

INSTRUCTION & SAFETY MANUAL

SIL 3 Power Supply System PSS1 250
24Vdc, 50-100-150 A, Zone 2 / Division 2
19" Rack for up to 6 power modules PSM1250
9" Rack for up to 2 power modules PSM1250
and diagnostic module PSO1250



Supply:

Input voltage: 100 to 264 Vac (48 to 62 Hz). Limit input voltage to 250 Vrms for Intrinsically Safe applications.
Power Factor Correction (AC input): 0.98 typ. @230Vac, 0.995 typ. @115Vac, full load.
Efficiency @24Vdc out (full load): better than 89 % @ 230 Vac and 86% @ 115 Vac.
Max. internal power dissipation @24Vdc out (full load): 150 W @ 230 Vac; 195 W @ 115 Vac.
AC input current (sinusoidal at full load) @24Vdc out: 14.2 A @ 100 Vac input voltage, 12.2 A @ 115 Vac input voltage, 6.1 A @ 230 Vac input voltage.
Inrush current: 37 A peak @ 264 Vac; 32 A peak @ 230 Vac; 16 A peak @ 115 Vac.
AC input connection: screw terminal blocks suitable for 4mm² wires on wall mounting panel.

Isolation (Test Voltage):

Input to Output isolation: 2500 Vrms (routine test).
Input to Ground isolation: 1500 Vrms (routine test).
Ground to Output isolation: 500 Vrms (routine test).
Output or Ground to Fault contact isolation: 500 Vrms (routine test)

Output:

Output voltage: 24 Vdc (adjustable from 21 to 28 Vdc).
Regulation: 0.4 % for a 100 % load change.
Stability: 0.01 % for a 20 % line voltage change.
Ripple: ≤ 250 mVpp.
Output current: 50 A nominal (@24Vdc out). Parallel connection for redundancy with load sharing capability within ±5 % of output voltage setting.
Output power: up to 1300 W nominal (@28Vdc out).
Output Rise Time: 2.5 s.
Dynamic Response: 2 ms for 0-100% load change (overshoot ±1.5% of Vout setting).
Connection: screw terminals on copper bars suitable for 300A available on wall mounting panel.
Hold-up time at full load: 20 ms (AC input).
Over voltage protection: output limited to 30 Vdc plus two redundant crowbars for over voltage protection at 31 Vdc.

Power good signaling:

Output good: 19.5 V ≤ Vout ≤ 29.5 V.
Indication: via LCD screen on PSO1250 and Modbus RTU RS-485 protocol.
Signaling: voltage free SPST normally energized relay (contact closed), de-energize in over/under voltage conditions (contact open).
Contact Rating: 2 A 50 Vac 100 VA, 2 A 50 Vdc 60 W (resistive load).
Connection: screw terminal blocks suitable for 1.5 mm² wires on wall mounting panel.

Compatibility:

CE CE mark compliant, conforms to directive 94/9/EC ATEX, 2004/108/EC EMC, 2006/95/EC LVD, 2011/65/EU RoHS; conforms to EN60950 for electrical safety.

Environmental conditions:

Operating temperature limits: -40 to +70°C de-rated linearly 65-70% load above 50°C (see below Power Output vs. Ambient Operating Temperature diagram).
Relative humidity limits (up to 40 °C): 10 to 90 %, non condensing.
Transport, storage temperature limits: - 45 to + 85 °C.

Safety Description:


ATEX: II 3G Ex nA nC IIC T4 Gc.
IECEX: Ex nA nC IIC T4 Gc.

Approvals:

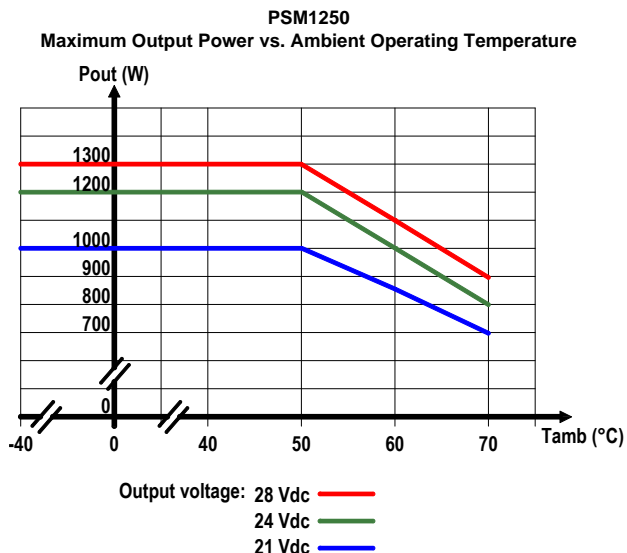
BVS 15 ATEX E 006 X conforms to EN60079-0, EN60079-11, EN60079-15,
 IECEx BVS 15.0006X conforms to IEC60079-0, IEC60079-11, IEC60079-15.
 SIL 3 / SIL 2 according to IEC 61508:2010 Ed. 2.
 TÜV Certificate No. C-IS-236198-09, SIL 3 Functional Safety Certificate conforms to IEC61508:2010 Ed.2, for Management of Functional Safety.

Mechanical:

Mounting: 9" or 19" Rack unit, 4 units high.
Weight: 9" fully equipped about 10 Kg, fully equipped with 2 PSM1250 and 1 PSO1250 module.
 19" fully equipped about 24 Kg, fully equipped with 6 PSM1250 and 1 PSO1250 module.
Location: Safe Area/Non Hazardous Locations or Zone 2, Group IIC T4, Class I, Zone 2, Group IIC, IIB, IIA T4 installation.
Protection class: IP 20.
Dimensions: see drawings page 27.

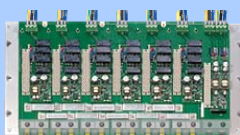

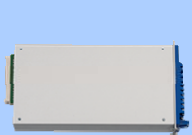
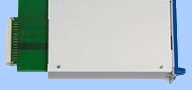


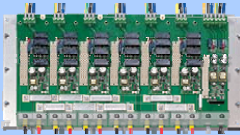

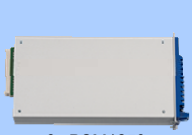
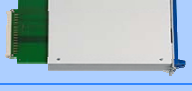


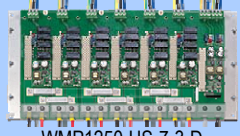

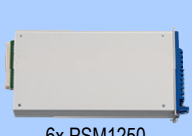
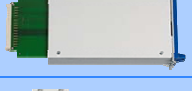


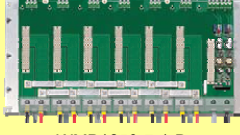

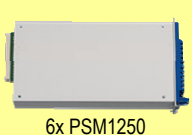
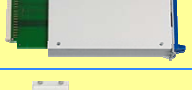


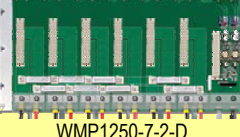

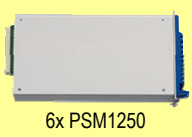
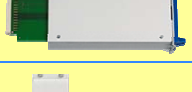
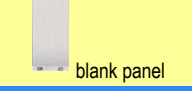

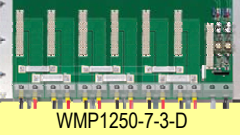
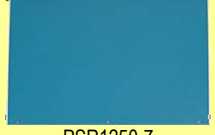
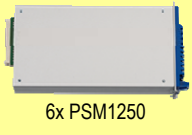
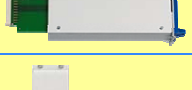
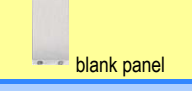

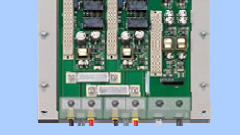

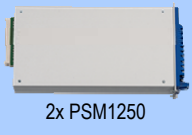
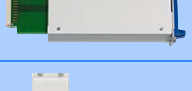


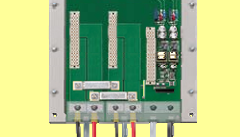

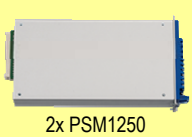
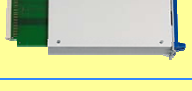



Features

- SIL 3 for NE Load according IEC 61508:2010, with single PSM1250 module or more PSM1250 modules in redundant configuration (see pages 10-13 (with HS models) and pages 18-21 (without HS models)).
- SIL 1 for ND Load according to IEC 61508:2010, with single PSM1250 module (see page 14 (with HS models) and page 22 (without HS models)).
- SIL 2 for ND Load according IEC 61508:2010, with more PSM1250 modules in redundant configuration (see pages 15-17 (with HS models) and pages 23-25 (without HS models)).
- Systematic capability SIL 3.
- 2 universal AC Input Lines, 100 to 264 Vac (48 to 62 Hz).
- Power factor correction.
- Installation in Zone 2 / Div.2 hazardous locations with hot swappable modules.
- EMC Compatibility to EN61000-6-2, EN61000-6-4.
- ATEX, IECEx Certifications.
- TÜV Certifications (pending).
- TÜV Functional Safety Certification.
- Type Approval Certificate DNV for marine applications (pending).
- Highly regulated output of 24 Vdc, 50 A, for PSM1250 module.
- Under and over voltage alarm monitoring.
- 3 over voltage redundant protections.
- Redundant parallel connections with load sharing.
- Reduces Power dissipation (in parallel/redundant configuration) by replacing a Schottky diode with Mosfet Active Ideal Diode.
- 89% efficiency @230 Vac input and 24 Vdc output and full load.
- Speed fan control depending on ambient temperature and output power.
- High load fuse breaking capability without interrupting operations.
- 19" or 9" Rack unit, 4 U high, anodized aluminium, durable metal enclosure.
- Tropicalization for electronic components.
- Modbus RTU RS-485 diagnostic output.

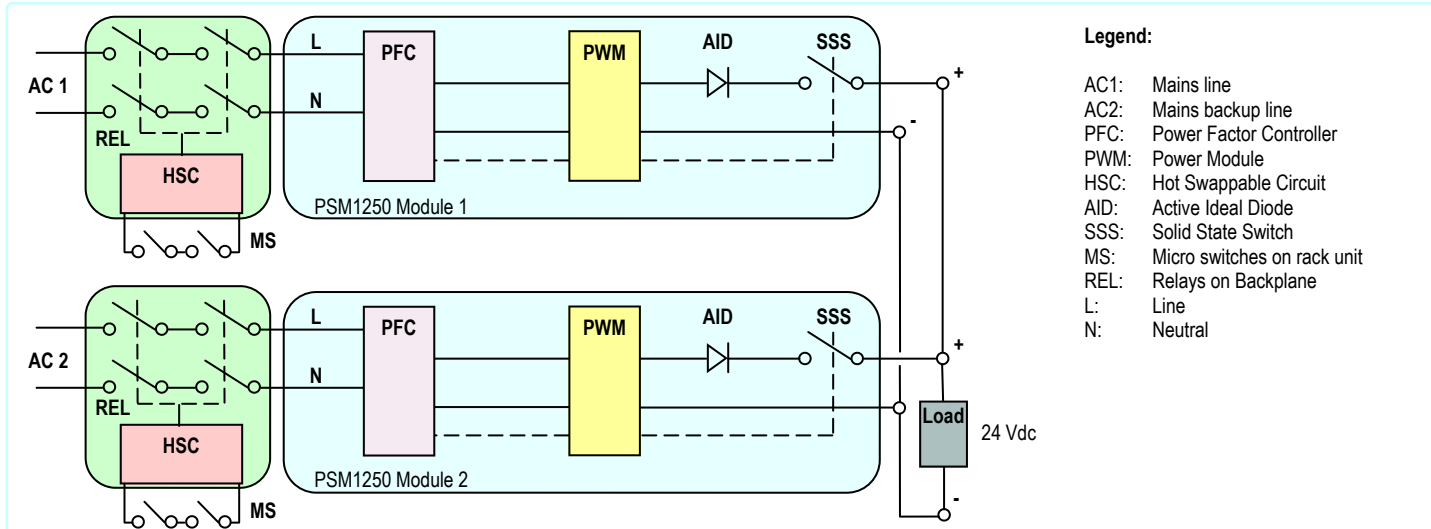


With 50% redundant configuration (two PSM1250 with paralleled outputs), each module can give 600 W power output up to 70°C operating ambient temperature, with output voltage range 21-28 Vdc and input voltage range 100-264 Vac.

Ordering Information:

Wall Mounting Panel	Rack unit	Power Module slots	Diagnostic Module slot	Ordering code
 WMP1250-HS-7-1-D with hot swapping	 PSR1250-HS-7	 6x PSM1250	1x PSO1250  1x MCHP228  blank panel	 PSS1250-HS-7-1-D 1 power supply 24 Vdc 1x 150A+150A redundancy
 WMP1250-HS-7-2-D with hot swapping	 PSR1250-HS-7	 6x PSM1250	1x PSO1250  1x MCHP228  blank panel	 PSS1250-HS-7-2-D 2 power supply 24 Vdc 1x 100A+100A redundancy 1x 50A+50A redundancy
 WMP1250-HS-7-3-D with hot swapping	 PSR1250-HS-7	 6x PSM1250	1x PSO1250  1x MCHP228  blank panel	 PSS1250-HS-7-3-D 3 power supply 24 Vdc 3x 50A+50A redundancy
 WMP1250-7-1-D without hot swapping	 PSR1250-7	 6x PSM1250	1x PSO1250  1x MCHP228  blank panel	 PSS1250-7-1-D 1 power supply 24 Vdc 1x 150A+150A redundancy
 WMP1250-7-2-D without hot swapping	 PSR1250-7	 6x PSM1250	1x PSO1250  1x MCHP228  blank panel	 PSS1250-7-2-D 2 power supply 24 Vdc 1x 100A+100A redundancy 1x 50A+50A redundancy
 WMP1250-7-3-D without hot swapping	 PSR1250-7	 6x PSM1250	1x PSO1250  1x MCHP228  blank panel	 PSS1250-7-3-D 3 power supply 24 Vdc 3x 50A+50A redundancy
 WMP1250-HS-3-D with hot swapping	 PSR1250-HS-3	 2x PSM1250	1x PSO1250  1x MCHP228  blank panel	 PSS1250-HS-3-D 1 power supply 24 Vdc 1x 50A+50A redundancy
 WMP1250-3-D without hot swapping	 PSR1250-3	 2x PSM1250	1x PSO1250  1x MCHP228  blank panel	 PSS1250-3-D 1 power supply 24 Vdc 1x 50A+50A redundancy
				 PSS1250-3 1 power supply 24 Vdc 1x 50A+50A redundancy

Hot swapping capability



PSS1250 Power Supply System is able to provide power and installed in Zone 2 / Div. 2 Hazardous Locations, without the need to monitor hazardous gas presence and without disturbing power supply operations, because it is fully protected from the Hot Swapping of any power, or diagnostic, module. This protection system operates for both the insertion and disconnection of the modules.

When inserting the module, the mains voltage is only applied when mechanical and electrical module connections are completely and correctly positioned, while before disconnecting the module the external electrical connections have to be at zero voltage level.

To achieve this result, a sophisticated 1002 mechanical and electrical protection circuit, using micro switches (MS), relays (REL) and special hot swapping circuits (HSC), has been designed. All power modules have a mains terminal block for Line-Neutral-Earth, placed in the Wall Mounting Panel that can be used for two independent mains lines (AC1 and AC2). The Line and Neutral are connected to the power module via two couples of 1002 series contact relays, driven from hot swapping circuit according to closed or open state of 1002 series mechanical switches. Two micro switches for each power module are placed in the front part of the 9" or 19" Rack unit and are activated (closed) by front panel top screws used to fix the module at rack. 24 relays (4 for each power module) are installed on the wall mounting rear panel, close to the mains terminal blocks, in 1002 architecture for safety purposes. For further safety, close to the relays, for each position, there is a red LED (total 6 LEDs). Before inserting a power module, the operator must verify that related red LED is OFF (see page 32). If the red LED is turned ON, a failure is present on a couple of series relays. Therefore no power module shall be inserted and fixed into that position of the rack unit, because it can be dangerous in Zone 2 / Div.2.

The opening of the micro switches, operated by unscrewing at least one of two front panel top screws, initiates the following two actions:

1. Mains line is disconnected from the power module, because hot swapping circuit de-energizes relays, opening their contacts;
2. Voltage on the power module connectors is brought to 0 volts, to avoid any sparking possibility. This is done by a MOSFET solid state switch (SSS) connected in series with the *active ideal diodes* (AID), which disconnects the output from the DC output bus. The internal voltage in the disconnected power module remains completely isolated from the output connections and therefore, even if an operator shorts the connections with a screw driver or any other tool, this will not generate a spark.

When a power module is inserted and fixed to rack unit by its screws, the MOSFET solid state switch remains open until the power supply starts to operate correctly, then it closes itself applying voltage to the load.

Reasons for using an Ideal Diode-OR Controller circuit, in N+1 redundant power supply applications with high availability systems

High availability systems often employ power supply modules connected in parallel to achieve redundancy and enhance system reliability.

ORing diodes have been a popular means of connecting these supplies at a point of load. The disadvantage of this approach is the forward voltage drop and resulting efficiency loss. This drop reduces the available supply voltage and dissipates significant power.

Replacing Schottky diodes with N-channel MOSFETs reduces power dissipation and eliminates the need for expensive heat sinks or large thermal layouts in high power applications. In the Ideal Diode-OR Controller circuit (*active ideal diode*), the voltage across source and drain is monitored by IN and OUT pins, and GATE pin drives the MOSFETs to control their operation. In effect the MOSFET source and drain serve as the anode and cathode of an ideal diode.

In the event of a power supply failure, for example if the output of a fully loaded supply is suddenly shorted to ground, reverse current temporarily flows through the MOSFETs that are ON. This current is sourced from any load capacitance and from the other supplies. The active ideal diode quickly responds to this condition turning off the MOSFETs in about 0.5 μ s, thus minimizing disturbance and oscillations to the output bus.

Using Oring diodes, to parallel two, or more, 24 VDC power supply modules for redundancy, one Schottky diode is used for each module. The voltage drop across the diode can reach about 0.8 V at 50 A, this means about 40 W dissipation for each module. Then, if six 50 A paralleled modules are used for full 150 + 150 A redundancy, a total power of about **240 W** is dissipated for this purpose. This reduces efficiency, reliability and increases space for heat sinks. Moreover, in case of module failure, diodes take time to recover and consequently they do not preserve the load from transients during the backup operation.

To avoid all these problems G.M. International has introduced, in the new PSS1250 Power Supply System, the use of *active ideal diodes*.

The MOSFETs resistance for *active ideal diodes* is about 1.2 m Ω resulting in 3.6 W dissipation for each power module. Then, if six 50 A paralleled modules are used for full 150 + 150 A redundancy, a total power of about **22 W** is dissipated for the purpose resulting in about **ten times less** dissipation compared to Schottky diodes solution. This increases efficiency, reliability, availability and reduces space for heat sinks.

This circuit provides also very smooth voltage switchovers without oscillations with fast turnoff, minimizing reverse current transients.

Output voltage setting - Fault indications - Diagnostic information

For each PSS1250 power module, the output voltage can be set to 24 Vdc + 18%; -14% via a front panel trimmer (see page 33 for more information about voltage adjust procedure). Under voltage threshold is set to 19.5 V, while Over voltage threshold is set to 29.5 V.

A front panel power ON green LED signals mains voltage is applied to the power module and normal DC output voltage is present on DC output bus.

Power module Fault conditions are signaled by opening contact of NE relay (contact closed in normal condition), positioned on WMP "Fault" terminal block. Faults can be:

- Under voltage $V_{out} < 19.5$ V.
- Over voltage $V_{out} > 29.5$ V.

In absence of under / over voltage fault, the green Power ON LED is ON if output voltage is within 19.5 V - 29.5 V range.

If output voltage goes below 19.5 V, the green Power ON LED blinks and remains steady for voltage lower than 20 V.

If output voltage goes over 29.5 V, the green Power ON LED is OFF for voltage higher than 29 V.

After under / over voltage fault, coming back to normal condition, the green Power ON LED is ON if output voltage is within 20 V - 29 V range.

Communication with six (for PSS1250-7) or two (for PSS1250-3) power modules is achieved via PSO1250 diagnostic module (only for PSS1250 with -D suffix), which incorporates a front panel color touch screen. The diagnostic module is able to query each power modules (using an internal proprietary bus) and read data such as, Input/Output Voltage, Current and Power; Input Line Frequency; Output current sharing percentage; Internal Temperature; alarm status (under/over out voltage, AC line absence, internal PFC or PWM stage in OFF state, internal high temperature, fans malfunctioning). This information is available via front panel LCD and externally via Modbus RTU on related wall mounting terminal block.

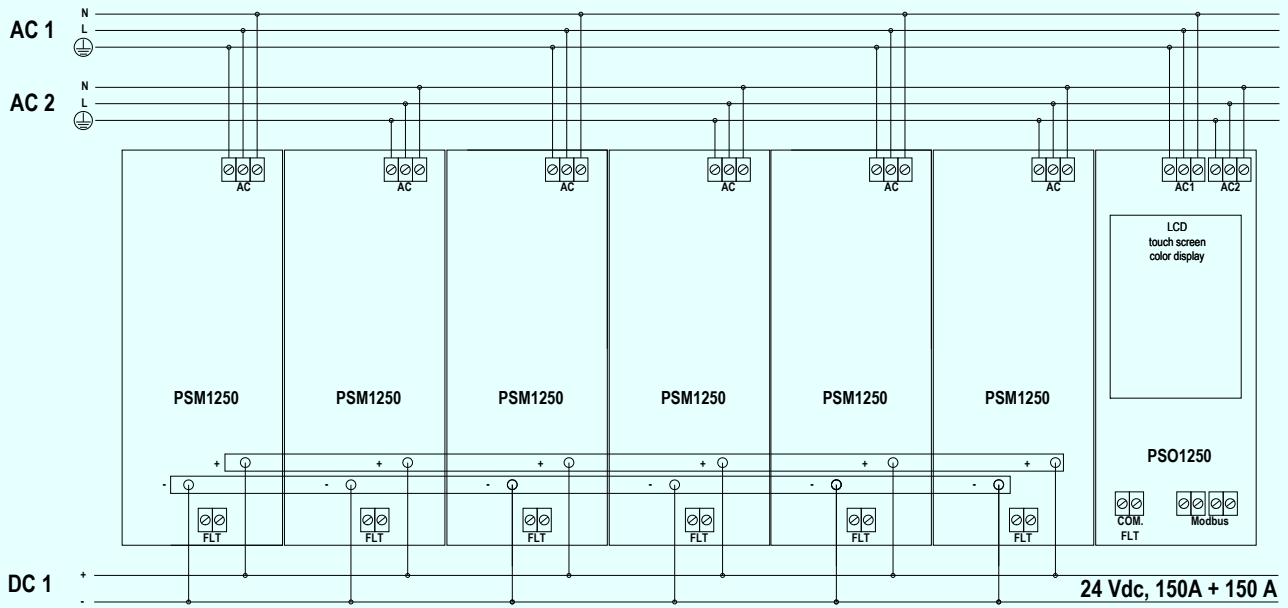
Under/Over voltage of one or more power modules is signaled by opening contact of NE relay (contact closed in normal condition), positioned on WMP "Comm. Fault" terminal block.

The diagnostic module **does not interfere** with the Power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the diagnostic module does not affect system performance, reliability and SIL level of Functional Safety applications.

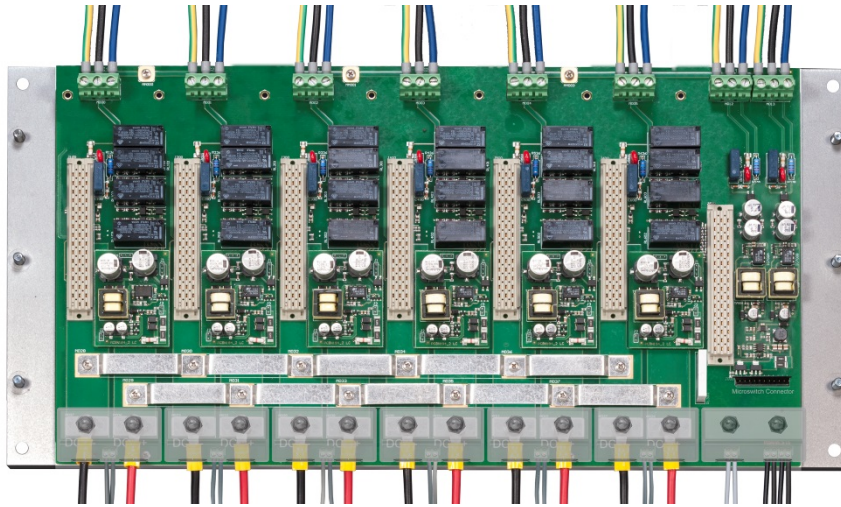
Function Diagram Dual AC Supply wiring architecture for PSS1250-HS-7-1-D or PSS1250-7-1-D:

SAFE AREA or ZONE 2 GROUP IIC T4,
NON HAZARDOUS LOCATIONS or CLASS I, DIVISION 2, GROUPS A, B, C, D T-Code T4, CLASS I, ZONE 2, GROUP IIC T4

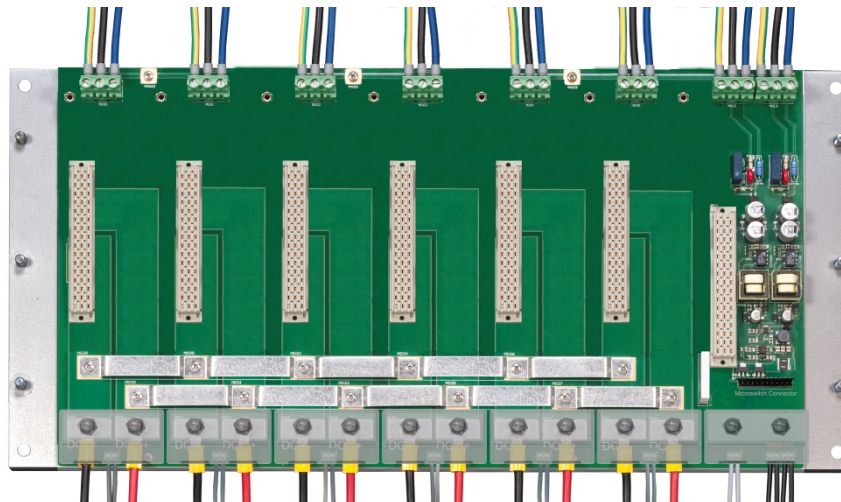
PSS1250-HS-7-1-D or PSS1250-7-1-D, dual AC supply, 1 redundant 150 A Output, PSO1250 overview module
six power modules connected in parallel to provide full redundancy on AC lines (AC1 and AC2) and one 150 A redundant output.



Wall Mounting Panel type WMP1250-HS-7-1-D with Hot Swapping circuits:



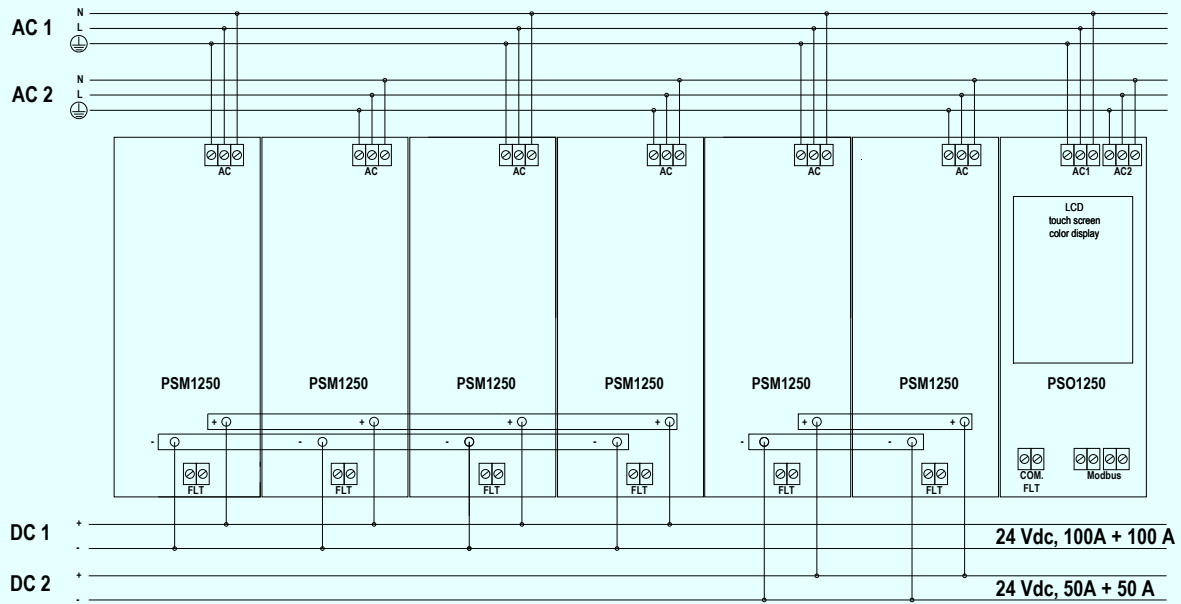
Wall Mounting Panel type WMP1250-7-1-D without Hot Swapping circuits:



Function Diagram Dual AC Supply wiring architecture for PSS1250-HS-7-2-D or PSS1250-7-2-D:

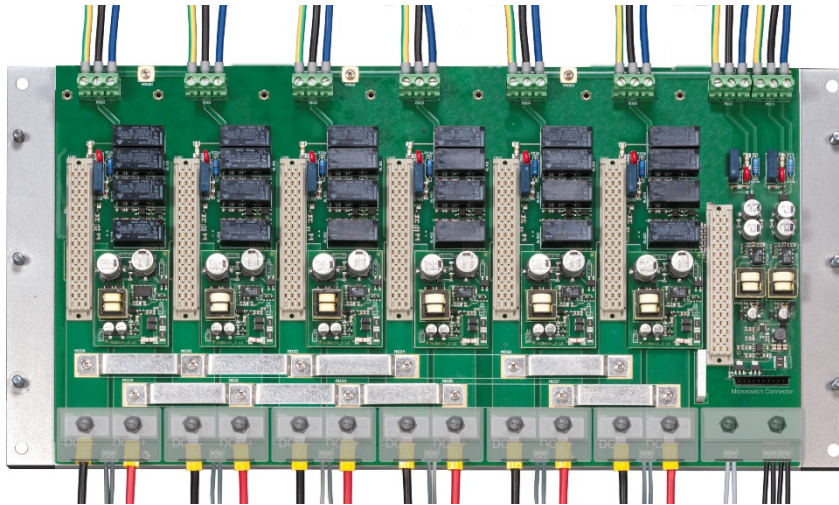
SAFE AREA or ZONE 2 GROUP IIC T4,
NON HAZARDOUS LOCATIONS or CLASS I, DIVISION 2, GROUPS A, B, C, D T-Code T4, CLASS I, ZONE 2, GROUP IIC T4

PSS1250-HS-7-2-D or PSS1250-7-2-D, dual AC supply, 1 redundant 100 A Output + 1 redundant 50 A Output, PSO1250 overview module
four power modules connected in parallel to provide full redundancy on AC lines (AC1 and AC2) and one 100 A redundant output.
two power modules connected in parallel to provide full redundancy on AC lines (AC1 and AC2) and one 50 A redundant output.

