INSTRUCTION & SAFETY MANUAL

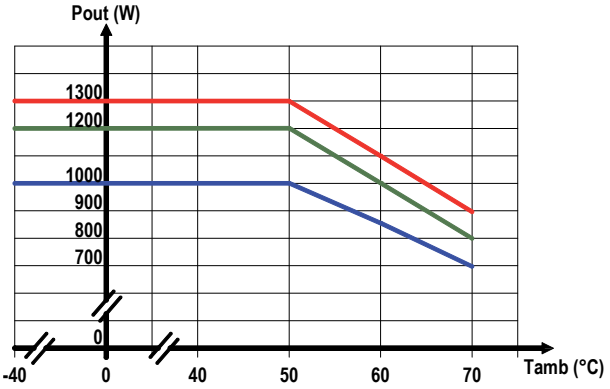
SIL3 Power Supply PSW1250, 24Vdc, 50 A, Zone 2 / Division 2 Wall Mounting

GM INTERNATIONAL
TECHNOLOGY FOR SAFETY

Characteristics

General Description:
The Power Supply type PSW1250 is stainless steel AISI 304 unit.
The Supply provides 24Vdc, 50 A output. PSW1250 unit can be paralleled, with load sharing circuits, which distribute current load equally to each power supply to increase reliability and reduce internal power dissipation. The Supply accepts AC power sources from 100 to 264 Vac.
Overvoltage protection: 3 independent overvoltage protections: 1 voltage limiting loop at 30 Vdc and 1+1 crowbars at 30 Vdc.
EMC: Fully compliant with CE marking applicable requirements.
High load fuses breaking capability:
In case of short circuit on the load, the Power supply system delivers a very high peak current (about 800 Amp) for a duration of 0.5 ms. This characteristic ensures the instant breakage of the protective fuse or circuit breaker. Because of the very short peak current duration, other equipment connected to the load are not affected by the failure event and continue to operate without interruption.
Functional Safety Management Certification:
G.M. International is certified by TUV to conform to IEC61508:2010 part 1 clauses 5-6 for safety related systems up to and included SIL3.

PSW1250
Output Power vs. Ambient Operating Temperature



With 50% redundant configuration (two PSW1250 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.

Output voltage: 28 Vdc
24 Vdc
21 Vdc

Valid for Input Voltage range 100 to 264 Vac

Technical Data

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 4mm^2 wires.
Isolation:
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 100A available on rear 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 30 Vdc.
Power good signaling:
Output good: 19.5 V ≤ Vout ≤ 29.5 V.
Signaling: voltage free SPST normally energized relay (contact closed), de-energize in over/under voltage conditions (contact open).
Contact Rating: 3 A 100 Vac 300 VA, 3 A 100 Vdc 90 W (resistive load).
Connection: screw terminal blocks suitable for 2.5 mm^2 wires.
Compatibility:
CE mark compliant, conforms to Directive: 2014/34/EU ATEX, 2014/30/EU EMC, 2014/35/EU 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 Power Output vs. Ambient Operating Temperature diagram).
Relative humidity limits: 95 %, up to 55 °C.
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,
TÜV Certificate No. C-IS-236198-04 SIL 2 / SIL 3 conform 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: Wall Mounting.
Weight: about 3.5 Kg.
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 13.

Features

- SIL 3 for NE Load according IEC 61508:2010, with single PSW1250 module or more PSW1250 modules in redundant configuration (see pages 5-8 for more information).
- SIL 1 for ND Load according to IEC 61508:2010, with single PSW1250 module (see page 9 for more information).
- SIL 2 for ND Load according IEC 61508:2010, with more PSW1250 modules in redundant configuration (see pages 10-12 for more information).
- Systematic capability SIL 3.
- Power factor correction.
- Installation in Zone 2 / Div.2 hazardous locations.
- EMC Compatibility to EN61000-6-2, EN61000-6-4.
- ATEX, IECEx Certifications.
- TÜV Certification.
- TÜV Functional Safety Certification.
- Type Approval Certificate DNV for marine applications (pending).
- Highly regulated output of 24 Vdc, 50 A, for PSW1250 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.
- Tropicalization for electronic components.

Ordering Information

Model:	PSW1250

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 the 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 0.5µs, thus minimizing disturbance and oscillations to the output bus.
Using Oring diodes, to parallel two, or more, 24VDC 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 two 50 A paralleled modules are used for full 50 + 50 A redundancy, a total power of about **80 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 PSW1250 Power Supply System, the use of *active ideal diodes*.
The MOSFETs resistance for *active ideal diodes* is about 1.2 mΩ resulting in 3.6 W dissipation for each power module. Then, if two 50 A paralleled modules are used for full 50 + 50 Amp redundancy, a total power of about **7.2 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

The output voltage can be set to 24 Vdc + 18%; -14% via a front panel trimmer.
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 that 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 (in normal condition contact is closed), positioned on back board “Fault” terminal block. Faults can be:

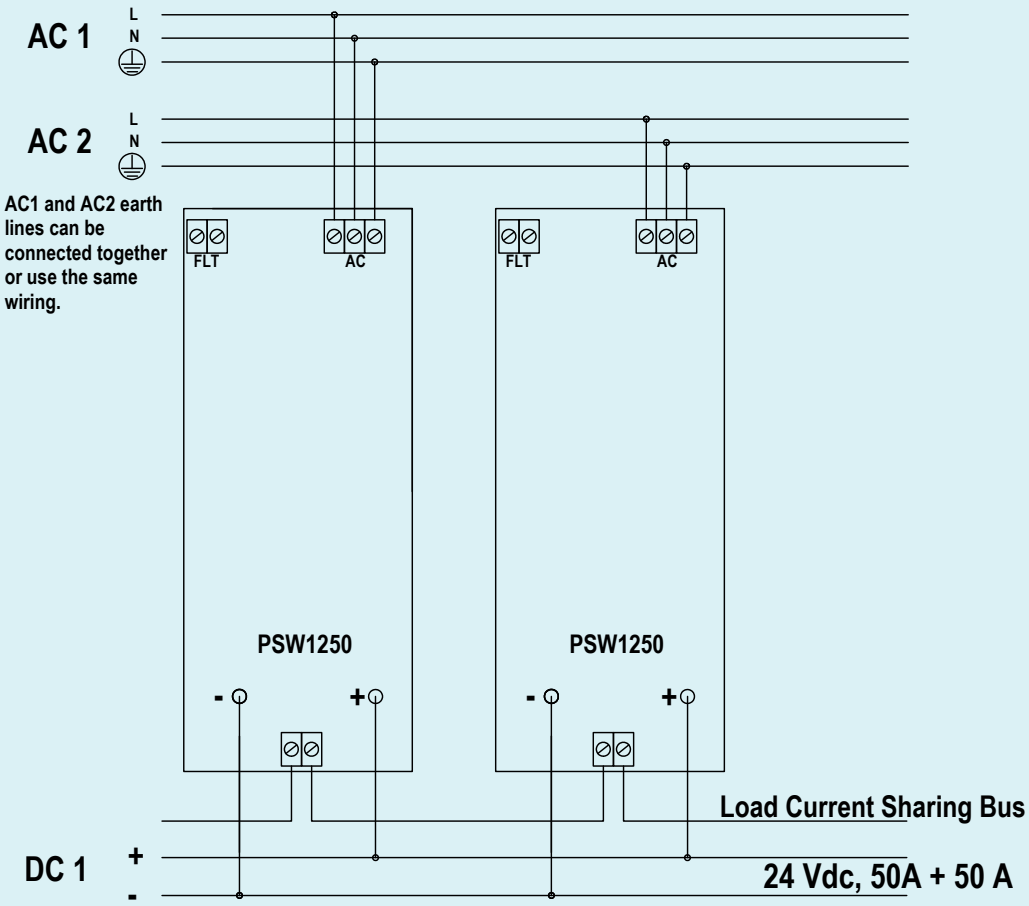
- Under voltage Vout < 19.5 V.
- Over voltage Vout > 29.5 V.

