), il funzionamento dell'accessorio di sicurezza non è più garantito.

In questi casi è opportuno togliere subito alimentazione all'accessorio di sicurezza, far controllare la sonda, il regolatore e il cavo da personale qualificato.

Solo dopo aver accertato che l'accessorio non è danneggiato, è possibile fornire nuovamente alimentazione.

4.1 - Sonda

Tutte le operazioni sulla sonda devono essere eseguite sempre esclusivamente da personale qualificato.

Le operazioni sulla sonda devono essere sempre fatte a caldaia depressurizzata e scaricata alla pressione atmosferica, e fredda.

Ricordare che una caldaia rimane a temperatura elevata anche dopo molto tempo che è stata tolta la pressione.

Contattare, se possibile, il costruttore della caldaia, per avere informazione sui livelli di allarme dell'acqua.

Considerare, che in alcuni casi, il livello dell'acqua in caldaia e quello visibile all'indicatore esterno, possono essere diversi.

L'elettrodo deve stare lontano dall'eventuale barilotto, o da una parete della caldaia, per almeno 14 mm.

Non installare la sonda all'esterno senza una protezione adeguata contro gli agenti atmosferici.

Il foro di sfiato e drenaggio deve essere libero, e non coperto.

4.2 - Regolatore

Tutte le operazioni sul regolatore devono essere eseguite sempre esclusivamente da personale qualificato.

Le operazioni sul regolatore devono essere sempre fatte senza la tensione di alimentazione elettrica, in quanto tensioni pericolose sono presenti all'interno del regolatore, se alimentato.

Prima di effettuare qualsiasi operazione o test sull'accessorio di sicurezza è necessario scaricarsi elettrostaticamente per evitare di danneggiare l'apparecchiatura.

Il regolatore deve essere protetto, per quanto riguarda l'alimentazione, da un opportuno sistema conforme alle norme di costruzione del quadro elettrico e dell'impianto, contro il rischio di corti circuiti o sovracorrenti, onde consentire facilmente la manutenzione, il service e la riparazione.

5 - Installazione

Sull'etichetta della sonda è presente una riga con dicitura " with electronic switch □ 230-1 / □ 231-1", con un pennarello indelebile spuntare il codice del regolatore a cui la sonda è abbinata, per riconoscere l'insieme utilizzato una volta installato l'impianto.

5.1 - Montaggio meccanico della sonda

La sonda serie **800** deve essere montata verticalmente nella caldaia.

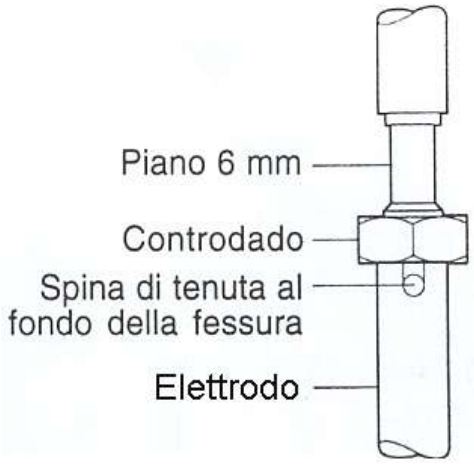
La quota di intervento per allarme di alto livello è all'estremità inferiore dell'elettrodo, che pertanto deve essere tagliato alla lunghezza necessaria.

Per il taglio dell'elettrodo, seguire la seguente procedura:

1. La sonda ha l'estremità inferiore filettata, con un foro di traverso, e deve essere fissata all'elettrodo con il filetto, la spinetta ed il controdado.
2. Avvitare completamente il controdado sulla sonda, ma non serrarlo in questa fase.
3. Tenere con una chiave piatta da 6mm il piano dell'estremità inferiore della sonda, per impedire che ruoti.

ATTENZIONE: se l'estremità filettata della sonda è lasciata libera di ruotare nel corpo della sonda stessa, potrebbe verificarsi un danneggiamento del cablaggio interno.

4. Avvitare l'elettrodo sulla sonda finché il foro della sonda si allinei con l'estremità della fessura nell'elettrodo (vedere la figura seguente).



