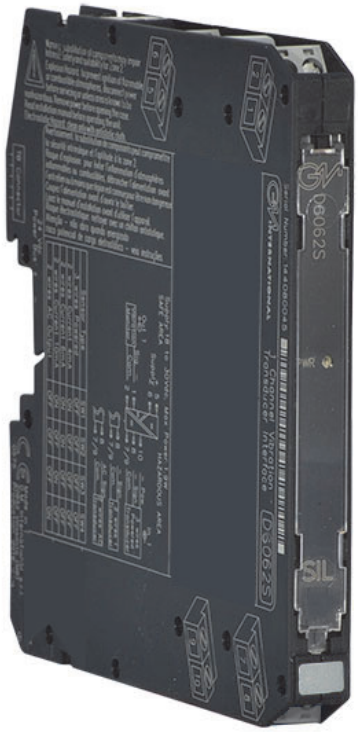


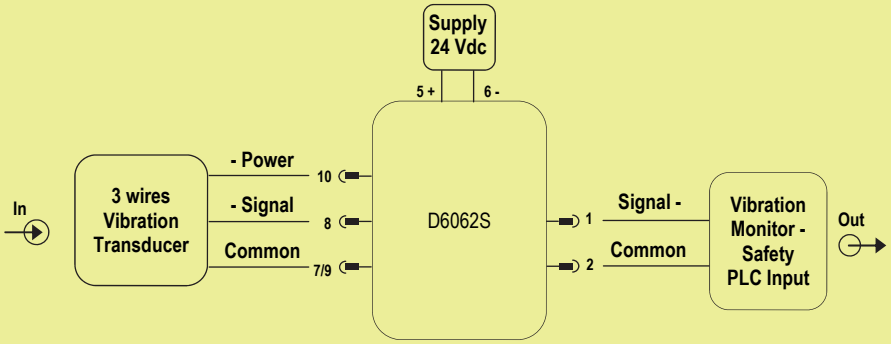
SAFETY MANUAL

SIL 2 Vibration Transducer Interface, DIN-Rail and Termination Board, Model D6062S

Reference must be made to the relevant sections within the instruction manual ISM0417, which contain basic guides for the installation of the equipment.

gmi technology for safety

1st Application for D6062S, with 3 wires powered transducer input



Description:

For this application, set the internal dip-switches in the following mode (see instruction manual for more information):

Dip-switch position (D6062S)	1	2	3	4
3 wires transducer	OFF	OFF	OFF	OFF

The D6062S module is supplied (with 18 to 30Vdc supply voltage) at Pins 5 (+) – 6 (-). The green LED is lit in presence of supply power.
The input transducer supply current is applied between Pins 7/9-10 (Common, -Power) and the input transducer signal (DC or AC) is applied between Pins 8-7/9 (-Signal, Common).
When a DC input transducer is used, a 0 to -20Vdc input signal is applied. For AC transducers, a sinusoidal signal is applied (0 to 20Vpp, DC to 20kHz) together with a -10Vdc offset.
For DC signals, the input signals (0 to -20Vdc) is identically repeated at output Pins 1-2 (-Signal, Common); for AC signals, the AC component of the input signal (0 to 20Vpp, DC to 20kHz) is identically repeated at output Pins 1-2, while the -10Vdc offset is not repeated at the output pins.

Safety Function and Failure behavior:

D6062S is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour is described by the following definitions:

- □ Fail-Safe State: is defined as the output going Low or High, considering that the safety logic solver can convert the Low or High fail (dangerous detected) to the fail-safe state.
- □ Fail Safe: a 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 (i.e. being unable to go to the defined fail-safe state) or deviates the output voltage by more than 5 % of full span (> ± 1 Vdc).
- □ Fail High: a failure mode that causes the output signal to go below the maximum negative voltage (< -20 Vdc). Assuming that the application program in the safety logic solver is configured to detect High failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ Fail Low: a failure mode that causes the output signal to go above the minimum negative voltage (> -0.5 Vdc). Assuming that the application program in the safety logic solver is configured to detect Low failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ 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 because the output voltage is deviated by less than 5 % of full span (< ± 1 Vdc). When calculating the SFF, this failure mode is not taken into account.
- □ Fail "Not part": failure mode of a component that 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.