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 values lower than 20 V.
If output voltage goes over 29.5 V, the green Power ON LED is OFF and remains steady for values 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.

Function Diagram Dual AC Supply wiring architecture for PSW1250:

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

PSW1250, dual AC supply, 1 redundant 50 A Output.
two modules connected in parallel to provide full redundancy on AC lines (AC1 and AC2) and one 50 A redundant output.



Warning

PSW1250 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°C ≤ Tamb ≤ +70°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.
PSW1250 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.
PSW1250 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.

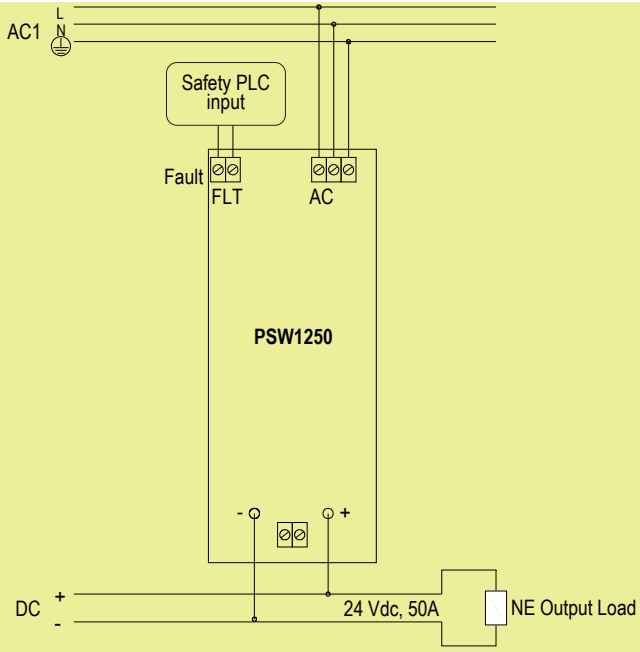
Storage

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 °C, the -45 to +80 °C is meant for limited periods, -10 to +30 °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.

A) Application of single PSW1250 module, for NE output load



Description:

In normal operation the PSW1250 module is powered by connecting AC input supply to related terminal blocks (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 PSW1250 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 PSW1250 is lit in presence of AC input supply. In this condition the NE output load (connected to related output copper bars with screw terminals) is Normally Energized (NE).

In absence of AC input supply, the PSW1250 module is shutdown (its fault relay contact is open) and output load is de-energized (Safe State).

Safety Function and Failure behavior:

Single PSW1250 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 PSW1250 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 PSW1250 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 ≥ 30 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.

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 / $\lambda_{tot\ safe}$) + 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 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**40 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**5.449E-05**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	1635.27 FIT	42.51 FIT	12.34 FIT	99.27%	0.00%	77.50%

PFDavg vs T[Proof] table (assuming Proof Test coverage of 90%), with determination of SIL supposing module contributes ≤10% of total SIF dangerous failures:

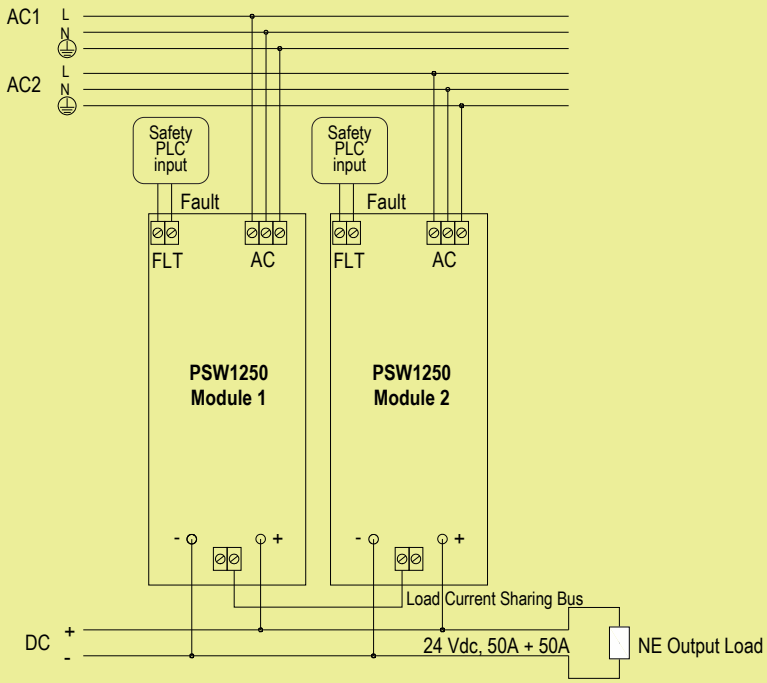
T[Proof] = 1.5 years	T[Proof] = 18 years
PFDavg = 8.17E-05 Valid for **SIL 3**	PFDavg = 9.81E-04 Valid for **SIL 2**

PFDavg vs T[Proof] table (assuming Proof Test coverage of 90%), with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

T[Proof] = 10 years	T[Proof] = 20 years
PFDavg = 5.45E-04 Valid for **SIL 3**	PFDavg = 1.09E-03 Valid for **SIL 2**

Systematic capability SIL 3.

B) Application of two paralleled PSW1250 modules, for NE output load



Description: In normal operation two paralleled PSW1250 modules are powered by connecting AC1 input supply to one module and AC2 input supply to other one by means of related terminal blocks (see previous functional diagram for more information). For each PSW1250 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 PSW1250 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 PSW1250 is lit in presence of AC input supply.
The outputs of two PSW1250 modules must be paralleled by external wiring. For current sharing operation, two PSW1250 modules must have their current sharing bus terminal blocks connected together by external wiring.The NE output load is connected to paralleled outputs of both PSW1250 modules (by related output copper bars with screw terminals). In normal condition, NE output load is Normally Energized (NE). In absence of one only AC input supply (AC1 or AC2), one PSW1250 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 PSW1250 modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State).

Safety Function and Failure behavior: Two paralleled PSW1250 modules are 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 PSW1250 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 PSW1250 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 ≥ 30 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.

