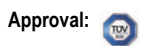


# SAFETY MANUAL

## SIL 2 Load Cell/Strain Gauge Bridge Isolating Converter DIN-Rail, Power Bus and Termination Board Model D6264S

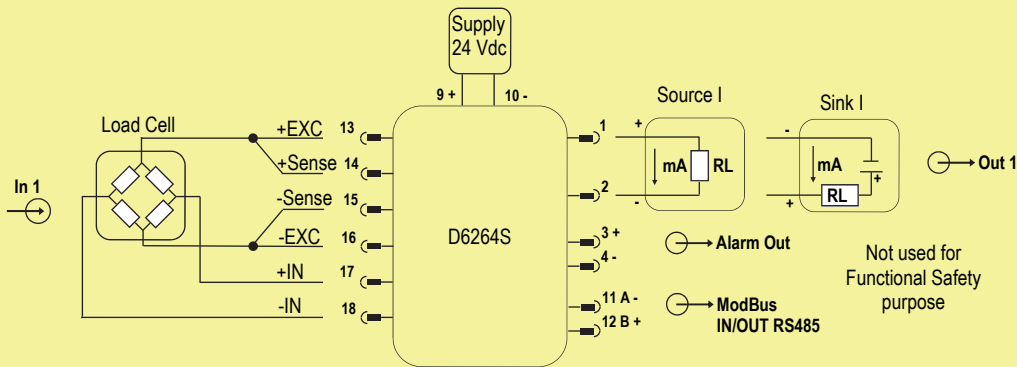


Approval: TÜV Certificate No. C-IS-722160171, SIL 2 conforms to IEC61508:2010 Ed.2 .  
SIL 3 Functional Safety TÜV Certificate conforms to IEC61508:2010 Ed.2, for Management of Functional Safety.

Reference must be made to the relevant sections within the instruction manual ISM0474 and  
ISM0154 (for SWC5090 Configuration Software instruction manual),  
which contain basic guides for the installation and configuration of the equipment.



## Application for D6264S - with 4-20 mA current source (or sink) output.

**Description:**

By means of SWC5090 Configuration Software, as user interface on PC to communicate with the module, select: Input/Output window with Type "4-20 mA Sink" or "4-20 mA Source". The module is powered by connecting 24 Vdc power supply to Pins 9 (+ positive) - 10 (- negative). The green LED is lit in presence of supply power.

Connect load cell or strain gauge bridge voltage supply at terminal "13" positive and terminal "16" negative.

Connect load cell or strain gauge bridge voltage sensing supply at terminal "14" positive and terminal "15" negative.

If load cell or strain gauge bridge has no internal voltage sensing capability always connect terminal "14" to terminal "13" and terminal "15" to terminal "16"; for better performance connect the wire at the end of the line near the load cells.

Connect load cell or strain gauge bridge output signal at terminal "17" positive and terminal "18" negative.

Connect current source mode positive output at terminal "1" and negative output at terminal "2" or current sink mode positive output at terminal "3" and negative output at terminal "4" (output can be used only one type at a time, not contemporary). Alarm output and ModBus communication are only used for service purpose (not for Functional Safety purpose).

**Safety Function and Failure behavior:**

D6264S is considered to be operating in Low Demand mode, as a Type B module, having Hardware Fault Tolerance (HFT) = 0.

The failure behavior of D6264S module with 4-20 mA current source (or sink) output is described by the following definitions:

- fail-Safe State: it is defined as the 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 % ( $\pm 0.8$  mA) of full span;
- fail High: failure mode that causes the output signal to go above the maximum output current ( $> 20$  mA). Assuming that the application program in the Safety logic solver is configured to detect High failures, they have been classified as Dangerous Detected (DD) failures.
- fail Low: failure mode that causes the output signal to go below the minimum output current ( $< 4$  mA). Assuming that the application program in the Safety logic solver is configured to detect Low failures, they have been classified as Dangerous Detected (DD) failures.
- fail Dangerous Detected: it's a dangerous failure which has been detected from module internal diagnostic so that output signal is forced below the minimum output current  $< 4$  mA (as Fail Low) or above the maximum output current  $> 20$  mA (as Fail High).
- fail "No effect": failure mode of a component that plays a part in implementing the safety function but 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 part of the circuit diagram and is listed for completeness; When calculating the SFF this failure mode is not taken into account.

