CERTIFICADO ◆ 인증서 ◆ CERTIFICATO ◆ CERTIFICATE ◆ 認証書 ◆ 认证证书 ◆ ZERTIFIKAT

CERTIFICATO

CERTIFICATE

Sicurezza Funzionale
Functional Safety

Certificato No.: *Certificate No.:*	**TUV IT 26 SIL 0768 A**
Nome ed indirizzo del fabbricante: *Name and address of manufacturer:*	G.M. International S.p.A. Via G. Mameli, 53-55 20852 Villasanta (MB) Italy
Sede/i di produzione: *Address of production site:*	Via G. Mameli, 53-55 20852 Villasanta (MB) Italy
Prodotto: *Product:*	SIL 2 Temperature Trip Amplifier with Zero/Span Trimmers for DIN-Rail and Power Bus
Modello/tipo: *Model/type:*	D5274S
Rapporto Tecnico: *Technical report:*	**TUV SIL 722407802 A M009**

Si certifica che il componente E/EE/EP / SIS soddisfa, per la(le) Funzione(i) di Sicurezza riportata(e) nell'allegato al presente certificato, i requisiti della(e) norma(e):

We herewith certify that the E/EE/PE component / SIS meets the requirements of the following standard(s) for the Safety Function(s) reported in the annex to this certificate:

IEC 61508-2:2010

Data 1a emissione: **29-07-2026**
First Issue date:

Data emissione: **29-07-2026**
Issue date:

Data di scadenza: **28-07-2029**
Expiry date:

00077

TÜV Italia S.r.l.

Alberto Carelli
Industry Service – Real Estate & Infrastructure Division
Managing Director

Allegato al Certificato
n° TUV IT 26 SIL 0768 A

1. Safety Function(s):

In the Functional Safety analysis of a single D5274S or of two D5274S with their channels in 1oo2 architecture, three different Safety Functions have been considered because of three different output types for each channel:

- when the 4 ÷ 20 mA analog (source or sink) current output configuration is used;
- when a single alarm trip amplifier is used, select “NO Contact position in alarm = Open” and “Type alarm Low or High or Window or Burnout Repeater (in case of burnout fault)” and consider to drive a NE load (by means of NO contact) or a ND load (by means of NC contact) so that, in case of trip, the NE load is de-energized (because NO contact is open) or the ND load is energized (because NC contact is closed);
- when two alarm trip amplifiers are used in 1oo2 architecture, program both trip amplifiers with the same setup, always selecting “NO Contact position in alarm = Open” and “Type alarm Low or High or Window or Burnout Repeater (in case of burnout fault)”, and consider to drive a NE load (by two NO contacts in series connection) or a ND load (by two NC contacts in parallel connection) so that, in case of trip, the NE load is de-energized (because series of NO contacts is open) or the ND load is energized (because parallel of NC contacts is closed).

For all following Safety Functions, the following failure behaviors are in common:

- Fail “No effect”: failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure. When calculating the SFF, this failure mode is not taken into account;
- Fail “Not part”: failure mode of a component which is not part of the Safety Function but is part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account.

1.1. Application with single D5274S

Operating with 4 ÷ 20 mA analog (source or sink) current output configuration (enabling detection of Burnout fault; with the alarm trip amplifiers considered as not part of the Safety Function; *with Zero and Span Trimmers do not enabled for output current calibration because they must not be used in Functional Safety applications*), the failure behavior of a single channel is defined by the following definitions:

- Fail Safe State: it is defined as the analog output going to 0 mA due to module shutdown;
- Fail Safe: failure mode that causes the module / (sub)system to go to the defined Fail-Safe state without a demand from the process;
- Fail Dangerous: failure mode that does not respond to a demand from the process or deviates the output current by more than 5% (= 1 mA) of full scale range (= 20 mA) respect to the correct value;

Allegato al Certificato
n° TUV IT 26 SIL 0768 A

- Fail High: failure mode that causes the output signal to go above the maximum output current (> 20 mA). This limit value can be programmed by the user, but in this analysis it is set to 20 mA. Assuming that the application program in the safety logic solver is configured to detect High failure, this failure has been classified as a dangerous detected (DD) failure;
- Fail Low: failure mode that causes the output signal to go below the minimum output current (< 4 mA). This limit value can be programmed by the user, but in this analysis it is set to 4 mA. Assuming that the application program in the safety logic solver is configured to detect Low failure, this failure has been classified as a dangerous detected (DD) failure;
- Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that analog output signal is forced below the minimum output current < 4mA (as Fail Low) or above the maximum output current > 20mA (as Fail High).

