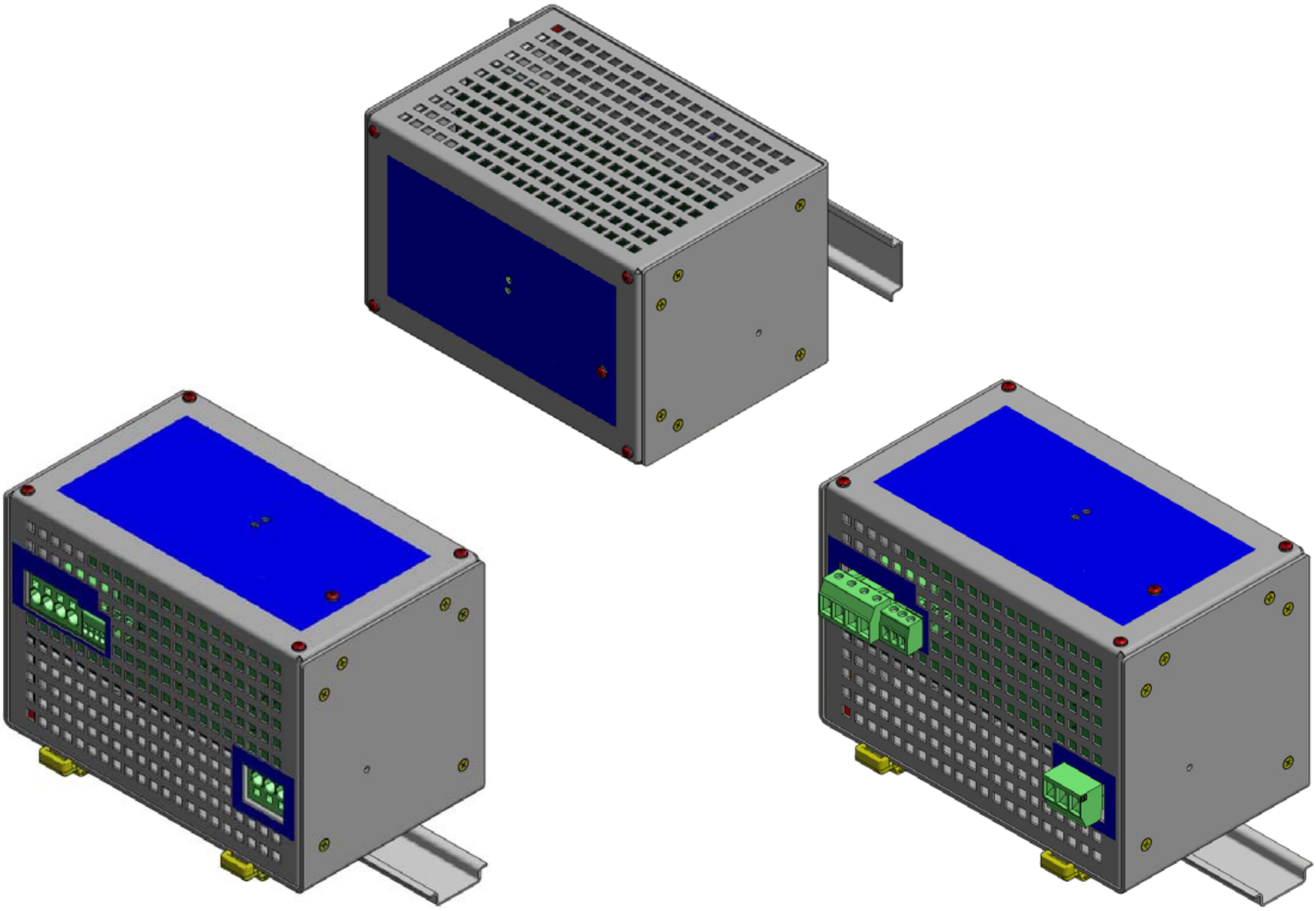


SAFETY MANUAL

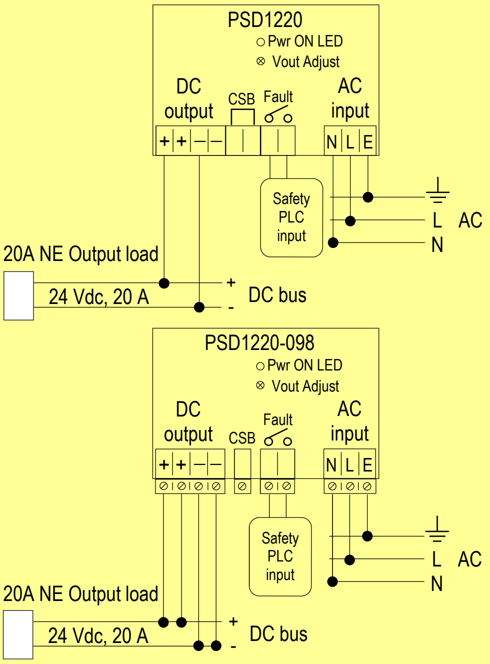
SIL 3 Power Supply PSD1220 and PSD1220-098 24Vdc, 20 A, Zone 2

DIN Rail Mounting

Reference must be made to the relevant sections within the instruction manual ISM0370, which contain basic guides for the installation of the equipment.

gmi
technology for safety

A) Application of single PSD1220 or PSD1220-098 module, for NE output load



Description: in normal operation, the PSD1220 or PSD1220-098 module is powered by connecting AC input supply to related terminal block, so that its green Power ON LED is lit and NE output load (connected to related output terminal block) is Normally Energized (NE) (see functional diagram in the instruction manual ISM0370 for more information). The fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify under/over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open. In absence of AC input supply, the module is shutdown (its fault relay contact is open) and output load is de-energized (Safe State).

Safety Function and Failure behavior:

Single PSD1220 or PSD1220-098 module is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behavior of PSD1220 or PSD1220-098 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 failed power supply module and to replace it with new 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 22 Vdc or above 28 Vdc, and internal diagnostic cannot detect and notify faults to logic solver.

□ Fail High - Overvoltage: failure mode that causes the output to go above 28 Vdc. Internal overvoltage protection tries to limit output voltage < 28.5 Vdc, otherwise internal crowbars trip to fail safe state for output ≥ 29 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 22 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 22 and 28 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	57.99
λ_{du} = Total Dangerous Undetected failures	4.02
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	879.28
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**941.29**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**121 years**
$\lambda_{no\ effect}$ = “No Effect” failures	763.23
$\lambda_{not\ part}$ = “Not Part” failures	9.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**1713.52**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**66 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**1.81E-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	879.28 FIT	57.99 FIT	4.02 FIT	99.57%	0.00%	93.52%