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) = λdu * (0.5*8760 + 8)h + λdd * 8h	**1.246E-05**

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

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

PFDavg vs T[Proof] table (assuming Proof Test coverage of 90%), with determination of SIL supposing module contributes ≤10% of total SIF dangerous failures:

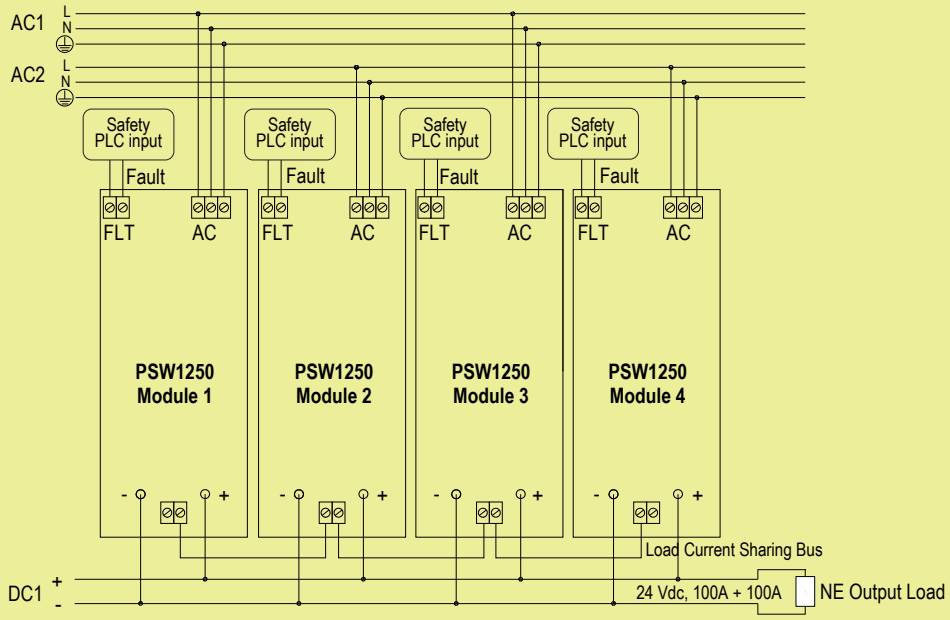
T[Proof] = 8 years
PFDavg = 9.97E-05 Valid for **SIL 3**

PFDavg vs T[Proof] table (assuming Proof Test coverage of 90%), with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

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

Systematic capability SIL 3.

C) Application of four paralleled PSW1250 modules, for NE output load



Description: In normal operation four paralleled PSW1250 modules are powered by connecting AC1 input supply to two modules and AC2 input supply to other ones by means of related terminal blocks (see previous functional diagram for more information). For each PSW1250 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 PSW1250 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 PSW1250 is lit in presence of AC input supply.
The outputs of four PSW1250 modules must be paralleled by external wiring. For current sharing operation, four PSW1250 modules must have their current sharing bus terminal blocks connected together by external wiring. The NE output load is connected to paralleled outputs of four PSW1250 modules (by related output copper bars with screw terminals). In normal condition, NE output load is Normally Energized (NE). In absence of one only AC input supply (AC1 or AC2), two PSW1250 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 PSW1250 modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State).

Safety Function and Failure behavior:

Four paralleled PSW1250 modules are 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 PSW1250 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 PSW1250 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 ≥ 30 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.

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) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.241E-05**

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

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

PFDavg vs T[Proof] table (assuming Proof Test coverage of 90%), with determination of SIL supposing module contributes ≤10% of total SIF dangerous failures:

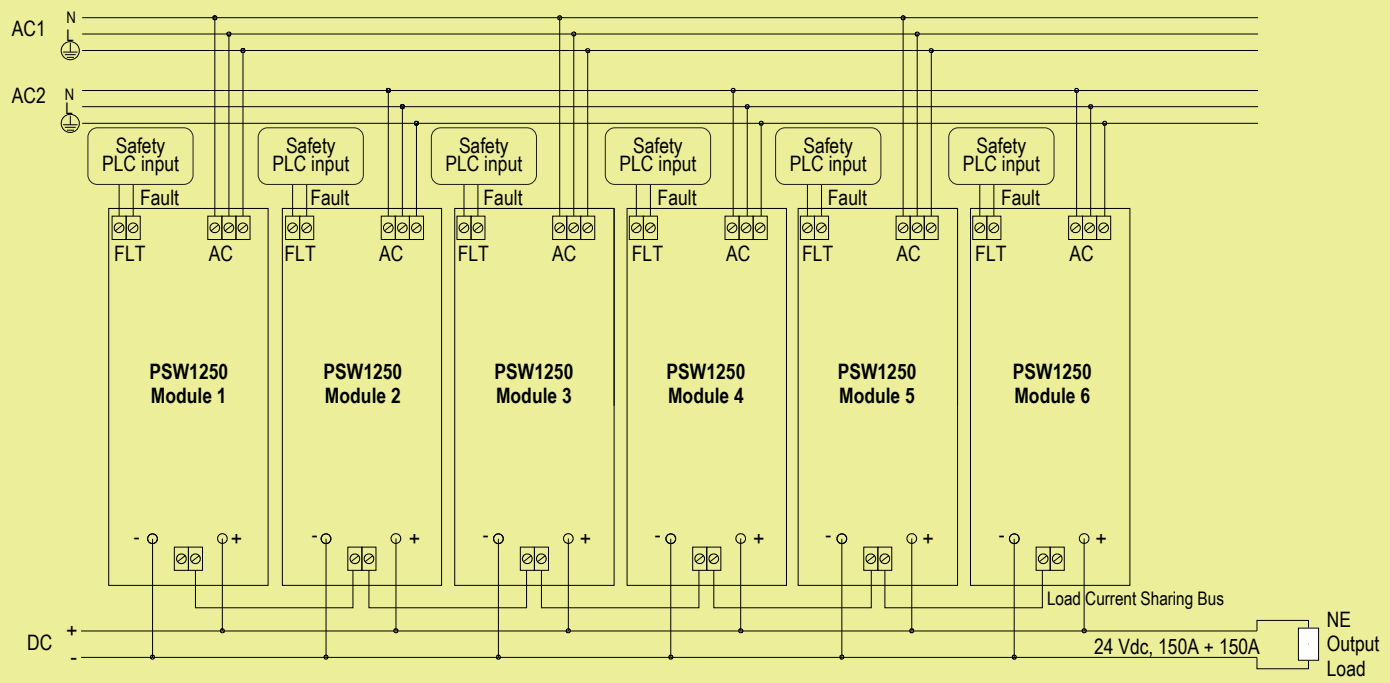
T[Proof] = 4 years
PFDavg = 8.96E-05 Valid for **SIL 3**

PFDavg vs T[Proof] table (assuming Proof Test coverage of 90%), with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

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

Systematic capability SIL 3.

D) Application of six paralleled PSW1250 modules, for NE output load



Description: In normal operation six paralleled PSW1250 modules are powered by connecting AC1 input supply to three modules and AC2 input supply to other ones by means of related terminal blocks (see previous functional diagram for more information). For each PSW1250 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 PSW1250 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 PSW1250 is lit in presence of AC input supply.
The outputs of six PSW1250 modules must be paralleled by external wiring. For current sharing operation, six PSW1250 modules must have their current sharing bus terminal blocks connected together by external wiring. The NE output load is connected to paralleled outputs of six PSW1250 modules (by related output copper bars with screw terminals). In normal condition, NE output load is Normally Energized (NE). In absence of one only AC input supply (AC1 or AC2), three PSW1250 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 PSW1250 modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State).