5. Sostenere l'insieme ed inserire la spina di fissaggio finché le sporgenze dai due lati dell'elettrodo siano uguali.
6. Serrare il controdado sull'elettrodo (con coppia 4÷7 Nm); queste operazioni servono per evitare lo svitamento e la perdita dell'elettrodo stesso.
7. Tagliare l'elettrodo all'altezza desiderata quale alto livello usando un seghetto per metalli a lama sottile.
8. Sbavare l'estremità dell'elettrodo.

Ora la sonda con elettrodo può essere montata in modo definitivo sulla caldaia.

Interporre le usuali guarnizioni di tenuta in rame.

Assicurarsi del buon contatto elettrico tra il filetto della sonda e il corpo caldaia; un cattivo contatto può causare il malfunzionamento del regolatore.

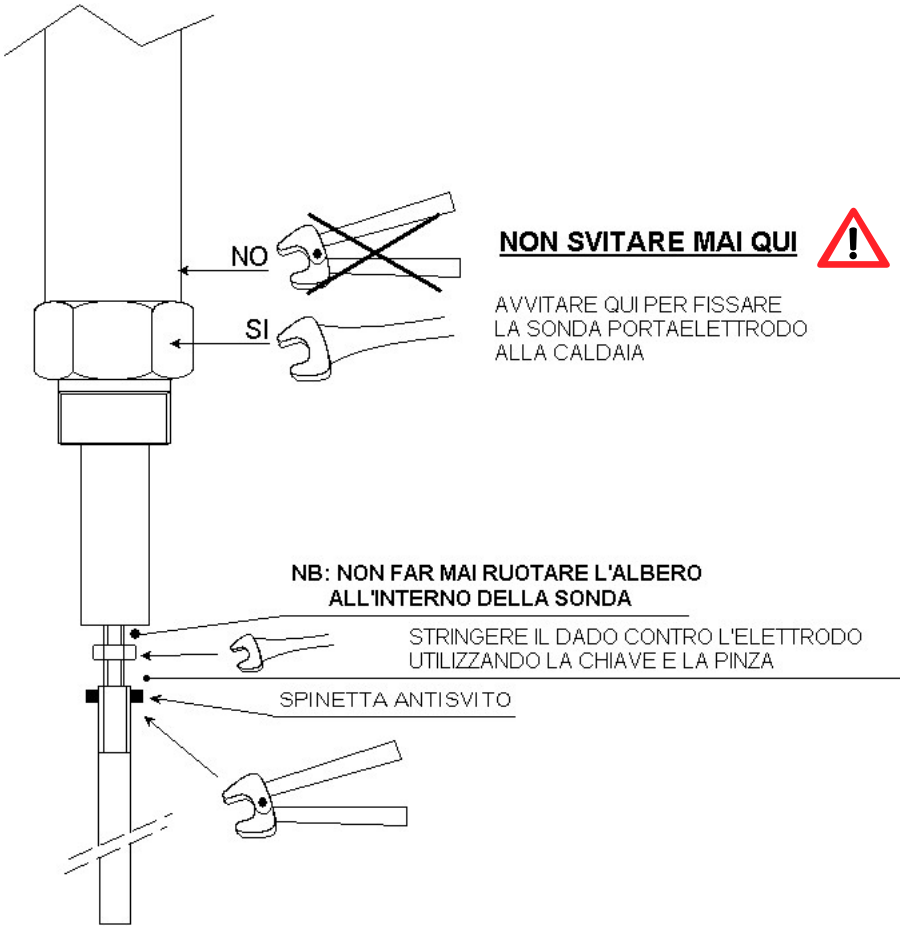
Per il suo corretto funzionamento la sonda serie 800 non deve essere montata necessariamente all'interno di un tubo o di un barilotto; tuttavia per ridurre gli effetti delle ondulazioni di livello, della schiuma o della turbolenza, un tubo può essere convenientemente usato.

In questo caso il tubo deve presentare dei fori che consentano la libera circolazione dell'acqua, la pulizia e che impediscano la formazione di depositi; questi fori, devono avere un diametro non inferiore a 20 mm e non superiore a 1/3 del diametro interno del tubo stesso. Detti fori saranno posizionati nella parte bassa e nella parte alta del tubo stesso.