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

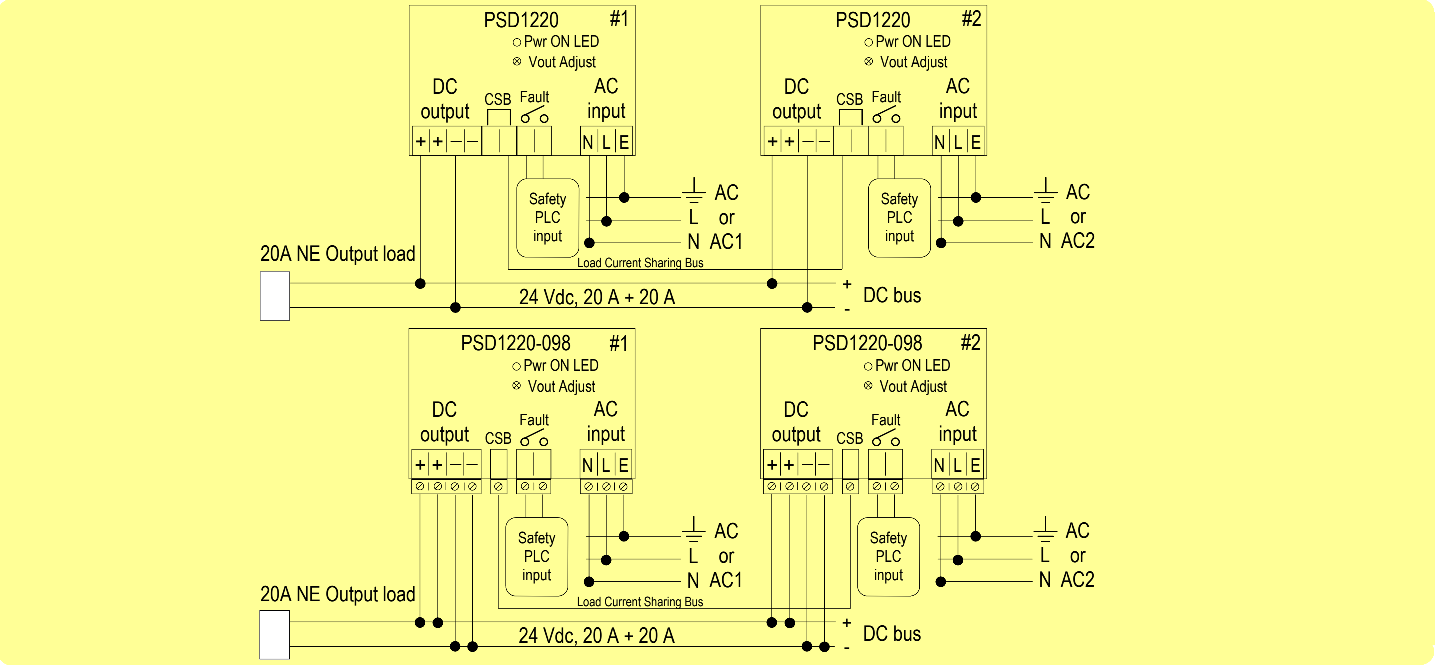
T[Proof] = 5 years	T[Proof] = 20 years
PFDavg = 9.05 E-05 - Valid for **SIL 3**	PFDavg = 3.62 E-04 - Valid for **SIL 2**

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 = 2.72 E-04 - Valid for **SIL 3**

Systematic capability SIL 3.

B) Application of two paralleled PSD1220 or PSD1220-098 modules, for NE output load and with single or double AC input supply



Description: in normal operation, two paralleled PSD1220 or PSD1220-098 modules are powered by connecting single AC or double AC1 / AC2 input supply to related terminal blocks so that their green Power ON LEDs are lit and NE output load (connected to external wiring paralleled outputs of both modules) is Normally Energized (NE). For load current sharing operation, both modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify under/over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open. In absence of AC input supply or both AC1 and AC2 input supplies, both paralleled modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State). With double AC1 / AC2 input supply, there is input redundancy because in absence of one only input supply (AC1 or AC2), one module is shutdown (its fault relay contact is open) but the other one operates in normal condition, so that output load is kept normally energized.

Safety Function and Failure behavior:

Two paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 1+1 on output (with single input supply) or 1+1 on output & input (with double input supply). The failure behavior of two paralleled modules for NE load is described as follows:

- □ Fail-Safe State: it is defined as the paralleled 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 malfunctioning power supply and to replace it with new 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 paralleled output voltage is blocked or oscillating between 2 and 22 Vdc or above 28 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 28 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 28.5 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 29 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 22 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 22 and 28 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	4.85
λ_{du} = Total Dangerous Undetected failures	2.05
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	43.96
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = λ_{dd} + λ_{du} + λ_{sd} + λ_{su}	**50.87**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**2244 years**
$\lambda_{no\ effect}$ = “No Effect” failures	3358.17
$\lambda_{not\ part}$ = “Not Part” failures	18.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{no\ effect}$ + $\lambda_{not\ part}$	**3427.04**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**33 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**9.05E-06**

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	43.96 FIT	4.85 FIT	2.05 FIT	95.96%	0.00%	70.25%

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

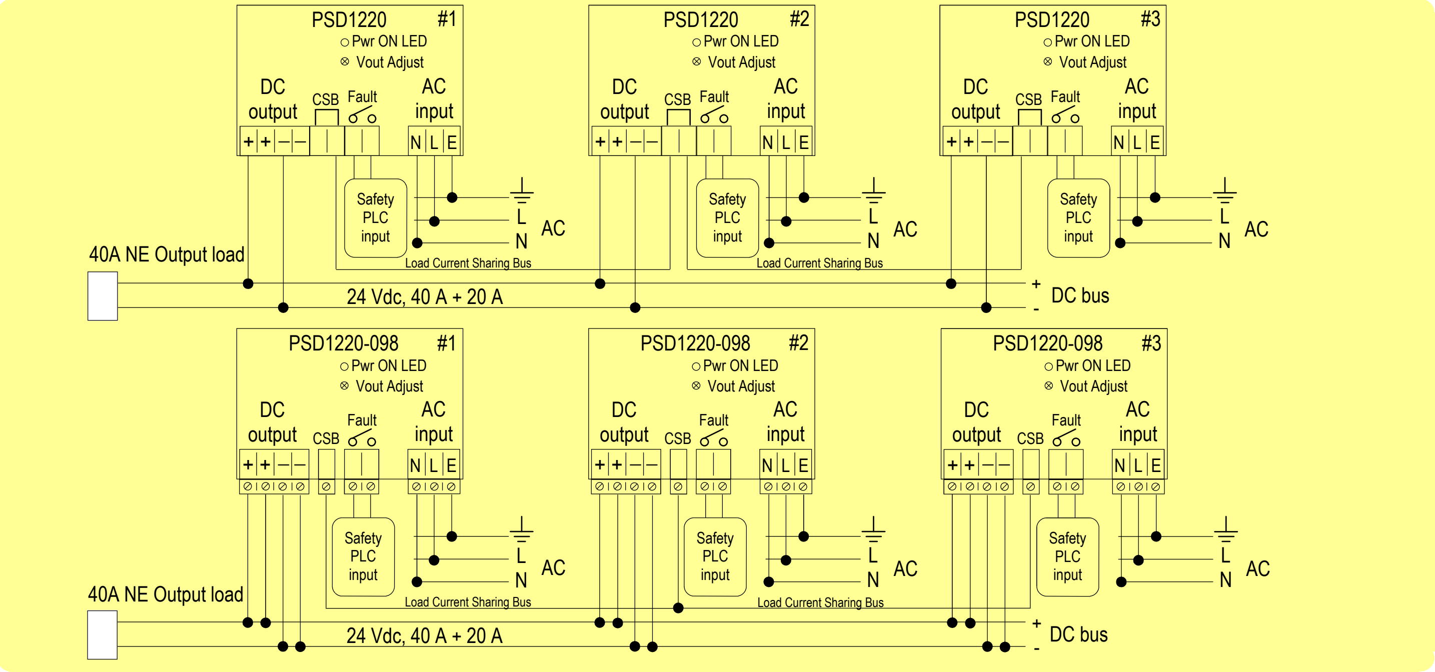
T[Proof] = 10 years	T[Proof] = 20 years
PFDavg = 9.05 E-05 - Valid for **SIL 3**	PFDavg = 1.81 E-04 - Valid for **SIL 2**

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] = 20 years
PFDavg = 1.81 E-04 - Valid for **SIL 3**

Systematic capability SIL 3.

