


SAFETY MANUAL

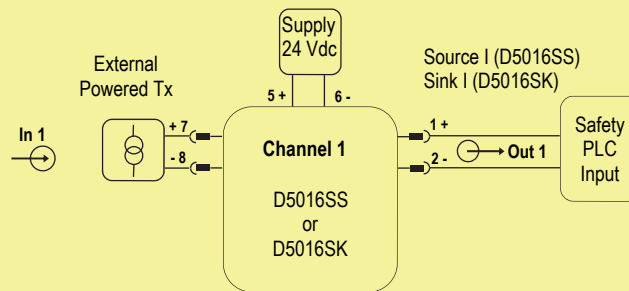
SIL 3 2-wire HART[®] Transmitter Current Repeater DIN-Rail and Termination Board, Models D5016SS, D5016SK, D5016DS, D5016DK

Approval:  TÜV Certificate No. TUV IT 25 SIL 0609 A, SIL 3 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 ISM0553,
which contain basic guides for the installation and configuration of the equipment.



Application for D5016SS or D5016SK



Description:

For this application, use D5016SS for 4 - 20 mA Source current output or D5016SK for 4 - 20 mA Sink current output. The module is powered by connecting 24 Vdc power supply to Pins 5 (+ positive) - 6 (- negative). The green LED is lit in presence of supply power. Active input signal from external powered Tx is applied to Pins 7-8 (In 1 - Ch.1). Source or Sink output current is applied to Pins 1-2 (Out 1 - Ch.1).

Safety Function and Failure behavior:

D5016 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 from 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 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 channel output current by more than 5% (0.8 mA) of full span.
- fail High: failure mode that causes the channel output signal to go above the maximum channel output current (> 20 mA). 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: failure mode that causes the channel output signal to go below the minimum channel output current (< 4 mA). 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.

- 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.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	67.69
λ_{du} = Total Dangerous Undetected failures	10.63
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	72.69
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	151.01
MTBF (safety function, one channel) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	756 years
$\lambda_{no\ effect}$ = "No Effect" failures	205.90
$\lambda_{not\ part}$ = "Not Part" failures	4.20
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	361.11
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	316 years

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	72.69 FIT	67.69 FIT	10.63 FIT	92.96%

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

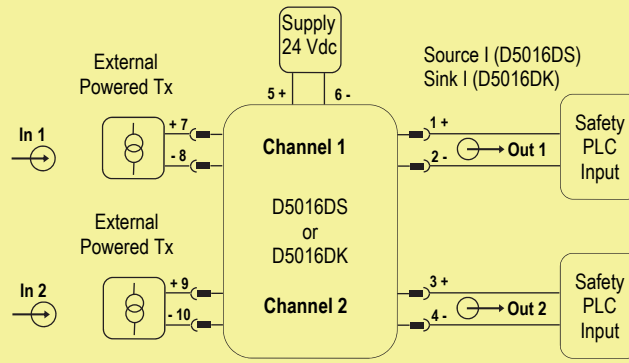
T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 20 years
PFDavg = 4.72E-05 Valid for SIL 3	PFDavg = 9.44E-05 Valid for SIL 3	PFDavg = 9.44E-04 Valid for SIL 2

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] = 6 years	T[Proof] = 20 years
PFDavg = 2.83E-04 Valid for SIL 3	PFDavg = 9.44E-04 Valid for SIL 2

SC3: Systematic capability SIL 3.

Application for D5016DS or D5016DK, for each channel



Description:

For this application, use D5016DS for 4 - 20 mA Source current outputs or D5016DK for 4 - 20 mA Sink current outputs. The module is powered by connecting 24 Vdc power supply to Pins 5 (+ positive) - 6 (- negative). The green LEDs are lit in presence of supply power. Active input signal from external powered Tx is applied to Pins 7-8 (In 1 - Ch.1) and to Pins 9-10 (In 2 - Ch.2). Source or Sink output currents are applied to Pins 1-2 (Out 1 - Ch.1) and to Pins 3-4 (Out 2 - Ch.2).

Safety Function and Failure behavior:

D5016 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 from the following definitions for each channel:

- 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 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 channel output current by more than 5% (0.8 mA) of full span.
- fail High: failure mode that causes the channel output signal to go above the maximum channel output current (> 20 mA). 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: failure mode that causes the channel output signal to go below the minimum channel output current (< 4 mA). 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. 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.

