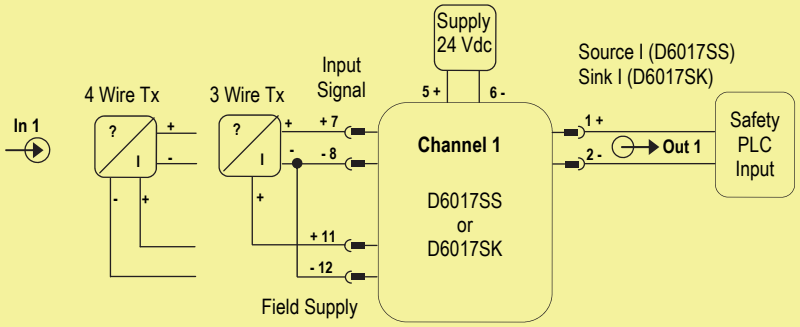
SAFETY MANUAL

SIL3 3/4-Wire HART® Transmitter Power Supply, DIN-Rail and Termination Board Models D6017SS, D6017SK

Reference must be made to the relevant sections within the instruction manual ISM0453, which contain basic guides for the installation of the equipment.

Application for D6017SS or D6017SK, with input connected to 3/4 Wire Transmitter (Tx)



Description:

For this application, use D6017SS for 4 - 20 mA Source current output or D6017SK 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.
The 3/4 Wire Transmitter (Tx) is supplied by Field Supply output Pins 7-8 of D6017 module.
Active input signal from 3/4 Wire Transmitter (Tx) is applied to Pins 7-8 (In 1 - Ch.1).
Source or Sink output current are applied to Pins 1-2 (Channel 1).

Safety Function and Failure behavior:

D6017 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 D6017 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 output current by more than 5% (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 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 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 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 date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	71.02
λ_{du} = Total Dangerous Undetected failures	14.98
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	78.51
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**164.51**
MTBF (safety function, one channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**694 years**
$\lambda_{no\ effect}$ = "No Effect" failures	209.88
$\lambda_{not\ part}$ = "Not Part" failures	6.20
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**380.59**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**300 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	78.51 FIT	71.02 FIT	14.98 FIT	90.89%

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] = 15 years
PFDavg = 6.63E-05 Valid for **SIL 3**	PFDavg = 9.95E-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] = 5 years	T[Proof] = 20 years
PFDavg = 3.32E-04 Valid for **SIL 3**	PFDavg = 1.33E-03 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. **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 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 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.