C) Application of three paralleled PSD1220 or PSD1220-098 modules, for NE output load and with single AC input supply



Description: in normal operation, three paralleled PSD1220 or PSD1220-098 modules are powered by connecting AC input supply to related terminal blocks so that their green Power ON LEDs are lit and NE output load (connected to external wiring paralleled outputs of all modules) is Normally Energized (NE). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information).

For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify under/over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open. In absence of AC input supply, all paralleled modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State).

Safety Function and Failure behavior:

Three paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 2+1 on output. The failure behavior of three paralleled modules for NE load is described as follows:

- □ Fail-Safe State: it is defined as the paralleled outputs 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 malfunctioning power supply and to replace it with new 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 paralleled output voltage is blocked or oscillating between 2 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.
- □ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 28.5 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 29 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 22 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 22 and 28 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	3.00
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	43.96
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**52.82**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**2161 years**
$\lambda_{no\ effect}$ = “No Effect” failures	5060.74
$\lambda_{not\ part}$ = “Not Part” failures	27.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**5140.56**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**22 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**1.323E-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	43.96 FIT	5.85 FIT	3.00 FIT	94.31%	0.00%	66.07%

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

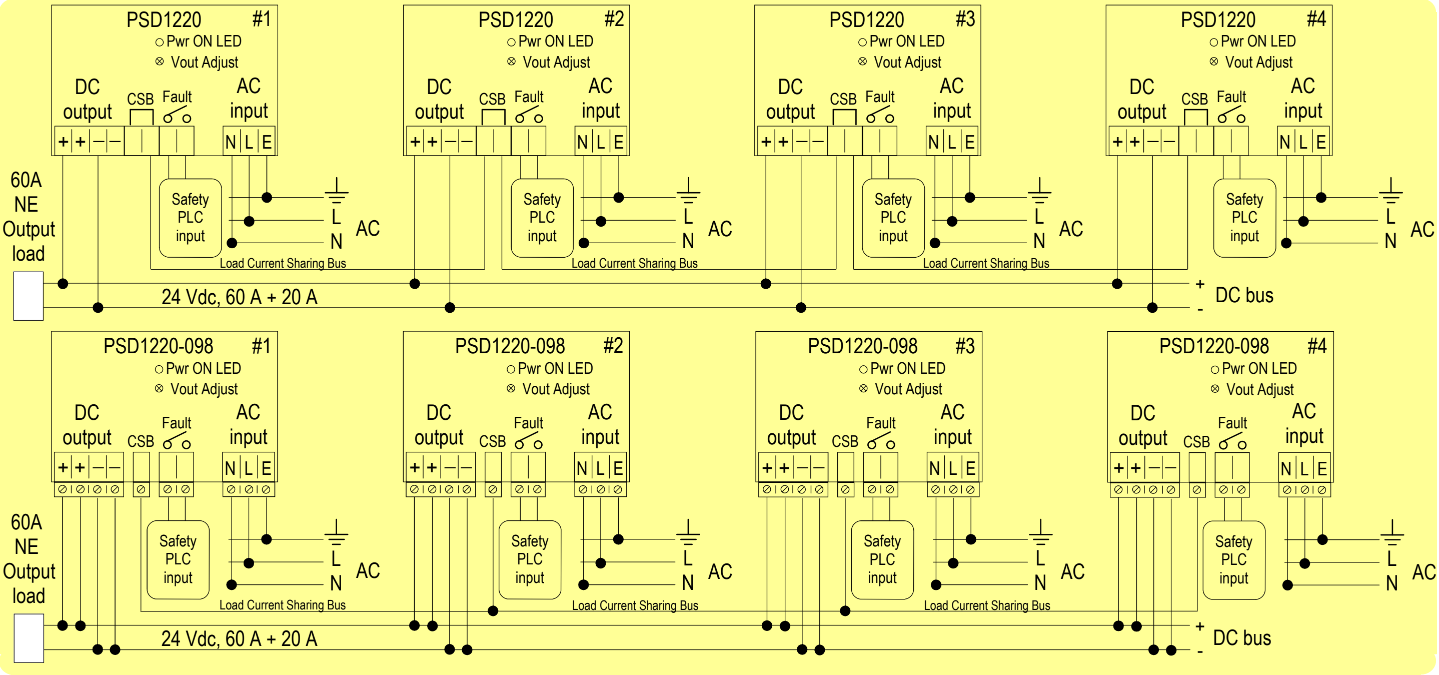
T[Proof] = 7 years	T[Proof] = 20 years
PFDavg = 9.26 E-05 - Valid for **SIL 3**	PFDavg = 2.65 E-04 - Valid for **SIL 2**

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] = 20 years
PFDavg = 2.65 E-04 - Valid for **SIL 3**

Systematic capability SIL 3.

D) Application of four paralleled PSD1220 or PSD1220-098 modules, for NE output load and with single AC input supply



Description: in normal operation, four paralleled PSD1220 or PSD1220-098 modules are powered by connecting AC input supply to related terminal blocks so that their green Power ON LEDs are lit and NE output load (connected to external wiring paralleled outputs of all modules) is Normally Energized (NE). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information).
For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify under/over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open. In absence of AC input supply, all paralleled modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State).

Safety Function and Failure behavior:

Four paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 3+1 on output. The failure behavior of four paralleled modules for NE load is described as follows:

- □ Fail-Safe State: it is defined as the paralleled 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 malfunctioning power supply and to replace it with new 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 paralleled output voltage is blocked or oscillating between 2 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.
- □ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 28.5 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 29 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 22 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 22 and 28 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	6.85
λ_{du} = Total Dangerous Undetected failures	3.95
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	43.96
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**54.77**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**2084 years**
$\lambda_{no\ effect}$ = “No Effect” failures	6763.31
$\lambda_{not\ part}$ = “Not Part” failures	36.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**6854.08**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**16 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**1.74E-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	43.96 FIT	6.85 FIT	3.95 FIT	92.78%	0.00%	63.40%