As the module has been evaluated in accordance with Route 2H (proven-in-use) of the IEC 61508:2010, Diagnostic Coverage DC  $\geq 60\%$  is required for Type B elements.

Being HFT = 0, in Low Demand mode the maximum achievable functional safety level is SIL 2.

Failure rate data: taken from Siemens Standard SN29500.

**Failure rate table:**

Failure category	Failure rates (FIT)
$\lambda_{dd}$ = Total Dangerous Detected failures	188.85
$\lambda_{du}$ = Total Dangerous Undetected failures	47.98
$\lambda_{sd}$ = Total Safe Detected failures	0.00
$\lambda_{su}$ = Total Safe Undetected failures	100.11
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	336.94
MTBF (safety function, single channel) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	339 years
$\lambda_{no\ effect}$ = "No effect" failures	254.16
$\lambda_{not\ part}$ = "Not Part" failures	65.70
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	656.80
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	174 years

**Failure rates table according to IEC 61508:2010 Ed.2:**

$\lambda_{sd}$	$\lambda_{su}$	$\lambda_{dd}$	$\lambda_{du}$	DC	SFF
0.00 FIT	100.11 FIT	188.85 FIT	47.98 FIT	79.74%	85.76%

where DC means the diagnostic coverage for the input sensor by module internal diagnostic circuits and by Safety logic solver. This type "B" system, operating in Low Demand mode with HFT = 0, has got DC = 79.74 %  $\geq 60$  % as required by Route 2H evaluation (proven-in-use) of the IEC 61508:2010.

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes  $\leq 10\%$  of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 4 years
PFDavg = 2.12 E-04 Valid for SIL 2	PFDavg = 8.48 E-04 Valid for SIL 2

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes  $> 10\%$  of total SIF dangerous failures:

T[Proof] = 20 years
PFDavg = 4.24 E-03 - Valid for SIL 2

SC 3: Systematic capability SIL 3.



## Testing procedure at T-proof

The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic.

This means that it is necessary to specify how dangerous undetected faults, which have been noted during the FMEDA, can be revealed during the proof test.

The test on **D6264S with 4-20 mA current source (or sink) output** consists of the following steps:

**Proof test 1** (to reveal approximately 50 % of possible Dangerous Undetected failures in the converter)

Steps	Action
1	Bypass the Safety PLC or take any other appropriate action to avoid a false trip.
2	Set the input load cell to the High (see Safety Function definition) voltage signal and verify that the related analog output current reaches the corresponding value. This test is for voltage compliance problems, such as a low power supply voltage or an increased wiring resistance, and for other possible failures .
3	Set the input load cell to the Low (see Safety Function definition) voltage signal and verify that the related analog output current reaches the corresponding value. This tests is for possible quiescent current related failures.
4	Restore the loop to full operation.
5	Remove the bypass from the Safety PLC or restore normal operation.

**Proof test 2** (to reveal approximately 99 % of possible Dangerous Undetected failures in the converter)

Steps	Action
1	Bypass the Safety PLC or take other appropriate action to avoid a false trip.
2	Perform steps 2 and 3 of <b>Proof Test 1</b> .
3	Perform a two-point calibration (i.e. down and full scale) of the connected load cell and verify that, forcing some values of the input range, the output current related values are within the specified accuracy (5 % ( $\pm 0.8$ mA) of full span) as defined in the Safety Function. This requires that the input load cell has already been tested without the converter and it does not contain any dangerous undetected failures.
4	Restore the loop to full operation.
5	Remove the bypass from the Safety PLC or restore normal operation.

The test on **D6264S with Alarm output** consists of the following steps:

**Proof test** (to reveal approximately 99 % of possible Dangerous Undetected failures in the converter)

Steps	Action
1	Bypass the Safety PLC or take any other appropriate action to avoid a false trip.
2	According to Alarm Function setting, force the input load cell to a voltage signal bigger than high limit for alarm tripping and verify that the alarm photo MOS is open because alarm output changes from normally energize state to de-energize to trip state .
3	According to Alarm Function setting, force the input load cell to a voltage signal smaller than low limit for alarm tripping and verify that the alarm photo MOS is open because alarm output changes from normally energize state to de-energize to trip state .
4	Restore the loop to full operation.
5	Remove the bypass from the Safety PLC or restore normal operation.