Safety Function and Failure behavior: Six paralleled PSW1250 modules are 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 PSW1250 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 PSW1250 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 ≥ 30 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.

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) = λ_{dd} + λ_{du} + λ_{sd} + λ_{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) = λdu * (0.5*8760 + 8)h + λdd * 8h	**3.24E-05**

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

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

PFDavg vs T[Proof] table (assuming Proof Test coverage of 90%), with determination of SIL supposing module contributes ≤10% of total SIF dangerous failures:

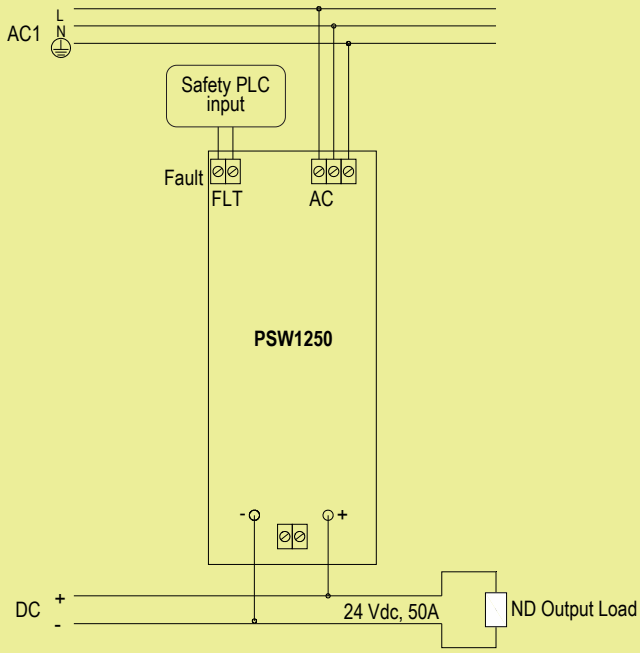
T[Proof] = 3 years	T[Proof] = 20 years
PFDavg = 9.72E-05 Valid for **SIL 3**	PFDavg = 6.48E-04 Valid for **SIL 2**

PFDavg vs T[Proof] table (assuming Proof Test coverage of 90%), with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

T[Proof] = 15 years
PFDavg = 4.86E-04 Valid for **SIL 3**

Systematic capability SIL 3.

E) Application of single PSW1250 module, for ND output load



Description:

In normal operation the PSW1250 module is unpowered because of absence of AC input supply, which is connected to related terminal blocks (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 PSW1250 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 PSW1250 is turned off, fault relay contact is open and the ND output load (connected to related output copper bars with screw terminals) is Normally De-energized (ND).

In presence of AC input supply, the green Power ON LED of PSW1250 is lit, fault relay contact is closed (if fault is absent) and output load is energized (Safe State).

Safety Function and Failure behavior:

Single PSW1250 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 PSW1250 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 ≥ 30 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 PSW1250 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 PSW1250 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.

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) = λdu * (0.5*8760 + 8)h + λdd * 8h	**7.42E-03**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	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 total SIF dangerous failures:

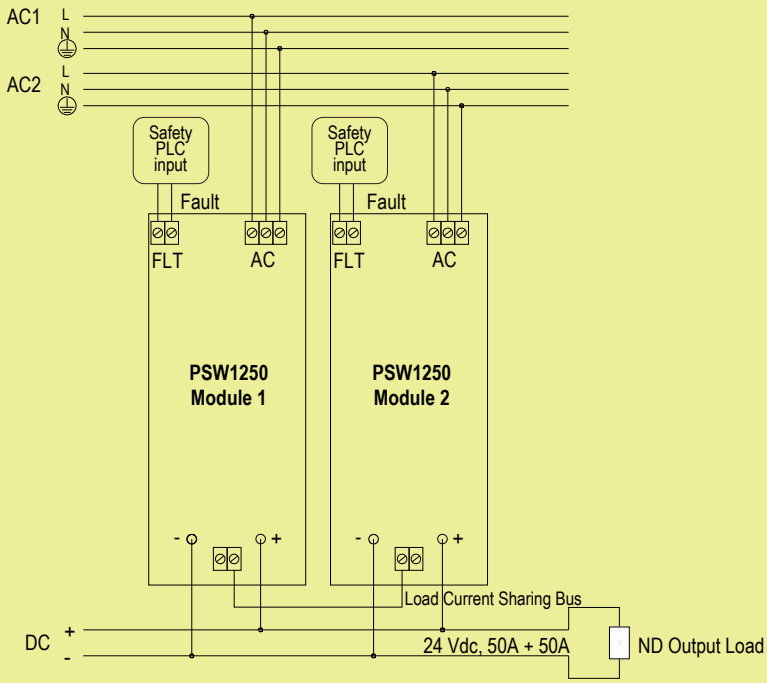
T[Proof] = 1 year
PFDavg = 7.42E-03 Valid for **SIL 1**

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

T[Proof] = 5 years
PFDavg = 3.71E-02 Valid for **SIL 1**

Systematic capability SIL 3.

F) Application of two paralleled PSW1250 modules, for ND output load



Description:

In normal operation two paralleled PSW1250 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 (see previous functional diagram for more information). For each PSW1250 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 PSW1250 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 PSW1250 modules must be paralleled by external wiring. For current sharing operation, two PSW1250 modules must have their current sharing bus terminal blocks connected together by external wiring.The ND output load is connected to paralleled outputs of both PSW1250 modules (by related output copper bars with screw terminals). In normal condition, absence of both AC input supplies (AC1 and AC2) implies that both green Power ON LEDs of PSW1250 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 PSW1250 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 PSW1250 modules are correctly turned on and output load is energized (Safe State).

Safety Function and Failure behavior:

Two paralleled PSW1250 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 PSW1250 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 PSW1250 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 ≥ 30 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 PSW1250 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.

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) = λdu * (0.5*8760 + 8)h + λdd * 8h	**3.80E-04**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	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 total SIF dangerous failures:

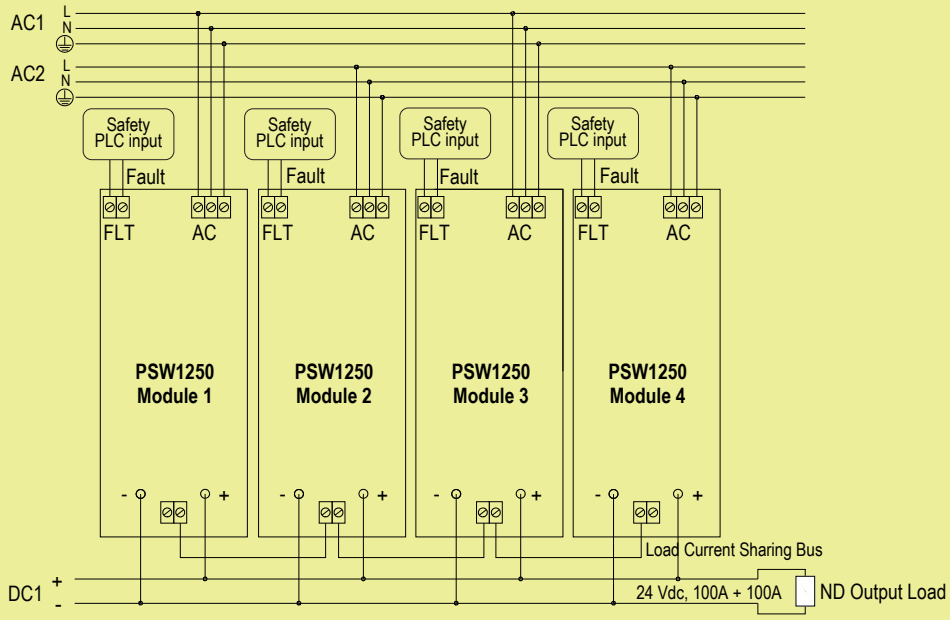
T[Proof] = 2 years	T[Proof] = 20 years
PFDavg = 7.60E-04 Valid for **SIL 2**	PFDavg = 7.60E-03 Valid for **SIL 1**

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

T[Proof] = 10 years
PFDavg = 3.80E-03 Valid for **SIL 2**

Systematic capability SIL 3.