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

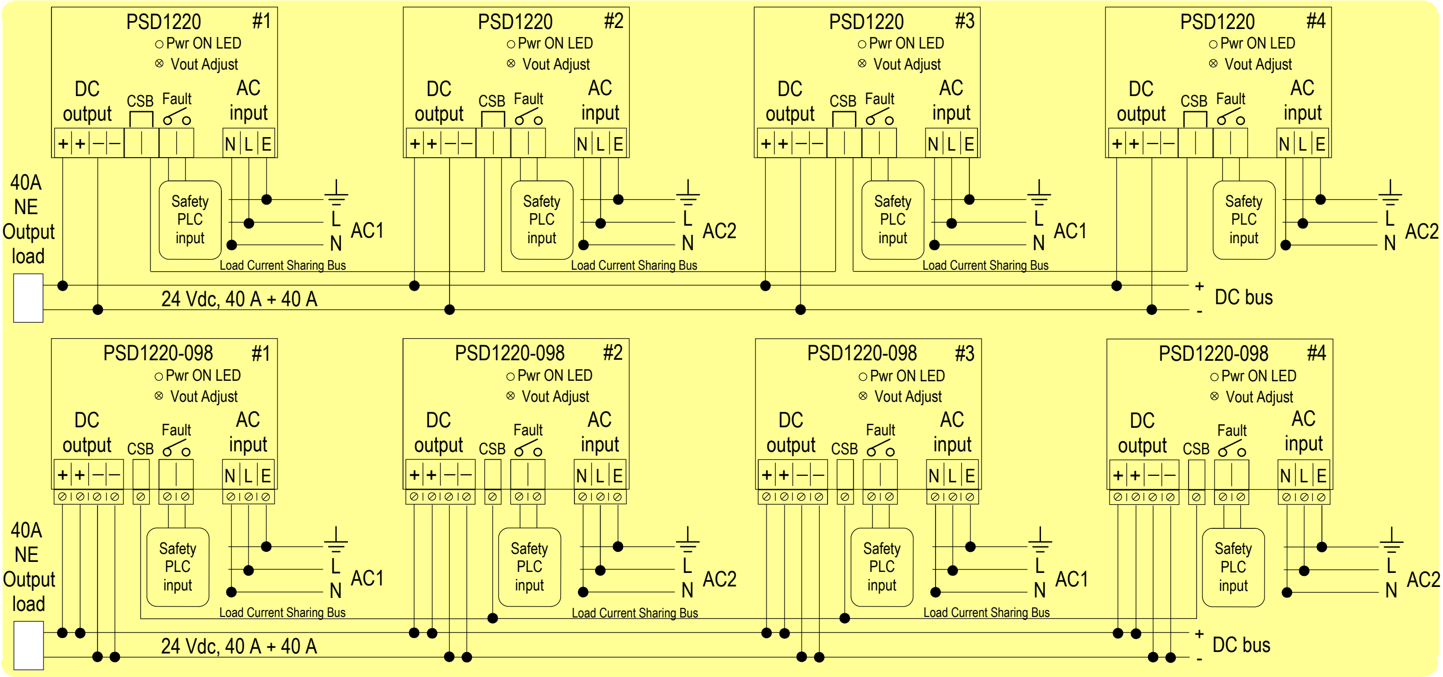
T[Proof] = 5 years	T[Proof] = 20 years
PFDavg = 8.70 E-05 - Valid for **SIL 3**	PFDavg = 3.48 E-04 - Valid for **SIL 2**

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 = 2.61 E-04 - Valid for **SIL 3**

Systematic capability SIL 3.

E) Application of four paralleled PSD1220 or PSD1220-098 modules, for NE output load and with double AC input supply



Description: in normal operation, four paralleled PSD1220 or PSD1220-098 modules are powered by connecting double AC1 / AC2 input supply to related terminal blocks, so that their green Power ON LEDs are lit and NE output load (connected to external wiring paralleled outputs of all modules) is Normally Energized (NE). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify under/over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open. In absence of both AC1 and AC2 input supplies, all paralleled modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State). With double AC1 / AC2 input supply, there is input redundancy because in absence of one only input supply (AC1 or AC2), two modules are shutdown (their fault relay contacts are open) but the other ones operate in normal condition, so that output load is kept normally energized.

Safety Function and Failure behavior:

Four paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 2+2 on output & input (because of double input supply). The failure behavior of four paralleled modules for NE load is described as follows:

- □ Fail-Safe State: it is defined as the paralleled 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 malfunctioning power supply and to replace it with new 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 paralleled output voltage is blocked or oscillating between 2 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.
- □ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 28.5 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 29 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 22 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 22 and 28 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	6.85
λ_{du} = Total Dangerous Undetected failures	3.95
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	43.96
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**54.77**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**2084 years**
$\lambda_{no\ effect}$ = “No Effect” failures	6763.31
$\lambda_{not\ part}$ = “Not Part” failures	36.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**6854.08**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**16 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**1.74E-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	43.96 FIT	6.85 FIT	3.95 FIT	92.78%	0.00%	63.40%

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

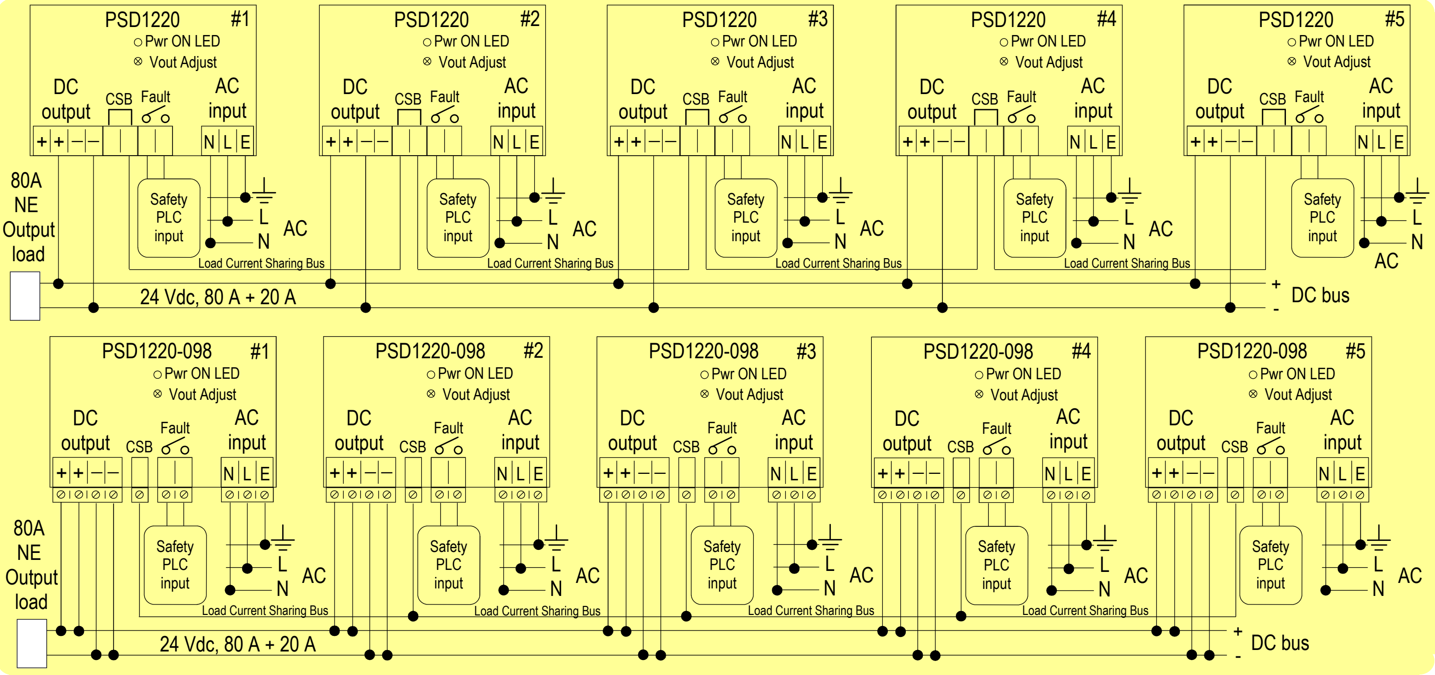
T[Proof] = 5 years	T[Proof] = 20 years
PFDavg = 8.70 E-05 - Valid for **SIL 3**	PFDavg = 3.48 E-04 - Valid for **SIL 2**

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 = 2.61 E-04 - Valid for **SIL 3**

Systematic capability SIL 3.