In ogni caso, la distanza minima tra l'elettrodo di misura e la massa, o le altre parti interne alla caldaia e il tubo, deve essere superiore a 14 mm.

All'interno di un tubo deve essere posizionata solo una sonda serie 800.

Seguire le indicazioni del disegno seguente.



5.2 - Installazione regolatore di livello

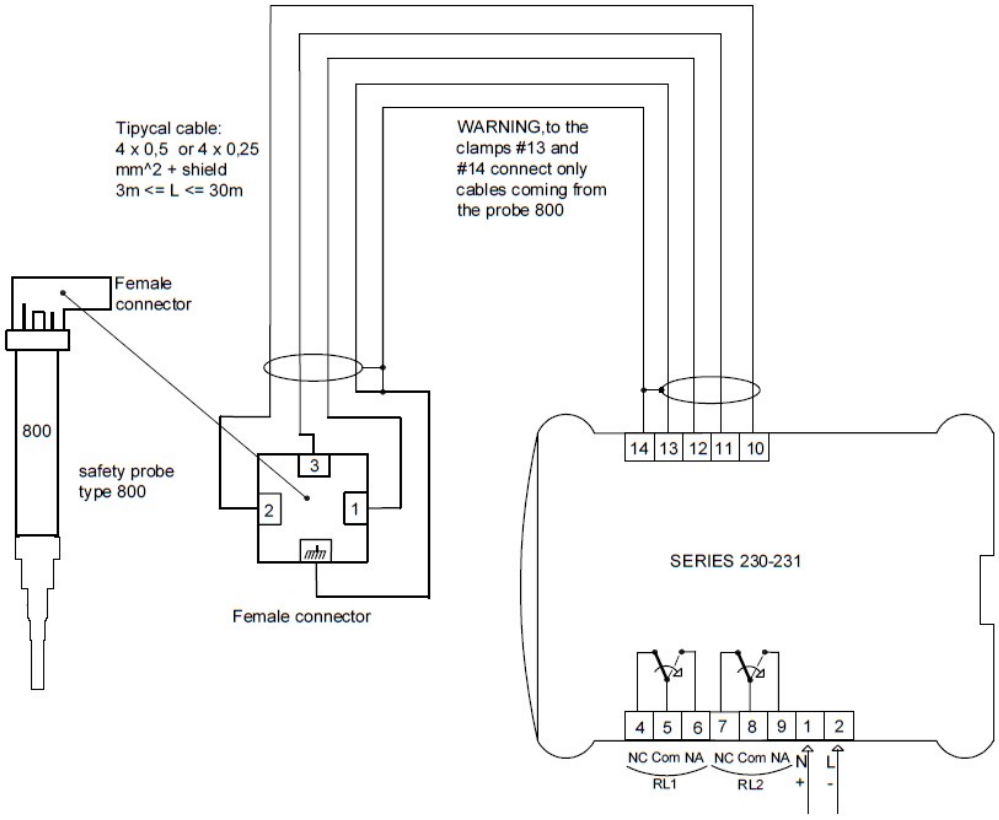
Il regolatore deve sempre essere inserito in un quadro elettrico con protezione adeguata all'ambiente di impiego, o in una custodia a prova di incendio, e comunque con grado di protezione IP4X o superiore.

Il regolatore va montato su guida a profilo DIN, usando l'aggancio di cui è munito (v. §2).

Nel caso di impiego di più regolatori in uno stesso quadro elettrico, lasciare almeno 15 mm di distanza tra di loro, per consentire la circolazione dell'aria.

ATTENZIONE: pericolo! durante il funzionamento, la morsettiera è sotto tensione: ciò comporta il pericolo di scariche elettriche. Le operazioni sul regolatore devono essere sempre fatte senza la tensione di alimentazione elettrica applicata ai morsetti; vedere anche §4.