G) Application of four paralleled PSW1250 modules, for ND output load



Description:

In normal operation four paralleled PSW1250 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 (see previous functional diagram for more information). For each PSW1250 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 PSW1250 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 PSW1250 modules must be paralleled by external wiring. For current sharing operation, four PSW1250 modules must have their current sharing bus terminal blocks connected together by external wiring. The ND output load is connected to paralleled outputs of four PSW1250 modules (by related output copper bars with screw terminals). In normal condition, absence of both AC input supplies (AC1 and AC2) implies that four green Power ON LEDs of PSW1250 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 PSW1250 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 PSW1250 modules are correctly turned on and output load is energized (Safe State).

Safety Function and Failure behavior:

Four paralleled PSW1250 modules are 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 PSW1250 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 PSW1250 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 ≥ 30 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 PSW1250 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.

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) = λdu * (0.5*8760 + 8)h + λdd * 8h	**3.90E-04**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	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 total SIF dangerous failures:

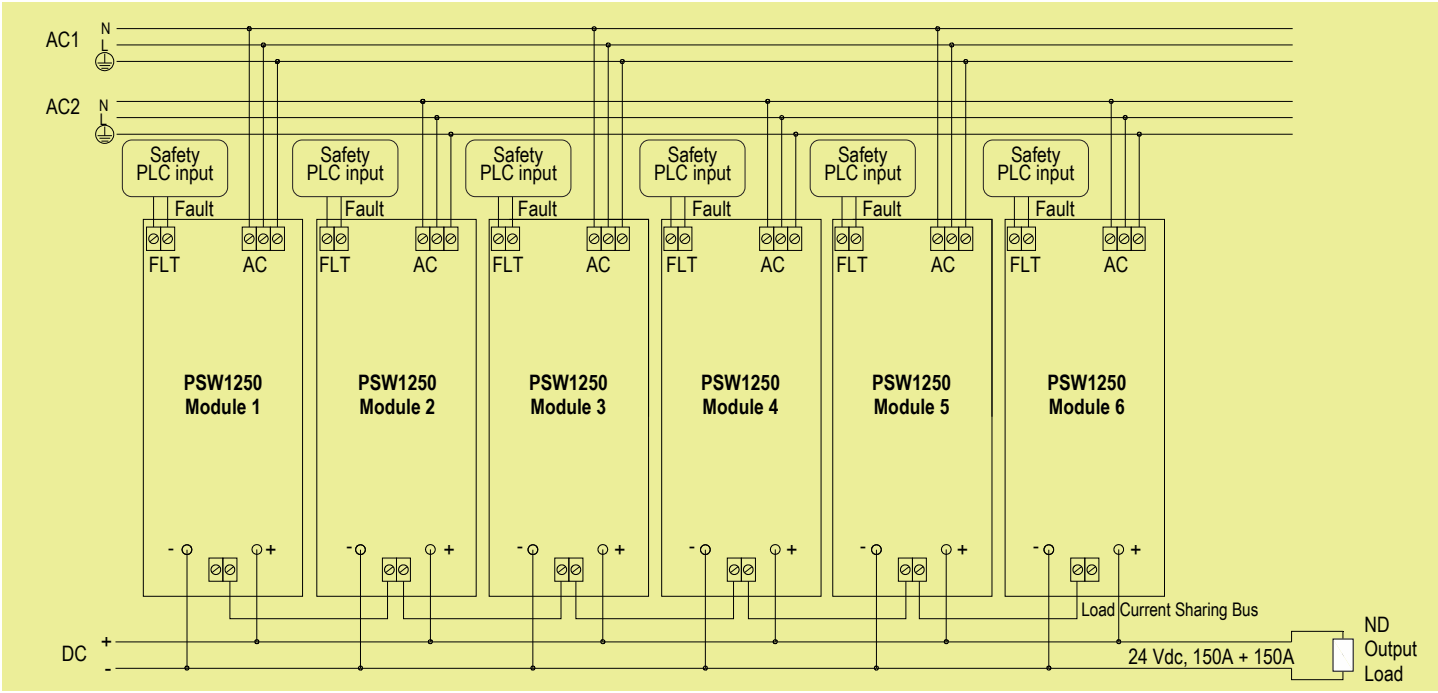
T[Proof] = 2 years	T[Proof] = 20 years
PFDavg = 7.80E-04 Valid for **SIL 2**	PFDavg = 7.80E-03 Valid for **SIL 1**

PFDavg vs T[Proof] table, with determination of SIL supposing module contributes >10% of total SIF dangerous failures:

T[Proof] = 10 years
PFDavg = 3.90E-03 Valid for **SIL 2**

Systematic capability SIL 3.

H) Application of six paralleled PSW1250 modules, for ND output load



Description:

In normal operation six paralleled PSW1250 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 (see previous functional diagram for more information). For each PSW1250 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 PSW1250 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 PSW1250 modules must be paralleled by external wiring. For current sharing operation, six PSW1250 modules must have their current sharing bus terminal blocks connected together by external wiring. The ND output load is connected to paralleled outputs of six PSW1250 modules (by related output copper bars with screw terminals). In normal condition, absence of both AC input supplies (AC1 and AC2) implies that six green Power ON LEDs of PSW1250 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 PSW1250 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 PSW1250 modules are correctly turned on and output load is energized (Safe State).

Safety Function and Failure behavior:

Six paralleled PSW1250 modules are 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 PSW1250 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 PSW1250 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 ≥ 30 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 PSW1250 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.

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) = λdu * (0.5*8760 + 8)h + λdd * 8h	**4.00E-04**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	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 total SIF dangerous failures:

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 >10% of total SIF dangerous failures:

T[Proof] = 10 years
PFDavg = 4.00E-03 Valid for **SIL 2**

Systematic capability SIL 3.