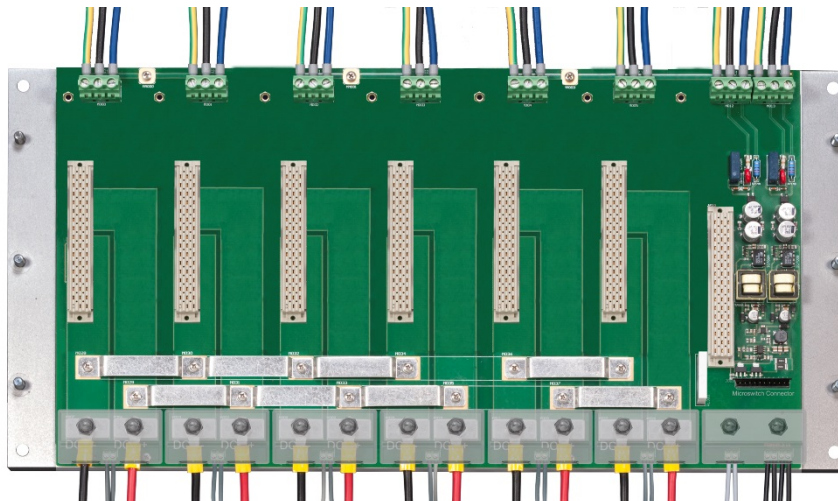


DC 1 (-) and DC 2 (-) negative lines can be connected together or use the same wiring.

Wall Mounting Panel type WMP1250-HS-7-2-D with Hot Swapping circuits:



Wall Mounting Panel type WMP1250-7-2-D without Hot Swapping circuits:

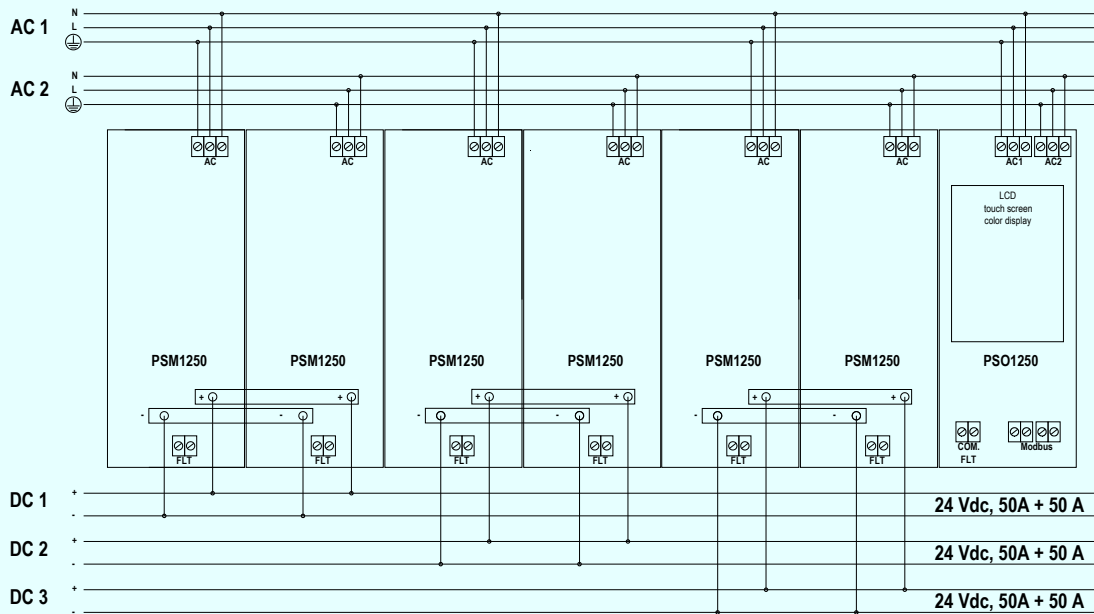


Function Diagram Dual AC Supply wiring architecture for PSS1250-HS-7-3-D or PSS1250-7-3-D:

SAFE AREA or ZONE 2 GROUP IIC T4,
NON HAZARDOUS LOCATIONS or CLASS I, DIVISION 2, GROUPS A, B, C, D T-Code T4, CLASS I, ZONE 2, GROUP IIC T4

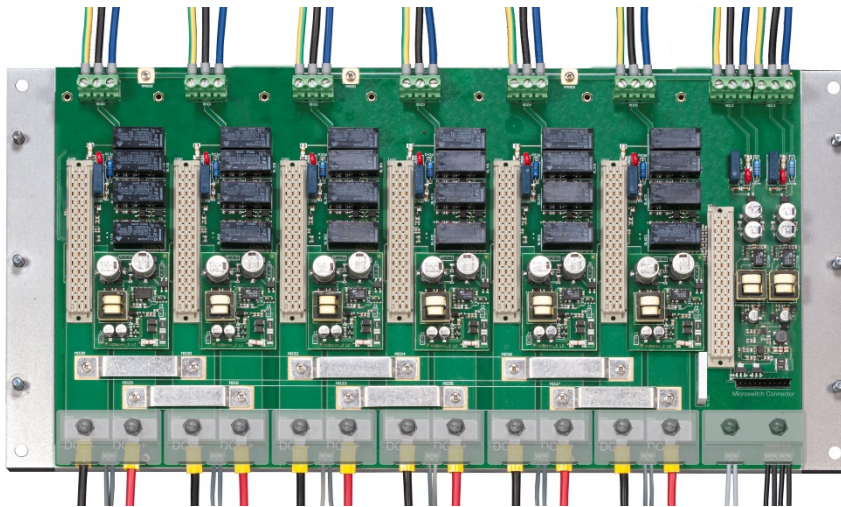
PSS1250-HS-7-3-D or PSS1250-7-3-D, dual AC supply, 3 redundant 50 A Outputs, PSO1250 overview module

six power modules connected in parallel in groups of two to provide full redundancy on AC lines (AC1 and AC2) and three independent 24 Vdc, 50 A redundant outputs.

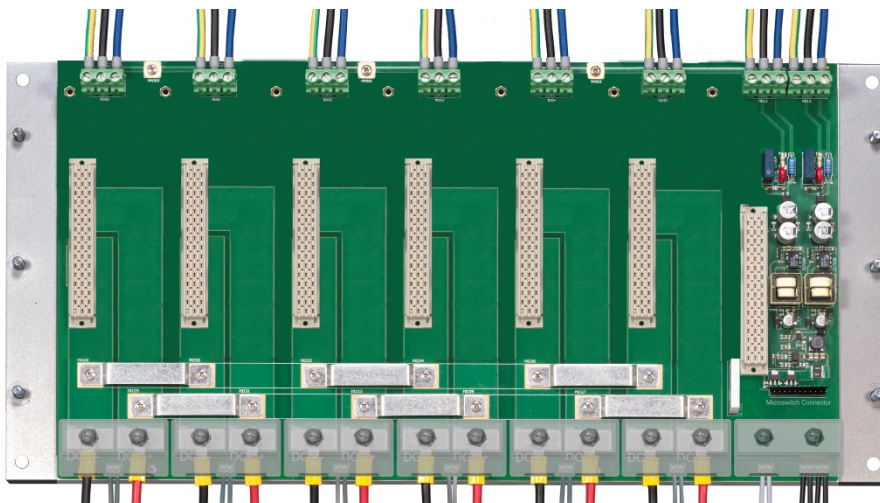


DC 1 (-), DC 2 (-) and DC 3 (-) negative lines can be connected together or use the same wiring.

Wall Mounting Panel type WMP1250-HS-7-3-D with Hot Swapping circuits:



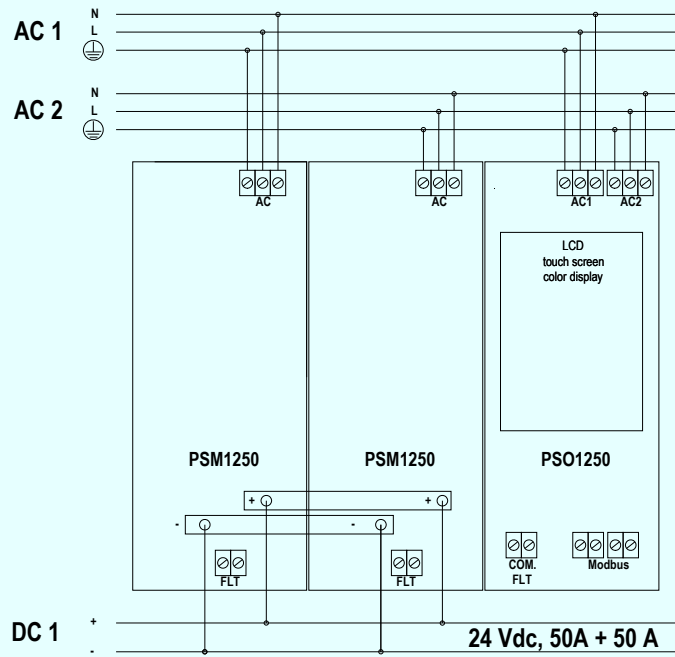
Wall Mounting Panel type WMP1250-7-3-D without Hot Swapping circuits:



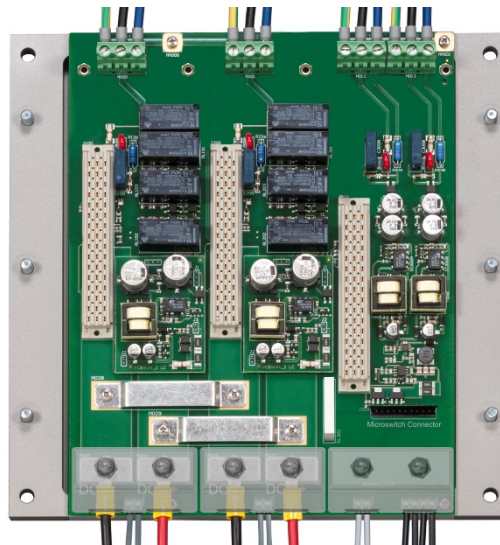
Function Diagram Dual AC Supply wiring architecture for PSS1250-HS-3-D or PSS1250-3-D:

SAFE AREA or ZONE 2 GROUP IIC T4,
NON HAZARDOUS LOCATIONS or CLASS I, DIVISION 2, GROUPS A, B, C, D T-Code T4, CLASS I, ZONE 2, GROUP IIC T4

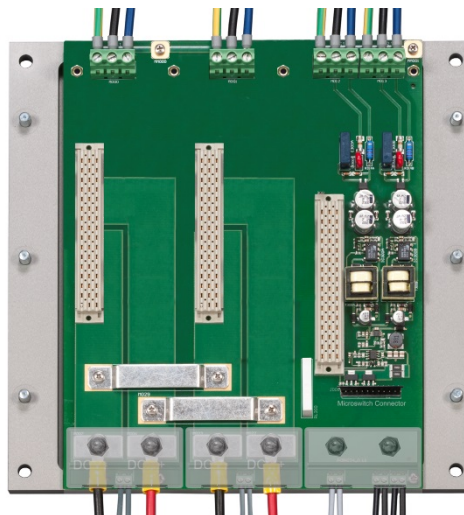
PSS1250-HS-3-D or PSS1250-3-D, dual AC supply, 1 redundant 50 A Output, PSO1250 overview module
two power modules connected in parallel to provide full redundancy on AC lines (AC1 and AC2) and one 50 A redundant output.



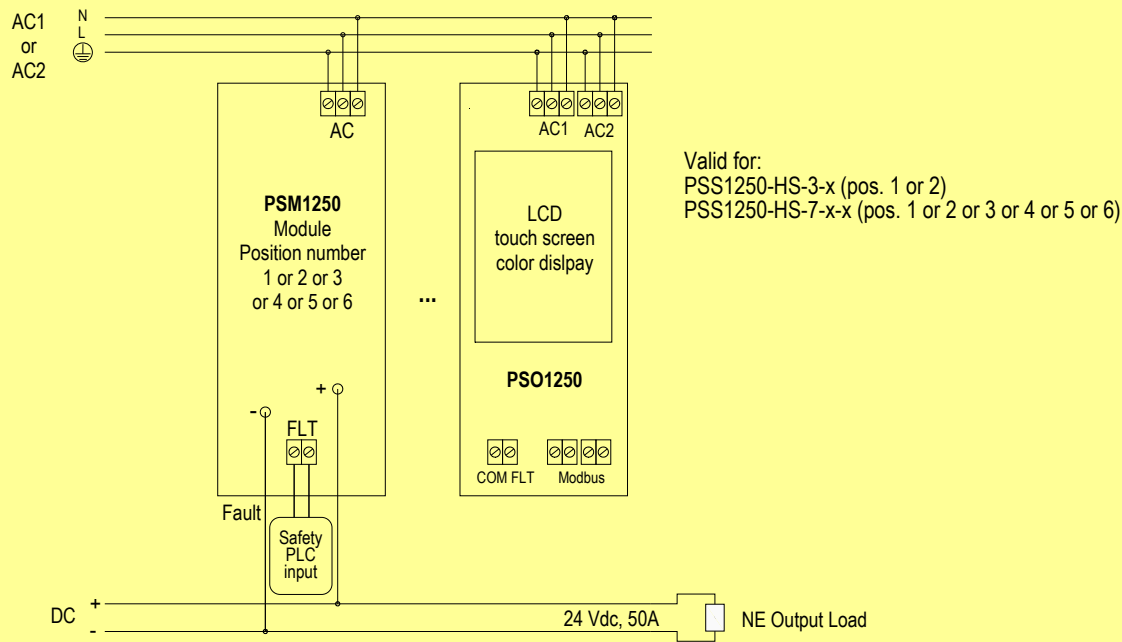
Wall Mounting Panel type WMP1250-HS-3-D with Hot Swapping circuits:



Wall Mounting Panel type WMP1250-3-D without Hot Swapping circuits:



Application of PSS1250 with HS and single PSM1250 module, for NE output load



Description:

In normal operation the PSM1250 module is powered by connecting AC input supply to related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). The fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies under/over voltage faults to logic solver, which can require to turn off power supply and to replace it with a new PSM1250 module. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

The green Power ON LED of PSM1250 is lit in presence of AC input supply. In this condition the NE output load (connected to related output copper bars with screw terminals on the Wall Mounting Panel backboard) is Normally Energized (NE).

In absence of AC input supply, the PSM1250 module is shutdown (its fault relay contact is open) and output load is de-energized (Safe State).

Safety Function and Failure behavior:

PSS1250 with HS and single PSM1250 module is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of PSM1250 for NE load is described by the following definitions :

- Fail-Safe State: it is defined as the output going below 2 Vdc. Internal diagnostic detects and notifies Low/High (Under/Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off power supply and to replace it with a new PSM1250 module.
- 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 (i.e. being unable to go to the defined fail-safe state), so that the output voltage is blocked or oscillating between 2 and 20 Vdc or above 30 Vdc, and internal diagnostic cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the output to go above 30 Vdc. Internal overvoltage protection tries to limit output voltage < 30 Vdc, otherwise internal crowbars trip to fail safe state for output ≥ 31 Vdc. Internal diagnostic detects and notifies High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the output to go between 2 and 20 Vdc. Internal diagnostic detects and notifies Low fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- 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, so that the output voltage is deviated between 20 and 30 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	42.76
λ_{du} = Total Dangerous Undetected failures	12.34
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	1890.87
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	1945.97
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	58 years
$\lambda_{no\ effect}$ = "No Effect" failures	1146.91
$\lambda_{not\ part}$ = "Not Part" failures	267.09
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	3359.97
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	34 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5*8760 + 8)h + \lambda_{dd} * 8h$	5.449E-05

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _s	DC _D
0.00 FIT	1890.87 FIT	42.76 FIT	12.34 FIT	99.37%	0.00%	77.60%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

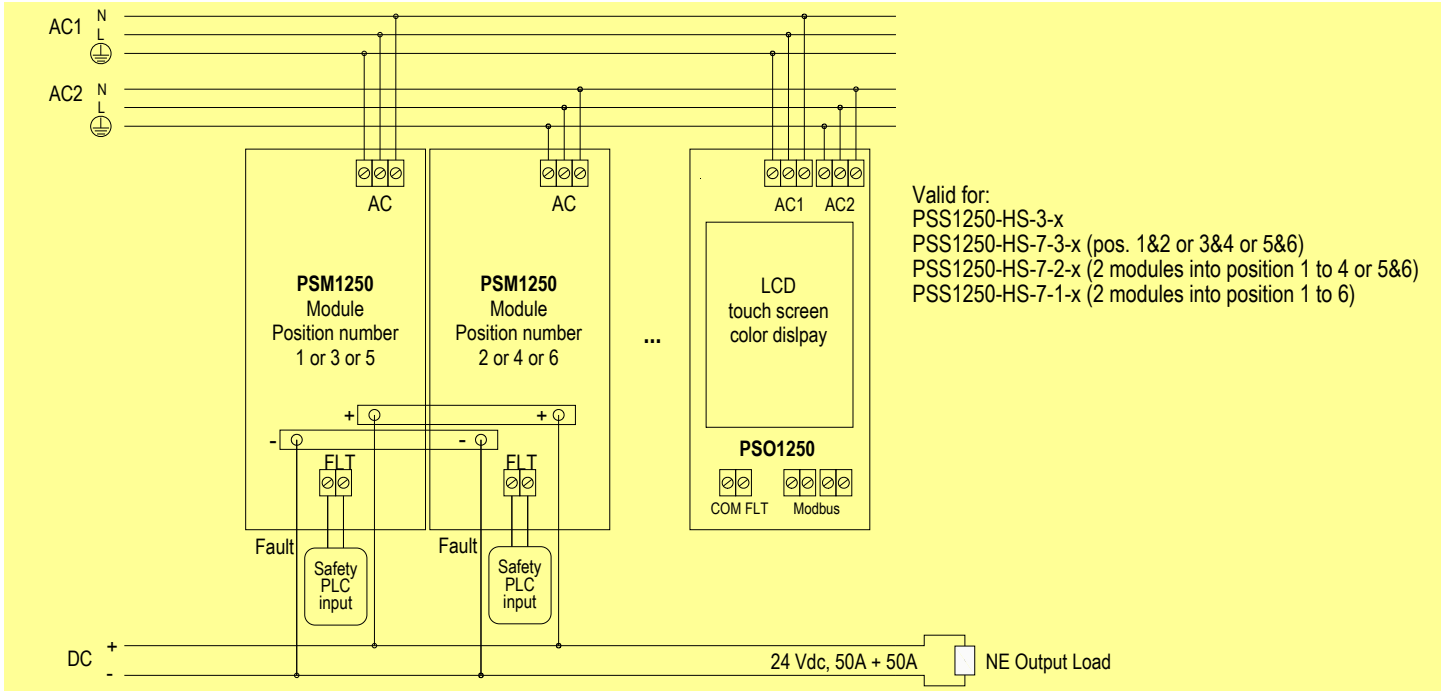
T[Proof] = 1 year	T[Proof] = 18 years
PFDavg = 5.45E-05 Valid for SIL 3	PFDavg = 9.81E-04 Valid for SIL 2

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 3 years	T[Proof] = 20 years
PFDavg = 1.63E-04 Valid for SIL 3	PFDavg = 1.09E-03 Valid for SIL 2

Systematic capability SIL 3.

Application of PSS1250 with HS and two paralleled PSM1250 modules, for NE output load



Valid for:
 PSS1250-HS-3-x
 PSS1250-HS-7-3-x (pos. 1&2 or 3&4 or 5&6)
 PSS1250-HS-7-2-x (2 modules into position 1 to 4 or 5&6)
 PSS1250-HS-7-1-x (2 modules into position 1 to 6)

Description: In normal operation two paralleled PSM1250 modules are powered by connecting AC1 input supply to one module and AC2 input supply to other one by means of related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). For each PSM1250 module, its fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies under/over voltage module faults to logic solver, which can require to turn off this power supply and to replace it with a new PSM1250 module. In absence of module fault the relay contact is closed, while in presence of module fault the relay contact is open. The green Power ON LED of each PSM1250 is lit in presence of AC input supply.

The outputs of two PSM1250 modules are already paralleled on the Wall Mounting Panel backboard by specific copper bars. Therefore, the NE output load is connected to outputs of both PSM1250 modules (by related output copper bars with screw terminals on the Wall Mounting Panel backboard). In normal condition, NE output load is Normally Energized (NE). In absence of one only AC input supply (AC1 or AC2), one PSM1250 module is shutdown (its fault relay contact is open) but the other one operates in normal condition, so that output load is normally energized. In absence of both AC input supplies (AC1 and AC2), both paralleled PSM1250 modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State).

Safety Function and Failure behavior: PSS1250 with HS and two paralleled PSM1250 modules is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0. The failure behaviour of two paralleled PSM1250 modules for NE load is described by the following definitions :

- Fail-Safe State: it is defined as the paralleled outputs going below 2 Vdc. Internal diagnostics detect and notify Low/High (Under/Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off all malfunctioning power supplies and to replace them with new PSM1250 modules.
- Fail Safe: failure mode that causes the 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), so that the paralleled output voltage is blocked or oscillating between 2 and 20 Vdc or above 30 Vdc, and both internal diagnostics cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the paralleled output to go above 30 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 30 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 31 Vdc. Internal diagnostics detect and notify High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the paralleled output to go between 2 and 20 Vdc. Internal diagnostics detect and notify Low fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- 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, so that the paralleled output voltage is deviated between 20 and 30 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	5.86
λ_{du} = Total Dangerous Undetected failures	2.83
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	94.54
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	103.23
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	1105 years
$\lambda_{no\ effect}$ = "No Effect" failures	6082.53
$\lambda_{not\ part}$ = "Not Part" failures	534.18
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	6719.94
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	17 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5*8760 + 8)h + \lambda_{dd} * 8h$	1.246E-05

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCD
0.00 FIT	94.54 FIT	5.86 FIT	2.83 FIT	97.26%	0.00%	67.47%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

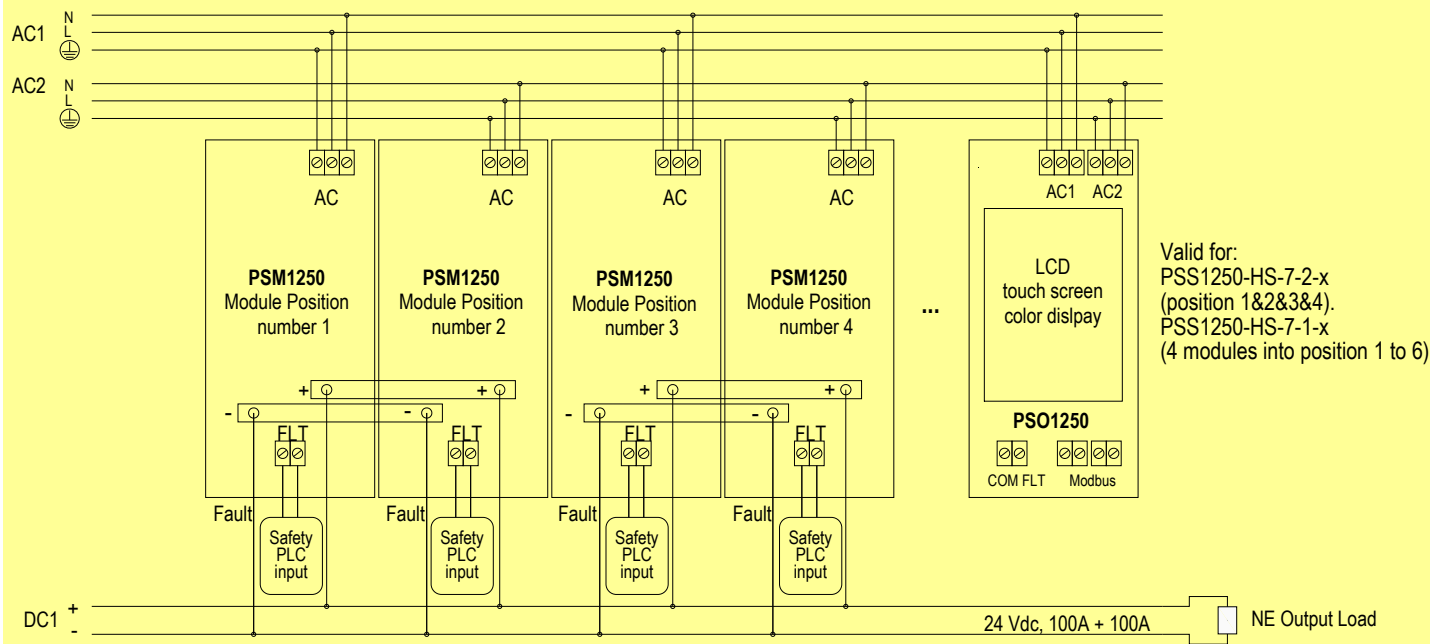
T[Proof] = 8 years	T[Proof] = 20 years
PFDavg = 9.97E-05 Valid for SIL 3	PFDavg = 2.49E-04 Valid for SIL 2

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 16 years	T[Proof] = 20 years
PFDavg = 1.99E-04 Valid for SIL 3	PFDavg = 2.49E-04 Valid for SIL 2

Systematic capability SIL 3.

Application of PSS1250 with HS and four PSM1250 modules, for NE output load



Description: In normal operation four paralleled PSM1250 modules are powered by connecting AC1 input supply to two modules and AC2 input supply to other ones by means of related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). For each PSM1250 module, its fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies under/over voltage module faults to logic solver, which can require to turn off this power supply and to replace it with a new PSM1250 module. In absence of module fault the relay contact is closed, while in presence of module fault the relay contact is open. The green Power ON LED of each PSM1250 is lit in presence of AC input supply.

The outputs of four PSM1250 modules are already paralleled on the Wall Mounting Panel backboard by specific copper bars. Therefore, the NE output load is connected to outputs of four PSM1250 modules (by related output copper bars with screw terminals on the Wall Mounting Panel backboard). In normal condition, NE output load is Normally Energized (NE). In absence of one only AC input supply (AC1 or AC2), two PSM1250 modules are shutdown (their fault relay contacts are open) but the other ones operate in normal condition, so that output load is normally energized.

In absence of both AC input supplies (AC1 and AC2), four paralleled PSM1250 modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State).