Failure rate date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	160.84
λ_{du} = Total Dangerous Undetected failures	71.56
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**232.40**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**491 years**
$\lambda_{no\ effect}$ = "No Effect" failures	269.70
$\lambda_{not\ part}$ = "Not Part" failures	22.70
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**524.80**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**217 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_D
0.0 FIT	0.00 FIT	160.84 FIT	71.56 FIT	69.21%	69.21%

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

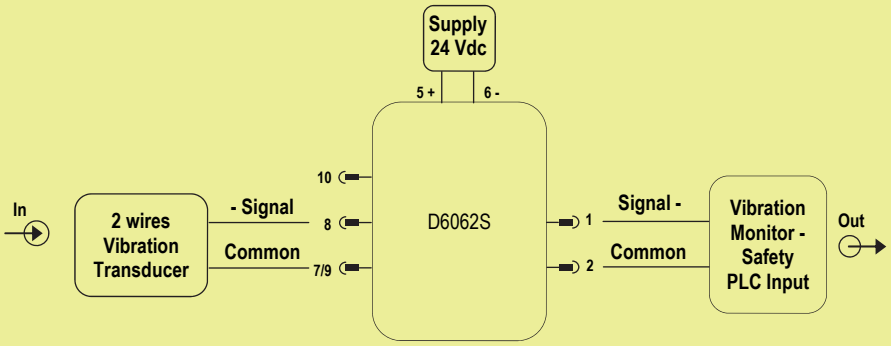
T[Proof] = 1 year	T[Proof] = 3 years
PFDavg = 3.15E-04 Valid for **SIL 2**	PFDavg = 9.46E-04 Valid for **SIL 2**

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 = 6.31E-03 Valid for **SIL 2**

Systematic capability SIL 3.

2nd Application for D6062S, with 2 wires powered transducer input



Description:

For this application, set the internal dip-switches in the following mode (see instruction manual for more information):

Dip-switch position(D6062S)	1	2	3	4
2 wires transducer (4 mA)	ON	OFF	OFF	OFF
2 wires transducer (6 mA)	ON	ON	OFF	OFF
2 wires transducer (10 mA)	ON	OFF	ON	OFF

The D6062S module is supplied (with 18 to 30Vdc supply voltage) at Pins 5 (+) – 6 (-). The green LED is lit in presence of supply power.
The input transducer voltage signal (0 to -20Vdc) is applied between Pins 8-7/9 (-Signal, Common). The input transducer supply current is imposed to 4, 6 or 10mA by means of the internal DIP-switches, as shown above.
The input signal (0 to -20Vdc) is identically repeated at output Pins 1-2 (-Signal, Common).

Safety Function and Failure behavior:

D6062S is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour is described by the following definitions:

- □ Fail-Safe State: is defined as the output going Low or High, considering that the safety logic solver can convert the Low or High fail (dangerous detected) to the fail-safe state.
- □ Fail Safe: a 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 (i.e. being unable to go to the defined fail-safe state) or deviates the output voltage by more than 5 % of full span (> ± 1 Vdc).
- □ Fail High: a failure mode that causes the output signal to go below the maximum negative voltage (< -20 Vdc). Assuming that the application program in the safety logic solver is configured to detect High failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ Fail Low: a failure mode that causes the output signal to go above the minimum negative voltage (> -0.5 Vdc). Assuming that the application program in the safety logic solver is configured to detect Low failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ 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 because the output voltage is deviated by less than 5 % of full span (< ± 1 Vdc). When calculating the SFF, this failure mode is not taken into account.
- □ Fail "Not part": failure mode of a component that 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.

Failure rate date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	161.96
λ_{du} = Total Dangerous Undetected failures	75.95
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**237.91**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**479 years**
$\lambda_{no\ effect}$ = "No Effect" failures	274.79
$\lambda_{not\ part}$ = "Not Part" failures	12.10
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**524.80**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**217 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_D
0.0 FIT	0.00 FIT	161.96 FIT	75.95 FIT	68.08%	68.08%

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

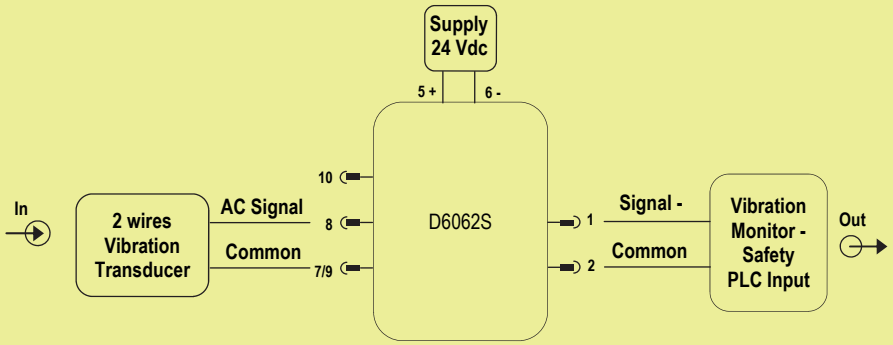
T[Proof] = 1 year	T[Proof] = 3 years
PFDavg = 3.35E-04 Valid for **SIL 2**	PFDavg = 1.00E-04 Valid for **SIL 2**

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 = 6.69E-03 Valid for **SIL 2**

Systematic capability SIL 3.