The two channels of D5016DS or D5016DK module should not be used to increase the hardware fault tolerance, needed for a Safety Function requiring higher SIL, as they are not completely independent from each other.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	67.69
λ_{du} = Total Dangerous Undetected failures	10.63
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	94.19
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	172.51
MTBF (safety function, each channel) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	662 years
$\lambda_{no\ effect}$ = "No Effect" failures	235.40
$\lambda_{not\ part}$ = "Not Part" failures	210.30
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	618.21
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	185 years

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	94.19 FIT	67.69 FIT	10.63 FIT	93.84%

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

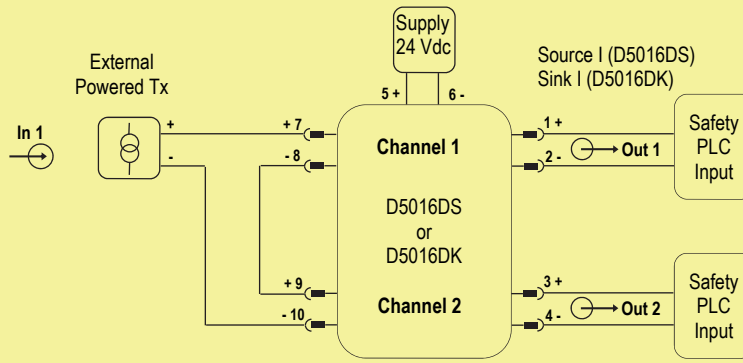
T[Proof] = 1 year	T[Proof] = 2 years	T[Proof] = 20 years
PFDavg = 4.72E-05 Valid for SIL 3	PFDavg = 9.44E-05 Valid for SIL 3	PFDavg = 9.44E-04 Valid for SIL 2

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] = 6 years	T[Proof] = 20 years
PFDavg = 2.83E-04 Valid for SIL 3	PFDavg = 9.44E-04 Valid for SIL 2

SC3: Systematic capability SIL 3.

Application for D5016DS or D5016DK, duplicator with input loop on two input channels



Description:

For this application, use D5016DS for 4 - 20 mA Source current outputs or D5016DK for 4 - 20 mA Sink current outputs. The module is powered by connecting 24 Vdc power supply to Pins 5 (+ positive) - 6 (- negative). The green LEDs are lit in presence of supply power. Active input signal from external powered Tx is applied, by input loop, to both Pins 7-8 (In 1 - Ch.1) and to Pins 9-10 (In 2 - Ch.2). Source or Sink output currents are applied to Pins 1-2 (Out 1 - Ch.1) and to Pins 3-4 (Out 2 - Ch.2).

Safety Function and Failure behavior:

D5016 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 from the following definitions for each channel:

- 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 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 channel output current by more than 5% (0.8 mA) of full span.
- fail High: failure mode that causes the channel output signal to go above the maximum channel output current (> 20 mA). 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: failure mode that causes the channel output signal to go below the minimum channel output current (< 4 mA). 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. 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.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	70.27
λ_{du} = Total Dangerous Undetected failures	10.63
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	94.19
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	175.09
MTBF (safety function, each channel of duplicator) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	652 years
$\lambda_{no\ effect}$ = "No Effect" failures	239.62
$\lambda_{not\ part}$ = "Not Part" failures	203.50
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	618.21
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	185 years

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	94.19 FIT	70.27 FIT	10.63 FIT	93.93%

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] = 2 years	T[Proof] = 20 years
PFDavg = 4.72E-05 Valid for SIL 3	PFDavg = 9.44E-05 Valid for SIL 3	PFDavg = 9.44E-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] = 6 years	T[Proof] = 20 years
PFDavg = 2.83E-04 Valid for SIL 3	PFDavg = 9.44E-04 Valid for SIL 2

SC3: 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, valid for each channel. **The Proof test 1** consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	By HART command or other technique, set the transmitter connected to the channel input of the current repeater in order to go to high alarm current and verify that the output current of the repeater reaches that value. This tests for problems related to not sufficient supply for internal input circuits.
3	By HART command or other technique, set the transmitter connected to the input of the current repeater in order to go to low alarm current and verify that the output current of the repeater reaches that value. This tests for possible input circuit quiescent current related failures.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or restore normal operation.

This test will reveal approximately 30 % of possible Dangerous Undetected failures in the repeater.

The **Proof test 2** consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	Perform step 2 and 3 of the Proof Test 1 .
3	Perform a two-point calibration (i.e. down scale as 4 mA and full scale as 20 mA) of the transmitter connected to the channel input of the current repeater. Then set the transmitter to impose some input current values of 4-20 mA range and verify that the correspondent output current values of repeater are within the specified accuracy. This proof requires that the transmitter has already been tested without the repeater and it works correctly according to its performance.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or restore normal operation.

This test will reveal approximately 99 % of possible Dangerous Undetected failures in the repeater.