Safety Function and Failure behavior: PSS1250 with HS and four paralleled PSM1250 modules is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0. The failure behaviour of four paralleled PSM1250 modules for NE load is described by the following definitions :

- Fail-Safe State: it is defined as the paralleled outputs going below 2 Vdc. Internal diagnostics detect and notify Low/High (Under/Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off all malfunctioning power supplies and to replace them with new PSM1250 modules.
- Fail Safe: failure mode that causes the 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), so that the paralleled output voltage is blocked or oscillating between 2 and 20 Vdc or above 30 Vdc, and both internal diagnostics cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the paralleled output to go above 30 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 30 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 31 Vdc. Internal diagnostics detect and notify High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the paralleled output to go between 2 and 20 Vdc. Internal diagnostics detect and notify Low fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- 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, so that the paralleled output voltage is deviated between 20 and 30 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	9.68
λ_{du} = Total Dangerous Undetected failures	5.09
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	94.54
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	109.32
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	1044 years
$\lambda_{no\ effect}$ = "No Effect" failures	12262.20
$\lambda_{not\ part}$ = "Not Part" failures	1068.36
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	13439.88
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	8 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5 * 8760 + 8)h + \lambda_{dd} * 8h$	2.241E-05

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _s	DC _D
0.00 FIT	94.54 FIT	9.68 FIT	5.09 FIT	95.34%	0.00%	65.53%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

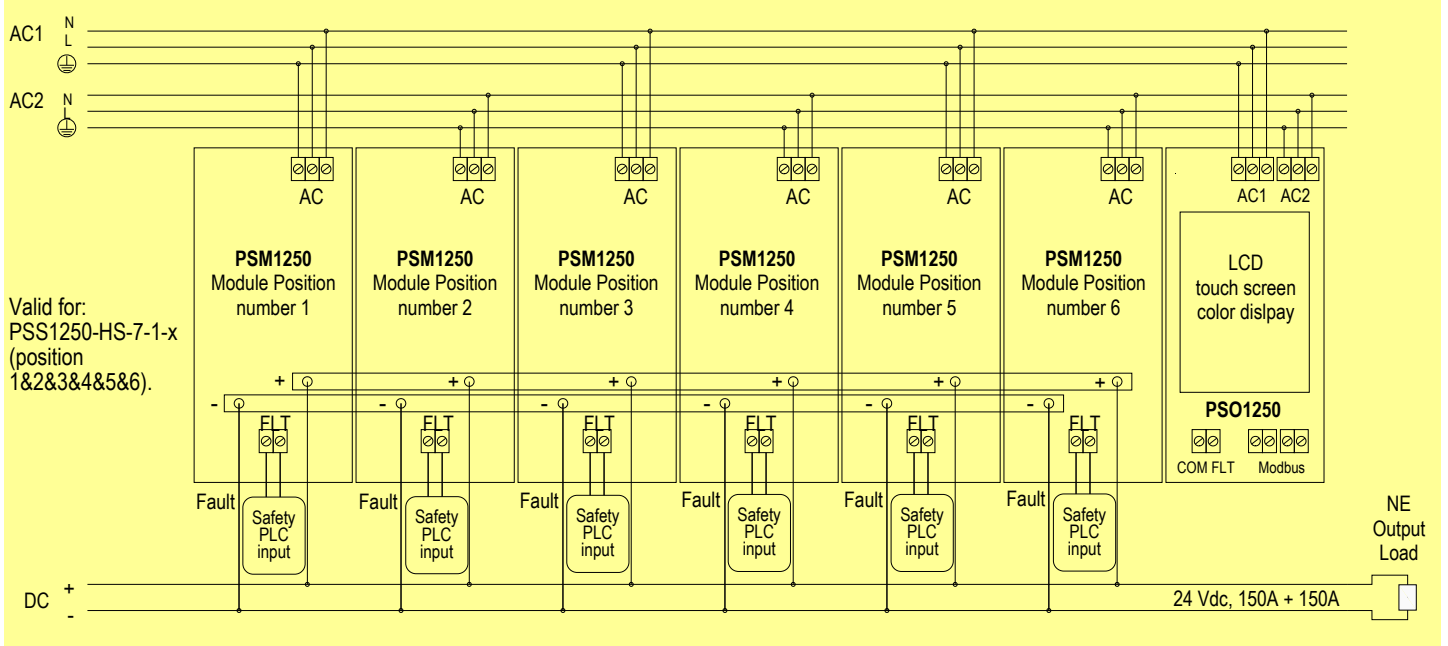
T[Proof] = 4 years	T[Proof] = 20 years
PFDavg = 8.96E-05 Valid for SIL 3	PFDavg = 4.48E-04 Valid for SIL 2

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 8 years	T[Proof] = 20 years
PFDavg = 1.79E-04 Valid for SIL 3	PFDavg = 4.48E-04 Valid for SIL 2

Systematic capability SIL 3.

Application of PSS1250 with HS and six paralleled PSM1250 modules, for NE output load



Description: In normal operation six paralleled PSM1250 modules are powered by connecting AC1 input supply to three modules and AC2 input supply to other ones by means of related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). For each PSM1250 module, its fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies under/over voltage module faults to logic solver, which can require to turn off this power supply and to replace it with a new PSM1250 module. In absence of module fault the relay contact is closed, while in presence of module fault the relay contact is open.

The green Power ON LED of each PSM1250 is lit in presence of AC input supply.

The outputs of six PSM1250 modules are already paralleled on the Wall Mounting Panel backboard by specific copper bars. Therefore, the NE output load is connected to outputs of six PSM1250 modules (by related output copper bars with screw terminals on the Wall Mounting Panel backboard). In normal condition, NE output load is Normally Energized (NE). In absence of one only AC input supply (AC1 or AC2), three PSM1250 modules are shutdown (their fault relay contacts are open) but the other ones operate in normal condition, so that output load is normally energized.

Safety Function and Failure behavior:

PSS1250 with HS and six paralleled PSM1250 modules is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of six paralleled PSM1250 modules for NE load is described by the following definitions :

- Fail-Safe State: it is defined as the paralleled outputs going below 2 Vdc. Internal diagnostics detect and notify Low/High (Under/Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off all malfunctioning power supplies and to replace them with new PSM1250 modules.
- Fail Safe: failure mode that causes the 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), so that the paralleled output voltage is blocked or oscillating between 2 and 20 Vdc or above 30 Vdc, and both internal diagnostics cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the paralleled output to go above 30 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 30 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 31 Vdc. Internal diagnostics detect and notify High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the paralleled output to go between 2 and 20 Vdc. Internal diagnostics detect and notify Low fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- 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, so that the paralleled output voltage is deviated between 20 and 30 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	13.50
λ_{du} = Total Dangerous Undetected failures	7.36
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	94.54
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	115.41
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	989 years
$\lambda_{no\ effect}$ = "No Effect" failures	18441.87
$\lambda_{not\ part}$ = "Not Part" failures	1602.54
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	20159.82
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	6 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5 * 8760 + 8)h + \lambda_{dd} * 8h$	3.24E-05

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _s	DC _D
0.00 FIT	94.54 FIT	13.50 FIT	7.36 FIT	93.62%	0.00%	64.72%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

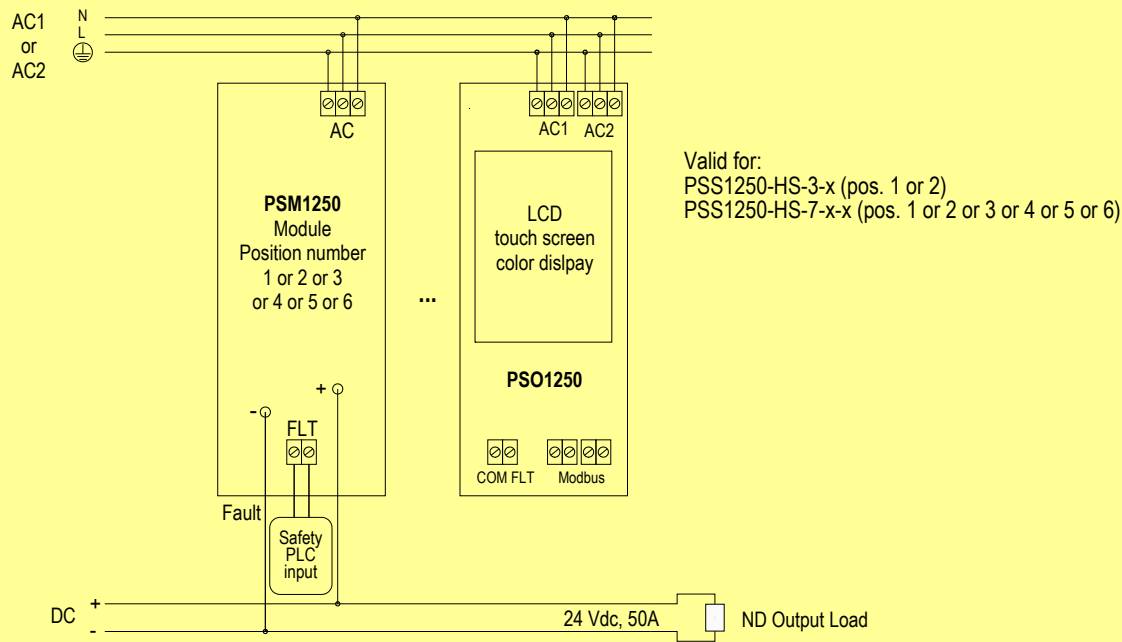
T[Proof] = 3 years	T[Proof] = 20 years
PFDavg = 9.72E-05 Valid for SIL 3	PFDavg = 6.48E-04 Valid for SIL 2

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 6 years	T[Proof] = 20 years
PFDavg = 1.94E-04 Valid for SIL 3	PFDavg = 6.48E-04 Valid for SIL 2

Systematic capability SIL 3.

Application of PSS1250 with HS and single PSM1250 module, for ND output load



Description:

In normal operation the PSM1250 module is unpowered because of absence of AC input supply, which is connected to related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). The fault relay contact can be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies under/over voltage dangerous faults to logic solver, which can only require to turn off power supply and to replace it with a new PSM1250 module. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

In normal condition, absence of AC input supply implies that the green Power ON LED of PSM1250 is turned off, fault relay contact is open and the ND output load (connected to related output copper bars with screw terminals on the Wall Mounting Panel backboard) is Normally De-energized (ND).

In presence of AC input supply, the green Power ON LED of PSM1250 is lit, fault relay contact is closed (if fault is absent) and output load is energized (Safe State).

Safety Function and Failure behavior:

PSS1250 with HS and single PSM1250 module is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0. The failure behaviour of PSM1250 for ND load is described by the following definitions :

- Fail-Safe State: it is defined as the output going between 20 and 30 Vdc.
- 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 (i.e. being unable to go to the defined fail-safe state), so that the output voltage is blocked or oscillating between 0 and 20 Vdc or above 30 Vdc, and internal diagnostic cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the output to go above 30 Vdc. Internal overvoltage protection tries to limit output voltage < 30 Vdc, otherwise for output ≥ 31 Vdc internal crowbars trip, turning off the power supply. In any case, this failure mode is dangerous, but internal diagnostic notifies High fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off power supply and to replace it with a new PSM1250 module.
- Fail Low - Undervoltage: failure mode that causes the output to go between 0 and 20 Vdc. This failure mode is dangerous, but internal diagnostic notifies Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off power supply and to replace it with a new PSM1250 module.
- 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application. Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.00
λ_{du} = Total Dangerous Undetected failures	1945.97
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	1146.91
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	3092.88
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	36 years
$\lambda_{not\ part}$ = "Not Part" failures	267.09
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	3359.97
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	34 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5*8760 + 8)h + \lambda_{dd} * 8h$	8.54E-03

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCD
0.00 FIT	1146.91 FIT	0.00 FIT	1945.97 FIT	37.08%	0.00%	0.00%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

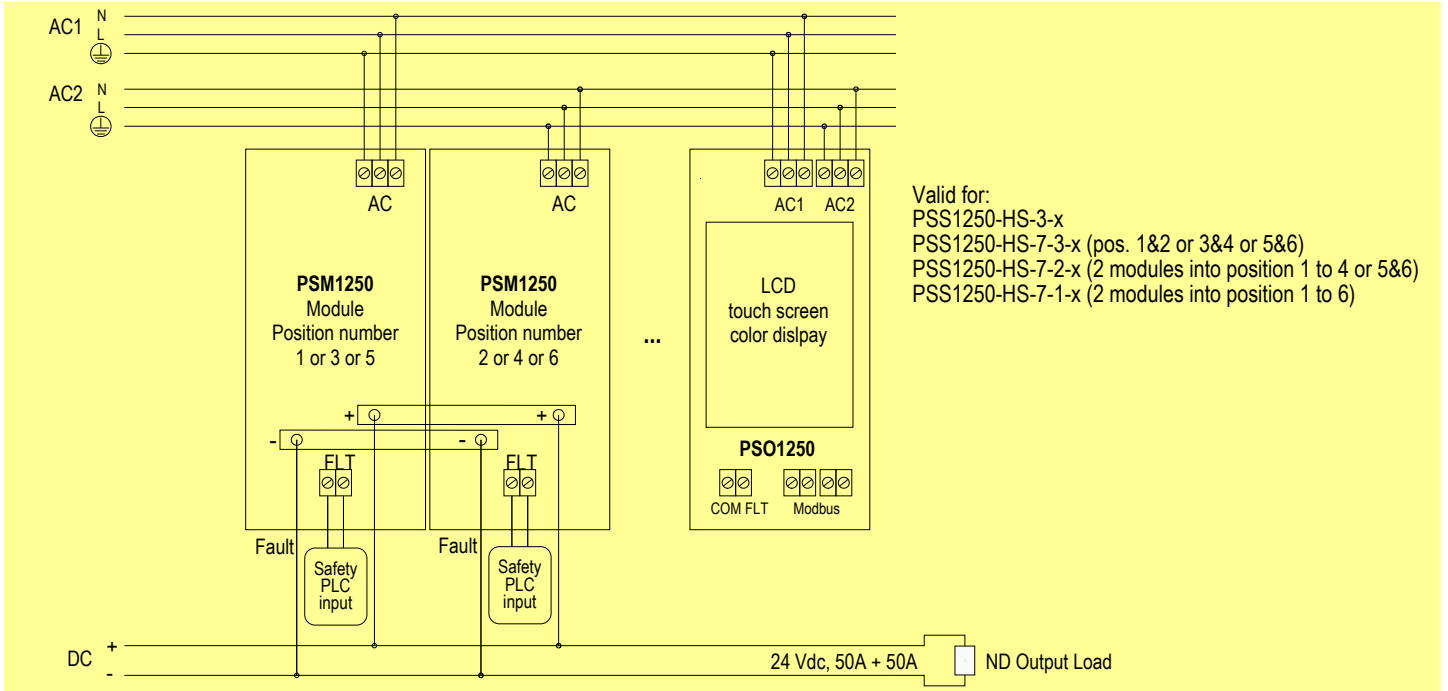
T[Proof] = 1 year
 PFDavg = 8.54E-03 Valid for SIL 1

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 2 years
 PFDavg = 1.71E-02 Valid for SIL 1

Systematic capability SIL 3.

Application of PSS1250 with HS and two paralleled PSM1250 modules, for ND output load



Valid for:
 PSS1250-HS-3-x
 PSS1250-HS-7-3-x (pos. 1&2 or 3&4 or 5&6)
 PSS1250-HS-7-2-x (2 modules into position 1 to 4 or 5&6)
 PSS1250-HS-7-1-x (2 modules into position 1 to 6)

Description: In normal operation two paralleled PSM1250 modules are unpowered because of absence of both AC input supplies (AC1 and AC2), where AC1 is connected to one module and AC2 to other one by means of related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). For each PSM1250 module, its fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies over voltage module faults to logic solver, which can require to turn off this power supply and to replace it with a new PSM1250 module. In absence of module fault the relay contact is closed, while in presence of module fault the relay contact is open.

The outputs of two PSM1250 modules are already paralleled on the Wall Mounting Panel backboard by specific copper bars. Therefore, the ND output load is connected to outputs of both PSM1250 modules (by related output copper bars with screw terminals on Wall Mounting Panel backboard). In normal condition, absence of both AC input supplies (AC1 and AC2) implies that both green Power ON LEDs of PSM1250 modules are turned off, both fault relay contacts are open and the ND output load is Normally De-energized (ND). In presence of one only AC input supply (AC1 or AC2), one PSM1250 module is shutdown (its fault relay contact is open) but the other one is correctly turned on, so that output load is energized (Safe State). In presence of both AC input supplies (AC1 and AC2), both paralleled PSM1250 modules are correctly turned on and output load is energized (Safe State).

Safety Function and Failure behavior:

PSS1250 with HS and two paralleled PSM1250 modules is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of two paralleled PSM1250 modules for ND load is described by the following definitions :

- Fail-Safe State: it is defined as the the paralleled outputs going between 20 and 30 Vdc. Internal diagnostics detect and notify High (Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off malfunctioning power supply and to replace it with new PSM1250 modules.
- Fail Safe: failure mode that causes the 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), so that the paralleled output voltage is blocked or oscillating between 0 and 20 Vdc or above 30 Vdc, and internal diagnostic cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the paralleled output to go above 30 Vdc. Internal overvoltage protection tries to limit output voltage < 30 Vdc, otherwise for output ≥ 31 Vdc internal crowbars trip, turning off malfunctioning power supply. Internal diagnostics detect and notify High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the paralleled output to go between 0 and 20 Vdc. This failure mode is dangerous, but internal diagnostic notifies Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off malfunctioning power supply and to replace it with a new PSM1250 module.
- 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	3.82
λ_{du} = Total Dangerous Undetected failures	99.41
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	6082.53
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	6185.76
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	18 years
$\lambda_{not\ part}$ = "Not Part" failures	534.18
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	6719.94
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	17 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5*8760 + 8)h + \lambda_{dd} * 8h$	4.36E-04

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _s	DC _D
0.00 FIT	6082.53 FIT	3.82 FIT	99.41 FIT	98.39%	0.00%	3.70%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

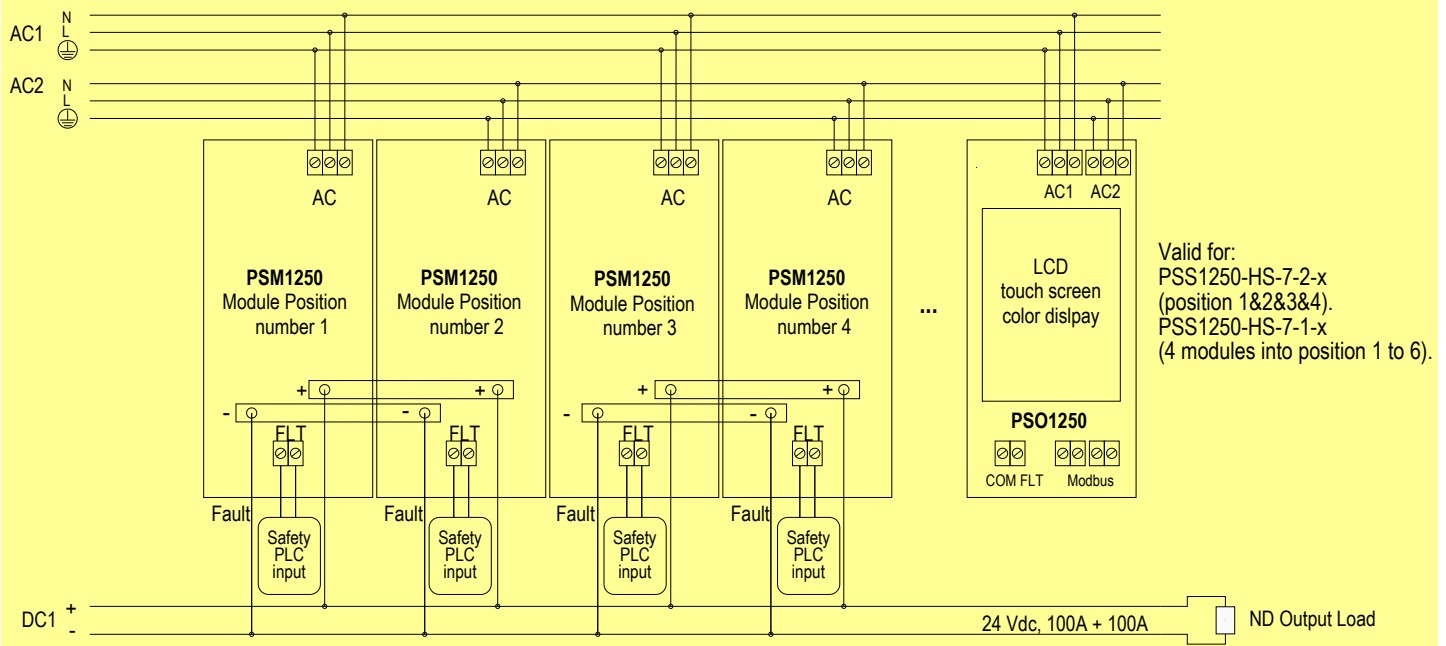
T[Proof] = 2 years	T[Proof] = 20 years
PFDavg = 8.72E-04 Valid for SIL 2	PFDavg = 8.72E-03 Valid for SIL 1

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 4 years	T[Proof] = 20 years
PFDavg = 1.74E-03 Valid for SIL 2	PFDavg = 8.72E-03 Valid for SIL 1

Systematic capability SIL 3.

Application of PSS1250 with HS and four PSM1250 modules, for ND output load



Valid for:
PSS1250-HS-7-2-x
(position 1&2&3&4).
PSS1250-HS-7-1-x
(4 modules into position 1 to 6).

Description: In normal operation four paralleled PSM1250 modules are unpowered because of absence of both AC input supplies (AC1 and AC2), where AC1 is connected to two modules and AC2 to other ones by means of related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). For each PSM1250 module, its fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies over voltage module faults to logic solver, which can require to turn off this power supply and to replace it with a new PSM1250 module. In absence of module fault the relay contact is closed, while in presence of module fault the relay contact is open.

The outputs of four PSM1250 modules are already paralleled on the Wall Mounting Panel backboard by specific copper bars. Therefore, the ND output load is connected to outputs of four PSM1250 modules (by related output copper bars with screw terminals on Wall Mounting Panel backboard). In normal condition, absence of both AC input supplies (AC1 and AC2) implies that four green Power ON LEDs of PSM1250 modules are turned off, four fault relay contacts are open and the ND output load is Normally De-energized (ND).

In presence of one only AC input supply (AC1 or AC2), two PSM1250 module are shutdown (their fault relay contact are open) but the other ones are correctly turned on, so that output load is energized (Safe State). In presence of both AC input supplies (AC1 and AC2), four paralleled PSM1250 modules are correctly turned on and output load is energized (Safe State).

Safety Function and Failure behavior:

PSS1250 with HS and four paralleled PSM1250 modules is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of four paralleled PSM1250 modules for ND load is described by the following definitions :

- Fail-Safe State: it is defined as the the paralleled outputs going between 20 and 30 Vdc. Internal diagnostics detect and notify High (Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off malfunctioning power supply and to replace it with new PSM1250 modules.
- Fail Safe: failure mode that causes the 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), so that the paralleled output voltage is blocked or oscillating between 0 and 20 Vdc or above 30 Vdc, and internal diagnostic cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the paralleled output to go above 30 Vdc. Internal overvoltage protection tries to limit output voltage < 30 Vdc, otherwise for output ≥ 31 Vdc internal crowbars trip, turning off malfunctioning power supply. Internal diagnostics detect and notify High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the paralleled output to go between 0 and 20 Vdc. This failure mode is dangerous, but internal diagnostic notifies Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off malfunctioning power supply and to replace it with a new PSM1250 module.
- 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	7.64
λ_{du} = Total Dangerous Undetected failures	101.68
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	12262.20
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	12371.52
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	9 years
$\lambda_{not\ part}$ = "Not Part" failures	1068.36
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	13439.88
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	8 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5*8760 + 8)h + \lambda_{dd} * 8h$	4.46E-04

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _s	DC _D
0.00 FIT	12262.20 FIT	7.64 FIT	101.68 FIT	99.18%	0.00%	6.99%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

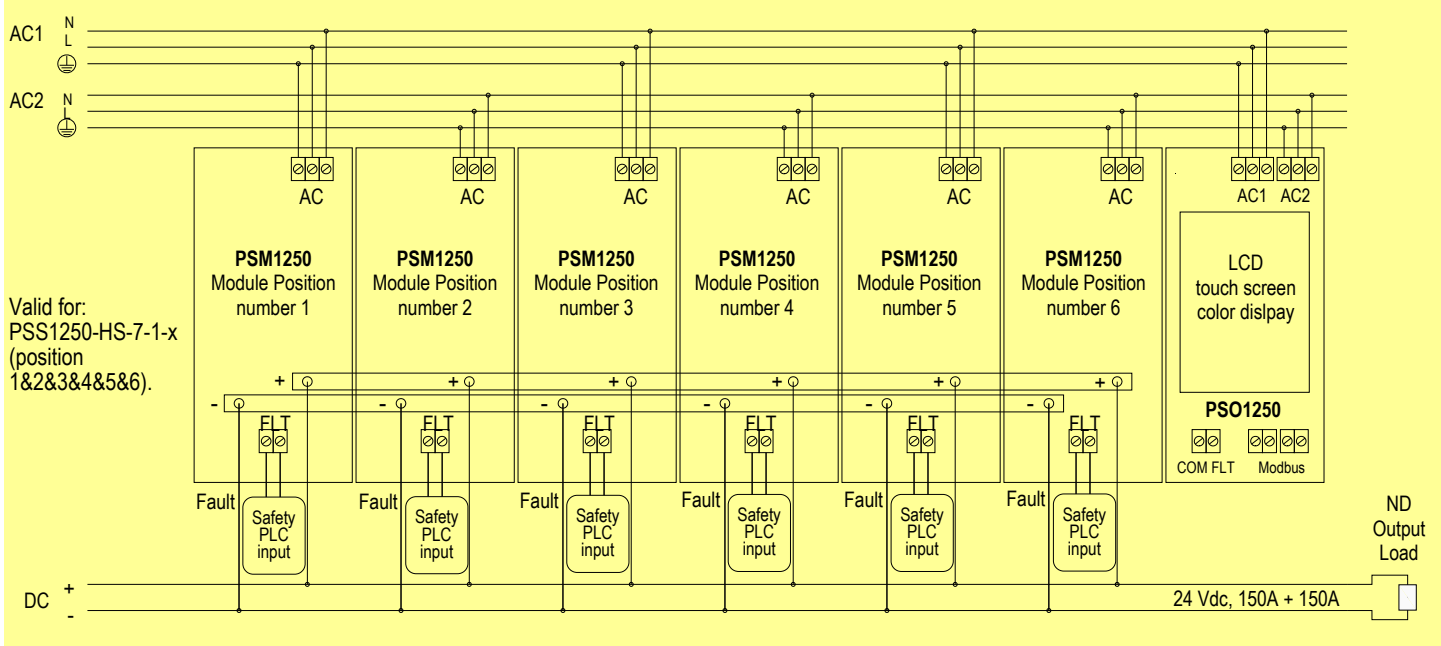
T[Proof] = 2 years	T[Proof] = 20 years
PFDavg = 8.92E-04 Valid for SIL 2	PFDavg = 8.92E-03 Valid for SIL 1

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 4 years	T[Proof] = 20 years
PFDavg = 1.78E-03 Valid for SIL 2	PFDavg = 8.92E-03 Valid for SIL 1

Systematic capability SIL 3.

Application of PSS1250 with HS and six paralleled PSM1250 modules, for ND output load



Description:

In normal operation six paralleled PSM1250 modules are unpowered because of absence of both AC input supplies (AC1 and AC2), where AC1 is connected to three modules and AC2 to other ones by means of related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). For each PSM1250 module, its fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies over voltage module faults to logic solver, which can require to turn off this power supply and to replace it with a new PSM1250 module. In absence of module fault the relay contact is closed, while in presence of module fault the relay contact is open.

The outputs of six PSM1250 modules are already paralleled on the Wall Mounting Panel backboard by specific copper bars. Therefore, the ND output load is connected to outputs of six PSM1250 modules (by related output copper bars with screw terminals on Wall Mounting Panel backboard). In normal condition, absence of both AC input supplies (AC1 and AC2) implies that six green Power ON LEDs of PSM1250 modules are turned off, six fault relay contacts are open and the ND output load is Normally De-energized (ND).

In presence of one only AC input supply (AC1 or AC2), three PSM1250 module are shutdown (their fault relay contact are open) but the other ones are correctly turned on, so that output load is energized (Safe State). In presence of both AC input supplies (AC1 and AC2), six paralleled PSM1250 modules are correctly turned on and output load is energized (Safe State).

Safety Function and Failure behavior:

PSS1250 with HS and six paralleled PSM1250 modules is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of six paralleled PSM1250 modules for ND load is described by the following definitions :

- Fail-Safe State: it is defined as the the paralleled outputs going between 20 and 30 Vdc. Internal diagnostics detect and notify High (Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off malfunctioning power supply and to replace it with new PSM1250 modules.
- Fail Safe: failure mode that causes the 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), so that the paralleled output voltage is blocked or oscillating between 0 and 20 Vdc or above 30 Vdc, and internal diagnostic cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the paralleled output to go above 30 Vdc. Internal overvoltage protection tries to limit output voltage < 30 Vdc, otherwise for output ≥ 31 Vdc internal crowbars trip, turning off malfunctioning power supply. Internal diagnostics detect and notify High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the paralleled output to go between 0 and 20 Vdc. This failure mode is dangerous, but internal diagnostic notifies Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off malfunctioning power supply and to replace it with a new PSM1250 module.
- 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	11.46
λ_{du} = Total Dangerous Undetected failures	103.95
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	18441.87
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	18557.28
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	6 years
$\lambda_{not\ part}$ = "Not Part" failures	1602.54
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	20159.82
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	6 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5*8760 + 8)h + \lambda_{dd} * 8h$	4.56E-04

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _s	DC _D
0.00 FIT	18441.87 FIT	11.46 FIT	103.95 FIT	99.44%	0.00%	9.93%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

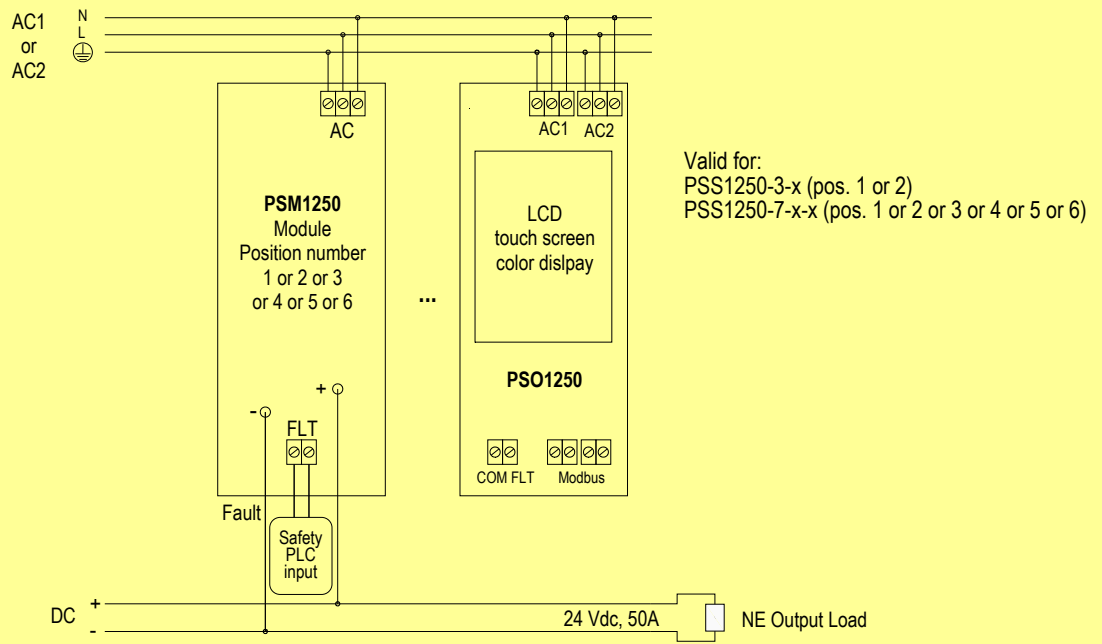
T[Proof] = 2 years	T[Proof] = 20 years
PFDavg = 9.12E-04 Valid for SIL 2	PFDavg = 9.12E-03 Valid for SIL 1

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 4 years	T[Proof] = 20 years
PFDavg = 1.82E-03 Valid for SIL 2	PFDavg = 9.12E-03 Valid for SIL 1

Systematic capability SIL 3.

