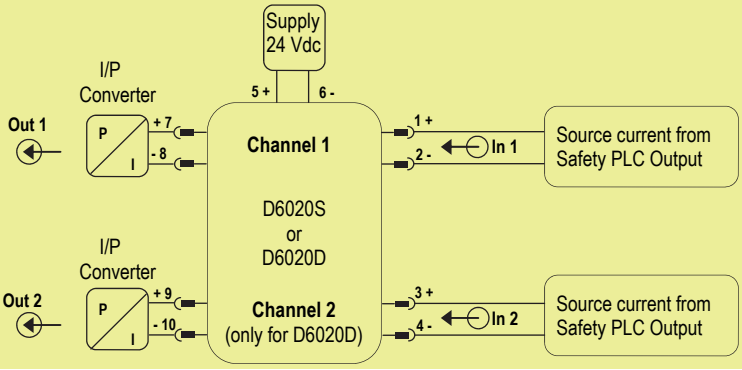
SAFETY MANUAL

SIL 2 Powered Isolating Driver
Hart, DIN-Rail and Termination Board,
Models D6020S, D6020D

Reference must be made to the relevant sections within the instruction manual ISM0212,
which contain basic guides for the installation of the equipment.

gmi technology for safety

Application for D6020S or D6020D



Description:

For this application, enable Short Circuit fault for ch. 1 or ch. 2, by set the internal dip-switches in the following mode (see instruction manual for more information):

Dip-switch position (D6020S)	1	2	3	4
Short Circuit fault	OFF	-	-	-

Dip-switch position (D6020D)	1	2	3	4
Short Circuit fault ch.1	OFF	-	-	-
Short Circuit fault ch.2	-	-	OFF	-

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.
Current Input signals from Safety PLC Outputs are applied to Pins 1-2 (In 1 - Ch.1) and Pins 3-4 (In 2 - Ch.2).
Source output currents for I/P converters are applied to Pins 7-8 (for Channel 1) and Pins 9-10 (for Channel 2).

Safety Function and Failure behavior:

For each channel, short circuit fault detection should be enabled (in case of fault, the output load is de-energized (low output current is imposed) until normal condition is restored and low sinking current is imposed to Safety PLC output because high impedance is reflected to the control device circuit).
D6020 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: is defined as the output going Low, considering that the safety logic solver can convert the Low fail (dangerous detected) to the fail-safe state;
- □ 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 (i.e. being unable to go to the defined fail-safe state) 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). This mode is considered a Dangerous Undetected 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.

The 2 channels of D6020D module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent each other, not containing common components. In fact, the analysis results got for D6020S (single channel) are also valid for each channel of D6020D (double channel).
This analysis is also valid for D6020D as Duplicator.
Failure rate date: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	136.38
λ_{du} = Total Dangerous Undetected failures	21.00
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**157.38**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**725 years**
$\lambda_{no\ effect}$ = "No Effect" failures	255.92
$\lambda_{not\ part}$ = "Not Part" failures	65.70
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**479.00**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**238 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	0.00 FIT	136.38 FIT	21.00 FIT	86.65%	0%	86.65%

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] = 10 years
PFDavg = 9.33 E-05 Valid for **SIL 2**	PFDavg = 9.33 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 = 1.87 E-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 PLC or take other appropriate action to avoid a false trip.
2	Set the following configuration for SW dip-switches: ● SW-1 (for Ch1) or SW-3 (for Ch2) = ON (to disable the field short circuit fault detection); ● SW-2 or SW-4 = ON or OFF (not used because load diagnostic is disabled). For each channel, the series connection of 700 Ω load resistor with an ammeter must be connected to output terminals of channel. Then, connect a current calibrator to input terminals of channel. Supply the D6020 at 24 Vdc and apply (by calibrator) the following input dc current values: ● 20 mA (high current limit) and verify that the output current is ≈ 20 mA (within the specified accuracy); ● 4 mA (low current limit) and verify that the output current is ≈ 4 mA (within the specified accuracy); ● 8 mA, 12 mA and 16 mA or other values included in the range 4 ÷ 20 mA and verify that the output current has the equivalent current value (within the specified accuracy). The same test must be executed with lower load resistance values, reaching 50 Ω (low resistance limit).
3	Set the following configuration for SW dip-switches: SW-1 (for Ch1) or SW-3 (for Ch2) = OFF (to enable the field short circuit fault detection). For each channel, connect the series connection of a current calibrator with an ammeter to input terminals of channel and supply the D6020 at 24 Vdc. Firstly, don't connect anything to the output terminals and verify that red fault LED is lit because of field open circuit. Then, connect the series connection of a decade resistor box (set to 250 Ω) with an ammeter to output terminals of channel. Applying (by calibrator) an input dc current in the range 4 ÷ 20 mA, consider the following configuration: ● SW-2 or SW-4 = OFF (to detect short circuit fault for load resistance < 100 Ω): reduce (by decade resistor box) the load resistance and verify that diagnostic circuit detects short circuit fault when load resistance is < 100 Ω; ● SW-2 or SW-4 = ON (to detect short circuit fault for load resistance < 50 Ω): reduce (by decade resistor box) the load resistance and verify that diagnostic circuit detects short circuit fault when load resistance is < 50 Ω; During short circuit fault, the red fault LED is lit, the input ammeter measures ≈ 2 mA because the D6020 module reflects a high impedance to the input calibrator (which reaches the overload state) and therefore the output ammeter shows a low current ≤ 2 mA. This situation is held until normal configuration (without short circuit fault) is restored.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or restore normal operation.

This test will reveal almost 99 % of possible Dangerous Undetected failures in the powered isolating driver.