F) Application of five paralleled PSD1220 or PSD1220-098 modules, for NE output load and with single AC input supply



Description: in normal operation, five paralleled PSD1220 or PSD1220-098 modules are powered by connecting AC input supply to related terminal blocks so that their green Power ON LEDs are lit and NE output load (connected to external wiring paralleled outputs of all modules) is Normally Energized (NE). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information).

For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify under/over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open. In absence of AC input supply, all paralleled modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State).

Safety Function and Failure behavior:

Five paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 4+1 on output. The failure behavior of five paralleled modules for NE load is described as follows:

- □ Fail-Safe State: it is defined as the paralleled 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 malfunctioning power supply and to replace it with new 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 paralleled output voltage is blocked or oscillating between 2 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.
- □ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 28.5 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 29 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 22 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 22 and 28 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	7.85
λ_{du} = Total Dangerous Undetected failures	4.90
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	43.96
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**56.72**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**2012 years**
$\lambda_{no\ effect}$ = “No Effect” failures	8465.88
$\lambda_{not\ part}$ = “Not Part” failures	45.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**8567.60**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**13 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.158E-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	43.96 FIT	7.85 FIT	4.90 FIT	91.35%	0.00%	61.55%

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

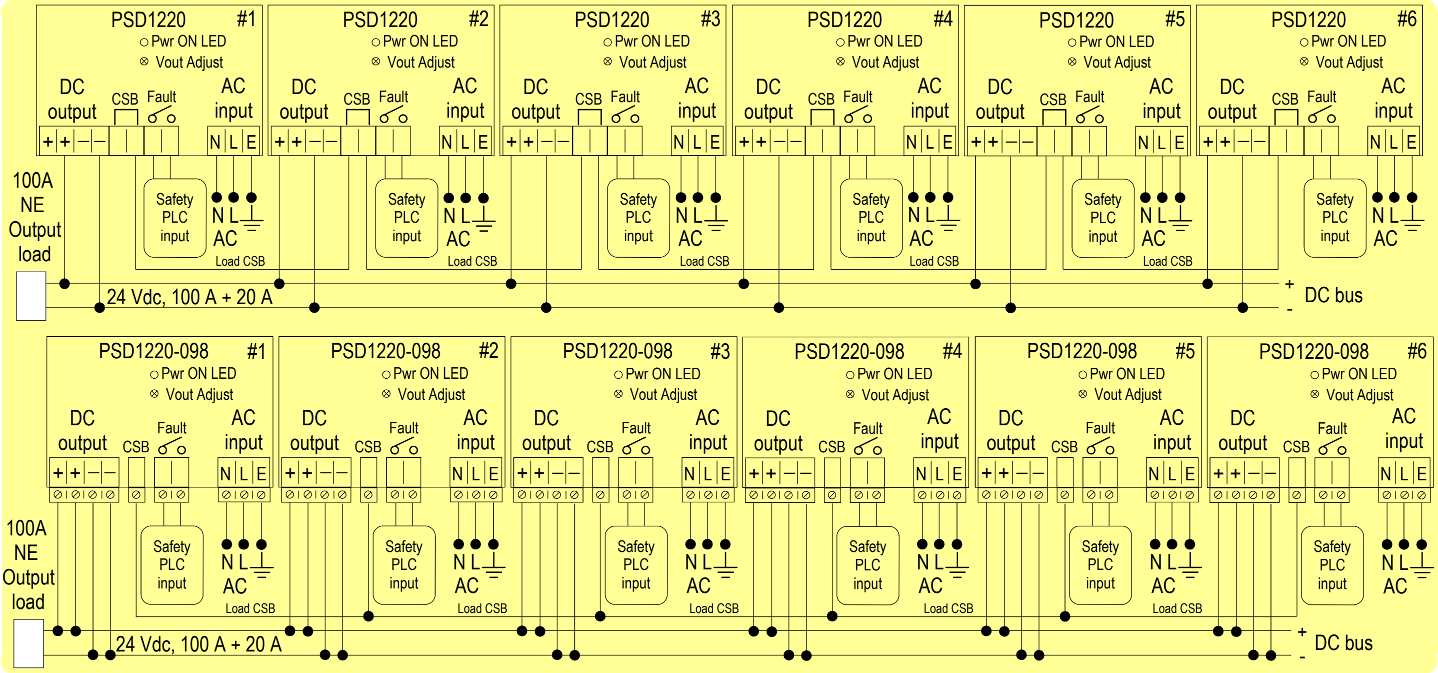
T[Proof] = 4 years	T[Proof] = 20 years
PFDavg = 8.63 E-05 - Valid for **SIL 3**	PFDavg = 4.32 E-04 - Valid for **SIL 2**

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 = 3.24 E-04 - Valid for **SIL 3**

Systematic capability SIL 3.

G) Application of six paralleled PSD1220 or PSD1220-098 modules, for NE output load and with single AC input supply



Description: in normal operation, six paralleled PSD1220 or PSD1220-098 modules are powered by connecting AC input supply to related terminal blocks so that their green Power ON LEDs are lit and NE output load (connected to external wiring paralleled outputs of all modules) is Normally Energized (NE). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information).
For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify under/over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open. In absence of AC input supply, all paralleled modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State).

Safety Function and Failure behavior:

Six paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 5+1 on output. The failure behavior of six paralleled modules for NE load is described as follows:

- □ Fail-Safe State: it is defined as the paralleled 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 malfunctioning power supply and to replace it with new 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 paralleled output voltage is blocked or oscillating between 2 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.
- □ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 28.5 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 29 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 22 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 22 and 28 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	8.85
λ_{du} = Total Dangerous Undetected failures	5.85
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	43.96
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**58.67**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**1945 years**
$\lambda_{no\ effect}$ = “No Effect” failures	10168.45
$\lambda_{not\ part}$ = “Not Part” failures	54.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**10281.12**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**11 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.576E-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	43.96 FIT	8.85 FIT	5.85 FIT	90.02%	0.00%	60.19%