Application of PSS1250 without HS and single PSM1250 module, for NE output load



Description:

In normal operation the PSM1250 module is powered by connecting AC input supply to related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). The fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies under/over voltage faults to logic solver, which can require to turn off power supply and to replace it with a new PSM1250 module. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open. The green Power ON LED of PSM1250 is lit in presence of AC input supply. In this condition the NE output load (connected to related output copper bars with screw terminals on the Wall Mounting Panel backboard) is Normally Energized (NE). In absence of AC input supply, the PSM1250 module is shutdown (its fault relay contact is open) and output load is de-energized (Safe State).

Safety Function and Failure behavior:

PSS1250 without HS and single PSM1250 module is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0. The failure behaviour of PSM1250 for NE load is described by the following definitions :

- Fail-Safe State: it is defined as the output going below 2 Vdc. Internal diagnostic detects and notifies Low/High (Under/Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off power supply and to replace it with a new PSM1250 module.
- 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 (i.e. being unable to go to the defined fail-safe state), so that the output voltage is blocked or oscillating between 2 and 20 Vdc or above 30 Vdc, and internal diagnostic cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the output to go above 30 Vdc. Internal overvoltage protection tries to limit output voltage < 30 Vdc, otherwise internal crowbars trip to fail safe state for output ≥ 31 Vdc. Internal diagnostic detects and notifies High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the output to go between 2 and 20 Vdc. Internal diagnostic detects and notifies Low fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- 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, so that the output voltage is deviated between 20 and 30 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	42.51
λ_{du} = Total Dangerous Undetected failures	12.34
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	1635.27
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	1690.12
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + \text{MTTR (8 hours)}$	67 years
$\lambda_{no\ effect}$ = "No Effect" failures	938.09
$\lambda_{not\ part}$ = "Not Part" failures	169.89
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	2798.10
MTBF (device) = $(1 / \lambda_{tot\ device}) + \text{MTTR (8 hours)}$	40 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5*8760 + 8)h + \lambda_{dd} * 8h$	5.449E-05

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _s	DC _D
0.00 FIT	1635.27 FIT	42.51 FIT	12.34 FIT	99.27%	0.00%	77.50%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

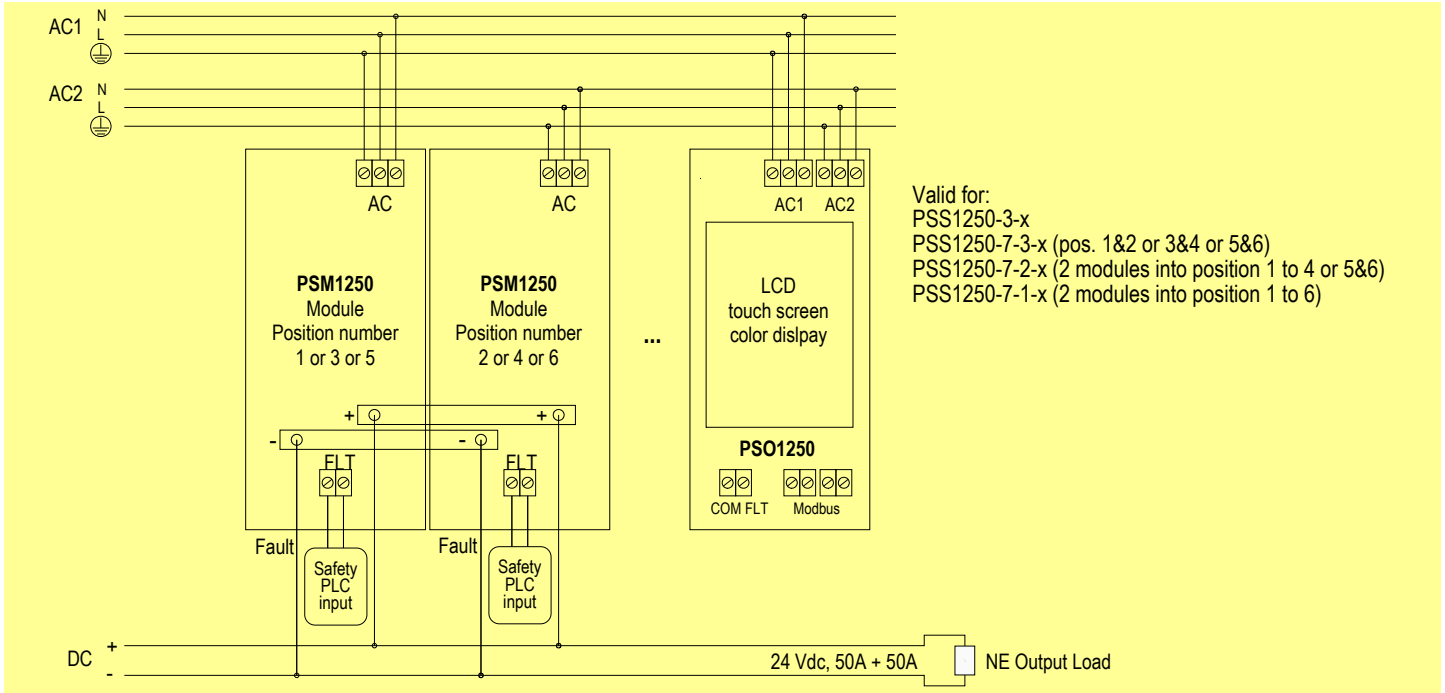
T[Proof] = 1 year	T[Proof] = 18 years
PFDavg = 5.45E-05 Valid for SIL 3	PFDavg = 9.81E-04 Valid for SIL 2

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 3 years	T[Proof] = 20 years
PFDavg = 1.63E-04 Valid for SIL 3	PFDavg = 1.09E-03 Valid for SIL 2

Systematic capability SIL 3.

Application of PSS1250 without HS and two paralleled PSM1250 modules, for NE output load



Description: In normal operation two paralleled PSM1250 modules are powered by connecting AC1 input supply to one module and AC2 input supply to other one by means of related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). For each PSM1250 module, its fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies under/over voltage module faults to logic solver, which can require to turn off this power supply and to replace it with a new PSM1250 module. In absence of module fault the relay contact is closed, while in presence of module fault the relay contact is open. The green Power ON LED of each PSM1250 is lit in presence of AC input supply.

The outputs of two PSM1250 modules are already paralleled on the Wall Mounting Panel backboard by specific copper bars. Therefore, the NE output load is connected to outputs of both PSM1250 modules (by related output copper bars with screw terminals on the Wall Mounting Panel backboard). In normal condition, NE output load is Normally Energized (NE). In absence of one only AC input supply (AC1 or AC2), one PSM1250 module is shutdown (its fault relay contact is open) but the other one operates in normal condition, so that output load is normally energized. In absence of both AC input supplies (AC1 and AC2), both paralleled PSM1250 modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State).

Safety Function and Failure behavior: PSS1250 without HS and two paralleled PSM1250 modules is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0. The failure behaviour of two paralleled PSM1250 modules for NE load is described by the following definitions :

- Fail-Safe State: it is defined as the paralleled outputs going below 2 Vdc. Internal diagnostics detect and notify Low/High (Under/Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off all malfunctioning power supplies and to replace them with new PSM1250 modules.
- Fail Safe: failure mode that causes the 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), so that the paralleled output voltage is blocked or oscillating between 2 and 20 Vdc or above 30 Vdc, and both internal diagnostics cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the paralleled output to go above 30 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 30 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 31 Vdc. Internal diagnostics detect and notify High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the paralleled output to go between 2 and 20 Vdc. Internal diagnostics detect and notify Low fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- 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, so that the paralleled output voltage is deviated between 20 and 30 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application. Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	5.85
λ_{du} = Total Dangerous Undetected failures	2.83
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	81.76
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	90.44
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	1262 years
$\lambda_{no\ effect}$ = "No Effect" failures	5165.98
$\lambda_{not\ part}$ = "Not Part" failures	339.78
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	5596.20
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	20 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5*8760 + 8)h + \lambda_{dd} * 8h$	1.246E-05

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCD
0.00 FIT	81.76 FIT	5.85 FIT	2.83 FIT	96.88%	0.00%	67.42%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

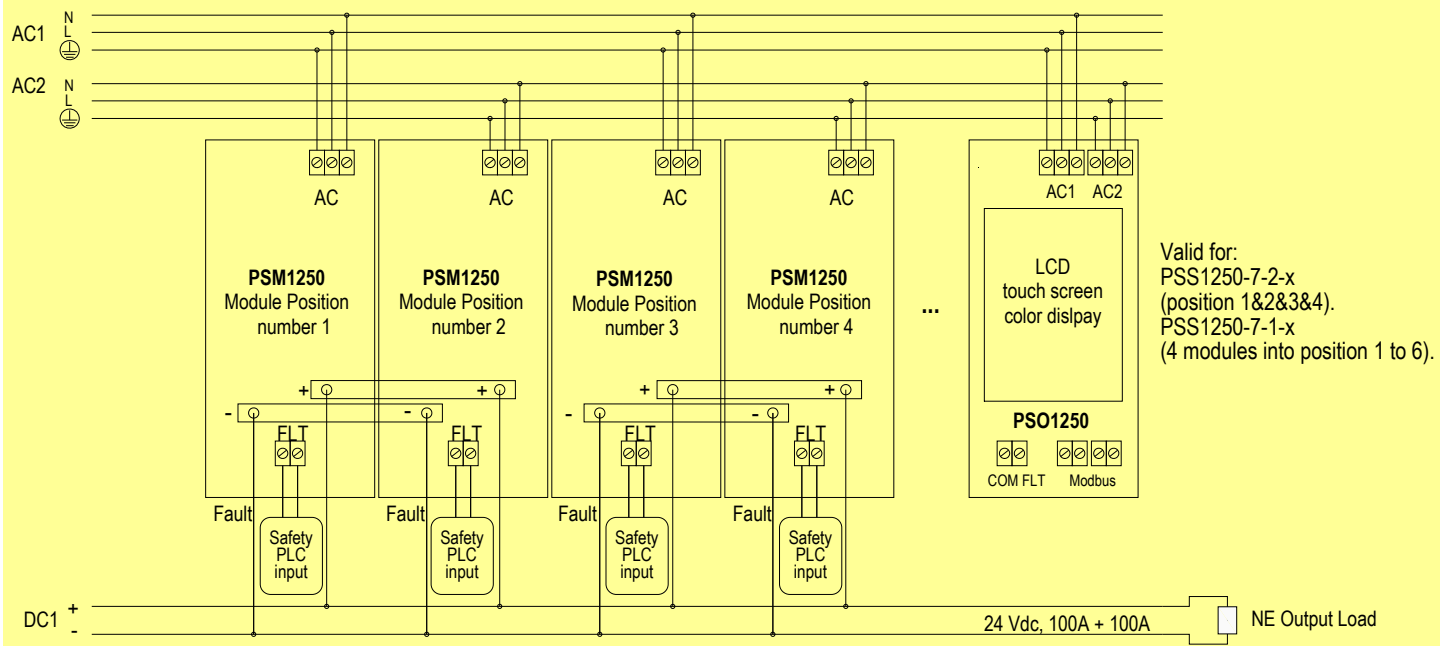
T[Proof] = 8 years	T[Proof] = 20 years
PFDavg = 9.97E-05 Valid for SIL 3	PFDavg = 2.49E-04 Valid for SIL 2

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 16 years	T[Proof] = 20 years
PFDavg = 1.99E-04 Valid for SIL 3	PFDavg = 2.49E-04 Valid for SIL 2

Systematic capability SIL 3.

Application of PSS1250 without HS and four PSM1250 modules, for NE output load



Description: In normal operation four paralleled PSM1250 modules are powered by connecting AC1 input supply to two modules and AC2 input supply to other ones by means of related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). For each PSM1250 module, its fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies under/over voltage module faults to logic solver, which can require to turn off this power supply and to replace it with a new PSM1250 module. In absence of module fault the relay contact is closed, while in presence of module fault the relay contact is open. The green Power ON LED of each PSM1250 is lit in presence of AC input supply. The outputs of four PSM1250 modules are already paralleled on the Wall Mounting Panel backboard by specific copper bars. Therefore, the NE output load is connected to outputs of four PSM1250 modules (by related output copper bars with screw terminals on the Wall Mounting Panel backboard). In normal condition, NE output load is Normally Energized (NE). In absence of one only AC input supply (AC1 or AC2), two PSM1250 modules are shutdown (their fault relay contacts are open) but the other ones operate in normal condition, so that output load is normally energized. In absence of both AC input supplies (AC1 and AC2), four paralleled PSM1250 modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State).

- Safety Function and Failure behavior:** PSS1250 without HS and four paralleled PSM1250 modules is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0. The failure behaviour of four paralleled PSM1250 modules for NE load is described by the following definitions :
- Fail-Safe State: it is defined as the paralleled outputs going below 2 Vdc. Internal diagnostics detect and notify Low/High (Under/Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off all malfunctioning power supplies and to replace them with new PSM1250 modules.
 - Fail Safe: failure mode that causes the 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), so that the paralleled output voltage is blocked or oscillating between 2 and 20 Vdc or above 30 Vdc, and both internal diagnostics cannot detect and notify faults to logic solver.
 - Fail High - Overvoltage: failure mode that causes the paralleled output to go above 30 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 30 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 31 Vdc. Internal diagnostics detect and notify High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
 - Fail Low - Undervoltage: failure mode that causes the paralleled output to go between 2 and 20 Vdc. Internal diagnostics detect and notify Low fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
 - 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, so that the paralleled output voltage is deviated between 20 and 30 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application. Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	9.67
λ_{du} = Total Dangerous Undetected failures	5.09
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	81.76
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	96.53
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	1182 years
$\lambda_{no\ effect}$ = "No Effect" failures	10416.31
$\lambda_{not\ part}$ = "Not Part" failures	679.56
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	11192.40
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	10 years
PFDAvg (TI = 1 year) = $\lambda_{du} * (0.5 * 8760 + 8)h + \lambda_{dd} * 8h$	2.241E-05

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCD
0.00 FIT	81.76 FIT	9.67 FIT	5.09 FIT	94.72%	0.00%	65.50%

PFDAvg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

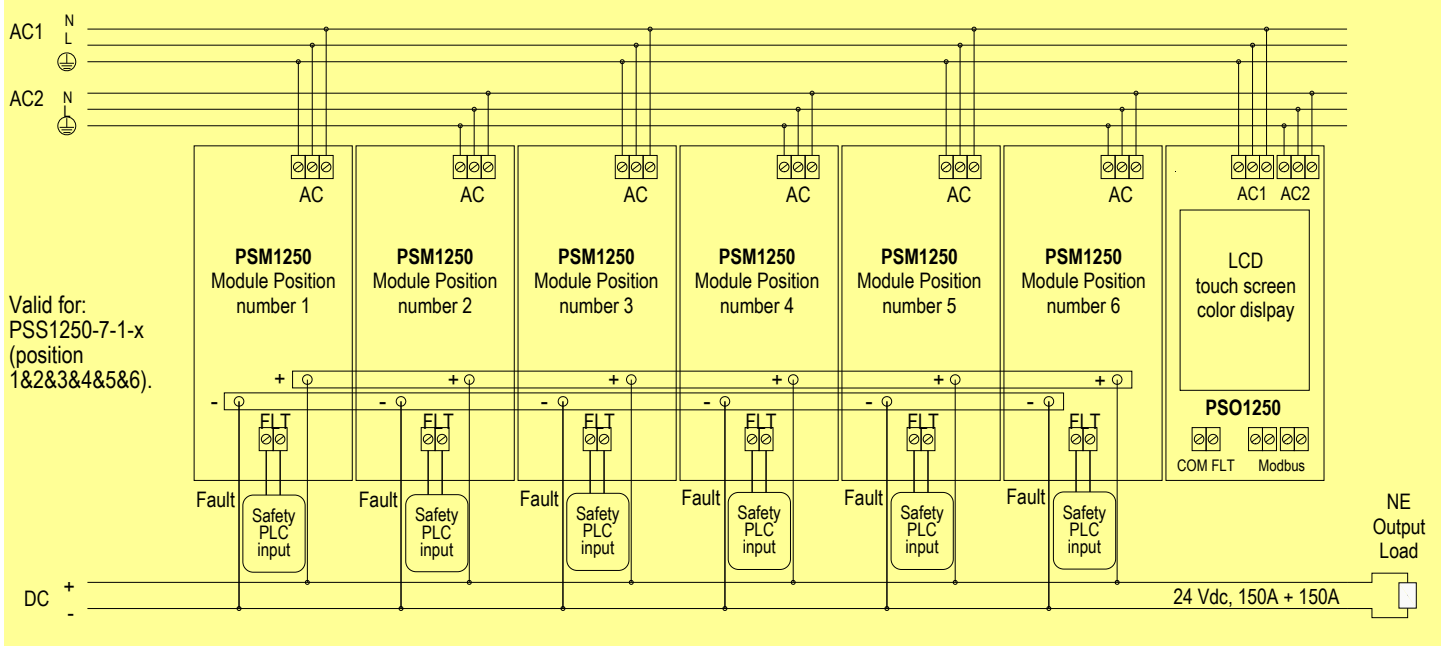
T[Proof] = 4 years	T[Proof] = 20 years
PFDAvg = 8.96E-05 Valid for SIL 3	PFDAvg = 4.48E-04 Valid for SIL 2

PFDAvg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 8 years	T[Proof] = 20 years
PFDAvg = 1.79E-04 Valid for SIL 3	PFDAvg = 4.48E-04 Valid for SIL 2

Systematic capability SIL 3.

Application of PSS1250 without HS and six paralleled PSM1250 modules, for NE output load



Description: In normal operation six paralleled PSM1250 modules are powered by connecting AC1 input supply to three modules and AC2 input supply to other ones by means of related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). For each PSM1250 module, its fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies under/over voltage module faults to logic solver, which can require to turn off this power supply and to replace it with a new PSM1250 module. In absence of module fault the relay contact is closed, while in presence of module fault the relay contact is open. The green Power ON LED of each PSM1250 is lit in presence of AC input supply.

The outputs of six PSM1250 modules are already paralleled on the Wall Mounting Panel backboard by specific copper bars. Therefore, the NE output load is connected to outputs of six PSM1250 modules (by related output copper bars with screw terminals on the Wall Mounting Panel backboard). In normal condition, NE output load is Normally Energized (NE). In absence of one only AC input supply (AC1 or AC2), three PSM1250 modules are shutdown (their fault relay contacts are open) but the other ones operate in normal condition, so that output load is normally energized. In absence of both AC input supplies (AC1 and AC2), six paralleled PSM1250 modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State).

Safety Function and Failure behavior: PSS1250 without HS and six paralleled PSM1250 modules is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0. The failure behaviour of six paralleled PSM1250 modules for NE load is described by the following definitions :

- Fail-Safe State: it is defined as the paralleled outputs going below 2 Vdc. Internal diagnostics detect and notify Low/High (Under/Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off all malfunctioning power supplies and to replace them with new PSM1250 modules.
- Fail Safe: failure mode that causes the 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), so that the paralleled output voltage is blocked or oscillating between 2 and 20 Vdc or above 30 Vdc, and both internal diagnostics cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the paralleled output to go above 30 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 30 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 31 Vdc. Internal diagnostics detect and notify High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the paralleled output to go between 2 and 20 Vdc. Internal diagnostics detect and notify Low fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- 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, so that the paralleled output voltage is deviated between 20 and 30 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	13.49
λ_{du} = Total Dangerous Undetected failures	7.36
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	81.76
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	102.61
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	1112 years
$\lambda_{no\ effect}$ = "No Effect" failures	15666.65
$\lambda_{not\ part}$ = "Not Part" failures	1019.34
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	16788.60
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	7 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5*8760 + 8)h + \lambda_{dd} * 8h$	3.24E-05

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DCs	DCD
0.00 FIT	81.76 FIT	13.49 FIT	7.36 FIT	92.83%	0.00%	64.70%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

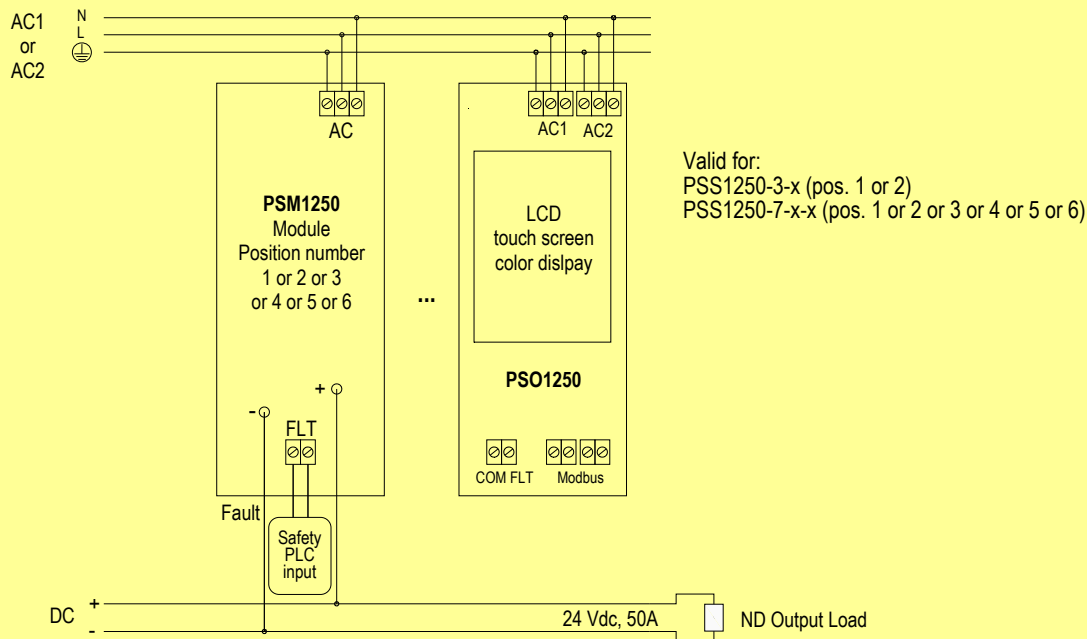
T[Proof] = 3 years	T[Proof] = 20 years
PFDavg = 9.72E-05 Valid for SIL 3	PFDavg = 6.48E-04 Valid for SIL 2

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 6 years	T[Proof] = 20 years
PFDavg = 1.94E-04 Valid for SIL 3	PFDavg = 6.48E-04 Valid for SIL 2

Systematic capability SIL 3.

Application of PSS1250 without HS and single PSM1250 module, for ND output load



Description:

In normal operation the PSM1250 module is unpowered because of absence of AC input supply, which is connected to related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). The fault relay contact can be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies under/over voltage dangerous faults to logic solver, which can only require to turn off power supply and to replace it with a new PSM1250 module. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.
 Absence of AC input supply implies that the green Power ON LED of PSM1250 is turned off, fault relay contact is open and the ND output load (connected to related output copper bars with screw terminals on the Wall Mounting Panel backboard) is Normally De-energized (ND).
 In presence of AC input supply, the green Power ON LED of PSM1250 is lit, fault relay contact is closed (if fault is absent) and output load is energized (Safe State).

Safety Function and Failure behavior:

PSS1250 without HS and single PSM1250 module is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of PSM1250 for ND load is described by the following definitions :

- Fail-Safe State: it is defined as the output going between 20 and 30 Vdc.
- 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 (i.e. being unable to go to the defined fail-safe state), so that the output voltage is blocked or oscillating between 0 and 20 Vdc or above 30 Vdc, and internal diagnostic cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the output to go above 30 Vdc. Internal overvoltage protection tries to limit output voltage < 30 Vdc, otherwise for output ≥ 31 Vdc internal crowbars trip, turning off the power supply. In any case, this failure mode is dangerous, but internal diagnostic notifies High fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off power supply and to replace it with a new PSM1250 module.
- Fail Low - Undervoltage: failure mode that causes the output to go between 0 and 20 Vdc. This failure mode is dangerous, but internal diagnostic notifies Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off power supply and to replace it with a new PSM1250 module.
- 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.00
λ_{du} = Total Dangerous Undetected failures	1690.12
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	938.09
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	2628.21
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	43 years
$\lambda_{not\ part}$ = "Not Part" failures	169.89
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	2798.10
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	40 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5 * 8760 + 8)h + \lambda_{dd} * 8h$	7.42E-03

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _s	DC _D
0.00 FIT	938.09 FIT	0.00 FIT	1690.12 FIT	35.69%	0.00%	0.00%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

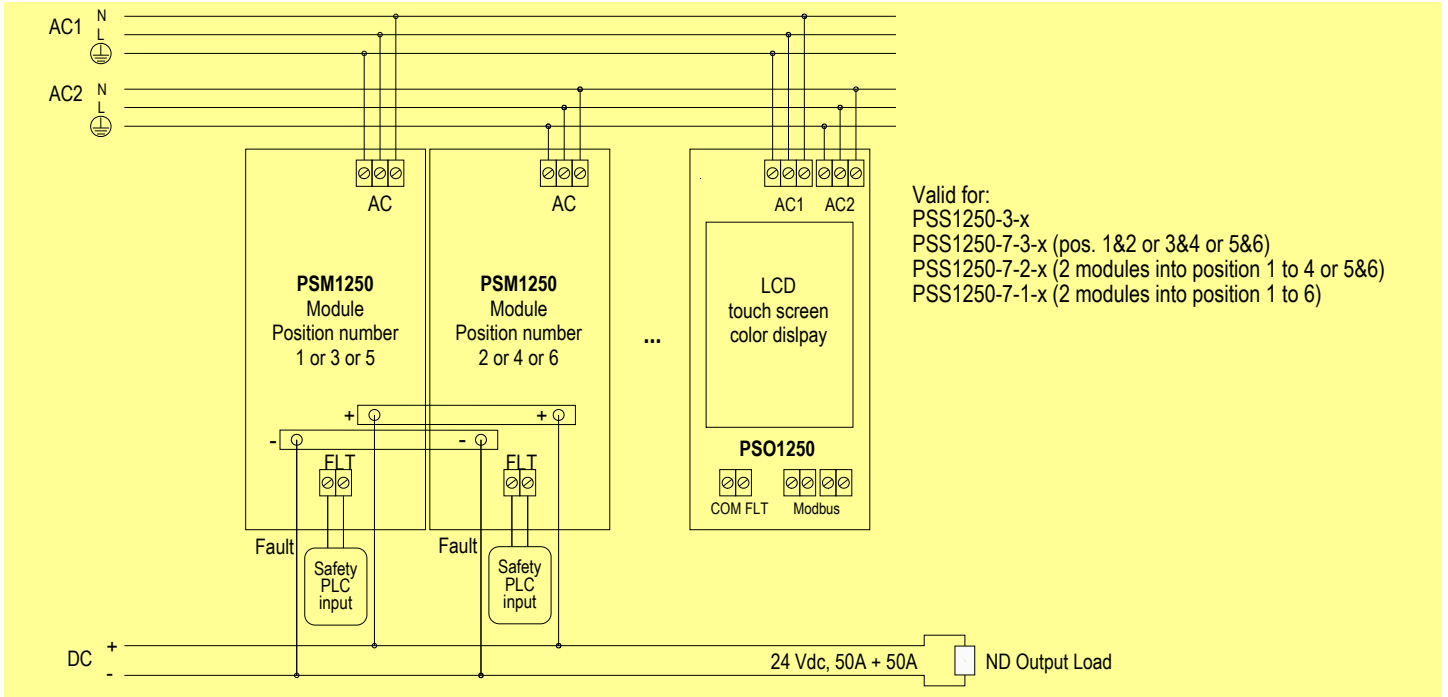
T[Proof] = 1 year
 PFDavg = 7.42E-03 Valid for SIL 1

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 2 years
 PFDavg = 1.48E-02 Valid for SIL 1

Systematic capability SIL 3.

Application of PSS1250 without HS and two paralleled PSM1250 modules, for ND output load



Description: In normal operation two paralleled PSM1250 modules are unpowered because of absence of both AC input supplies (AC1 and AC2), where AC1 is connected to one module and AC2 to other one by means of related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). For each PSM1250 module, its fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies over voltage module faults to logic solver, which can require to turn off this power supply and to replace it with a new PSM1250 module. In absence of module fault the relay contact is closed, while in presence of module fault the relay contact is open.

The outputs of two PSM1250 modules are already paralleled on the Wall Mounting Panel backboard by specific copper bars. Therefore, the ND output load is connected to outputs of both PSM1250 modules (by related output copper bars with screw terminals on Wall Mounting Panel backboard). In normal condition, absence of both AC input supplies (AC1 and AC2) implies that both green Power ON LEDs of PSM1250 modules are turned off, both fault relay contacts are open and the ND output load is Normally De-energized (ND). In presence of one only AC input supply (AC1 or AC2), one PSM1250 module is shutdown (its fault relay contact is open) but the other one is correctly turned on, so that output load is energized (Safe State). In presence of both AC input supplies (AC1 and AC2), both paralleled PSM1250 modules are correctly turned on and output load is energized (Safe State).