Per i collegamenti elettrici, riferirsi allo schema seguente:

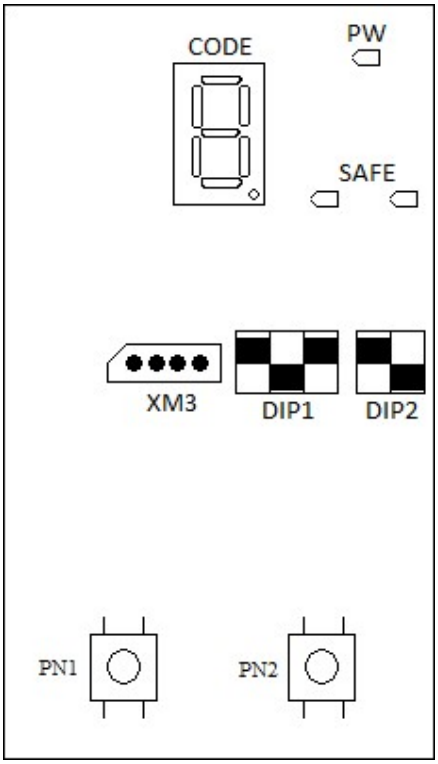


5.3 Alimentazione elettrica (morsetti 1-2)

Prima di alimentare il dispositivo, verificare che la tensione di alimentazione corrisponda a quanto riportato sull'etichetta di identificazione.

Verificare che alimentando il regolatore, si accenda il led verde frontale, denominato "PW".

Funzionamento del DIP2
Sollevare il frontalino basculante trasparente.
Sarà così possibile accedere ai dip switch DIP1 e DIP2.
Assicurarsi che entrambi i dip del dip switch DIP2 siano in posizione 1 (ON).



PN2: se premuto, viene visualizzato sul dispaly del master l'ultimo codice di allarme verificatosi da quando il regolatore è stato alimentato l'ultima volta. Appena si dà alimentazione, questo codice è impostato al valore di default '0'.

DIP2, PIN1: dip switch per il test del cavo
- posizione OFF= test
- posizione ON= normale

DIP2, PIN2: dip switch per il test dell'eletrodo di misura
- posizione OFF= test
- posizione ON= normale

Riabbassare il frontalino basculante trasparente.

5.4 - Collegamento tra sonda e regolatore (morsetti 10-11-12-13-14)

La connessione tra la sonda e il regolatore deve essere effettuata con un cavo schermato a 4 conduttori con sezione 0.25 mm^2 oppure 0.50 mm^2; il cavo deve essere adeguato alla temperatura dell'ambiente in cui viene utilizzato, in particolare nelle vicinanze della caldaia.

La lunghezza del cavo non deve superare i 30 m.

Come si vede dallo schema di cui sopra, è necessario cablare l'estremità del cavo ad un connettore DIN femmina, fornito in dotazione (cod. 999-027-00), per poter poi effettuare il collegamento con la testa della sonda in un modo veloce e sicuro.

Lo schermo del cavo di collegamento costituisce una terra funzionale, non una terra di protezione.

Collegare lo schermo del cavo come indicato nello schema di cui sopra.

Ai morsetti #13 e #14 del regolatore non deve essere connesso alcun filo di terra di protezione: ciò potrebbe creare anelli di massa indesiderati, ridurre le prestazioni del regolatore, ed eventualmente danneggiarlo.

5.5 - Collegamanto utenze (morsetti 4-5-6 e 7-8-9)

Il regolatore rende disponibili in uscita 2 contatti in scambio, puliti e indipendenti, che possono essere utilizzati per il controllo del bruciatore della caldaia e per dare l'allarme.

I contatti sono in chiusura in caso di non allarme; in apertura in caso di allarme (sicurezza positiva).

Uno schema di impiego consigliato è al § 6.4.

Se il carico ai contatti dei relè è induttivo, la commutazione dei contatti produce picchi di tensione che possono influenzare in funzionamento dei sistemi di misura e controllo.

L'utilizzatore dovrà pertanto impiegare appropriati soppressori di scariche (surge arrester) ai contatti, in funzione del carico che applicherà ai contatti stessi.

6 - Funzionamento

Il regolatore misura continuamente due diverse resistenze elettriche: la prima tra l'elettrodo di misura e la massa della caldaia; la seconda tra l'elettrodo di riferimento e la massa della caldaia.