Testing procedure at T-proof

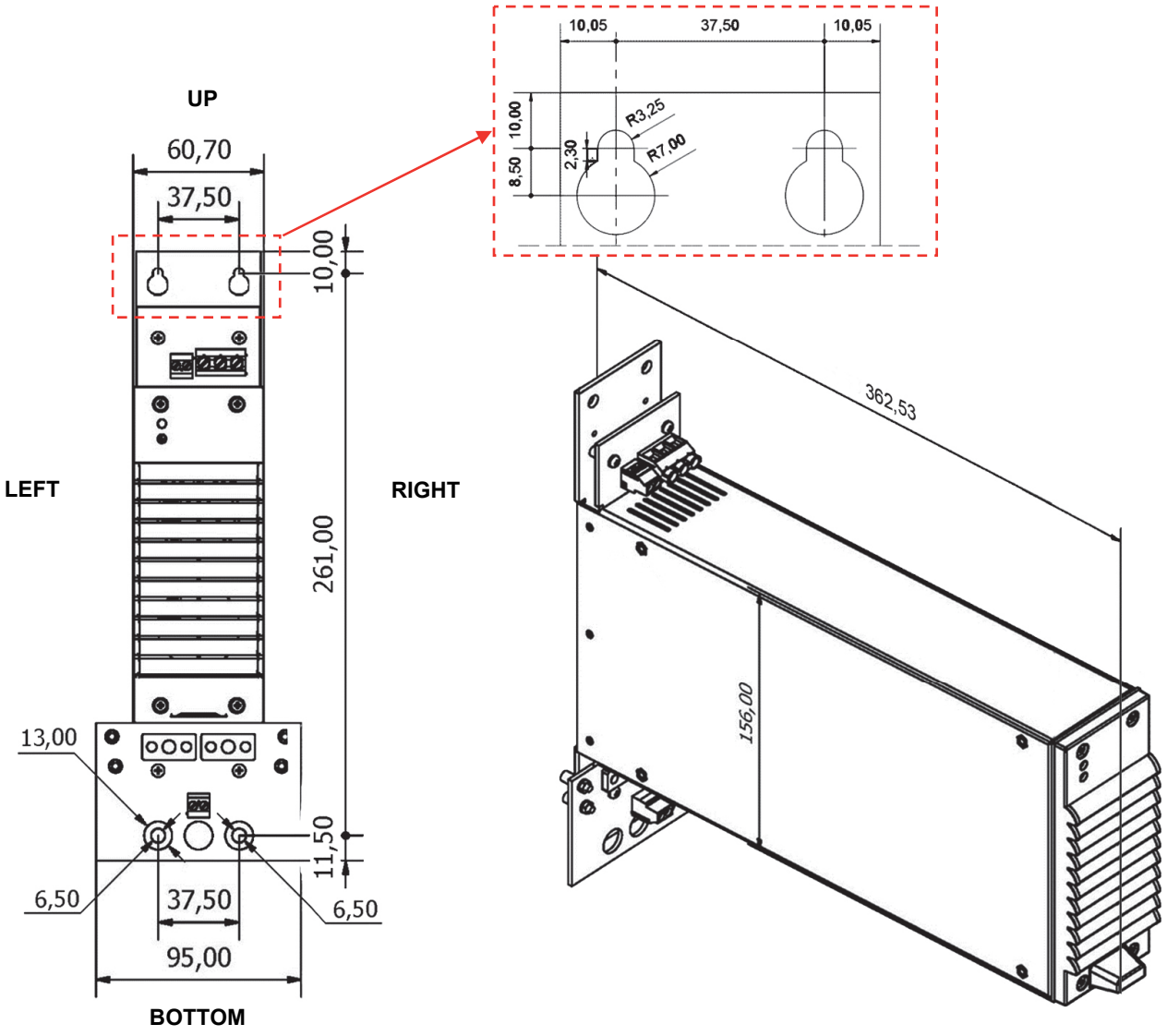
According to IEC 61508-2, the proof test will be performed to reveal dangerous faults which cannot be otherwise detected. This means that it is necessary to specify how dangerous undetected faults, which have been noted during the FMEDA analysis, can be revealed during the proof test.
For **Functional Safety applications with two or more paralleled power supply modules in redundant configuration for NE output load**, the following **Proof Test** must be executed **for each PSW1250** composing the Functional Safety used application. It consists of the following steps:

Steps	Action
1	In order to control correct operating of the fault contact (FLT), necessary to give information about dangerous failures, take appropriate action on the safety-related PLC to acquire presence of fault but to not take any action because fault condition is intentionally provoked .
2	Shutdown the tested power supply module by unpowering AC lines of PSW1250. This action does not affect output load operating, which holds normally energized because of fully redundant configuration on input (two independent AC lines) and output (paralleling connection implies high availability) of the Functional Safety application. The power supply module turn off time lasts some seconds (typically 5 to 10 sec). During this time, the power supply module output voltage goes below 19.5 Vdc (undervoltage UV condition), therefore the fault relay contact must be open and the green Power ON LED must blink. The safety-related PLC must acquire presence of fault, which proves that power supply internal diagnostic operates correctly. If the safety-related PLC does not acquire any fault, this means that fault relay contact is blocked in closed position (for welding) or power supply internal diagnostic is wrongly operating. Therefore this power supply module must be replaced with new one.
3	Turn on the tested power supply module by powering AC lines of PSW1250. After about 3 seconds the power supply module operates correctly in current sharing mode with other paralleled power supply modules.
4	Restore normal operation of the safety-related PLC, so that it can take any action if fault is acquired.
5	Unplug two M6 nylon-capped lock nuts, to unfix IP20 polycarbonate cover from the DC (+ / -) couple screw output terminals of the tested power supply module.
6	Use an AC true rms voltmeter and connect its probes to DC (+ / -) couple screw output terminals in order to measure AC rms voltage. In normal operation conditions, the output supply voltage should have no AC component, that is its rms value should be ideally null. But little ripple is allowed, therefore this value must be less than 100 mVrms. If higher rms value (as some volts) is measured, a dangerous failure which has produced an oscillation of the output voltage regulator is detected. Therefore this power supply module must be replaced with new one.
7	Plug two M6 nylon-capped lock nuts, to fix IP20 polycarbonate cover on the DC (+ / -) couple screw output terminals of the tested power supply module.

This test reveals 90% of all possible Dangerous Undetected failures in the PSW1250 power supply module, when the output load is NE type.

Installation procedure - 1st step: Installation of PSW1250 on wall

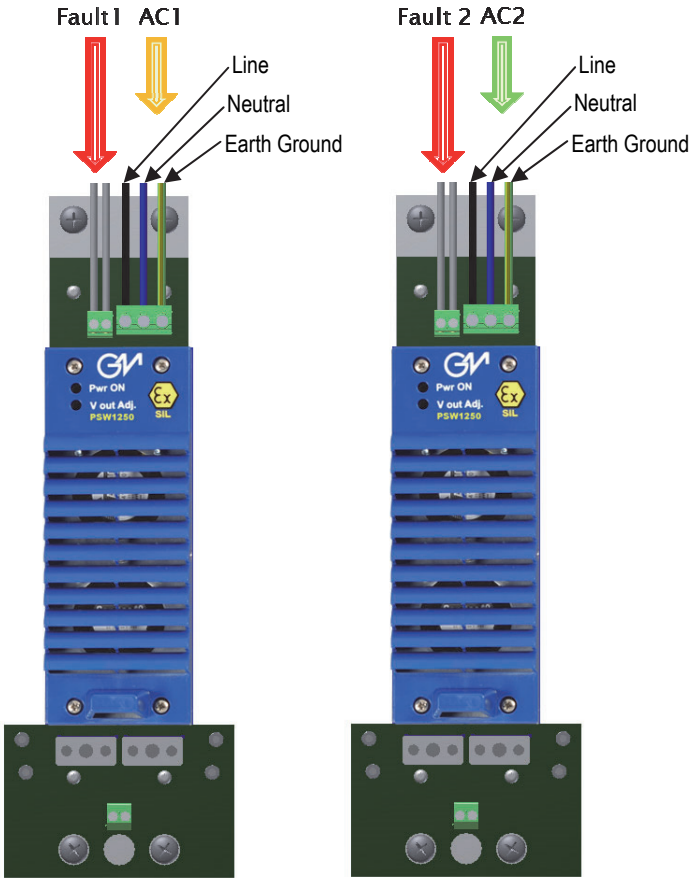
Fix the PSW1250 to a vertical wall by means of four screws through four 6.50 mm diameter holes, shown in the following drawing with overall dimensions (mm).
In the position of two bottom screws there are two holes in the PCB with 13.00 mm diameter to allow crossing of screw head during screw installation.
The PSW1250 must only be installed as oriented in the following drawing.