Safety Function and Failure behavior:

PSS1250 without HS and two paralleled PSM1250 modules is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of two paralleled PSM1250 modules for ND load is described by the following definitions :

- Fail-Safe State: it is defined as the the paralleled outputs going between 20 and 30 Vdc. Internal diagnostics detect and notify High (Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off malfunctioning power supply and to replace it with new PSM1250 modules.
- Fail Safe: failure mode that causes the 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), so that the paralleled output voltage is blocked or oscillating between 0 and 20 Vdc or above 30 Vdc, and internal diagnostic cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the paralleled output to go above 30 Vdc. Internal overvoltage protection tries to limit output voltage < 30 Vdc, otherwise for output ≥ 31 Vdc internal crowbars trip, turning off malfunctioning power supply. Internal diagnostics detect and notify High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the paralleled output to go between 0 and 20 Vdc. This failure mode is dangerous, but internal diagnostic notifies Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off malfunctioning power supply and to replace it with a new PSM1250 module.
- 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	3.82
λ_{du} = Total Dangerous Undetected failures	86.62
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	5165.98
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	5256.42
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	21 years
$\lambda_{not\ part}$ = "Not Part" failures	339.78
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	5596.20
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	20 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5*8760 + 8)h + \lambda_{dd} * 8h$	3.80E-04

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _s	DC _D
0.00 FIT	5165.98 FIT	3.82 FIT	86.62 FIT	98.35%	0.00%	4.22%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

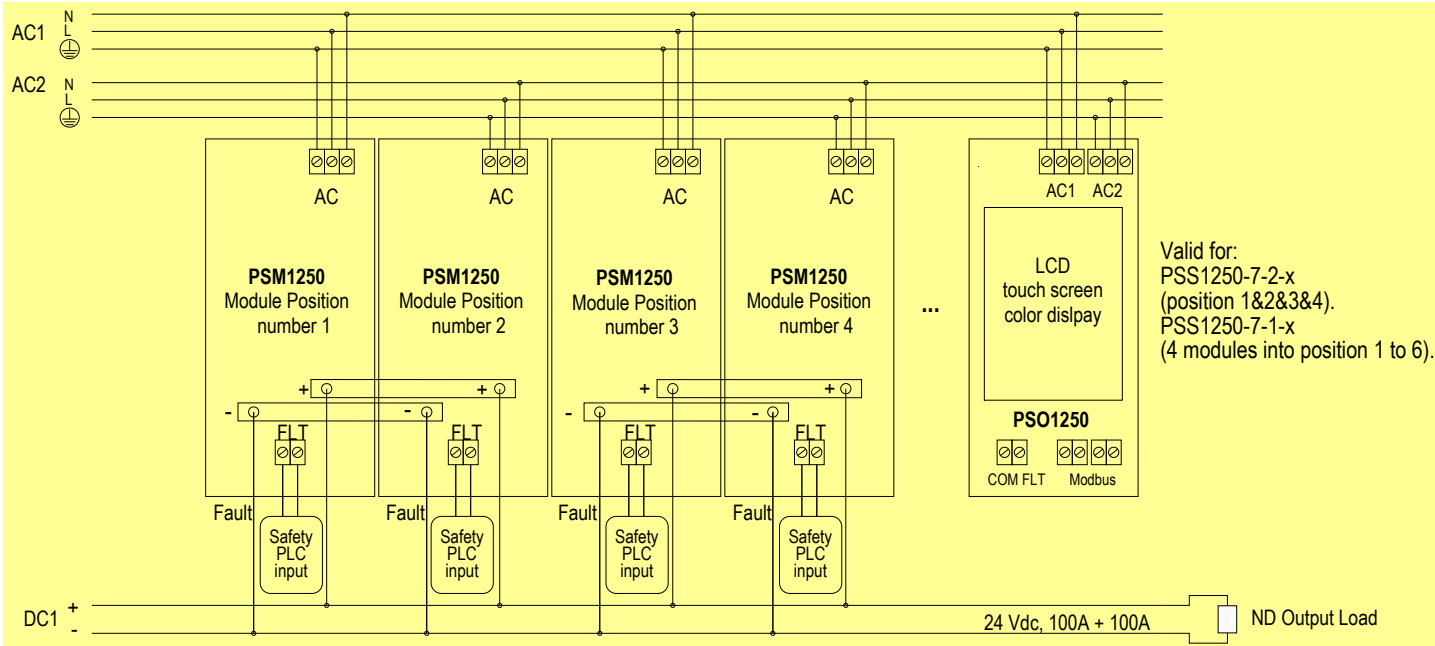
T[Proof] = 2 years	T[Proof] = 20 years
PFDavg = 7.60E-04 Valid for SIL 2	PFDavg = 7.60E-03 Valid for SIL 1

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 5 years	T[Proof] = 20 years
PFDavg = 1.90E-03 Valid for SIL 2	PFDavg = 7.60E-03 Valid for SIL 1

Systematic capability SIL 3.

Application of PSS1250 without HS and four PSM1250 modules, for ND output load



Valid for:
 PSS1250-7-2-x
 (position 1&2&3&4).
 PSS1250-7-1-x
 (4 modules into position 1 to 6).

Description:

In normal operation four paralleled PSM1250 modules are unpowered because of absence of both AC input supplies (AC1 and AC2), where AC1 is connected to two modules and AC2 to other ones by means of related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). For each PSM1250 module, its fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies over voltage module faults to logic solver, which can require to turn off this power supply and to replace it with a new PSM1250 module. In absence of module fault the relay contact is closed, while in presence of module fault the relay contact is open.

The outputs of four PSM1250 modules are already paralleled on the Wall Mounting Panel backboard by specific copper bars. Therefore, the ND output load is connected to outputs of four PSM1250 modules (by related output copper bars with screw terminals on Wall Mounting Panel backboard). In normal condition, absence of both AC input supplies (AC1 and AC2) implies that four green Power ON LEDs of PSM1250 modules are turned off, four fault relay contacts are open and the ND output load is Normally De-energized (ND).

In presence of one only AC input supply (AC1 or AC2), two PSM1250 module are shutdown (their fault relay contact are open) but the other ones are correctly turned on, so that output load is energized (Safe State). In presence of both AC input supplies (AC1 and AC2), four paralleled PSM1250 modules are correctly turned on and output load is energized (Safe State).

Safety Function and Failure behavior:

PSS1250 without HS and four paralleled PSM1250 modules is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of four paralleled PSM1250 modules for ND load is described by the following definitions :

- Fail-Safe State: it is defined as the the paralleled outputs going between 20 and 30 Vdc. Internal diagnostics detect and notify High (Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off malfunctioning power supply and to replace it with new PSM1250 modules.
- Fail Safe: failure mode that causes the 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), so that the paralleled output voltage is blocked or oscillating between 0 and 20 Vdc or above 30 Vdc, and internal diagnostic cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the paralleled output to go above 30 Vdc. Internal overvoltage protection tries to limit output voltage < 30 Vdc, otherwise for output ≥ 31 Vdc internal crowbars trip, turning off malfunctioning power supply. Internal diagnostics detect and notify High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the paralleled output to go between 0 and 20 Vdc. This failure mode is dangerous, but internal diagnostic notifies Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off malfunctioning power supply and to replace it with a new PSM1250 module.
- 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	7.64
λ_{du} = Total Dangerous Undetected failures	88.89
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	10416.31
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	10512.84
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	11 years
$\lambda_{not\ part}$ = "Not Part" failures	679.56
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	11192.40
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	10 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5*8760 + 8)h + \lambda_{dd} * 8h$	3.90E-04

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _s	DC _D
0.00 FIT	10416.31 FIT	7.64 FIT	88.89 FIT	99.15%	0.00%	7.91%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

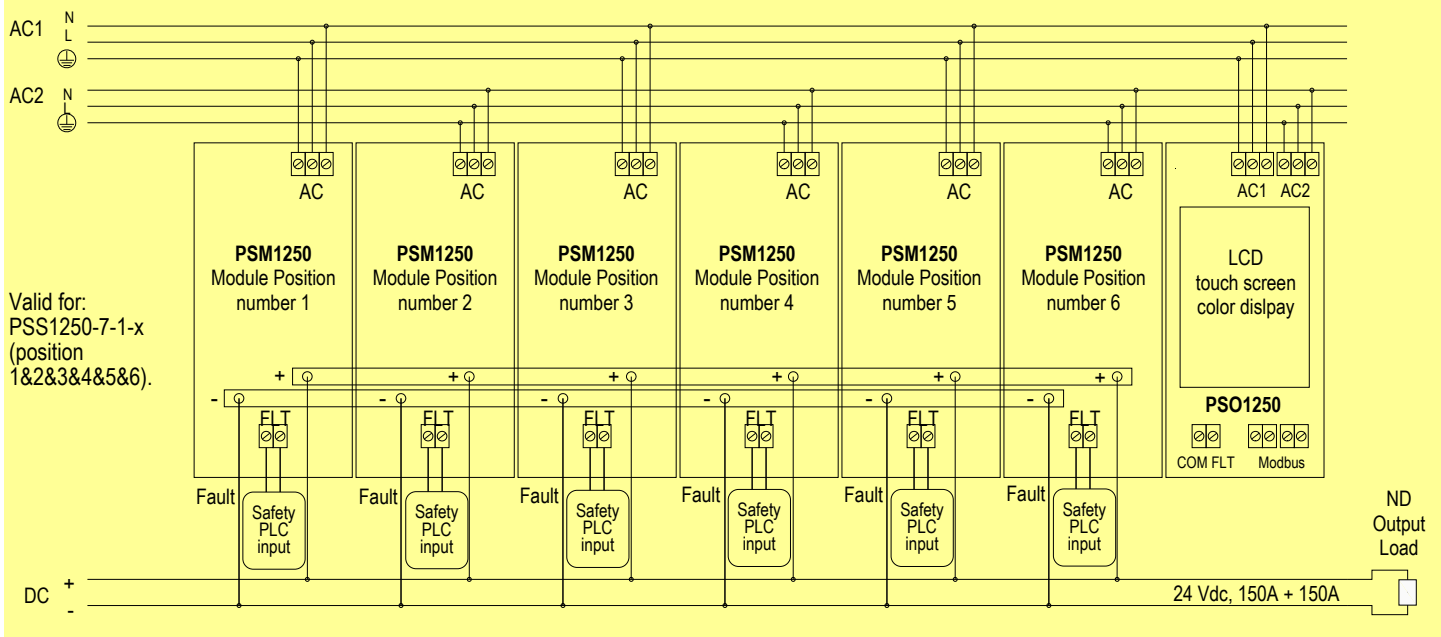
T[Proof] = 2 years	T[Proof] = 20 years
PFDavg = 7.80E-04 Valid for SIL 2	PFDavg = 7.80E-03 Valid for SIL 1

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 5 years	T[Proof] = 20 years
PFDavg = 1.95E-03 Valid for SIL 2	PFDavg = 7.80E-03 Valid for SIL 1

Systematic capability SIL 3.

Application of PSS1250 without HS and six paralleled PSM1250 modules, for ND output load



Description:

In normal operation six paralleled PSM1250 modules are unpowered because of absence of both AC input supplies (AC1 and AC2), where AC1 is connected to three modules and AC2 to other ones by means of related terminal blocks on the Wall Mounting Panel backboard (see previous functional diagram for more information). For each PSM1250 module, its fault relay contact must be connected to Safety PLC or Safety logic solver because power supply internal diagnostic uses this contact to notifies over voltage module faults to logic solver, which can require to turn off this power supply and to replace it with a new PSM1250 module. In absence of module fault the relay contact is closed, while in presence of module fault the relay contact is open.

The outputs of six PSM1250 modules are already paralleled on the Wall Mounting Panel backboard by specific copper bars. Therefore, the ND output load is connected to outputs of six PSM1250 modules (by related output copper bars with screw terminals on Wall Mounting Panel backboard). In normal condition, absence of both AC input supplies (AC1 and AC2) implies that six green Power ON LEDs of PSM1250 modules are turned off, six fault relay contacts are open and the ND output load is Normally De-energized (ND). In presence of one only AC input supply (AC1 or AC2), three PSM1250 module are shutdown (their fault relay contact are open) but the other ones are correctly turned on, so that output load is energized (Safe State). In presence of both AC input supplies (AC1 and AC2), six paralleled PSM1250 modules are correctly turned on and output load is energized (Safe State).

Safety Function and Failure behavior:

PSS1250 without HS and six paralleled PSM1250 modules is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behaviour of six paralleled PSM1250 modules for ND load is described by the following definitions :

- Fail-Safe State: it is defined as the the paralleled outputs going between 20 and 30 Vdc. Internal diagnostics detect and notify High (Over voltage) fails (DD) to logic solver, which can operate to convert these fails to the fail-safe state, requiring to turn off malfunctioning power supply and to replace it with new PSM1250 modules.
- Fail Safe: failure mode that causes the 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), so that the paralleled output voltage is blocked or oscillating between 0 and 20 Vdc or above 30 Vdc, and internal diagnostic cannot detect and notify faults to logic solver.
- Fail High - Overvoltage: failure mode that causes the paralleled output to go above 30 Vdc. Internal overvoltage protection tries to limit output voltage < 30 Vdc, otherwise for output ≥ 31 Vdc internal crowbars trip, turning off malfunctioning power supply. Internal diagnostics detect and notify High fail to logic solver, which does not automatically trip on this failure, classified as Dangerous Detected (DD).
- Fail Low - Undervoltage: failure mode that causes the paralleled output to go between 0 and 20 Vdc. This failure mode is dangerous, but internal diagnostic notifies Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off malfunctioning power supply and to replace it with a new PSM1250 module.
- 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.

The PSO1250 diagnostic module **does not interfere** with the power system functional safety. The power system can perfectly work without the diagnostic module and any failure of the PSO1250 diagnostic module does not affect system performance, reliability and SIL level of this Functional Safety application.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	11.46
λ_{du} = Total Dangerous Undetected failures	91.15
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	15666.65
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	15769.26
MTBF (safety function) = $(1 / \lambda_{tot\ safe}) + MTTR$ (8 hours)	7 years
$\lambda_{not\ part}$ = "Not Part" failures	1019.34
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	16788.60
MTBF (device) = $(1 / \lambda_{tot\ device}) + MTTR$ (8 hours)	7 years
PFDavg (TI = 1 year) = $\lambda_{du} * (0.5 * 8760 + 8)h + \lambda_{dd} * 8h$	4.00E-04

Failure rates table according to IEC 61508:2010 :

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC _s	DC _D
0.00 FIT	15666.65 FIT	11.46 FIT	91.15 FIT	99.42%	0.00%	11.17%

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 10% of entire safety function:

T[Proof] = 2 years	T[Proof] = 20 years
PFDavg = 8.00E-04 Valid for SIL 2	PFDavg = 8.00E-03 Valid for SIL 1

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 5 years	T[Proof] = 20 years
PFDavg = 2.00E-03 Valid for SIL 2	PFDavg = 8.00E-03 Valid for SIL 1

Systematic capability SIL 3.

Warning

PSS1250 series are isolated Switching Power Supply units located in Safe Area or Zone 2 / Div.2, Gas Group IIC, Temperature T4 Hazardous Area within the specified operating temperature limits $-40^{\circ}\text{C} \leq T_{\text{amb}} \leq +70^{\circ}\text{C}$ and mounting conditions.

For Intrinsic Safety application, limit the line supply voltage to a maximum of 250 Vrms, not to be connected to control equipment that uses or generates more than 250 Vrms or Vdc with respect to earth ground.

Read installation manual before operating the unit. Failure of proper installation or use of the equipment may damage the unit or cause severe personal injury.

PSS1250 must be installed, wired, operated and maintained only by qualified personnel, in accordance to the relevant national/international installation standards (e.g. IEC/EN60079-14 Explosive atmospheres - Part 14: Electrical installations design, selection and erection), following the established installation guide lines.

PSS1250 must be placed in an enclosure with IP4X protection degree when used in locations providing adequate protection against the entry of solid foreign objects or water, capable of impairing safety, or be placed in an enclosure with IP54 protection degree for other locations. Substitution of components may impair suitability for Zone 2 / Div.2.

Explosion Hazard: to prevent ignition of flammable or combustible atmospheres, disconnect power before servicing or unless area is known to be nonhazardous. Remove power before opening the case.

Electrostatic Hazard: clean only with antistatic cloth.

Green Power ON LED of PSM1250 power module: check that green LED is OFF before screwing out PSM1250 module front panel.

Red LED (one for each PSM1250 slot position) on wall mounting panel board: connect a PSM1250 power module to the rack unit only if corresponding red LED on back panel board is in OFF state.

Storage

If after an incoming inspection the unit is not installed directly on a system (parts for spare or expansion with long storage periods) it must be conveniently stocked. Stocking area characteristics must comply with the following parameters:

Temperature -40 to $+70^{\circ}\text{C}$, the -45 to $+80^{\circ}\text{C}$ is meant for limited periods, -10 to $+30^{\circ}\text{C}$ is preferred.

Humidity 0 to 95 %, 0 to 60 % humidity is preferred.

Vibration: no prolonged vibration should be perceivable in the stocking area to avoid loosening of parts or fatigue ruptures of components terminals.

Pollution: presence of pollutant or corrosive gases or vapors must be avoided to prevent corrosion of conductors and degradation of insulating surfaces.

Disposal

The product should not be disposed with other wastes at the end of its working life. It may content hazardous substances for the health and the environment, to prevent possible harm from uncontrolled waste disposal, please separate this equipment from other types of wastes and recycle it responsibly to promote the sustainable reuse of material resources.

This product should not be mixed with other commercial wastes for disposal.

System composition

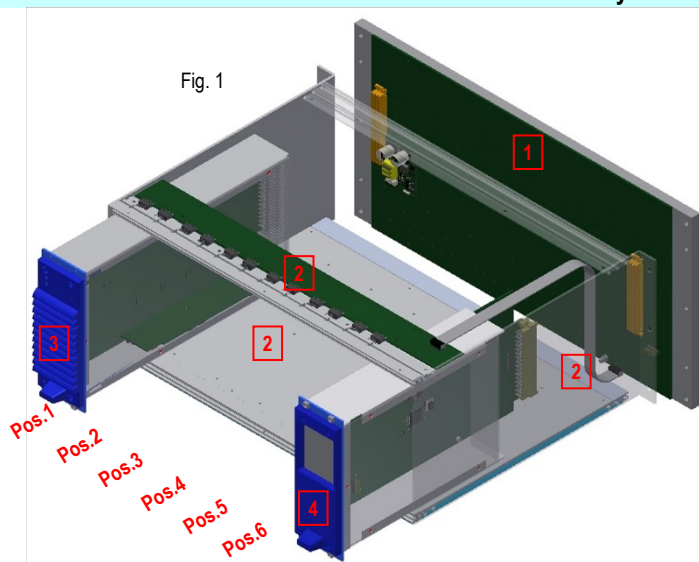
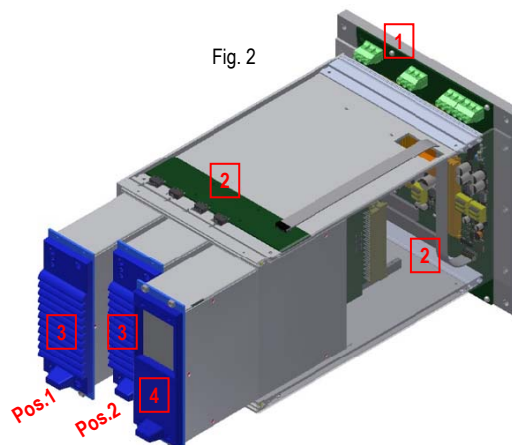


Fig. 1 shows PSS1250-HS-7-D system, which includes the following parts:

- 1 Wall Mounting Panel (WMP1250-HS-7-x-D) with connections for power and diagnostic modules and hot swapping control circuits;
- 2 19" Rack unit (PSR1250-xx-7), enclosure with guides for inserting modules and microswitches board connected (by flat cable) with hot swapping control on Wall Mounting Panel WMP1250-HS-7-x-D;
- 3 6 Power Supply Modules (PSM1250), for each inserting position (Pos.1, Pos.2, Pos.3, Pos.4, Pos.5, Pos.6)
- 4 Diagnostic module (PSO1250) with TFT color screen for diagnostic information about each power module.

Fig. 2 shows PSS1250-HS-3-D system, which includes the following parts:

- 1 Wall Mounting Panel (WMP1250-HS-3-D) with connections for power and diagnostic modules and hot swapping control circuits;
- 2 9" Rack unit (PSR1250-xx-3), enclosure with guides for inserting modules and microswitches board connected (by flat cable) with hot swapping control on Wall Mounting Panel WMP1250-HS-3-D;
- 3 2 Power Supply Modules (PSM1250), for each inserting position (Pos.1, Pos.2)
- 4 Diagnostic module (PSO1250) with TFT color screen for diagnostic information about each power module.

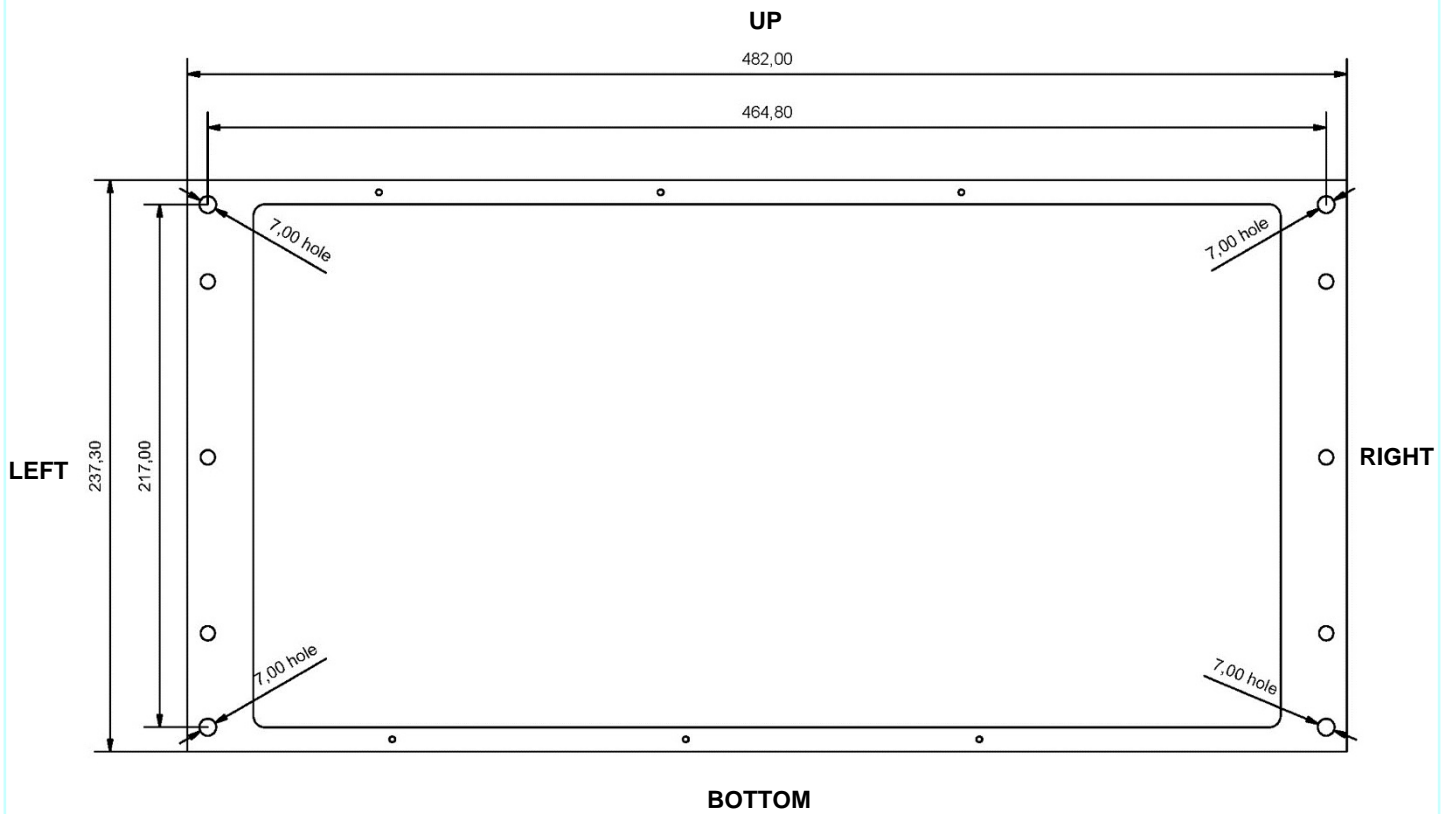


Installation Procedure - 1st step: Installation of Wall Mounting Panels type WMP1250-xx-7-x-D and WMP1250-xx-3-D

The following drawing with overall dimensions (mm) is applicable to types: WMP1250-HS-7-x-D and WMP1250-7-x-D.

Fix the wall mounting panel to a vertical wall by means of four screws through four 7.00 mm diameter holes shown in the drawing.

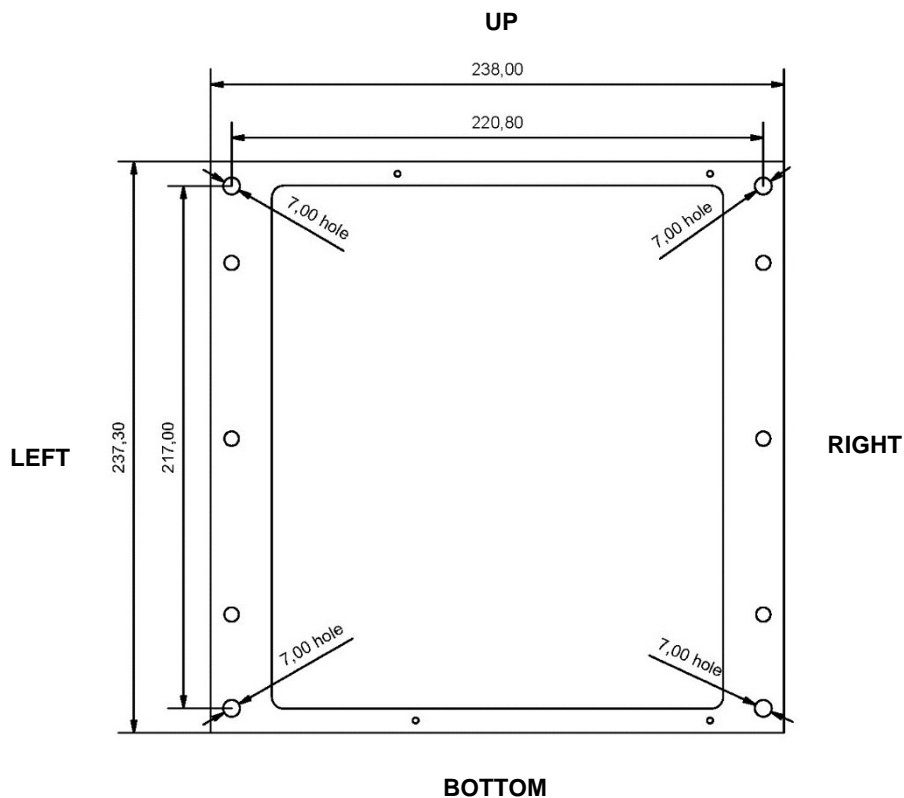
The wall mounting panel must only be installed as oriented in the following drawing.



The following drawing with overall dimensions (mm) is applicable to types: WMP1250-HS-3-D and WMP1250-3-D.

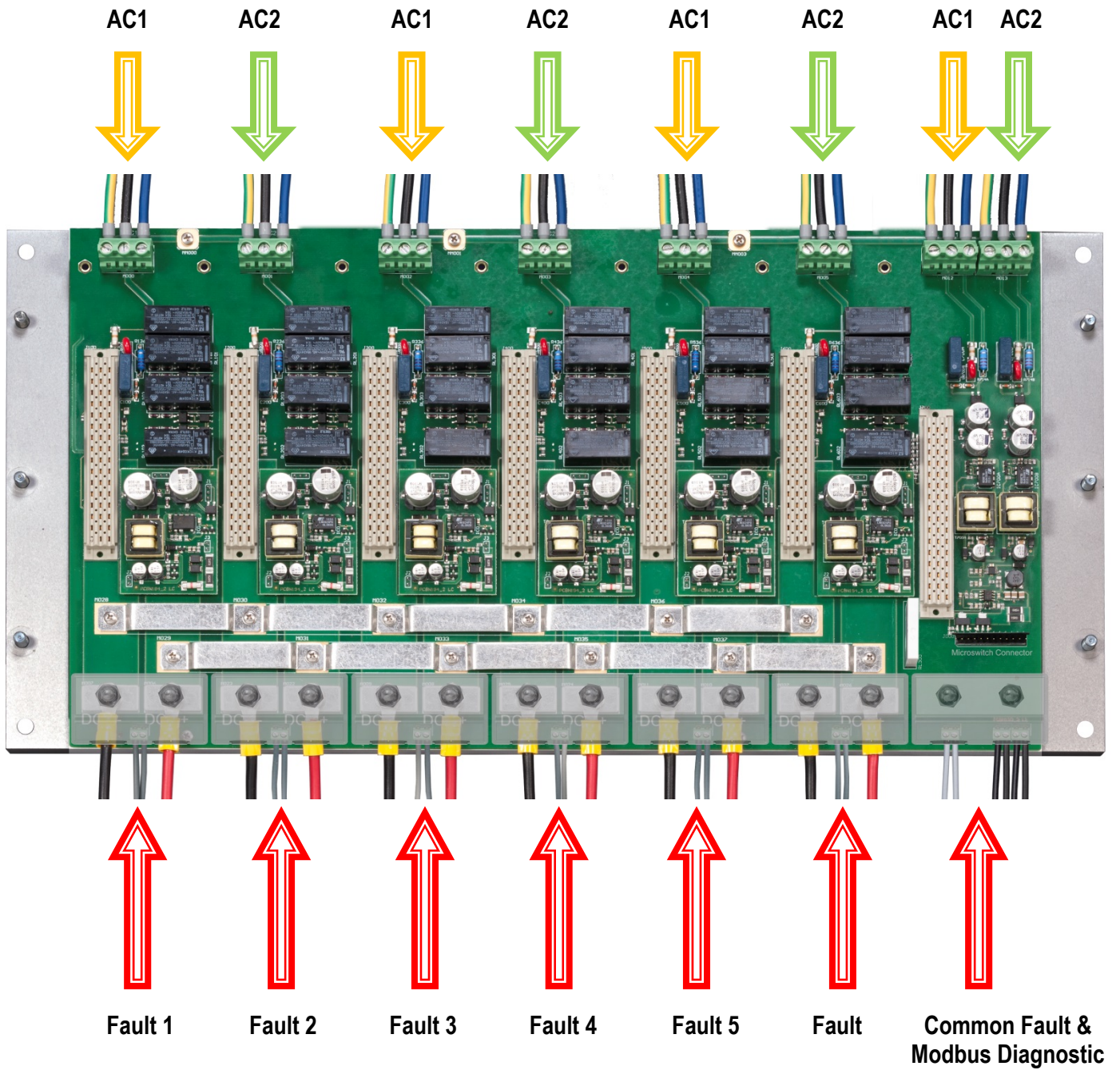
Fix the wall mounting panel to a vertical wall by means of four screws through four 7.00 mm diameter holes shown in the drawing.