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

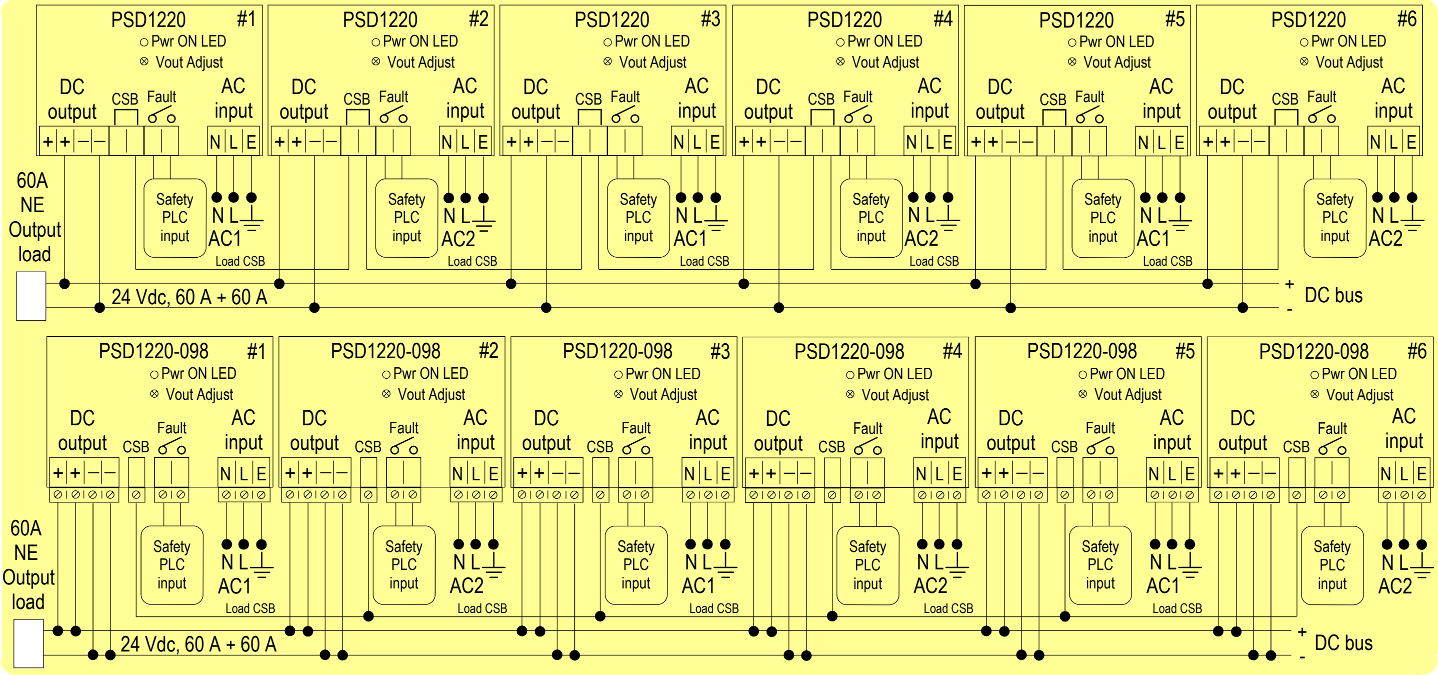
T[Proof] = 3.5 years	T[Proof] = 20 years
PFDavg = 9.02 E-05 - Valid for **SIL 3**	PFDavg = 5.15 E-04 - Valid for **SIL 2**

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] = 12 years
PFDavg = 3.09 E-04 - Valid for **SIL 3**

Systematic capability SIL 3.

H) Application of six paralleled PSD1220 or PSD1220-098 modules, for NE output load and with double AC input supply



Description: in normal operation, six paralleled PSD1220 or PSD1220-098 modules are powered by connecting double AC1 / AC2 input supply to related terminal blocks, so that their green Power ON LEDs are lit and NE output load (connected to external wiring paralleled outputs of all modules) is Normally Energized (NE). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify under/over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open. In absence of both AC1 and AC2 input supplies, all paralleled modules are shutdown (their fault relay contacts are open) and output load is de-energized (Safe State). With double AC1 / AC2 input supply, there is input redundancy because in absence of one only input supply (AC1 or AC2), three modules are shutdown (their fault relay contacts are open) but the other ones operate in normal condition, so that output load is kept normally energized.

Safety Function and Failure behavior:

Six paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 3+3 on output & input (because of double input supply). The failure behavior of six paralleled modules for NE load is described as follows:

□ Fail-Safe State: it is defined as the paralleled 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 malfunctioning power supply and to replace it with new 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 paralleled output voltage is blocked or oscillating between 2 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.

□ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protections try to limit paralleled output voltage < 28.5 Vdc, otherwise internal crowbars trip to fail safe state for paralleled output ≥ 29 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 22 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 22 and 28 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	8.85
λ_{du} = Total Dangerous Undetected failures	5.85
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	43.96
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**58.67**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**1945 years**
$\lambda_{no\ effect}$ = “No Effect” failures	10168.45
$\lambda_{not\ part}$ = “Not Part” failures	54.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**10281.12**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**11 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.576E-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	43.96 FIT	8.85 FIT	5.85 FIT	90.02%	0.00%	60.19%

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

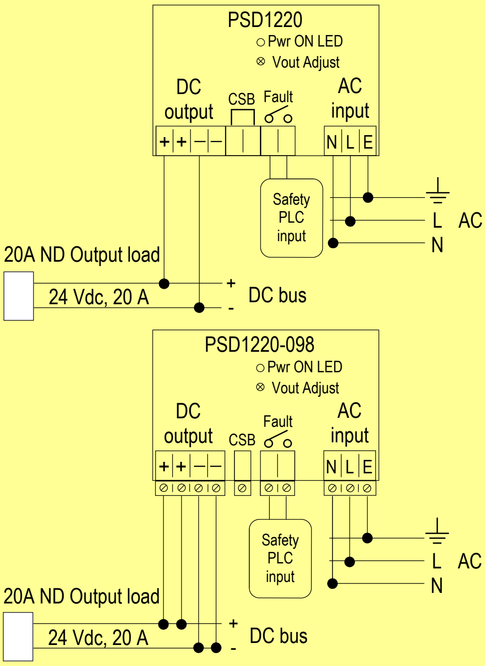
T[Proof] = 3.5 years	T[Proof] = 20 years
PFDavg = 9.02 E-05 - Valid for **SIL 3**	PFDavg = 5.15 E-04 - Valid for **SIL 2**

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] = 12 years
PFDavg = 3.09 E-04 - Valid for **SIL 3**

Systematic capability SIL 3.

I) Application of single PSD1220 or PSD1220-098 module, for ND output load



Description: in normal operation, the PSD1220 or PSD1220-098 module is unpowered because of absence of AC input supply, which is connected to related terminal block, so that its green Power ON LED is turned off and ND output load (connected to related output terminal block) is Normally De-energized (ND) (see functional diagram in the instruction manual ISM0370 for more information). The fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify under/ over voltage faults to logic solver, which can only require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open. In absence of AC input supply, the module is shutdown (its fault relay contact is open) and output load is normally de-energized (ND). In presence of AC input supply, module is powered, its green Power ON LED is lit, its fault relay contact is closed (if fault is absent) and output load is energized (Safe State).

Safety Function and Failure behavior:

Single PSD1220 or PSD1220-098 module is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0.

The failure behavior of PSD1220 or PSD1220-098 for ND load is described by the following definitions:

□ Fail-Safe State: it is defined as the output going between 22 and 28 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 22 Vdc or above 28 Vdc, and internal diagnostic cannot detect and notify faults to logic solver.

□ Fail High - Overvoltage: failure mode that causes the output to go above 28 Vdc. Internal overvoltage protection tries to limit output voltage < 28.5 Vdc, otherwise for output ≥ 29 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 failed power supply and to replace it with new one.

□ Fail Low - Undervoltage: failure mode that causes the output to go between 0 and 22 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 failed power supply and to replace it with new one.