Analizzando il valore di queste 2 resistenze, il dispositivo è in grado di determinare se c'è acqua a contatto dell'elettrodo di misura e se la sonda ha una perdita di isolamento.

Periodicamente il dispositivo effettua test diangnostici, atti a verificare la funzionalità nelle misure ohmiche all'elettrodo di riferimento e all'elettrodo di misura; e per verificare l'integrità del cavo di collegamento.

L'analisi di tutte le misure porta alla determinazione dello stato del sistema: se si è in una delle condizioni di allarme riconosciute, il dispositivo si porta nella condizione sicura di allarme.

Essendo il sistema a sicurezza positiva, in condizione di non allarme i 2 relè interni sono ON, i led frontali rossi sotto la scritta "SAFE" sono entrambi accesi e il display a 8 segmenti visualizza '0'.

In caso di allarme entrambi i relè cadono, entrambi i led frontali rossi si spengono, il display visualizza un codice diverso da '0' corrispondente alla situazione di allarme e i contatti in scambio possono essere usati da una logica esterna.

Elenco dei vari codici di allarme con la corrispondente situazione:

Codice	Situazione
0	nessun allarme, assenza d'acqua al massimo livello
1	presenza acqua al massimo livello
2	cavo interrotto o non comunicazione con sonda
3	funzionamento anomalo
4	resistenza cavo di collegamento sonda-regolatore troppo elevata
6	cavo interrotto o non comunicazione con sonda
7-9	funzionamento anomalo
8	presenza acqua all'elettrodo di riferimento o suo sporcamento
C	verifica della resistenza interna da 100 ohm non nei limiti
F	cavo interrotto o non comunicazione con sonda
H	funzionamento anomalo rilevato dal secondo processore

6.2 - Possibili soluzioni a guasti e malfunzionamenti

Codici 1	Verificare che il livello dell'acqua sia effettivamente superiore al livello massimo stabilito. Se il livello è inferiore e permane la situazione di allarme, verificare i collegamenti con la sonda, e l'integrità della sonda stessa e dell'elettrodo.
Codici 2, 6, F	Verificare il collegamento con la sonda; se è stato eseguito come da schema riportato al §5.2 e permane la situazione di allarme, significa che c'è un'interruzione del collegamento. Verificare che entrambi i pin del DIP2 siano in posizione N, altrimenti spostare i selettori dalla posizione T alla posizione N.
Codici 3, 7, 9, C, H	Si tratta di un possibile guasto all'interno del regolatore, relativo all'autodiagnosi; se permane, è necessario sostituire il regolatore.
Codice 4	Verificare il collegamento tra sonda e regolatore. Il cavo è troppo lungo o ha resistenza troppo elevata.
Codice 8	Verificare che la conducibilità dell'acqua della caldaia sia entro i limiti di conducibilità del regolatore usato; se è al di fuori, è necessario sostituire il regolatore con uno adatto alla conducibilità dell'acqua usata. Se la conducibilità è nei limiti, è necessario smontare la sonda dalla caldaia (seguendo le istruzioni di cui al §4), e verificare che non ci siano incrostazioni o depositi sulla sonda stessa. Se non ci sono depositi, potrebbe essersi verificata una infiltrazione nella testa della sonda; in questo caso è necessario sostituire la sonda.

Se dopo aver fatto tutte le verifiche previste per ogni situazione di allarme, la condizione permane, oppure si presentano situazioni diverse da quelle previste, sarà necessario sostituire l'intero accessorio di sicurezza (regolatore + sonda), e contattare il nostro servizio tecnico.

E' possibile verificare manualmente alcune funzionalità importanti del regolatore.
Questa verifica deve essere effettuata soltanto da personale tecnico qualificato (v. §4).