The wall mounting panel must only be installed as oriented in the following drawing.



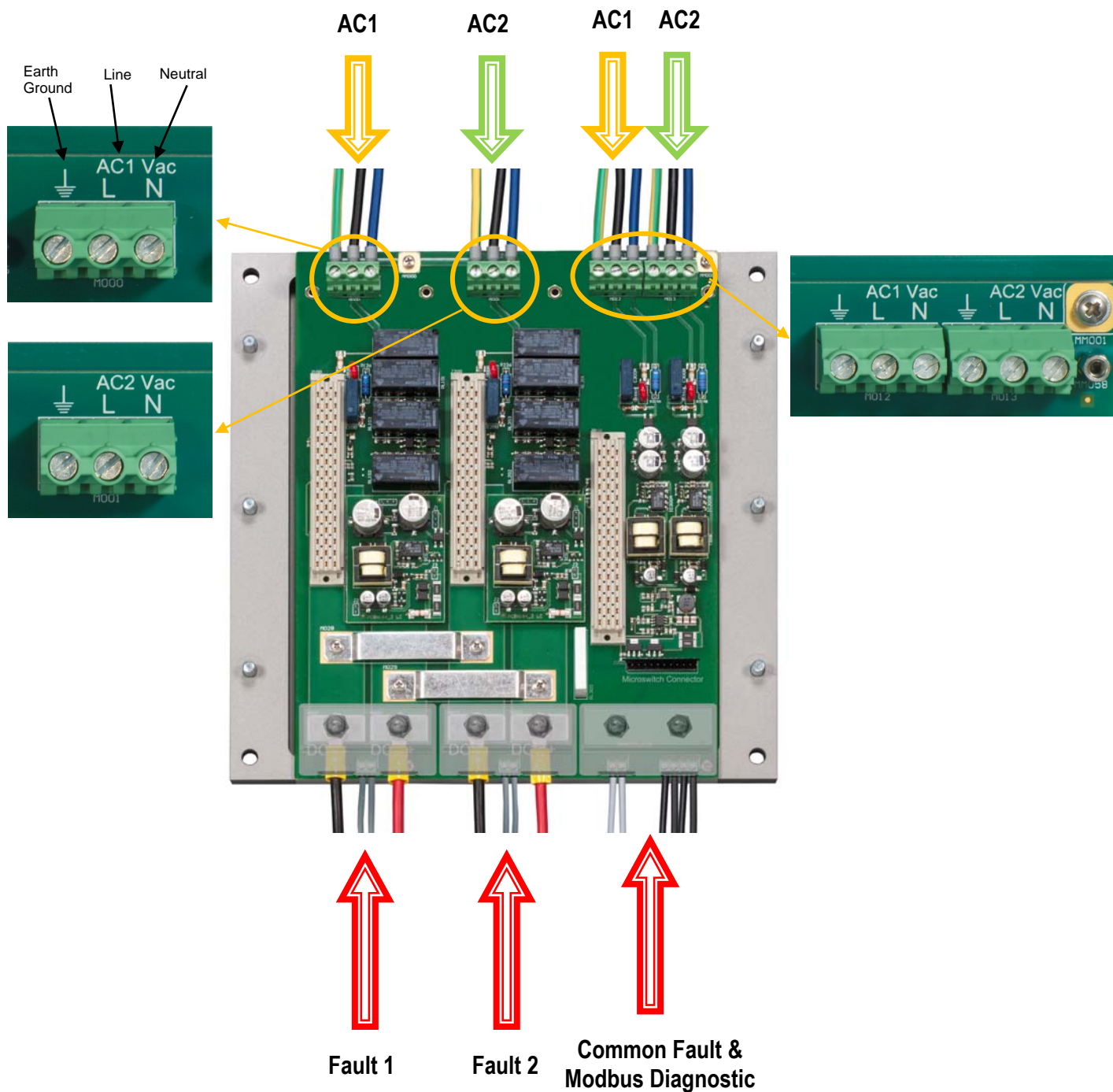
Installation Procedure - 2nd step: Wiring of top terminal blocks (AC input lines, faults, modbus) of wall mounting panels type WMP1250-xx-7-x-D and WMP1250-xx-3-D

The following picture shows for example WMP1250-HS-7-x-D terminal block wiring.



Installation Procedure - 2nd step: Wiring of top terminal blocks (AC input lines, faults, modbus) of wall mounting panels type WMP1250-xx-7-x-D and WMP1250-xx-3-D

The following picture shows for example WMP1250-HS-3-D terminal block wiring.



The PSS1250 redundant system requires to use two AC input power lines (AC1 and AC2) with different lines and neutrals but the same earth ground connection, in order to guarantee fully redundant configuration from the input to the output of power system.

For WMP1250-xx-7-x-D, connect AC1 input power line to input terminal blocks of positions N.1, 3, 5 (odd positions) and connect AC2 input power line to input terminal blocks of positions N.2, 4, 6 (even positions). See functional diagrams at pages 6-7-8 for more information about wiring connection.

For WMP1250-xx-3-D, connect AC1 input power line to input terminal blocks of positions N.1 (odd position) and connect AC2 input power line to input terminal blocks of position N.2 (even position). See functional diagrams at page 9 for more information about wiring connection.

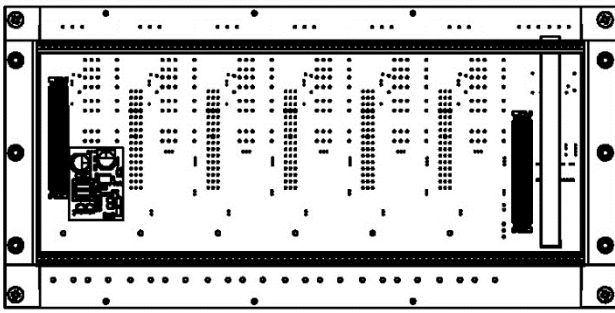
The last position on the right is used for PSO1250 diagnostic module, connect both AC1 and AC2 input power lines to related terminal blocks in order to guarantee continuous operation of diagnostic module even after shutdown of one AC input line.

For AC input terminal blocks, use a typical cable section of AWG12 (maximum AWG11 or 4 mm²).

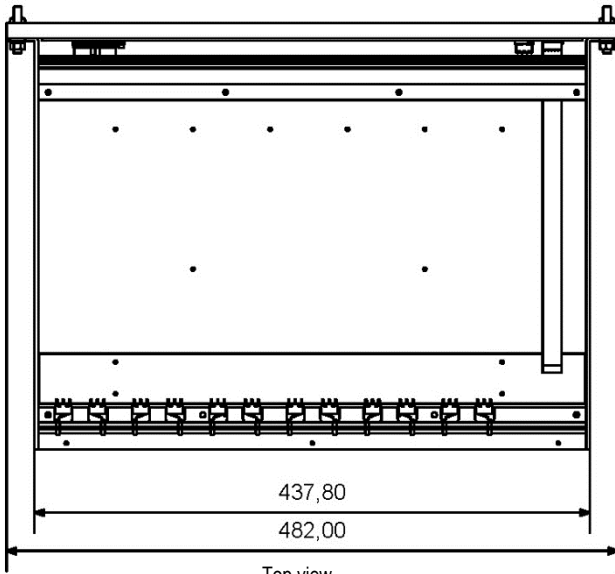
For fault contact output (of each PSM1250 or common of PSO1250) and Modbus terminal blocks, use a typical cable section of AWG18 (maximum AWG16 or 1.5 mm²).

Installation Procedure - 3rd step: Installation of Rack unit type PSR1250-xx-7 and PSR1250-xx-3 on related wall mounting panel

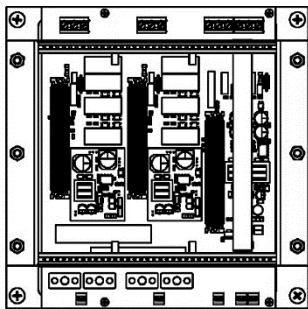
The following drawing shows overall dimensions (mm) of PSR1250-xx-7, mounted on WMP1250-xx-7-x-D, and PSR1250-xx-3, mounted on WMP1250-xx-3-D.
 Fix the rack unit to 6 wall mounting panel bolts (3 on the right side and 3 on the left side) by means of 6 M6 nuts and groovers.



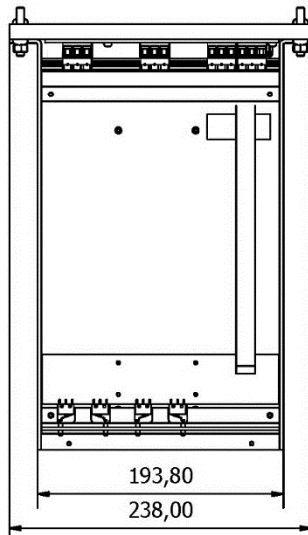
Front view



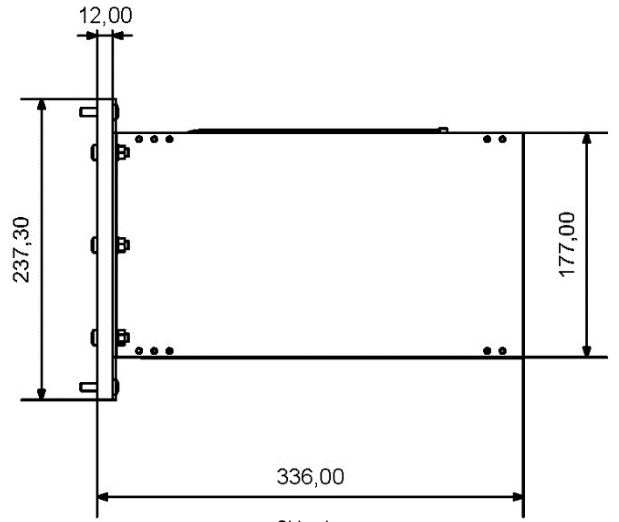
Top view



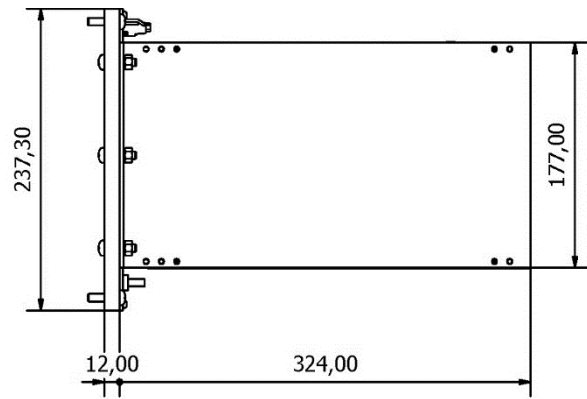
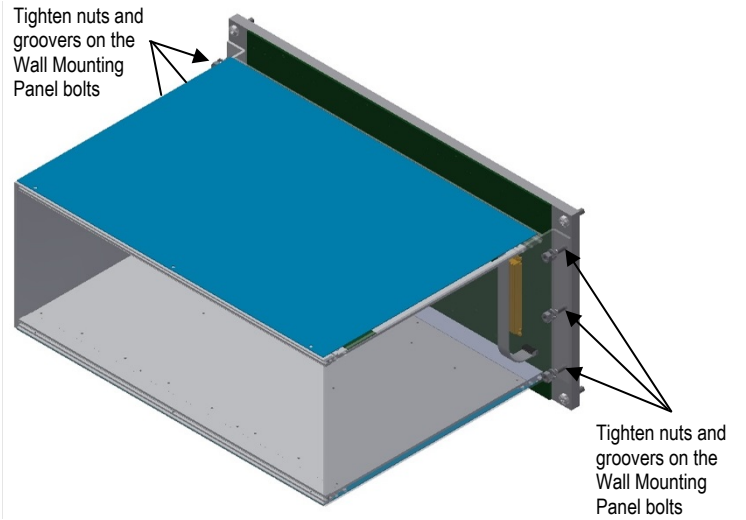
Front view



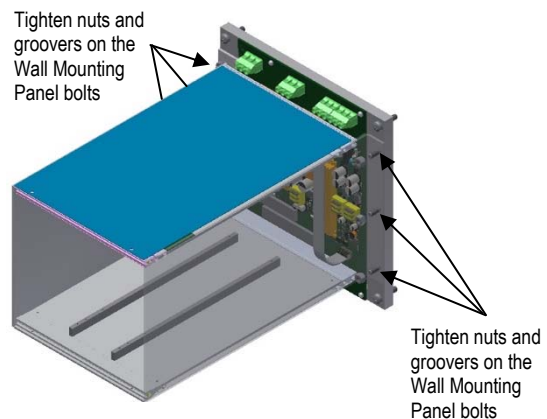
Top view



Side view



Side view



Installation Procedure - 4th step (for models with HS) - Section A: Installation of flat cable between microswitches PCB and wall mounting panel back board for Hot Swapping control

Fig. 4 shows wall mounting panel back board with a 12 poles male connector, which must be connected with the flat cable coming from the microswitches PCB of the PSR1250 rack unit. In the figures 1-2-3-4 is shown how to connect this flat cable.

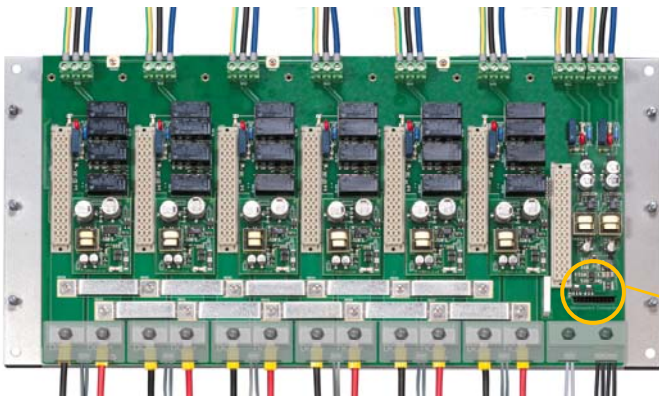


Fig. 1

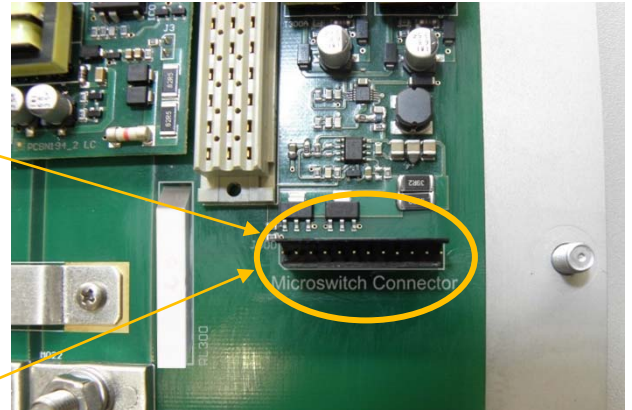
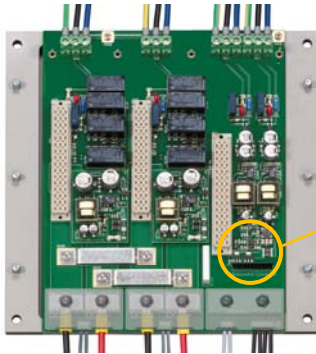


Fig. 2

During installation of the PSR1250-HS-7 or PSR1250-HS-3 on WMP1250-HS-7-x-D or WMP1250-HS-3-D, connect the flat cable, coming from the microswitches PCB, to the 12 poles male connector, as shown in figures 3-4.

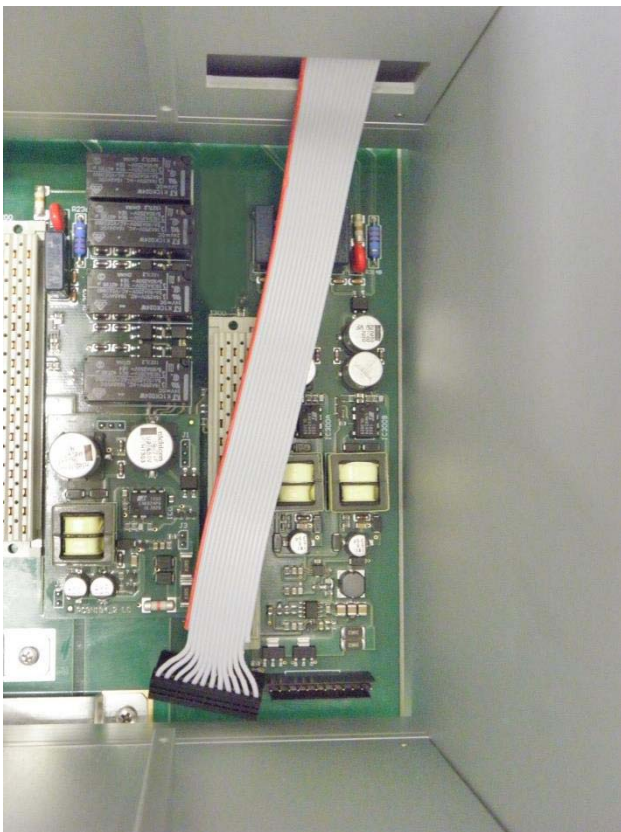


Fig. 3

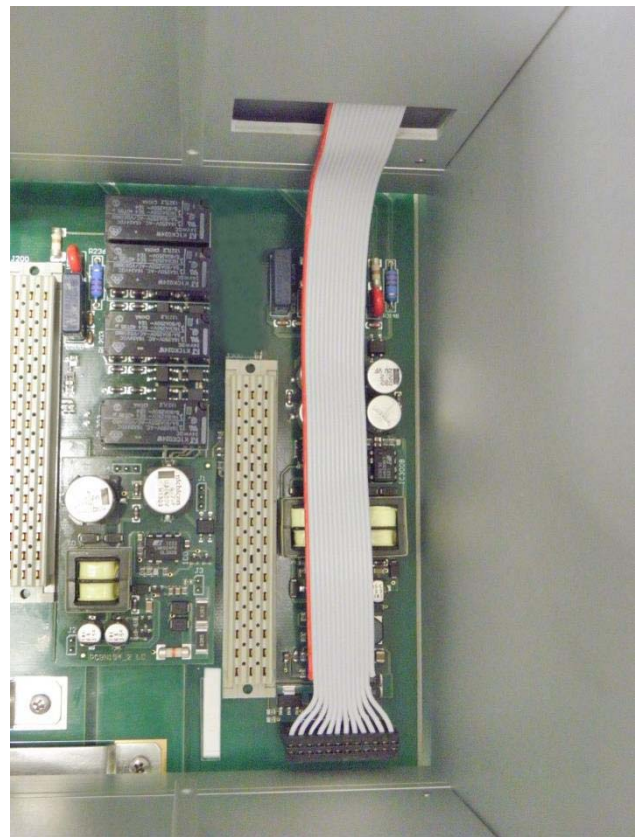
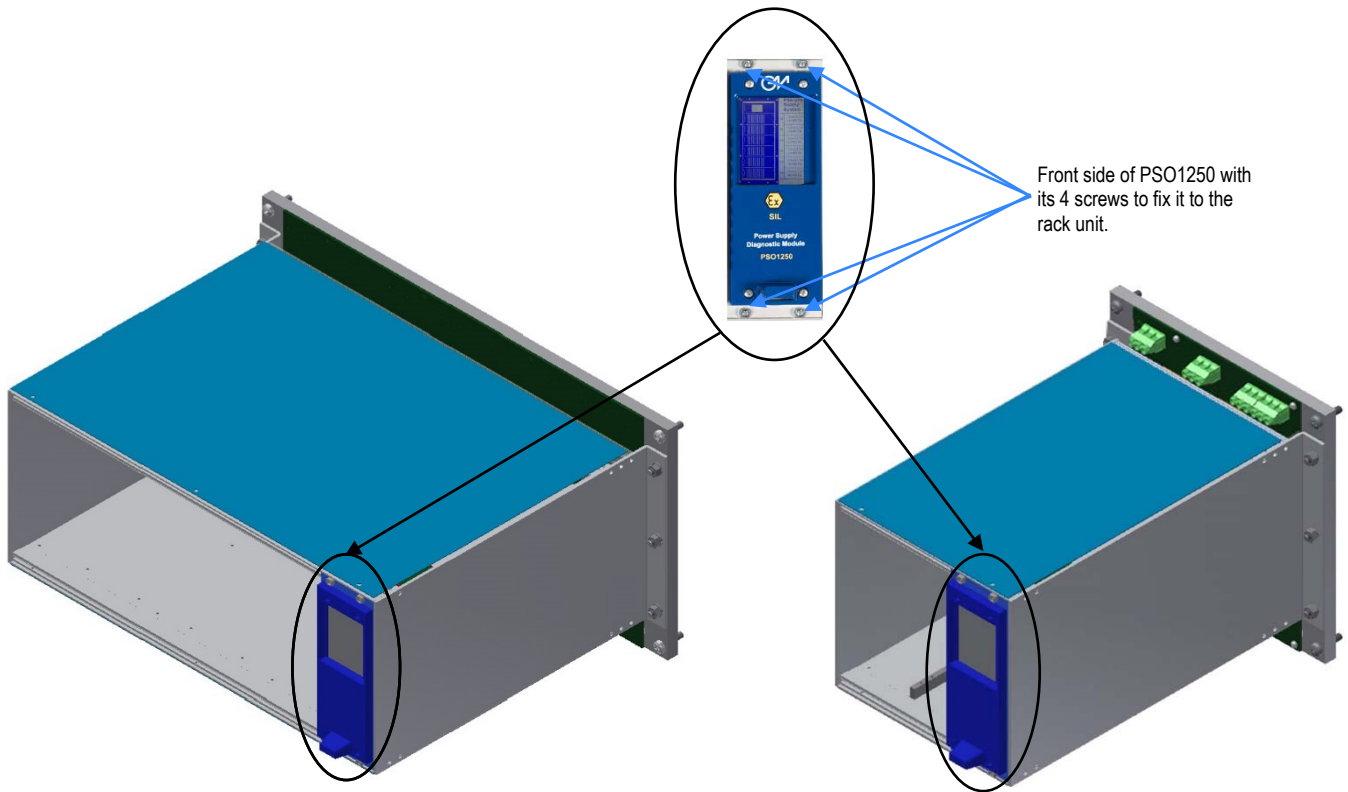


Fig. 4

Installation Procedure - 4th step (for models with HS) - Section B: Installation and start up of PSO1250 Diagnostic Module and HSC red LED signalling

Insert the PSO1250 diagnostic module in the last position on the right of the PSR1250 rack unit and fix the module to the rack unit by means of its 4 screws on its front side.



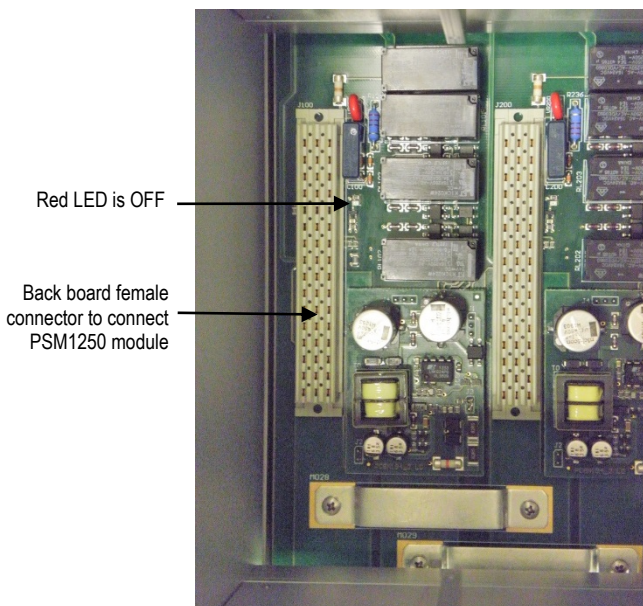
After installation of the PSO1250 module, **power AC1 and AC2 input power lines** in order to turn on diagnostic module. For more information about diagnostic module features and its set up, please see description from page 39. If it is not required the installation of the PSO1250 module, **power AC1 and AC2 input power lines** anyway.

Each Hot Swapping control circuit (one for each PSM1250 position) is supplied from AC1 or AC2 input line. The Hot Swapping control circuit controls if PSM1250 can be installed and fixed to the rack unit.

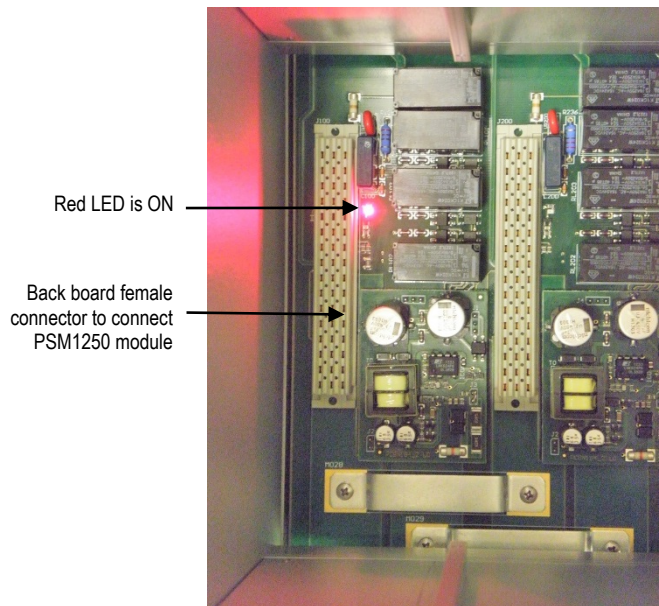
If no PSM1250 module is installed and fixed into the rack unit, no Hot Swapping control circuit can give input power lines to the back board female connector. In this condition, each red LED must be OFF.

If a red LED is ON, it means that related Hot Swapping control circuit is not correctly operating and therefore no PSM1250 module shall be insert and fixed into its rack position.

PSM1250 module can be installed and fixed into the rack unit only if corresponding back panel red LED is OFF.



Normal condition: the red LED is OFF.
The PSM1250 module can be installed and fixed into the rack unit position.

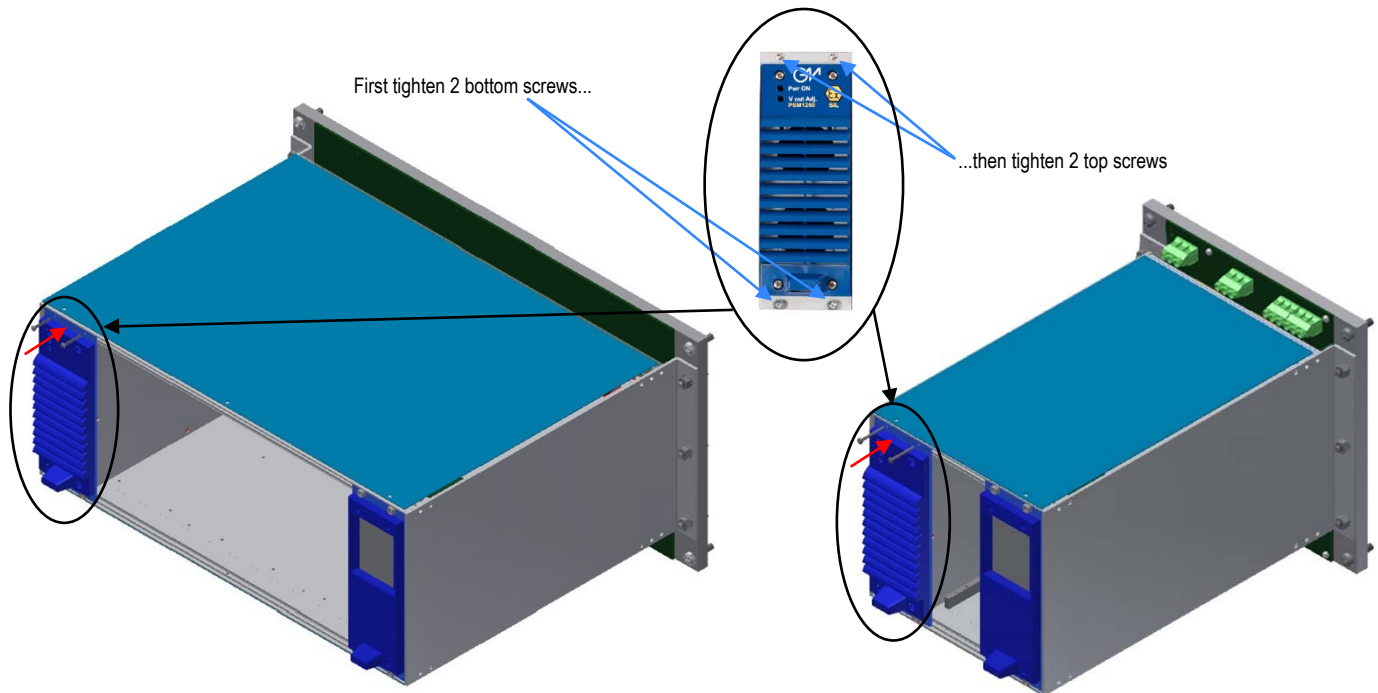


Dangerous condition: the red LED is ON.
The PSM1250 module must not be installed.