Installation procedure - 2nd step: Wiring of top terminal blocks (AC input lines and fault)

The following image shows the wiring of top terminal blocks for a single PSW1250, not used in parallel/redundant configuration.
For AC input terminal blocks, use a typical cable section of AWG12 (maximum AWG11 or 4 mm^2).
For fault contact output terminal blocks, use a typical cable section of AWG16 (maximum AWG14 or 2.5 mm^2).

The following image shows the wiring of top terminal blocks for two PSW1250 modules, used in parallel/redundant configuration.
When two or more (maximum 6 pieces) PSW1250 modules are in parallel/redundant configuration, it's necessary 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 full redundance configuration from the input to the output of the whole power system.
Connect AC1 input power line to the input terminal blocks of the 1st power module while connect AC2 input power line to the input terminal blocks of the 2nd power module.
At page 4, it's shown a functional diagram of two PSW1250 modules, used in parallel/redundant configuration.
For AC input terminal blocks, use a typical cable section of AWG12 (maximum AWG11 or 4 mm^2).
For fault contact output terminal blocks, use a typical cable section of AWG16 (maximum AWG14 or 2.5 mm^2).



Installation procedure - 3rd step (only for PSW1250 not used in parallel/redundant configuration):
Wiring of bottom screw output terminals on copper bars (DC output lines) and start up of PSW1250

See Fig. 1-2-3-4-5 for wiring bottom screw output terminals on copper bars (DC output lines): DC- is negative out pole, DC+ is positive out pole.
For DC screw output terminals, use a typical cable section of AWG7 (maximum AWG5 or 16 mm²).

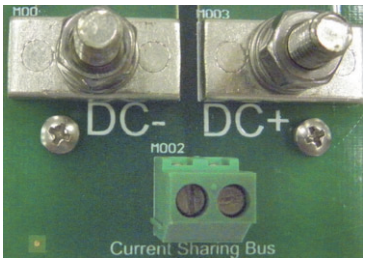


Fig. 1

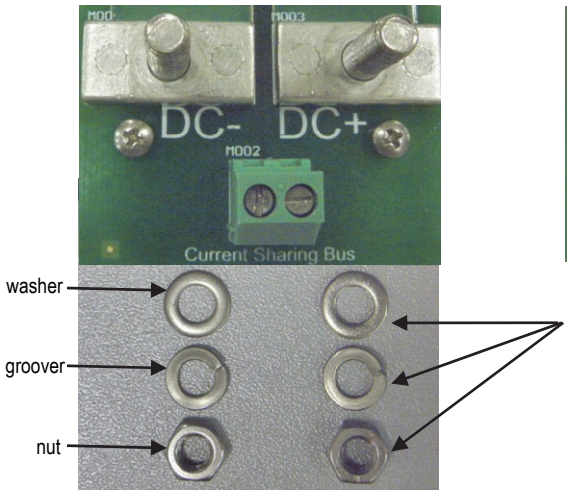


Fig. 2

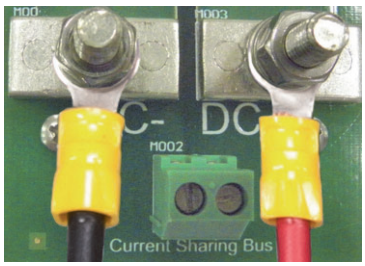


Fig. 3

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.

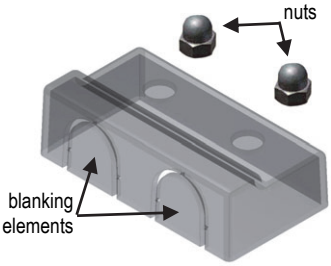


Fig. 4

For IP20 protection, a polycarbonate cover is used to protect each couple of screw output terminals. Break two preformed blanking elements to allow connection on screw output terminals with cable lugs just wired.
Then insert the cover on couple of screw output terminals and fix it by means of M6 nylon-capped lock nut.

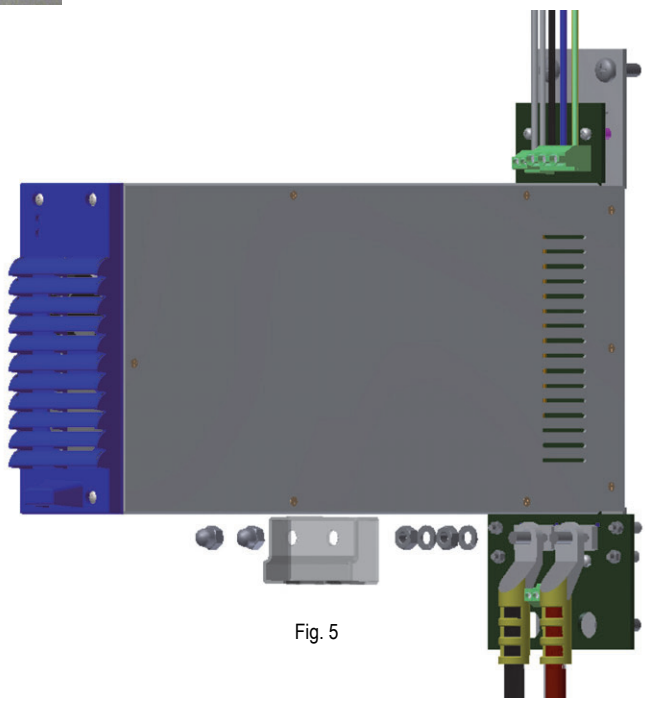
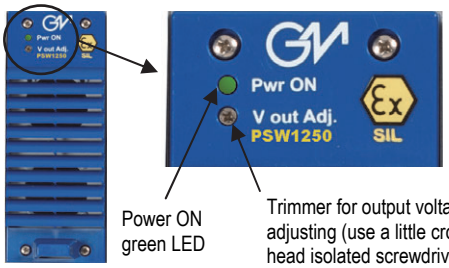
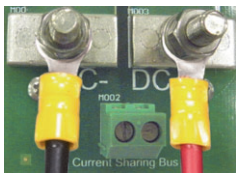


Fig. 5



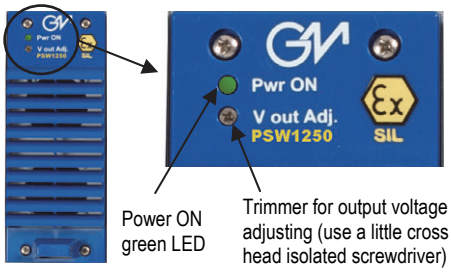
Start up: **power the AC line** to turn on PSW1250 module: Power ON green LED, on front panel, is ON and 24 Vdc (factory setting) output voltage is present on screw output terminals DC- and DC+. See page 3 for more information about Power ON green LED signalling.
The output voltage can be measured on 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).