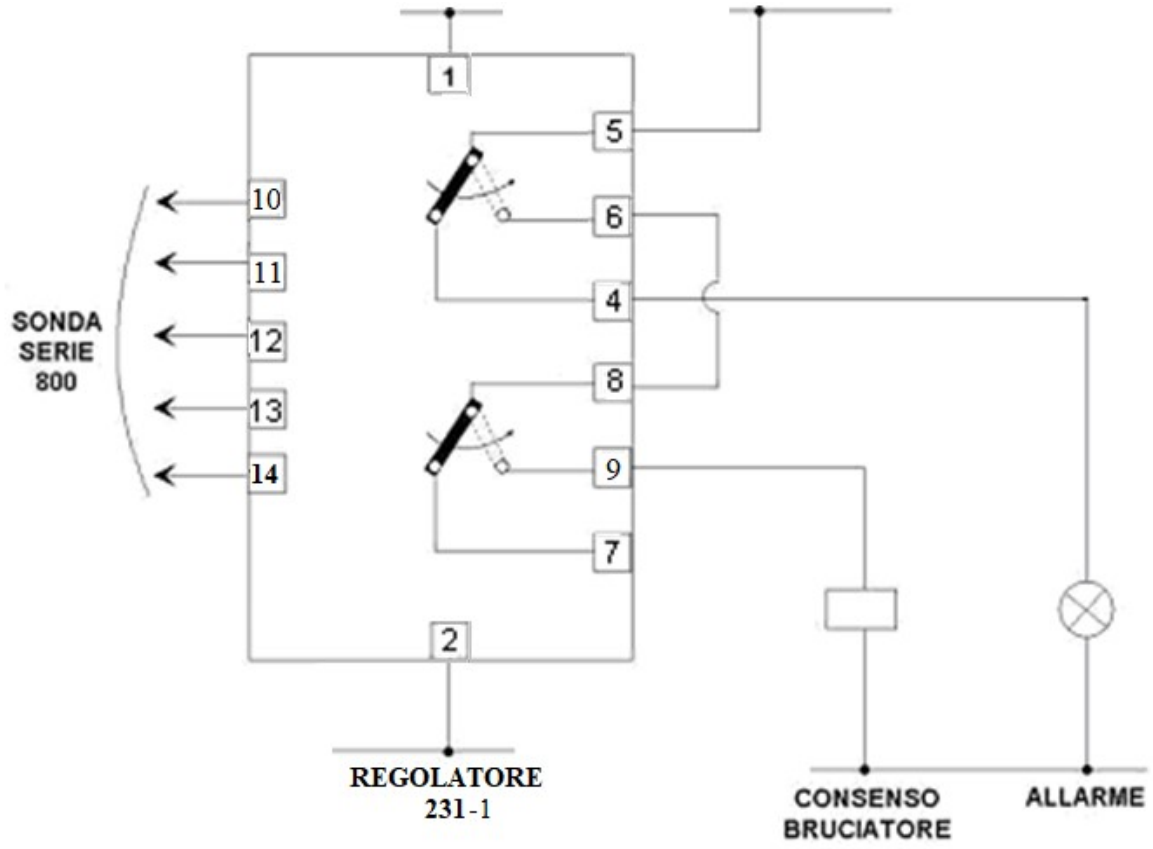
Attenzione: considerare attentamente che nel corso di questi test manuali, viene generato volutamente un allarme e la caldaia andrà in blocco; prendere tutte le precauzioni necessarie affinchè ciò non comporti rischi per il funzionamento della caldaia stessa, per le persone, o per l'ambiente.
Prima di effettuare qualsiasi operazione o test sull'accessorio di sicurezza è necessario scaricarsi elettrostaticamente per evitare di danneggiare l'apparecchiatura.

Per effettuare queste verifiche, è necessario sollevare il frontalino basculante trasparente.