Installation Procedure - 4th step (for models with HS) - Section C: Installation and pre-start up of PSM1250 Power Supply Module

AC1 and AC2 input power lines are powered. Therefore PSM1250 module can be installed and fixed into the rack unit only if corresponding back panel red LED is OFF. The following procedure is split in 3 sub-steps and it is the same for each PSM1250, independently from its position in the rack unit. Starting from position 1 to position 6 (for PSS1250-7) or 2 (for PSS1250-3), execute pre-start up of each PSM1250 module.

1st sub-step: insert and fix the PSM1250 module into the rack unit by means of its 4 screws on its front side. Two of them in the bottom part are only used for mechanical purpose; the other two, in the top part, when completely tightened, close the microswitches and enable the hot swap control circuit to provide input power lines to PSM1250 module by back board female connector. First of all, tighten 2 bottom screws and then tighten 2 top ones.



Power ON green LED

Trimmer for output voltage adjusting (use a little cross head isolated screwdriver)

2nd sub-step: with PSM1250 module powered, its front panel Power ON green LED is ON and 24 Vdc (factory setting) output voltage is present on PSM1250 screw output terminals DC- and DC+ (see page 5 for more information about Power ON green LED signalling).

On the TFT color screen of PSO1250 diagnostic module it is possible to monitor the PSM1250 module status and to collect information about the power supply: for example output voltage value (see description from page 39). If no PSO1250 diagnostic module is present, the output voltage can be measured on PSM1250 screw output terminals by means of a multimeter.

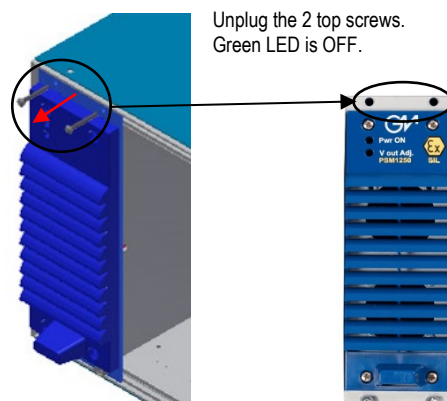
If it is required to set an output voltage value different from factory setting (24 Vdc), use the trimmer for output voltage adjusting. Turn the trimmer clockwise (to the right) to increase output voltage (max. 28 Vdc) or turn the trimmer counterclockwise (to the left) to decrease output voltage (min. 21 Vdc).

Warning: for correct current sharing operation, power supply modules must have output voltages calibrated within ± 0.5 V.



PSM1250 screw output terminals on copper bars:
DC- is negative out pole,
DC+ is positive out pole.
(in the figure it's shown DC1- and DC1+ which are related to PSM1250 in position 1 of PSS1250 system).

3rd sub-step: after having adjusted PSM1250 output voltage, shut down the power module unplugging the 2 top screws in order to repeat sub-steps 1 to 3 procedure for other modules and complete the setting for all PSM1250 of PSS1250 power system.



Installation Procedure - 4th step (for models with HS) - Section D: Wiring of bottom screw output terminals on copper bars (DC output lines) of wall mounting panels type WMP1250-HS-7-x-D and WMP1250-HS-3-D and start up of PSS1250 power system

At this step, PSO1250 diagnostic module is installed and fixed to rack unit with 4 screws, while each PSM1250 power module is installed and fixed to rack unit with **2 bottom screws only** (2 top screws are unplugged to keep PSM1250 shutdown).

Unpower AC1 and AC2 input power lines (also PSO1250 will turn off) before starting the wiring of bottom screw output terminals on copper bars (DC output lines) of wall mounting panels type WMP1250-HS-7-x-D and WMP1250-HS-3-D.

To wire bottom screw output terminals on copper bars (DC output lines: DC- is negative out pole, DC+ is positive out pole), see Fig. 1-2-3-4-5, where DC1- and DC1+ are shown, related to PSM1250 in position 1 of PSS1250 system.

For WMP1250-HS-7-x-D, see functional diagrams at pages 6-7-8 for more information about wiring connection.

For WMP1250-HS-3-D, see functional diagrams at page 9 for more information about wiring connection.



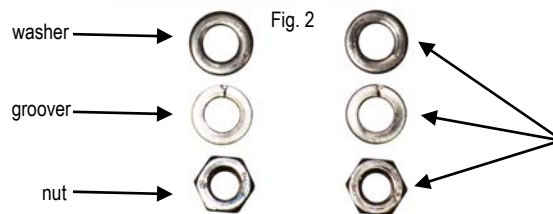
Fig. 1



Fig. 2



Fig. 3



Unplug M6 nuts, groovers and washers. Then insert a cable lug with wire, washer and groover on each screw output

For DC screw output terminals, use a typical cable section of AWG7 (maximum AWG5 or 16 mm²).

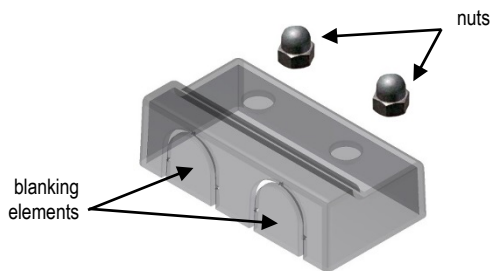


Fig. 4

A polycarbonate cover is used for IP20 to protect each couple of screw output terminals. Break two preformed blanking elements to allow cable passage. Then insert and fix the cover on couple of screw output terminals by means of M6 nylon-capped lock nut.



Fig. 5

After having wired all DC output lines, starting from position 1 to position 6 (for PSS1250-7) or 2 (for PSS1250-3), tighten 2 top screws.

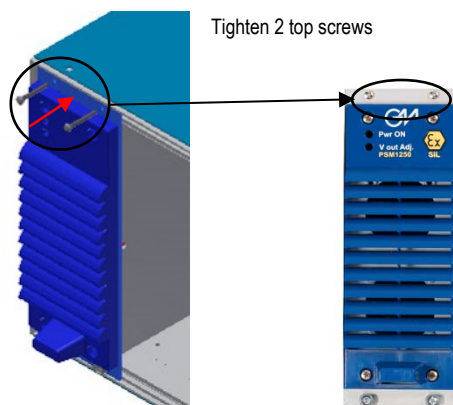
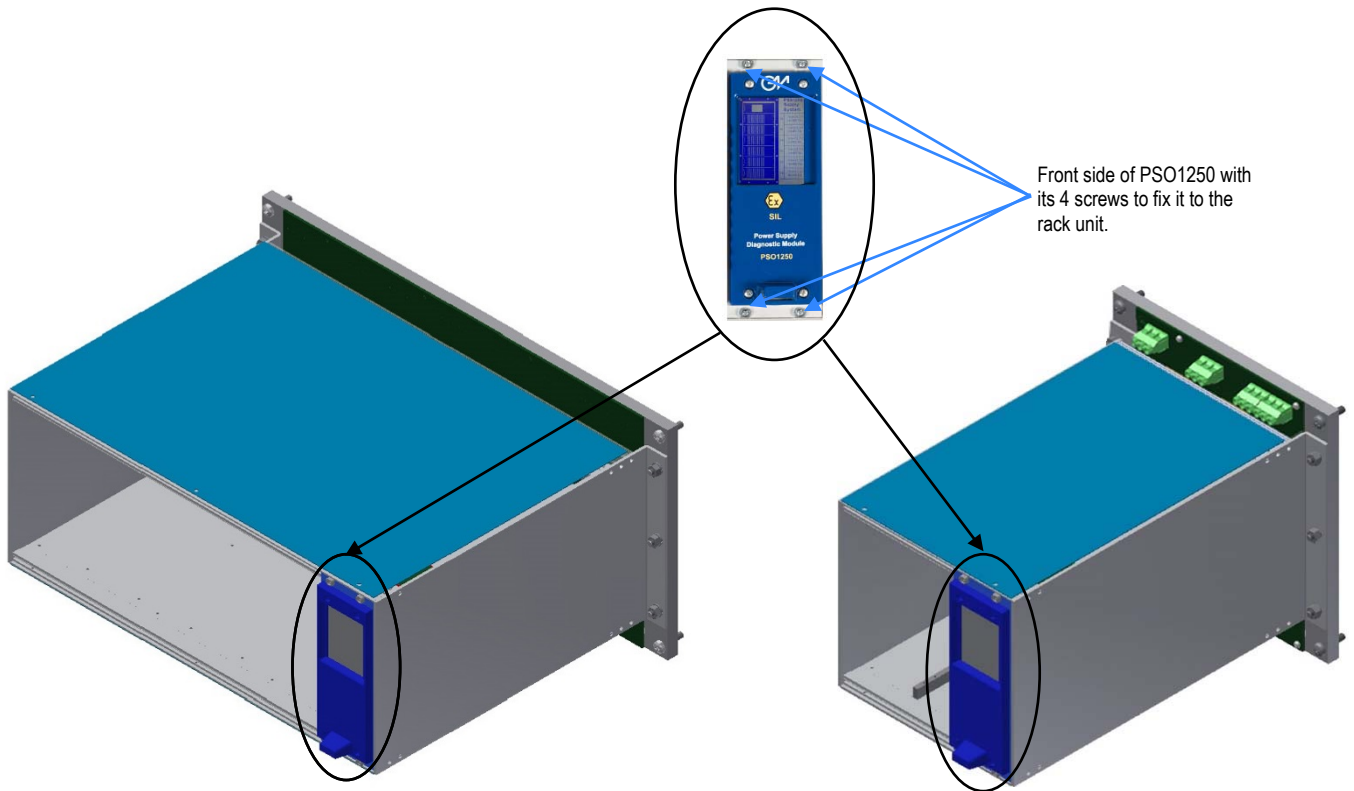


Fig. 6

Now power AC1 and AC2 input power lines. PSO1250 diagnostic module and each PSM1250 power module turn on and the DC output lines power the load.

Installation Procedure - 4th step (for models without HS) - Section A: Installation and start up of PSO1250 Diagnostic Module

Insert PSO1250 diagnostic module in the last position on the right of the PSR1250 rack unit and fix the module to the rack unit by means of its 4 screws on its front side.



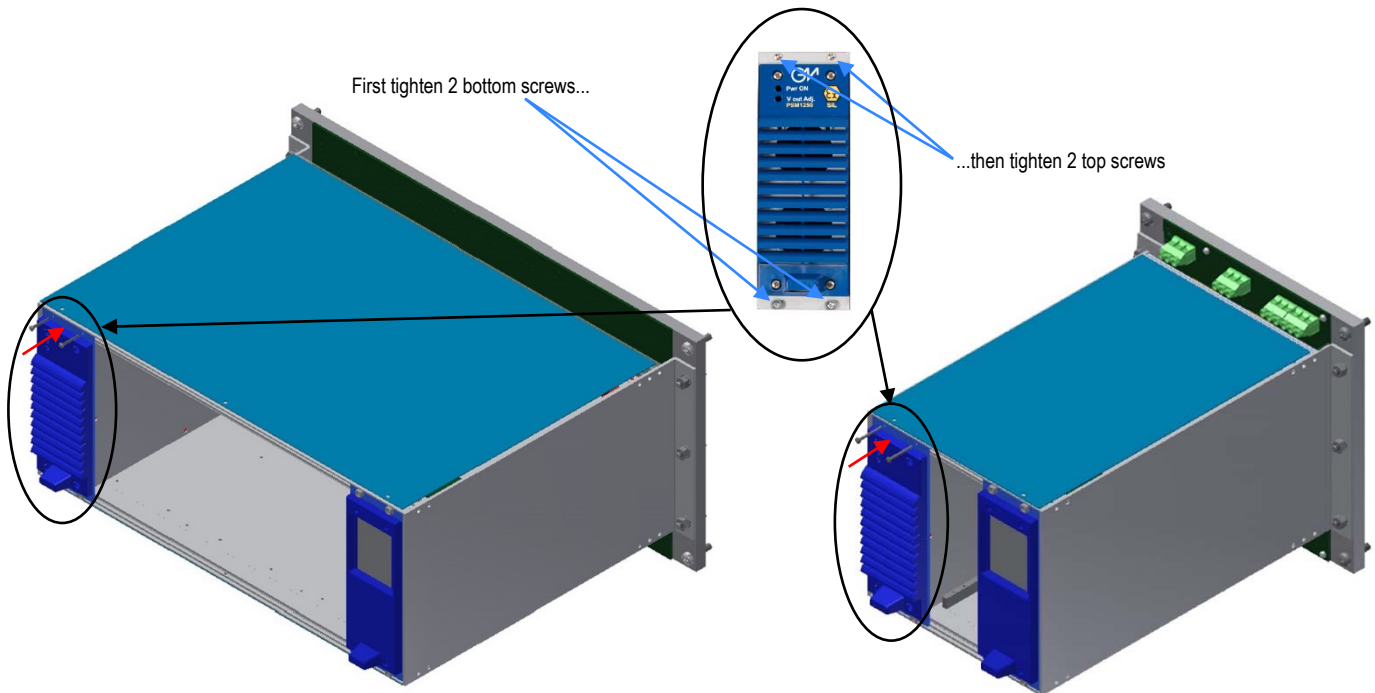
After installation of the PSO1250 module, **power AC1 and AC2 input power lines** in order to turn on the diagnostic module.
For more information about diagnostic module features and its set up, please see description from page 39.
After setting up the PSO1250 module, **unpower AC1 and AC2 input power lines**.
If it is not required the installation of the PSO1250 module, **unpower AC1 and AC2 input power lines** anyway.

Installation Procedure - 4th step (for models without HS) - Section B: Installation and pre-start up of PSM1250 Power Supply Module

AC1 and AC2 input power lines are unpowered.

The following procedure is split in 3 sub-steps and it is the same for each PSM1250, independently from its position in the rack unit. Starting from position 1 to position 6 (for PSS1250-7) or 2 (for PSS1250-3), execute pre-start up of each PSM1250 module.

1st sub-step: insert and fix the PSM1250 module into the rack unit by means of its 4 screws on its front side.



Power ON green LED

Trimmer for output voltage adjusting (use a little cross head isolated screwdriver)

2nd sub-step: powering AC1 and AC2 input power lines, PSM1250 module is turned on, its front panel Power ON green LED is ON and 24 Vdc (factory setting) output voltage is present on PSM1250 screw output terminals DC- and DC+ (see page 5 for more information about Power ON green LED signalling).

On the TFT color screen of PSO1250 diagnostic module it is possible to monitor the PSM1250 module status and to collect information about the power supply: for example output voltage value (see description from page 39). If no PSO1250 diagnostic module is present, the output voltage can be measured on PSM1250 screw output terminals by means of a multimeter.

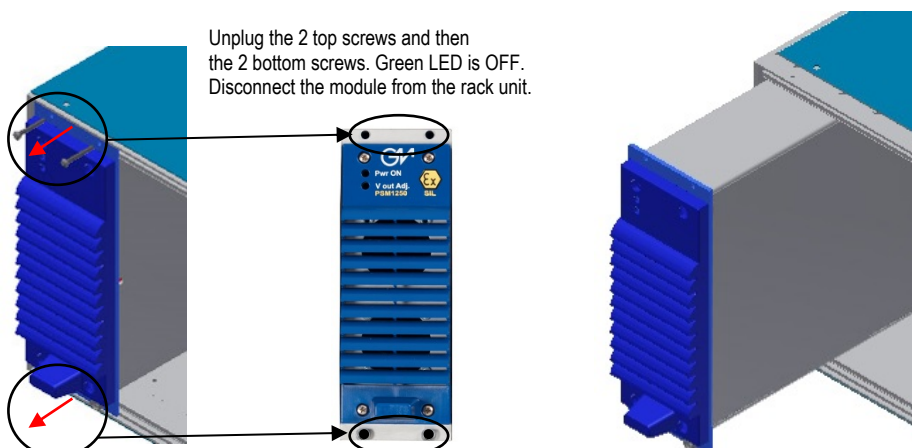
If it is required to set an output voltage value different from factory setting (24 Vdc), use the trimmer for output voltage adjusting. Turn the trimmer clockwise (to the right) to increase output voltage (max. 28 Vdc) or turn the trimmer counterclockwise (to the left) to decrease output voltage (min. 21 Vdc).

Warning: for correct current sharing operation, power supply modules must have output voltages calibrated within ± 0.5 V.



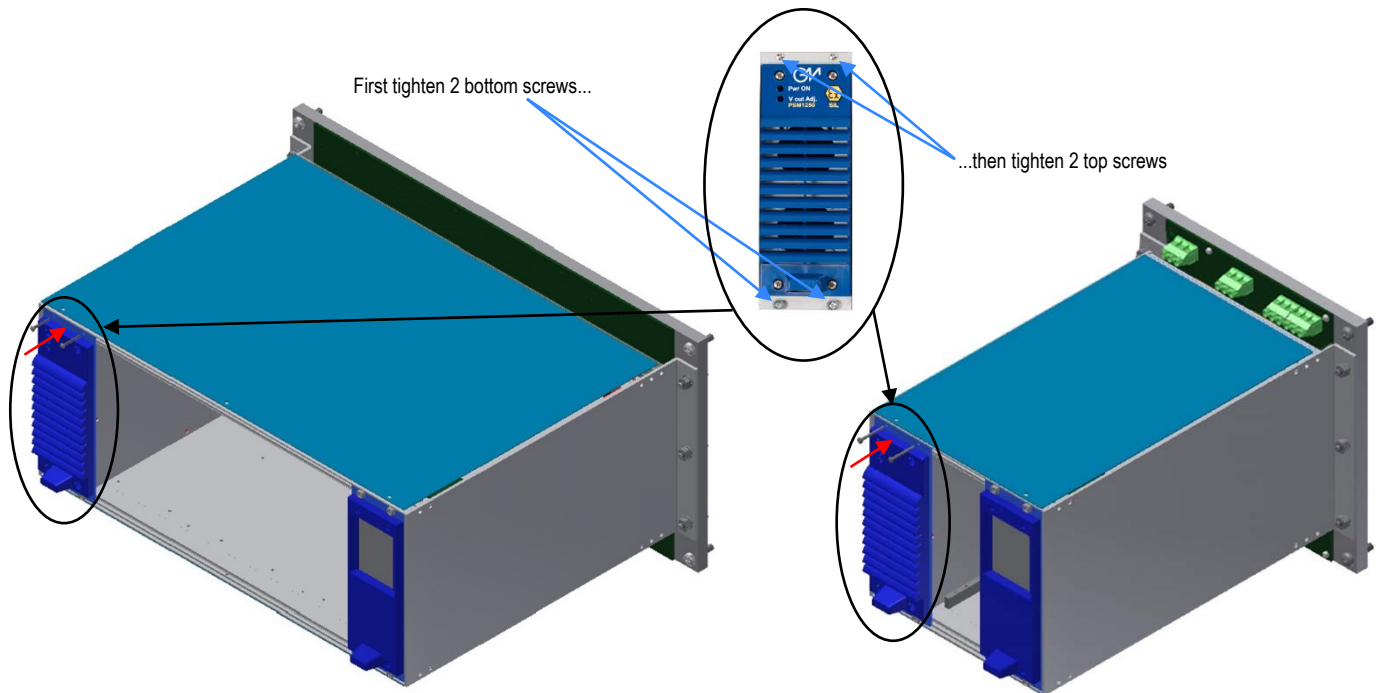
PSM1250 screw output terminals on copper bars:
DC- is negative out pole,
DC+ is positive out pole.
(in the figure it's shown DC1- and DC1+ which are related to PSM1250 in position 1 of PSS1250 system).

3rd sub-step: after having adjusted the PSM1250 output voltage, unpower AC1 and AC2 input power lines to turn off the power module. Then release 4 screws on its front side and disconnect the module from the rack unit in order to repeat sub-steps 1 to 3 procedure for other modules and complete the setting for all PSM1250 of PSS1250 power system.



Installation Procedure - 4th step (for models without HS) - Section C: Wiring of bottom screw output terminals on copper bars (DC output lines) of wall mounting panels type WMP1250-7-x-D and WMP1250-3-D and star up of PSS1250 power system

At this step, **AC1 and AC2 input power lines are unpowered**, PSO1250 diagnostic module is installed and fixed to rack unit with 4 screws, while all PSM1250 modules are disconnected. Starting from position 1 to position 6 (for PSS1250-7) or 2 (for PSS1250-3), insert and fix each PSM1250 module into the rack unit by means of its 4 screws on its front side.



To wire bottom screw output terminals on copper bars (DC output lines: DC- is negative out pole, DC+ is positive out pole), see Fig. 1-2-3-4-5, where it's shown DC1- and DC1+, related to PSM1250 in position 1 of PSS1250 system.

For WMP1250-7-x-D, see functional diagrams at pages 6-7-8 for more information about wiring connection.

For WMP1250-3-D, see functional diagrams at page 9 for more information about wiring connection.



Fig. 1



Fig. 2



Fig. 3



Unplug M6 nuts, groovers and washers. Then insert a cable lug with wire, washer and groover on each screw output terminal. Finally tighten nut to fix wire.

For DC screw output terminals, use a typical cable section of AWG7 (maximum AWG5 or 16 mm²).

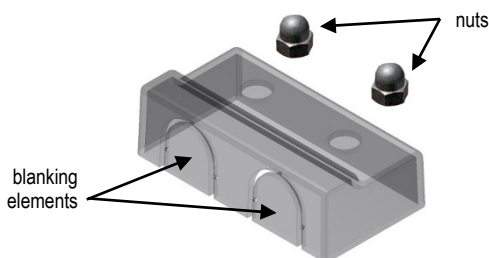


Fig. 4

A polycarbonate cover is used for IP20 to protect each couple of screw output terminals. Break two preformed blanking elements to allow cable passage. Then insert and fix the cover on couple of screw output terminals by means of M6 nylon-capped lock nut.



Fig. 5

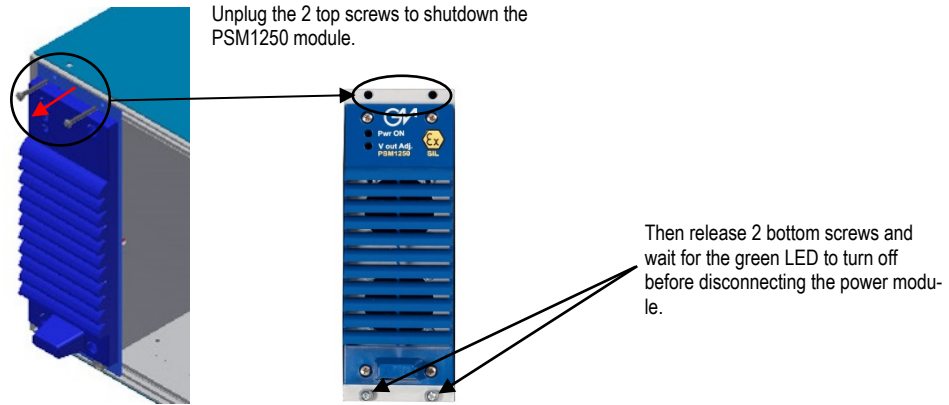
After having wired all DC output lines and tighten front panel screws, **power AC1 and AC2 input power lines**. PSO1250 diagnostic module and each PSM1250 power module turn on and the DC output lines power the load.

Shutdown and Disconnecting Procedure of PSM1250 power module from the rack unit : - for models with HS

Disconnection of PSM1250 module from the rack unit, can be done without switching off the power from AC1 and AC2 lines, because of the fully redundant configuration from the input to the output of the power system.

To remove a PSM1250 power module unplug the 2 top screws and then release the other 2 bottom screws.

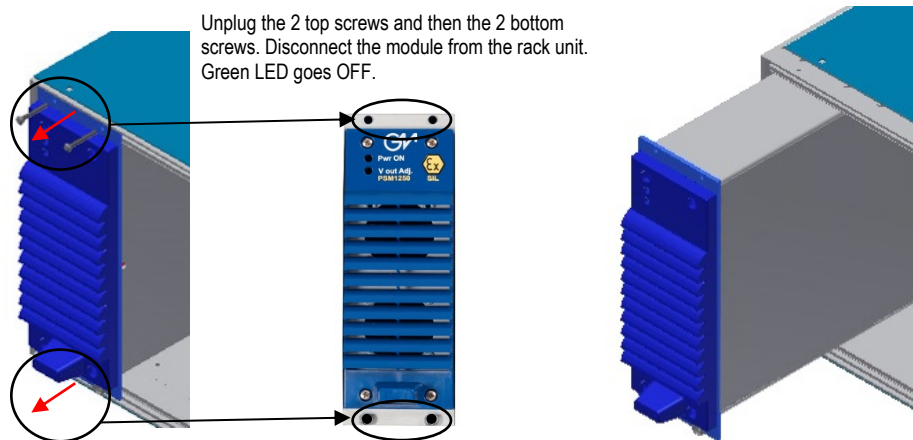
Check that Power ON LED is OFF before disconnecting the module from the rack unit.



Shutdown and Disconnecting Procedure of PSM1250 power module from the rack unit : - for models without HS

Disconnection of PSM1250 module from the rack unit, can be done without switching off the power from AC1 and AC2 lines, because of the fully redundant configuration from the input to the output of the power system.

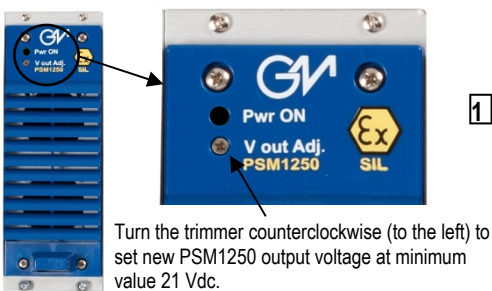
To remove a PSM1250 power module release 4 screws on its front side and disconnect the module from the rack unit.



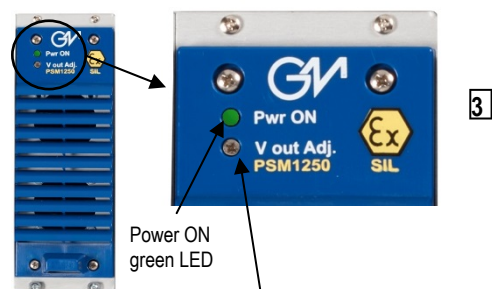
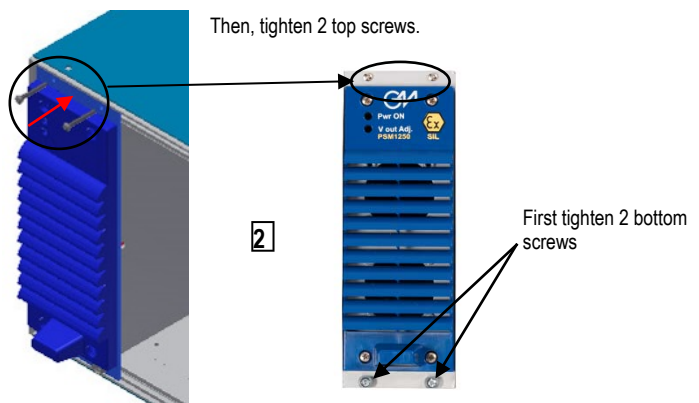
Replacement Procedure of PSM1250 power module from the rack unit (for models with or without HS)

To disconnect a PSM1250 module from the rack unit, follow the previous procedure "Shutdown and disconnecting procedure of PSM1250 power module from the rack unit (for models with or without HS)" to unplug the PSM1250 module.

Then, take a new PSM1250 power module and follow this procedure (1-2-3).



Then insert and fix the new PSM1250 module into the rack unit by means of its 4 screws on front side. First tighten 2 bottom screws and then tighten 2 top ones.



The new PSM1250 module is powered and its green LED is ON, but the module is not operating in current sharing with other PSM1250 modules paralleled with it, because its output voltage is too low (21 Vdc).

For correct current sharing operation, all power supply modules in parallel/redundant configuration, must have output voltages calibrated within ± 0.5 V.

Read the output voltage of the new PSM1250 on TFT color screen of PSO1250 diagnostic module, and slowly increase it with the trimmer to reach the output voltage (within ± 0.5 V) of all other PSM1250 modules paralleled with it, to guarantee a correct current sharing operation.

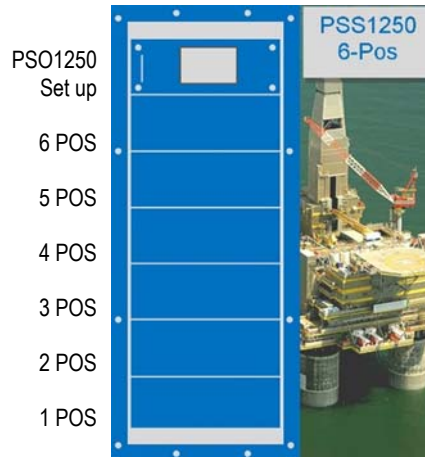
Slowly turn the trimmer clockwise (to the right) to increase new PSM1250 output voltage and reach the output voltage (within ± 0.5 V) of all other PSM1250 modules paralleled with it.

PSO1250 Diagnostic Module: features and set up

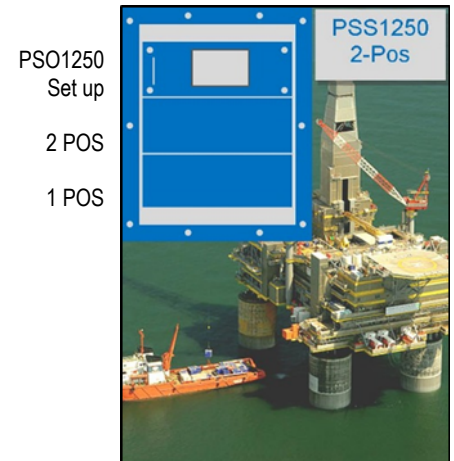
Communication with six (for PSS1250-7) or two (for PSS1250-3) power modules is achieved via PSO1250 diagnostic module (only for PSS1250 with -D suffix), which incorporates a front panel color touch screen. The diagnostic module is able to query each power modules (using an internal proprietary bus) and read data such as: Input/Output Voltage, Current and Power; Input Line Frequency; Output current sharing percentage; Internal Temperature; alarm status (under/over out voltage, AC line absence, internal PFC or PWM stage in OFF state, internal high temperature, fans malfunction). These information are available via front panel LCD and externally via Modbus RTU on related wall mounting terminal block. The following figures are screenshots of TFT LCD and show the setting up of the PSO1250 diagnostic module and reading data from each power module.