PSW1250 screw output terminals on copper bars:
DC- is negative out pole,
DC+ is positive out pole.

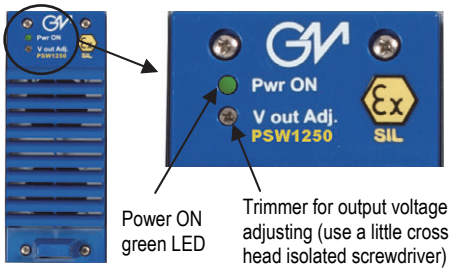
Installation procedure - 3rd step (only for PSW1250 used in parallel/redundant configuration): pre-start up of PSW1250

The following procedure is split in 2 sub-steps and it is the same for each PSW1250 used in paralle/redundant configuration. Starting from the 1st power supply module connected to AC1 power line and then go on with the 2nd power supply module connected to AC2 power line, it's possible to start up each PSW1250.



1st sub-step: **power AC1 line** to turn on the 1st PSW1250 module: Power ON green LED, on front panel, is ON and 24 Vdc (factory setting) output voltage is present on screw output terminals DC- and DC+. See page 3 for more information about Power ON green LED signalling.
The output voltage can be measured on 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, the power supply modules must have output voltages calibrated within ± 0.5 V.
Then, **unpower AC1 line**, turning off the 1st PSW1250 module.

PSW1250 screw output terminals on copper bars:
DC- is negative out pole,
DC+ is positive out pole.



2nd sub-step: **power AC2 line** to turn on the 2nd PSW1250 module: Power ON green LED, on front panel, is ON and 24 Vdc (factory setting) output voltage is present on screw output terminals DC- and DC+. See page 3 for more information about Power ON green LED signalling.
The output voltage can be measured on 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, the power supply modules must have output voltages calibrated within ± 0.5 V.
Then, **unpower AC2 line**, turning off the 2nd PSW1250 module.

PSW1250 screw output terminals on copper bars:
DC- is negative out pole,
DC+ is positive out pole.

Installation procedure - 4th step (only for PSW1250 used in parallel/redundant configuration): Wiring of bottom screw output terminals on copper bars (DC output lines) and current sharing bus, in order to start up of whole power system

AC1 and AC2 input power lines are unpowered.
For each PSW1250 module of whole power system, see Fig. 1-2-3-4-5 for wiring bottom screw output terminals on copper bars (DC output lines): DC- is negative out pole, DC+ is positive out pole.
For DC screw output terminals, use a typical cable section of AWG7 (maximum AWG5 or 16 mm^2).
For current sharing operation, all PSW1250 modules used in parallel/redundant configuration must have their current sharing bus terminal blocks connected together by wiring.
For current sharing bus terminal block, use a typical cable section of AWG16 (maximum AWG14 or 2.5 mm^2).
At page 4, it's shown a functional diagram of two PSW1250 modules, used in parallel/redundant configuration.

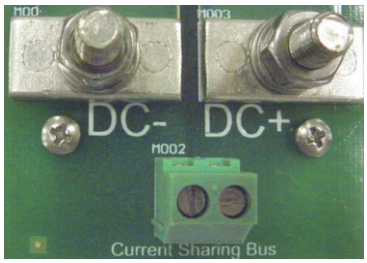
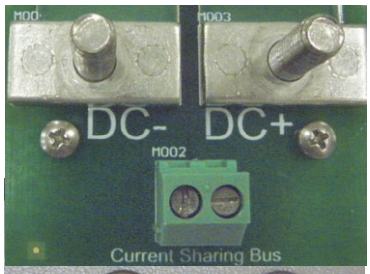


Fig. 1



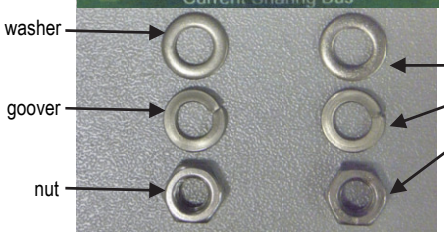


Fig. 2

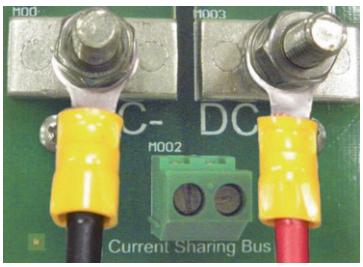


Fig. 3

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.

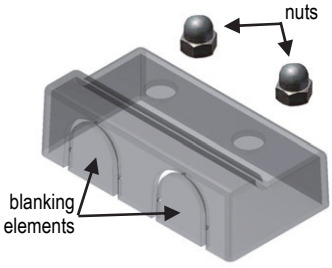


Fig. 4

For IP20 protection, a polycarbonate cover is used to protect each couple of screw output terminals. Break two preformed blanking elements to allow connection on screw output terminals with cable lugs just wired.
Then insert the cover on couple of screw output terminals and fix it by means of M6 nylon-capped lock nut.

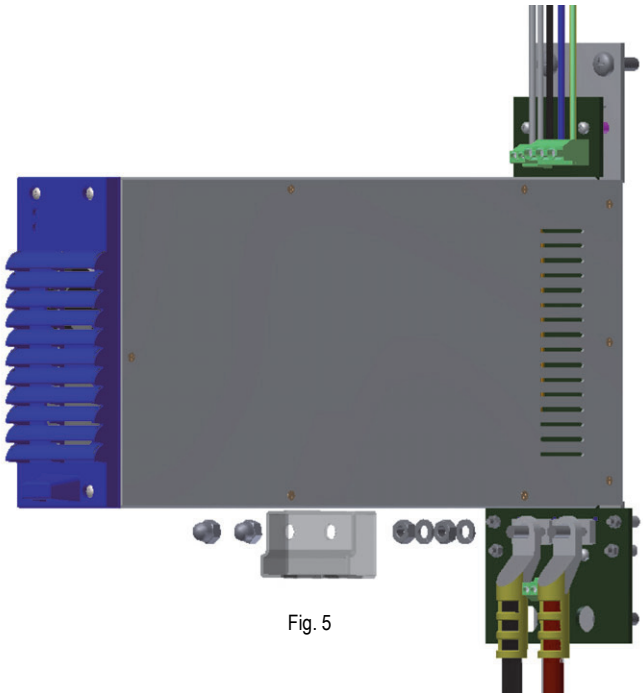


Fig. 5

After wiring of the DC output lines and current sharing bus, **power AC1 and AC2 input power lines**. Therefore, each PSW1250 turns on and the whole power system can drive the loads connected to the DC output lines.