Operating with a single alarm trip amplifier (enabling detection of Burnout fault; with other alarm trip amplifier and analog current output considered as not part of the Safety Function), the failure behavior of a single channel is defined by the following definitions:

- Fail-Safe State: is defined as the output relay being de-energized or NO contact remaining open (de-energizing the NE load) or NC contact remaining closed (energizing the ND load) (the user can program the trip point value, according to the input measured value, at which the output relay must be de-energized);
- Fail Safe: failure mode that causes the module / (sub)system to go to the defined Fail-Safe state without a demand from the process;
- Fail Dangerous: failure mode that leads to a measurement error more than 5% of the correct value and therefore it has not the potential to respond to a demand from the process (i.e. being unable to go to the defined fail-safe state), so that the output relay remains energized or NO contact fixes closed or NC contact fixes open;
- Fail Dangerous Detected: it’s a dangerous failure which has been detected from module internal diagnostic so that output relay is forced to be de-energized (that is to Fail-Safe state), with NO contact open or NC contact closed.

Operating with two alarm trip amplifiers used in 1oo2 architecture (enabling detection of Burnout fault; with the analog current output considered as not part of the Safety Function), the failure behavior of a single channel is defined by the following definitions:

- Fail-Safe State: is defined as the output relays being de-energized or NO series contacts remaining open (de-energizing the NE load) or NC parallel contacts remaining closed (energizing the ND load) (user must program for both alarm amplifiers the same trip point in according with input measured value, at which both output relays must be de-energized);

Allegato al Certificato
n° TUV IT 26 SIL 0768 A

- Fail Safe: failure mode that causes the module / (sub)system to go to the defined Fail-Safe state without a demand from the process;
- Fail Dangerous: failure mode that leads to a measurement error more than 5% of the correct value and therefore it has not the potential to respond to a demand from the process (i.e. being unable to go to the defined fail-safe state), so that the output relays remain energized or NO series contacts fix closed or NC parallel contacts fix open;
- Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that output relays are forced to be de-energized (that is to Fail-Safe state), with NO series contacts open or NC parallel contacts closed.

1.2. Application with two D5274S having their channels in 1oo2 architecture

Two D5274S have their channels in 1oo2 architecture (with β factor of common cause failure of 5%), that is two input channels with the same type of sensor and two output channels with the same configuration.

For each channel operating with 4 ÷ 20 mA analog (source or sink) current output configuration (enabling detection of Burnout fault; with the alarm trip amplifiers considered as not part of the Safety Function; *with Zero and Span Trimmers do not enabled for output current calibration because they must not be used in Functional Safety applications*), the failure behavior of 1oo2 channel architecture is defined by the following definitions:

- Fail Safe State: it is defined as an analog output going to 0 mA due to module shutdown;
- Fail Safe: failure mode that causes the module / (sub)system to go to the defined Fail-Safe state without a demand from the process;
- Fail Dangerous: failure mode that does not respond to a demand from the process or deviates both output currents by more than 5% (= 1 mA) of full scale range (= 20 mA) respect to the correct value;
- Fail High: failure mode that causes an output signal to go above the maximum output current (> 20 mA). This limit value can be programmed by the user, but in this analysis it is set to 20 mA. Assuming that the application program in the safety logic solver is configured to detect High failure, this failure has been classified as a dangerous detected (DD) failure;
- Fail Low: failure mode that causes an output signal to go below the minimum output current (< 4 mA). This limit value can be programmed by the user, but in this analysis it is set to 4 mA. Assuming that the application program in the safety logic solver is configured to detect Low failure, this failure has been classified as a dangerous detected (DD) failure;
- Fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that an analog output signal is forced below the minimum output current < 4mA (as Fail Low) or above the maximum output current > 20mA (as Fail High).