At start up of PSO1250 diagnostic module, this image is shown for some seconds.



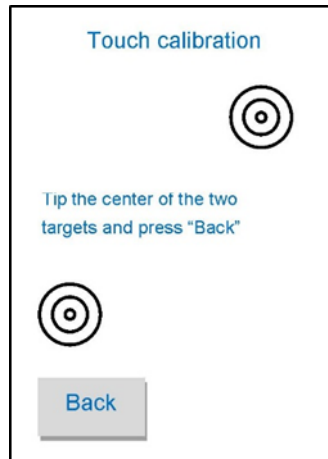
This image is the main menu of PSS1250-xx-7-x-D when no PSM1250 module is operating in power system.



This image is the main menu of PSS1250-xx-3-D when no PSM1250 module is operating in power system.



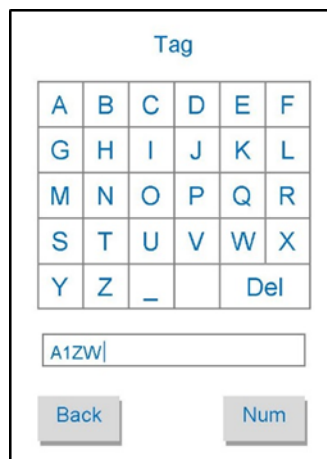
This set up menu image is shown when touching the "PSO1250 set up" cell in the main menu screen.



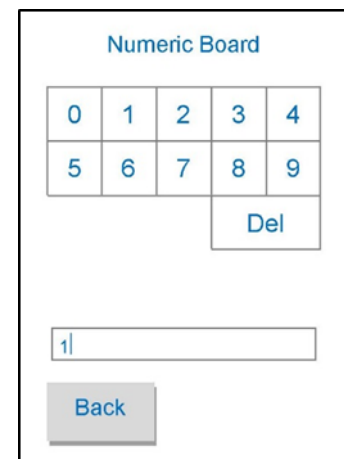
This image is shown when touching the "Calib" cell in the set up menu screen. Tip the center of the two targets and press back, for calibration of touch screen.



This image is shown when touching the "Modbus" cell in the set up menu screen. Here is possible to set Modbus communication parameters as baudrate, parity, terminal resistance, endianness and address, touching related cells.

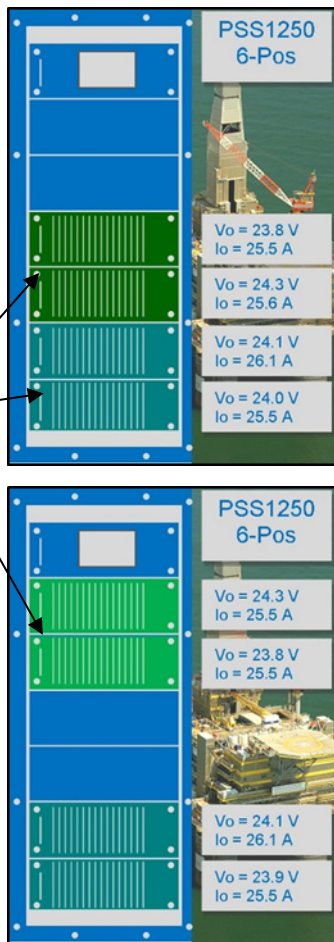


This image is shown when touching the "Tag" cell in the set up menu screen. Alphabetical board to introduce a tag to identify PSS1250.



This image (numeric board) is shown when touching the "Addr" cell in Modbus menu or "Num" cell in Tag menu screen.

Different green colors for each current sharing group



All PSM1250 modules are normally operating (their pos. cells are all green). This image is related to PSS1250-xx-7-3-D because there are 3 current sharing groups.

Module 1

In AC voltage = 231 Vrms
 In AC current = 3.6 Arms
 In act. power = 757 W
 In frequency = 49.8 Hz

Out DC voltage = 24.0 V
 Out DC current = 25.5 A
 Out power = 612 W
 Current share = 49 %

Internal Temp = 30 °C

Back More

Touching "1 pos." cell on the main menu screen, the PSM1250 module 1 (Pos.1) first page data are shown. Touch "Back" cell to return on the main menu or touch "More" cell to go on the second page data.

Module 1

Bulk voltage = 395 V
 Cap. out volt. = 24.2 V
 Fan virt. speed = 10362 rpm
 Fans enabled

Back

PSM1250 module 1 (Pos.1) second page data is also used to show fault alarm. Touch "Back" cell to return on the first page.

Module 2

In AC voltage = 228 Vrms
 In AC current = 3.4 Arms
 In act. power = 705 W
 In frequency = 49.7 Hz

Out DC voltage = 24.3 V
 Out DC current = 25.5 A
 Out power = 620 W
 Current share = 50 %

Internal Temp = 30 °C

Back More

Touching "2 pos." cell on the main menu screen, the PSM1250 module 2 (Pos.2) first page data are shown. Touch "Back" cell to return on the main menu or touch "More" cell to go on the second page data.

Module 2

Bulk voltage = 399 V
 Cap. out volt. = 24.2 V
 Fan virt. speed = 10470 rpm
 Fans enabled

Back

The PSM1250 module 2 (Pos.2) second page data is also used to show fault alarm. Touch "Back" cell to return on the first page.

Module 3

In AC voltage = 235 Vrms
 In AC current = 3.4 Arms
 In act. power = 727 W
 In frequency = 50.0 Hz

Out DC voltage = 24.3 V
 Out DC current = 25.6 A
 Out power = 622 W
 Current share = 50 %

Internal Temp = 30 °C

Back More

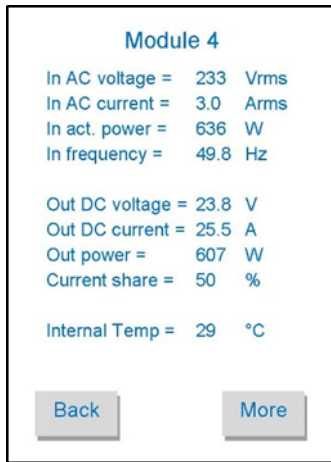
Touching "3 pos." cell on the main menu screen, the PSM1250 module 3 (Pos.3) first page data are shown. Touch "Back" cell to return on the main menu or touch "More" cell to go on the second page data.

Module 3

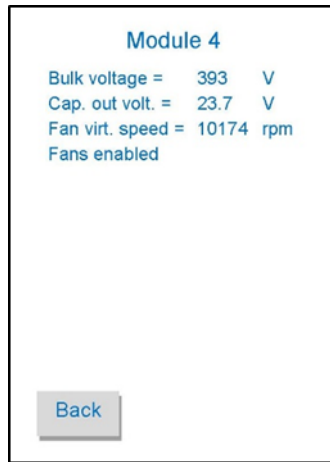
Bulk voltage = 399 V
 Cap. out volt. = 24.2 V
 Fan virt. speed = 10497 rpm
 Fans enabled

Back

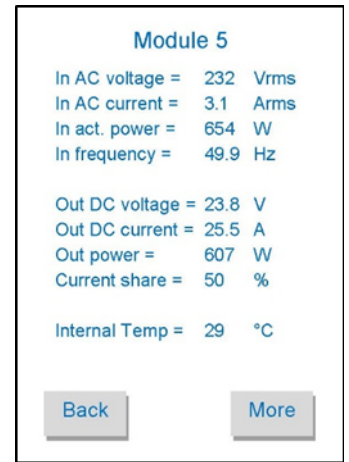
The PSM1250 module 3 (Pos.3) second page data is also used to show fault alarm. Touch "Back" cell to return on the first page.



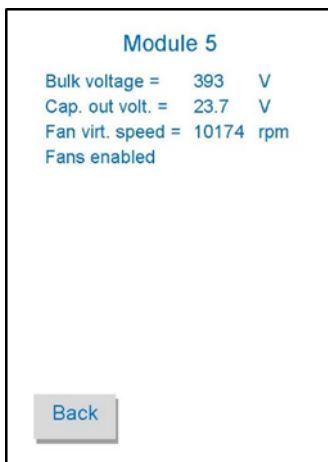
Touching "4 pos." cell on the main menu screen, the PSM1250 module 4 (Pos.4) first page data are shown. Touch "Back" cell to return on the main menu or touch "More" cell to go on the second page data.



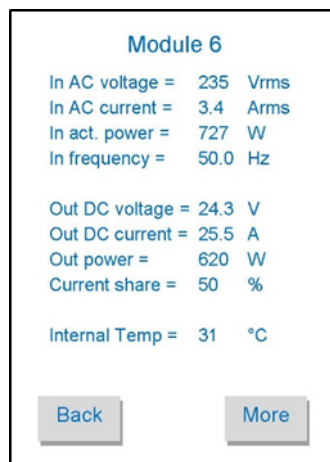
The PSM1250 module 4 (Pos.4) second page data is also used to show fault alarm. Touch "Back" cell to return on the first page.



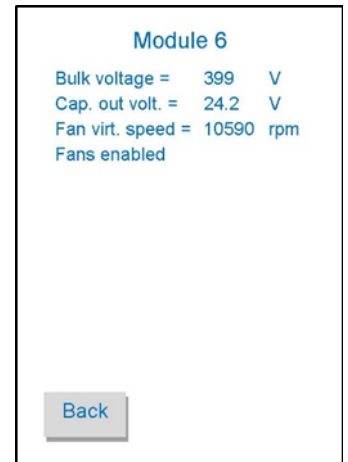
Touching "5 pos." cell on the main menu screen, the PSM1250 module 5 (Pos.5) first page data are shown. Touch "Back" cell to return on the main menu or touch "More" cell to go on the second page data.



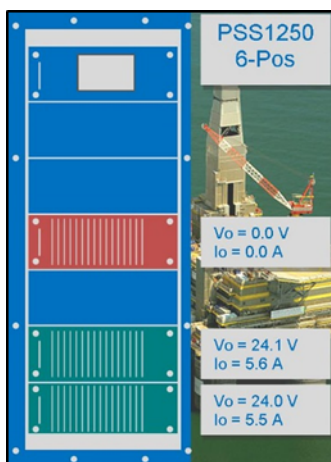
The PSM1250 module 5 (Pos.5) second page data is also used to show fault alarm. Touch "Back" cell to return on the first page.



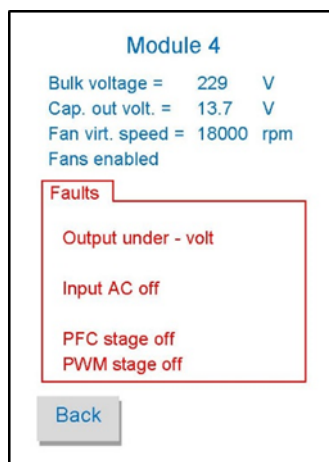
Touching "6 pos." cell on the main menu screen, the PSM1250 module 6 (Pos.6) first page data are shown. Touch "Back" cell to return on the main menu or touch "More" cell to go on the second page data.



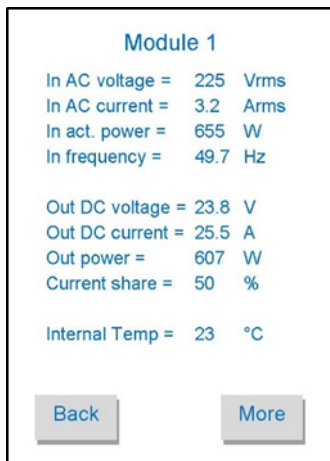
The PSM1250 module 6 (Pos.6) second page data is also used to show fault alarm. Touch "Back" cell to return on the first page.



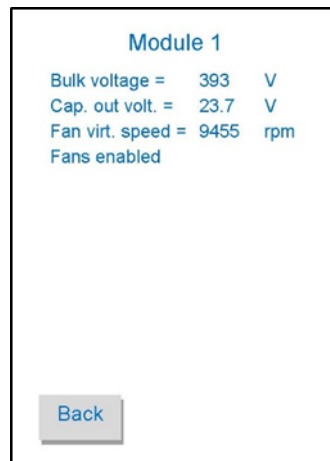
PSM1250 module 4 (Pos.4) second page data shows fault alarms. There is absence of input AC line, internal PFC and PWM stages are OFF and therefore DC output is in undervoltage condition.



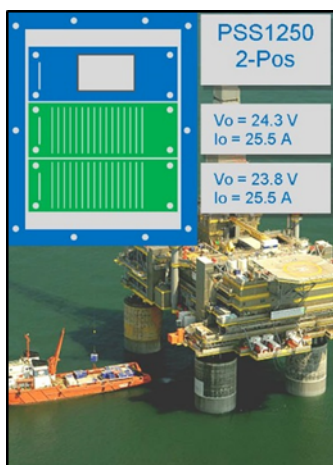
PSM1250 module 4 (Pos.4) second page data shows fault alarms. There is absence of input AC line, internal PFC and PWM stages are OFF and therefore DC output is in undervoltage condition.



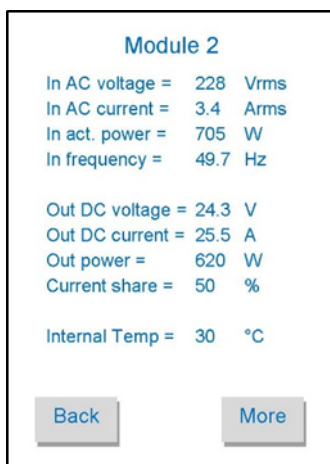
Touching "1 pos." cell on the main menu screen, the PSM1250 module 1 (Pos.1) first page data are shown. Touch "Back" cell to return on the main menu or touch "More" cell to go on the second page data.



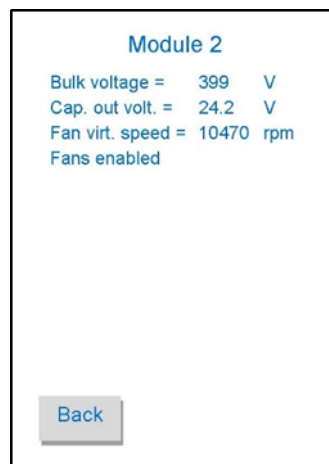
PSM1250 module 1 (Pos.1) second page data is also used to show fault alarm. Touch "Back" cell to return on the first page.



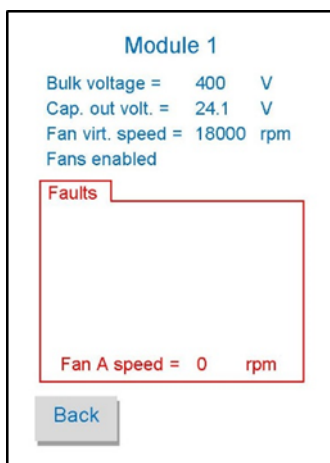
All PSM1250 modules are normally operating (their pos. cells are all green).



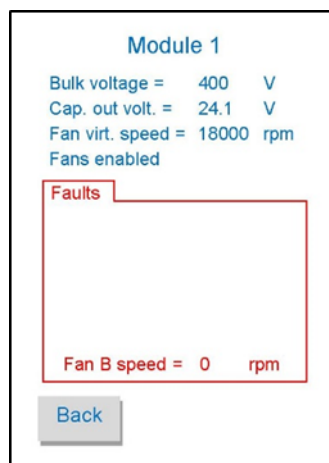
Touching "2 pos." cell on the main menu screen, the PSM1250 module 2 (Pos.1) first page data are shown. Touch "Back" cell to return on the main menu or touch "More" cell to go on the second page data.



PSM1250 module 1 (Pos.1) second page data is also used to show fault alarm. Touch "Back" cell to return on the first page.



Module 1: fan A is not operating (0 rpm)



Module 1: fan B is not operating (0 rpm)

Supported Modbus parameters:

PSS1250 with -D suffix can communicate via Modbus RTU RS-485 protocol. Below is a list of all available registers.

Addr.	Description	Notes	Type (15)	Addr.	Description	Notes	Type (15)
0	G.M. Factory Code	Identification Data	R	137	PSM1250 Internal temperature ⁽²⁾	4th position PSM1250 Module Data	R
1	Instrument Code						
2	Option Code						
3	Hardware Release						
4	Software Release						
16	Modbus Address	Communication Data	R/W	138	Input active power ⁽³⁾		
17	Modbus Baudrate ⁽¹⁾						
18	Modbus Format ⁽¹⁾						
71	PSM1250 Internal temperature ⁽²⁾	1st position PSM1250 Module Data	R	139	Output power ⁽³⁾		
72	Input active power ⁽³⁾						
73	Output power ⁽³⁾						
74	Power efficiency ⁽⁴⁾						
75	Bulk electrolytic capacitor voltage ⁽⁵⁾						
76	AC input voltage ⁽⁶⁾						
77	AC input current ⁽⁷⁾						
78	AC input frequency ⁽⁸⁾						
79	Primary side fault information ⁽¹⁾						
81	Output electrolytic capacitor voltage ⁽⁹⁾						
82	Output voltage ⁽⁹⁾						
83	Output current ⁽¹⁰⁾						
84	Fan driver enable ⁽¹⁾						
85	Fan driver inverted duty cycle ⁽¹³⁾						
86	Fan driver speed ⁽¹¹⁾						
87	Fan A read frequency ⁽¹²⁾						
88	Fan A read speed ⁽¹¹⁾						
89	Fan B read frequency ⁽¹²⁾						
90	Fan B read speed ⁽¹¹⁾						
91	Secondary side fault information ⁽¹⁾						
92	Secondary side extra fault information ⁽¹⁾						
93	PSM1250 Internal temperature ⁽²⁾			2nd position PSM1250 Module Data	R	140	Power efficiency ⁽⁴⁾
94	Input active power ⁽³⁾						
95	Output power ⁽³⁾						
96	Power efficiency ⁽⁴⁾						
97	Bulk electrolytic capacitor voltage ⁽⁵⁾						
98	AC input voltage ⁽⁶⁾						
99	AC input current ⁽⁷⁾						
100	AC input frequency ⁽⁸⁾						
101	Primary side fault information ⁽¹⁾						
103	Output electrolytic capacitor voltage ⁽⁹⁾						
104	Output voltage ⁽⁹⁾						
105	Output current ⁽¹⁰⁾						
106	Fan driver enable ⁽¹⁾						
107	Fan driver inverted duty cycle ⁽¹³⁾						
108	Fan driver speed ⁽¹¹⁾						
109	Fan A read frequency ⁽¹²⁾						
110	Fan A read speed ⁽¹¹⁾						
111	Fan B read frequency ⁽¹²⁾						
112	Fan B read speed ⁽¹¹⁾						
113	Secondary side fault information ⁽¹⁾						
114	Secondary side extra fault information ⁽¹⁾						
115	PSM1250 Internal temperature ⁽²⁾	3rd position PSM1250 Module Data	R			141	Bulk electrolytic capacitor voltage ⁽⁵⁾
116	Input active power ⁽³⁾						
117	Output power ⁽³⁾						
118	Power efficiency ⁽⁴⁾						
119	Bulk electrolytic capacitor voltage ⁽⁵⁾						
120	AC input voltage ⁽⁶⁾						
121	AC input current ⁽⁷⁾						
122	AC input frequency ⁽⁸⁾						
123	Primary side fault information ⁽¹⁾						
125	Output electrolytic capacitor voltage ⁽⁹⁾						
126	Output voltage ⁽⁹⁾						
127	Output current ⁽¹⁰⁾						
128	Fan driver enable ⁽¹⁾						
129	Fan driver inverted duty cycle ⁽¹³⁾						
130	Fan driver speed ⁽¹¹⁾						
131	Fan A read frequency ⁽¹²⁾						
132	Fan A read speed ⁽¹¹⁾						
133	Fan B read frequency ⁽¹²⁾						
134	Fan B read speed ⁽¹¹⁾						
135	Secondary side fault information ⁽¹⁾						
136	Secondary side extra fault information ⁽¹⁾						
142	AC input voltage ⁽⁶⁾			5th position PSM1250 Module Data	R	142	AC input voltage ⁽⁶⁾
143	AC input current ⁽⁷⁾						
144	AC input frequency ⁽⁸⁾						
145	Primary side fault information ⁽¹⁾						
147	Output electrolytic capacitor voltage ⁽⁹⁾						
148	Output voltage ⁽⁹⁾						
149	Output current ⁽¹⁰⁾						
150	Fan driver enable ⁽¹⁾						
151	Fan driver inverted duty cycle ⁽¹³⁾						
152	Fan driver speed ⁽¹¹⁾						
153	Fan A read frequency ⁽¹²⁾						
154	Fan A read speed ⁽¹¹⁾						
155	Fan B read frequency ⁽¹²⁾						
156	Fan B read speed ⁽¹¹⁾						
157	Secondary side fault information ⁽¹⁾						
158	Secondary side extra fault information ⁽¹⁾						
159	PSM1250 Internal temperature ⁽²⁾	6th position PSM1250 Module Data	R			159	PSM1250 Internal temperature ⁽²⁾
160	Input active power ⁽³⁾						
161	Output power ⁽³⁾						
162	Power efficiency ⁽⁴⁾						
163	Bulk electrolytic capacitor voltage ⁽⁵⁾						
164	AC input voltage ⁽⁶⁾						
165	AC input current ⁽⁷⁾						
166	AC input frequency ⁽⁸⁾						
167	Primary side fault information ⁽¹⁾						
169	Output electrolytic capacitor voltage ⁽⁹⁾						
170	Output voltage ⁽⁹⁾						
171	Output current ⁽¹⁰⁾						
172	Fan driver enable ⁽¹⁾						
173	Fan driver inverted duty cycle ⁽¹³⁾						
174	Fan driver speed ⁽¹¹⁾						
175	Fan A read frequency ⁽¹²⁾						
176	Fan A read speed ⁽¹¹⁾						
177	Fan B read frequency ⁽¹²⁾						
178	Fan B read speed ⁽¹¹⁾						
179	Secondary side fault information ⁽¹⁾						
180	Secondary side extra fault information ⁽¹⁾						
181	PSM1250 Internal temperature ⁽²⁾	1st pos. PSM1250 Data	R	181	PSM1250 Internal temperature ⁽²⁾		
182	Input active power ⁽³⁾		R	182	Input active power ⁽³⁾		
183	Output power ⁽³⁾		R	183	Output power ⁽³⁾		
184	Power efficiency ⁽⁴⁾		R	184	Power efficiency ⁽⁴⁾		
185	Bulk electrolytic capacitor voltage ⁽⁵⁾		R	185	Bulk electrolytic capacitor voltage ⁽⁵⁾		
186	AC input voltage ⁽⁶⁾		R	186	AC input voltage ⁽⁶⁾		
187	AC input current ⁽⁷⁾		R	187	AC input current ⁽⁷⁾		
188	AC input frequency ⁽⁸⁾		R	188	AC input frequency ⁽⁸⁾		
189	Primary side fault information ⁽¹⁾		R	189	Primary side fault information ⁽¹⁾		
191	Output electrolytic capacitor voltage ⁽⁹⁾		R	191	Output electrolytic capacitor voltage ⁽⁹⁾		
192	Output voltage ⁽⁹⁾		R	192	Output voltage ⁽⁹⁾		
193	Output current ⁽¹⁰⁾		R	193	Output current ⁽¹⁰⁾		
194	Fan driver enable ⁽¹⁾		R	194	Fan driver enable ⁽¹⁾		
195	Fan driver inverted duty cycle ⁽¹³⁾		R	195	Fan driver inverted duty cycle ⁽¹³⁾		
196	Fan driver speed ⁽¹¹⁾		R	196	Fan driver speed ⁽¹¹⁾		
197	Fan A read frequency ⁽¹²⁾		R	197	Fan A read frequency ⁽¹²⁾		
198	Fan A read speed ⁽¹¹⁾		R	198	Fan A read speed ⁽¹¹⁾		
199	Fan B read frequency ⁽¹²⁾		R	199	Fan B read frequency ⁽¹²⁾		
200	Fan B read speed ⁽¹¹⁾	R	200	Fan B read speed ⁽¹¹⁾			
201	Secondary side fault information ⁽¹⁾	R	201	Secondary side fault information ⁽¹⁾			
202	Secondary side extra fault information ⁽¹⁾	R	202	Secondary side extra fault information ⁽¹⁾			
203	Current sharing value ⁽⁴⁾	2nd pos. PSM1250 Data	R	203	Current sharing value ⁽⁴⁾		
204	Current sharing value ⁽⁴⁾	3rd pos. PSM1250 Data	R	204	Current sharing value ⁽⁴⁾		
205	Current sharing value ⁽⁴⁾	4th pos. PSM1250 Data	R	205	Current sharing value ⁽⁴⁾		
206	Current sharing value ⁽⁴⁾	5th pos. PSM1250 Data	R	206	Current sharing value ⁽⁴⁾		
207	Current sharing value ⁽⁴⁾	6th pos. PSM1250 Data	R	207	Current sharing value ⁽⁴⁾		
208	Current sharing value ⁽⁴⁾	Command	W	208	Current sharing value ⁽⁴⁾		
464	Command execution ⁽¹⁴⁾	Inter-modules protocol	R	464	Command execution ⁽¹⁴⁾		
516	Inter-modules communication error counter	Inter-modules protocol	R	516	Inter-modules communication error counter		
517	Inter-modules missed communication ⁽¹⁾	Inter-modules protocol	R	517	Inter-modules missed communication ⁽¹⁾		
518	Modbus error counter	Modbus protocol	R	518	Modbus error counter		
533	Common Under or Over Voltage fault status ⁽¹⁾	Common fault data	R	533	Common Under or Over Voltage fault status ⁽¹⁾		

(To be continued on next page)

Supported Modbus parameters:

Addr.	Description	Notes	Type ⁽¹⁴⁾
556	Chars 0, 1	PSS1250 Tag	R/W
557	Chars 2, 3		
558	Chars 4, 5		
559	Chars 6, 7		
560	Chars 8, 9		
561	Chars 10, 11		
562	Chars 12, 13		
563	Chars 14, 15		

Supported modbus functions:

Code	Name	Notes
03	read holding registers	reads a stream of words from memory
04	read input registers	reads a stream of words from memory
08	diagnostics: subcode 0	returns query data
06	write single register	writes a word in memory
16	write multiple registers	writes a stream of words in memory

Notes:

Each Modbus parameter is described by one 16-bit word.

- See command details on this page.
- Expressed in °C.
- Expressed in W.
- Expressed in %.
- Expressed in V.
- Expressed in Vrms.
- Expressed in 100 mArms.
- Expressed in 100 mHz.
- Expressed in 100 mV.
- Expressed in 100 mA.
- Expressed in Round Per Minute (RPM).
- Expressed in Hz.
- Expressed in %: inverted duty cycle (%) = 100% - duty cycle (%).
- All configurations must be confirmed via Addr. 464, see details on this page.
- Parameter Type:
R = read only,
W = write only,
R/W = read and write.

Modbus parameters details:

Address 17: Supported Modbus Baudrates	
Index	Baudrate
0	4800
1	9600
2	19200
3	38400
4	57600
5	115200

Address 18: Supported Modbus Formats															
High Byte	Low Byte														
Bit position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Endianness 32 bit Data (0 = Little; 1 = Big) →

Termination resistance (1 = enabled) →

- Supported Modbus Parity:
- 8 data bit, no parity, 1 stop bit
 - 8 data bit, even parity, 1 stop bit
 - 8 data bit, odd parity, 1 stop bit

Address 79:		Primary side fault information													
Address 101:															
Address 123:															
Address 145:															
Address 167:															
Address 189:															
High Byte		Low Byte													
Bit position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

PFC stage status (1 = operative ; 0 = shutdown and fault) →

High temperature status (1 = presence and fault ; 0 = absence) →

AC line status (1 = absence and fault ; 0 = presence) →

Address 91:		Secondary side fault information													
Address 113:															
Address 135:															
Address 157:															
Address 179:															
Address 201:															
High Byte		Low Byte													
Bit position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Over Voltage fault (1 = presence ; 0 = absence) →

Under Voltage fault (1 = presence ; 0 = absence) →

PWM stage status (1 = operative ; 0 = shutdown and fault) →

Address 92:		Secondary side extra fault information													
Address 114:															
Address 136:															
Address 158:															
Address 180:															
Address 202:															
High Byte		Low Byte													
Bit position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Inter-modules protocol comm. fault from PSO1250 (1=fault; 0=ok) →

Intra-module protocol communication fault (1=fault ; 0=ok) →

Fan B fault (1=fault, change > 5000 rpm on driver speed; 0=ok) →

Fan A fault (1=fault, change > 5000 rpm on driver speed; 0=ok) →

Address 464: Various commands															
High Byte	Low Byte														
Bit position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

- Save Input/Output Configuration
- Save Modbus configuration
- Save Tags
- Lock Alarms
- Analog Output Sink/Source Switch

Address 517: Inter-modules missed communication															
High Byte	Low Byte														
Bit position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

All bits '1' →

6th position PSM1250 module (1=missed; 0=present) →

5th position PSM1250 module (1=missed; 0=present) →

4th position PSM1250 module (1=missed; 0=present) →

3rd position PSM1250 module (1=missed; 0=present) →

2nd position PSM1250 module (1=missed; 0=present) →

1st position PSM1250 module (1=missed; 0=present) →

Address 533: Common Under or Over Voltage fault status															
High Byte	Low Byte														
Bit position															
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

All bits '1' →

6th position PSM1250 module (1=UV or OV fault ; 0=ok) →

5th position PSM1250 module (1=UV or OV fault ; 0=ok) →

4th position PSM1250 module (1=UV or OV fault ; 0=ok) →

3rd position PSM1250 module (1=UV or OV fault ; 0=ok) →

2nd position PSM1250 module (1=UV or OV fault ; 0=ok) →

1st position PSM1250 module (1=UV or OV fault ; 0=ok) →