□ 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	00.00
λ_{du} = Total Dangerous Undetected failures	941.29
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	763.23
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**1704.52**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**67 years**
$\lambda_{not\ part}$ = "Not Part" failures	9.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	**1713.52**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**66 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**4.13E-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	763.23 FIT	0.00 FIT	941.29 FIT	44.78%	0.00%	0.00%

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

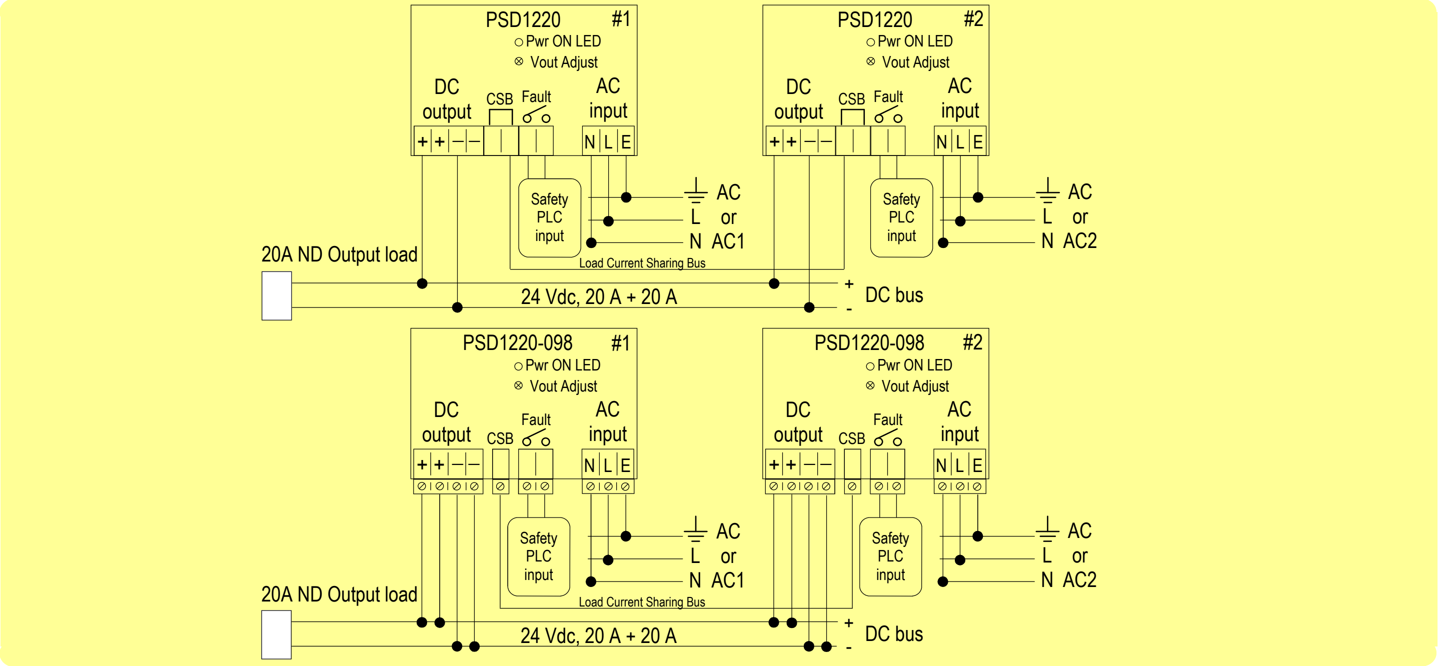
T[Proof] = 2 years
PFDavg = 8.26 E-03 - Valid for **SIL 1**

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] = 6 years
PFDavg = 2.48 E-02 - Valid for **SIL 1**

Systematic capability SIL 3.

J) Application (HFT=1) of two paralleled PSD1220 or PSD1220-098 modules, for ND output load and with single or double AC input supply



Description: in normal operation, two paralleled PSD1220 or PSD1220-098 modules are unpowered because of absence of single AC or double AC1 / AC2 input supply, which is connected to related terminal blocks, so that their green Power ON LEDs are turned off and ND output load (connected to external wiring paralleled outputs of both modules) is Normally De-energized (ND) (see functional diagram in the instruction manual ISM0370 for more information). For load current sharing operation, both modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

In absence of AC input supply or both AC1 and AC2 input supplies, both paralleled modules are shutdown (their fault relay contacts are open) and output load is normally de-energized. In presence of AC input supply or both AC1 and AC2 input supplies, both paralleled modules are powered, their green Power ON LEDs are lit, their fault relay contacts are closed (if fault is absent) and output load is energized (Safe State). With double AC1 / AC2 input supply, there is input redundancy because in absence of one only input supply (AC1 or AC2), one module is shutdown (its fault relay contact is open) but the other one operates in normal condition, so that output load is kept energized (Safe State).

Safety Function and Failure behavior:

Two paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 1+1 on output (with single input supply) or 1+1 on output & input (with double input supply). The failure behavior of two paralleled modules for ND load is described as follows:

□ Fail-Safe State: it is defined as the paralleled output going between 22 and 28 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 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 paralleled output voltage is blocked or oscillating between 0 and 22 Vdc or above 28 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 28 Vdc. Internal overvoltage protection tries to limit paralleled output voltage < 28.5 Vdc, otherwise for paralleled output ≥ 29 Vdc internal crowbars trip, turning off failed 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 22 Vdc. This failure mode is dangerous, but internal diagnostics notify Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off failed power supply and to replace it with new one.

□ 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	02.00
λ_{du} = Total Dangerous Undetected failures	48.87
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	3358.17
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**3409.04**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**33 years**
$\lambda_{not\ part}$ = “Not Part” failures	18.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	**3427.04**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**33 years**
PFDavg (TI = 1 year) = λ_{du} * (0.5*8760 + 8)h + λ_{dd} * 8h	**2.144E-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	3358.17 FIT	2.00 FIT	48.87 FIT	98.57%	0.00%	3.93%