3rd Application for D6062S, with 2 wires AC (unpowered) transducer input



Description:

For this application, set the internal dip-switches in the following mode (see instruction manual for more information):

Dip-switch position (D6062S)	1	2	3	4
2 wires AC transducer	OFF	OFF	OFF	ON

The D6062S module is supplied (with 18 to 30Vdc supply voltage) at Pins 5 (+) – 6 (-). The green LED is lit in presence of supply power.
The input transducer AC signal (0 to 20Vpp, DC to 20kHz) is applied between Pins 8-7/9 (-Signal, Common). No DC offset must be applied.
The input signal (0 to 20Vpp, DC to 20kHz) is identically repeated at output Pins 1-2 (-Signal, Common).

Safety Function and Failure behavior:

D6062S is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.
The failure behaviour is described by the following definitions:

- □ Fail-Safe State: is defined as the output going Low or High, considering that the safety logic solver can convert the Low or High fail (dangerous detected) to the fail-safe state.
- □ Fail Safe: a 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 (i.e. being unable to go to the defined fail-safe state) or deviates the output voltage by more than 5 % of full span (> ± 1 Vdc).
- □ Fail High: a failure mode that causes the output signal to go below the maximum negative voltage (< -20 Vdc). Assuming that the application program in the safety logic solver is configured to detect High failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ Fail Low: a failure mode that causes the output signal to go above the minimum negative voltage (> -0.5 Vdc). Assuming that the application program in the safety logic solver is configured to detect Low failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure.
- □ 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 because the output voltage is deviated by less than 5 % of full span (< ± 1 Vdc). When calculating the SFF, this failure mode is not taken into account.
- □ Fail "Not part": failure mode of a component that 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.

Failure rate date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	160.84
λ_{du} = Total Dangerous Undetected failures	71.96
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**232.80**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**490 years**
$\lambda_{no\ effect}$ = "No Effect" failures	269.70
$\lambda_{not\ part}$ = "Not Part" failures	22.70
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**525.20**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**217 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_D
0.0 FIT	0.00 FIT	160.84 FIT	71.96 FIT	69.09%	69.09%

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] = 1 year	T[Proof] = 3 years
PFDavg = 3.17E-04 Valid for **SIL 2**	PFDavg = 9.51E-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 = 6.34E-03 Valid for **SIL 2**

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 fault, which have been noted during the FMEDA, can be revealed during proof test.
The **Proof test** consists of the following steps:

Steps	Action
1	Bypass the safety-related Vibration Monitor/PLC or take any other appropriate action in order to avoid a false trip.
2	Connect a calibrated DC input voltage to the interface (terminals 7/9 and 8); in the 0 to -20 Vdc range, check with a 1 Vdc step that the output voltage corresponds to each input step with a deviation smaller than 1%. This test detects any failure in the basic DC loop transfer function.
3	Connect a frequency generator to the interface (terminals 7/9 and 8); impose a 1 kHz square wave input signal with amplitude in the 0 to -20 Vpp range and -10 Vdc offset, then check with an oscilloscope that the output waveform maintains the peak-to-peak value with a deviation smaller than 1%. In addition, impose a zero input signal and verify that the output ripple is ≤ 20 mVrms. This test detects any other possible failure in the loop transfer function.
4	Connect a current sinking source (i.e.: 0 ÷ 20 mA current calibrator) between terminals 10 (negative supply) and 7/9 (common) and connect a DVM across the calibrator terminals. Set the current sink at 1 mA and check if the voltage measure is ≤ -21 Vdc at terminal 10, referred to terminal 7/9. Then, set the current sink at 15 mA and check if the voltage measure is ≤ -16 Vdc at terminal 10, referred to terminal 7/9. This test detects any failure in the input channel circuit.
5	Restore the loop to full operation.
6	Remove the bypass from the safety-related Vibration Monitor/PLC or restore normal operation.

This test will reveal around 99% of the possible Dangerous Undetected failures.