Sarà così possibile accedere ai dip switch DIP1 e DIP2.
Con il livello dell'acqua superiore al minimo di sicurezza, e perciò con il regolatore in stato di sicurezza, ponendo PIN1 del DIP2 in posizione di test (=OFF), viene provocata un'interruzione del cavo di collegamento tra la sonda e il regolatore. Viene visualizzato l'allarme 'F' sul display di destra, con commutazione del relè di allarme.
Terminato il test, rimettere il PIN1 del DIP2 in posizione Normal (=ON). Il regolatore torna in stato di non allarme entro 10 secondi.
Se esiste un circuito di blocco caldaia con riarmo manuale, la caldaia richiederà l'intervento di un operatore per poter ripartire.
Ponendo PIN2 del DIP2 in posizione di test (=OFF), viene provocata una interruzione del cavo di collegamento tra l'elettrodo di misura e il regolatore. Viene visualizzato l'allarme '2' sul display di destra, con commutazione del relè di allarme.
Terminato il test, rimettere il PIN1 del DIP2 in posizione Normal (=ON). Il regolatore torna in stato di non allarme entro 10 secondi.
Anche in questo caso, se esiste un circuito di blocco caldaia con riarmo manuale, la caldaia richiederà l'intervento di un operatore per poter ripartire.
Riabbassare il frontalino basculante trasparente.
Se almeno uno dei 2 test manuali di cui sopra non è portato a termine con successo, come descritto, significa che il regolatore non funziona correttamente, e deve pertanto essere sotituito ed avviato alla riparazione, secondo le procedure operative di impianto previste.

6.4 - Esempio di collegamento

Un esempio tipico di impiego per la serie 231-1 è il seguente:



7 - Manutenzione

Il regolatore non richiede particolare manutenzione o service.

La sonda deve essere pulita e ispezionata una volta all'anno.

Per acque aggressive, verificare periodicamente l'elettrodo di misura; eventualmente pulirlo con una carta abrasiva fine, smontare la sonda comunque ad impianto fermo, come descritto al §4.

Saltuariamente, testare la funzionalità dell'apparecchiatura simulando manualmente una possibile condizione di allarme (es. scollegando il connettore) e verificando la corretta risposta dell'apparecchiatura stessa.

Dopo la manutenzione rimontare il tutto seguendo le istruzioni dal punto §***4*** del presente manuale di istruzioni.

8 - Dismissione

Affidare questa operazione a personale qualificato.

Le apparecchiature inutilizzabili devono essere smaltite con una procedura che garantisca la sicurezza.

9 - Accessori

Di serie vengono forniti:

– connettore DIN 43650A femmina cod. 999-027-00, quale parte terminale del cavo di collegamento tra la sonda e il regolatore
– guarnizione di tenuta in rame

Optional a richiesta:
– elettrodo diametro 10 mm, con lunghezza 500 mm (cod. 999-800-05)
– elettrodo diametro 10 mm, con lunghezza 1000 mm (cod. 999-800-10)

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

Summary

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

2. Equipment identification and ordering code

Ordering codes:

- 230-11Y-0Z low level safety controller with diagnostic

Code	Characteristics	Power supply
230-110-09	Conductivity>100 µS/cm	24V a.c.
230-110-08	Conductivity>100 µS/cm	230Va.c.
230-112-09	Conductivity 0.5 ÷ 20 µS/cm	24V a.c.
230-112-08	Conductivity 0.5 ÷ 20 µS/cm	230Va.c.

- 231-11Y-0Z high level safety controller with diagnostic

Code	Characteristics	Power supply
231-110-09	Conductivity>100 µS/cm	24V a.c.
231-110-08	Conductivity>100 µS/cm	230Va.c.
231-112-09	Conductivity 0.5 ÷ 20 µS/cm	24V a.c.
231-112-08	Conductivity 0.5 ÷ 20 µS/cm	230Va.c.

- 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

3. Introduction

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.

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.

3.3 Relevant Standards and Directives

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.

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).

4 Planning

4.1 System constraint and SIL loop determination

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).

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)

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.

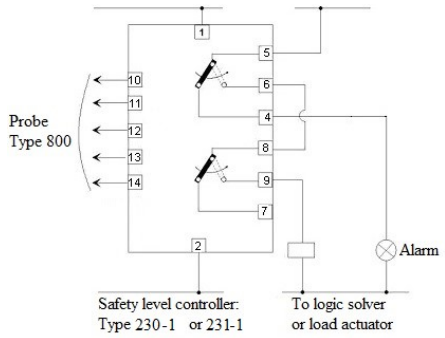
Contact MMT experts in case of any doubts on SFF calculation constraints.

5 Assumptions

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.

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.

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

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

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.

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.

11 Proof Test

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 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