Allegato al Certificato
n° TUV IT 26 SIL 0768 A

For each channel operating with a single alarm trip amplifier (enabling detection of Burnout fault; with other alarm trip amplifier and analog current output considered as not part of the Safety Function), the failure behavior of 1oo2 channel architecture is defined by the following definitions:

- Fail-Safe State: is defined as an output relay being de-energized or a NO contact remaining open (de-energizing the NE load) or a NC contact remaining closed (energizing the ND load) (the user can program the trip point value, according to the input measured value, at which the output relay must be de-energized);
- Fail Safe: failure mode that causes the module / (sub)system to go to the defined Fail-Safe state without a demand from the process;
- Fail Dangerous: failure mode that leads to a measurement error more than 5% of the correct value and therefore it has not the potential to respond to a demand from the process (i.e. being unable to go to the defined fail-safe state), so that both output relays remain energized or both NO contacts fix closed or both NC contacts fix open;
- Fail Dangerous Detected: it’s a dangerous failure which has been detected from module internal diagnostic so that an output relay is forced to be de-energized (that is to Fail-Safe state), with a NO contact open or a NC contact closed.

For each channel operating with two alarm trip amplifiers used in 1oo2 architecture (enabling detection of Burnout fault; with the analog current output considered as not part of the Safety Function), the failure behavior of 1oo2 channel architecture is defined by the following definitions:

- Fail-Safe State: is defined as output relays of a channel being de-energized or NO series contacts of a channel remaining open (de-energizing the NE load) or NC parallel contacts of a channel remaining closed (energizing the ND load) (user must program for both alarm amplifiers the same trip point in according with input measured value, at which both output relays must be de-energized);
- Fail Safe: failure mode that causes the module / (sub)system to go to the defined Fail-Safe state without a demand from the process;
- Fail Dangerous: failure mode that leads to a measurement error more than 5% of the correct value and therefore it has not the potential to respond to a demand from the process (i.e. being unable to go to the defined fail-safe state), so that output relays of both channels remain energized or NO series contacts of both channels fix closed or NC parallel contacts of both channels fix open;
- Fail Dangerous Detected: it’s a dangerous failure which has been detected from module internal diagnostic so that output relays of a channel are forced to be de-energized (that is to Fail-Safe state), with NO series contacts of a channel open or NC parallel contacts of a channel closed.

Allegato al Certificato
n° TUV IT 26 SIL 0768 A

2. Main Technical Features

Item name	Proof test time (T_{Proof})	Configuration	Allowed SIL	Allowed Systematic SIL	Notes
D5274S	7,5 years	Analog current output (source or sink mode)***	SIL2*	SIL2	none
	20 years		SIL2**		none

(*)Considering the products do not contribute more than 10% of total SIF dangerous failure
(**)Considering the products contribute more than 10% of total SIF dangerous failure
(***)Low demand mode of operation

Item name	Proof test time (T_{Proof})	Configuration	Allowed SIL	Allowed Systematic SIL	Notes
D5274S	4 years	Single alarm trip amplifier & relay output***	SIL2*	SIL2	none
	20 years		SIL2**		none

(*)Considering the products do not contribute more than 10% of total SIF dangerous failure
(**)Considering the products contribute more than 10% of total SIF dangerous failure
(***)Low demand mode of operation

Item name	Proof test time (T_{Proof})	Configuration	Allowed SIL	Allowed Systematic SIL	Notes
D5274S	10,5 years	1oo2 architecture of alarm trip amplifiers & relay outputs***	SIL2*	SIL2	none
	20 years		SIL2**		none

(*)Considering the products do not contribute more than 10% of total SIF dangerous failure
(**)Considering the products contribute more than 10% of total SIF dangerous failure
(***)Low demand mode of operation

Two D5274S modules in HFT = 1 configuration, having their channels in 1oo2 architecture (with β factor of common cause failure = 5%) with input channels have the same type of sensor and two equal output channels (each as: analog current OR single alarm trip amplifier & relay OR 1oo2 architecture of alarm trip amplifiers & relays) with the same configuration. Considering that both equivalent sensors measure the same physical quantity and give two equivalent input signals to two D5274S, the couple of two Type B modules can operate in High demand mode because having HFT = 1 (being two channels completely independent each other except for common cause failure) with functional safety level up to SIL 2 also for Systematic capability.

3. Notes

A copy of technical report n.: TUV SIL 722407802 A M009 Rev.0 is given to the manufacturer.

This annex is an integral part of the certificate TUV IT 26 SIL 0768 A

Milan, 29-07-2026