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

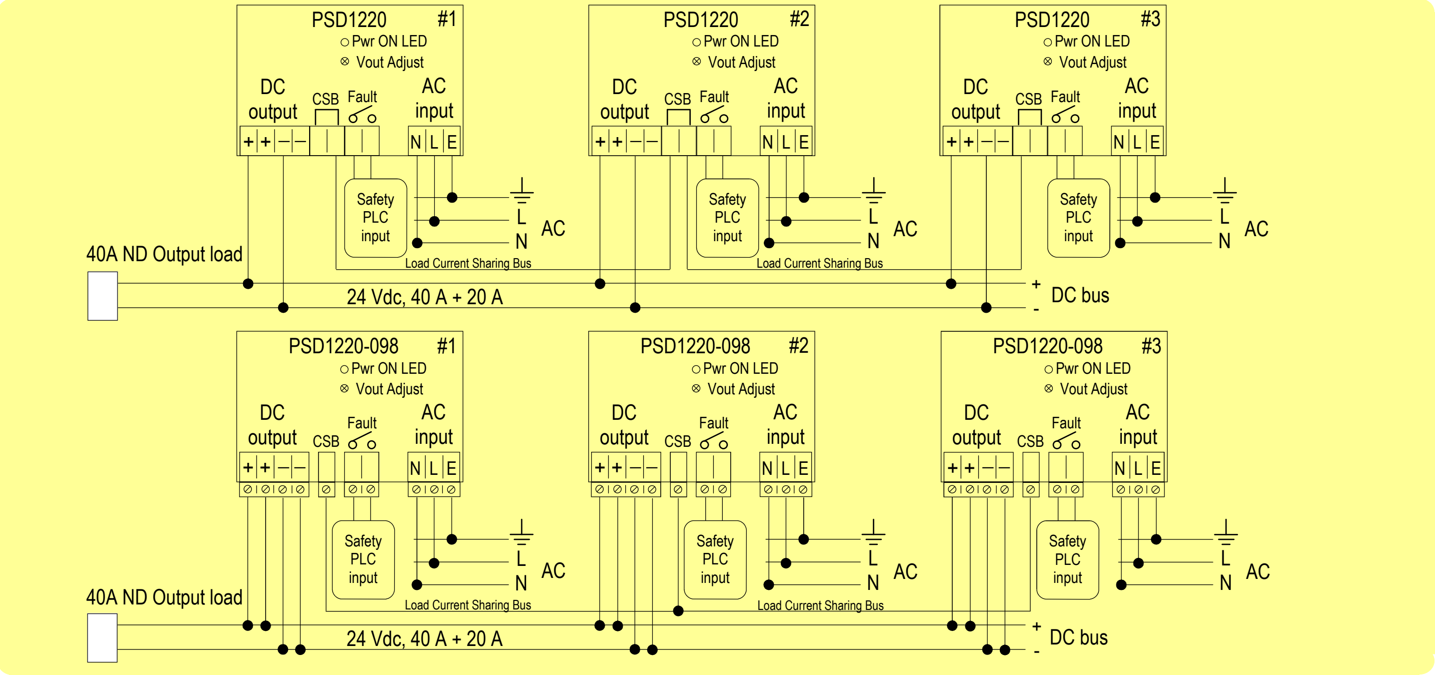
T[Proof] = 4 years	T[Proof] = 20 years
PFDavg = 8.58 E-04 - Valid for **SIL 2**	PFDavg = 4.29 E-03 - Valid for **SIL 1**

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] = 12 years
PFDavg = 2.57 E-03 - Valid for **SIL 2**

Systematic capability SIL 3.

K) Application (HFT=1) of three paralleled PSD1220 or PSD1220-098 modules, for ND output load and with single AC input supply



Description: in normal operation, three paralleled PSD1220 or PSD1220-098 modules are unpowered because of absence of AC input supply, which is connected to related terminal blocks, so that their green Power ON LEDs are turned off and ND output load (connected to external wiring paralleled outputs of all modules) is Normally De-energized (ND) (see functional diagram in the instruction manual ISM0370 for more information). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

In absence of AC input supply, all paralleled modules are shutdown (their fault relay contacts are open) and output load is normally de-energized. In presence of AC input supply, all paralleled modules are powered, their green Power ON LEDs are lit, their fault relay contacts are closed (if fault is absent) and output load is energized (Safe State).

Safety Function and Failure behavior:

Three paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 2+1 on output. The failure behavior of three paralleled modules for ND load is described as follows:

- □ Fail-Safe State: it is defined as the paralleled output going between 22 and 28 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 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 paralleled output voltage is blocked or oscillating between 0 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.
- □ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protection tries to limit paralleled output voltage < 28.5 Vdc, otherwise for paralleled output ≥ 29 Vdc internal crowbars trip, turning off failed 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 22 Vdc. This failure mode is dangerous, but internal diagnostics notify Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off failed power supply and to replace it with new one.
- □ 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	03.00
λ_{du} = Total Dangerous Undetected failures	49.82
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	5060.74
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**5113.56**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**22 years**
$\lambda_{not\ part}$ = "Not Part" failures	27.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	**5140.56**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**22 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.186E-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	5060.74 FIT	3.00 FIT	49.82 FIT	99.03%	0.00%	5.68%

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

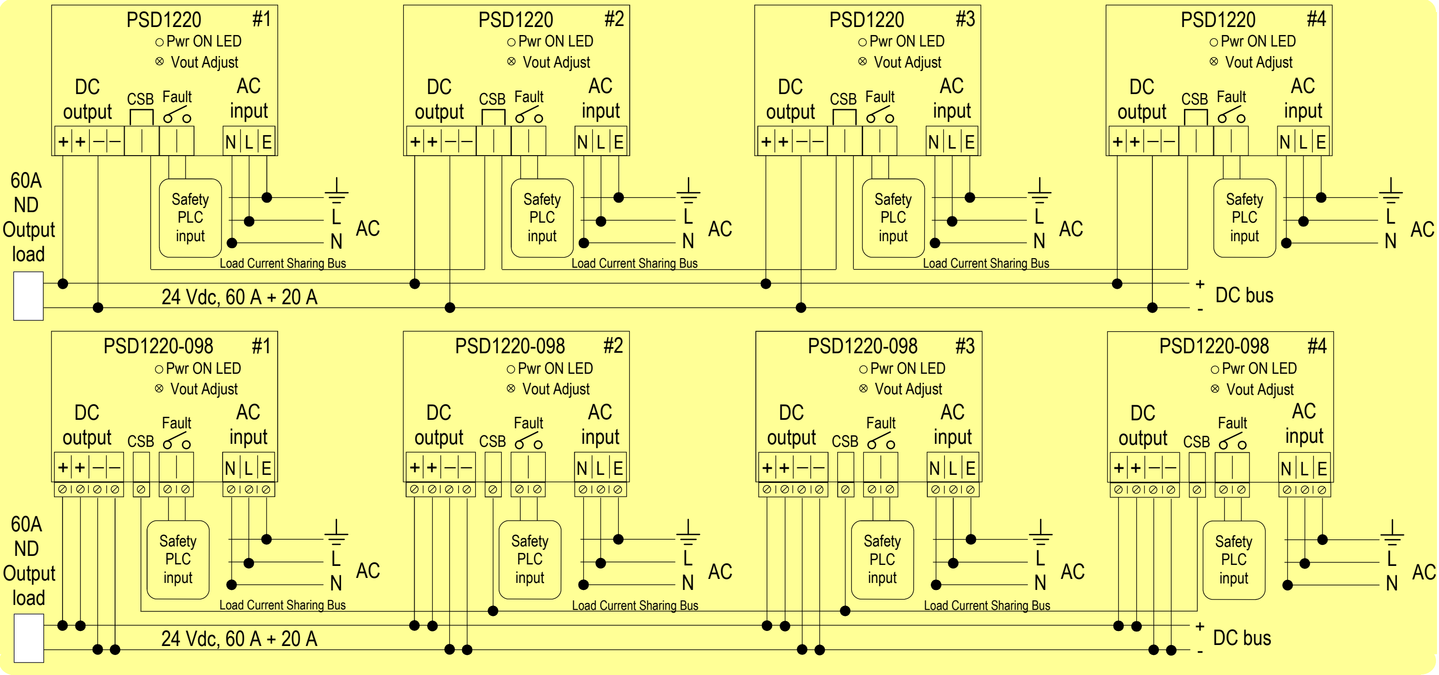
T[Proof] = 4 years	T[Proof] = 20 years
PFDavg = 8.74 E-04 - Valid for **SIL 2**	PFDavg = 4.37 E-03 - Valid for **SIL 1**

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] = 12 years
PFDavg = 2.62 E-03 - Valid for **SIL 2**

Systematic capability SIL 3.

L) Application (HFT=1) of four paralleled PSD1220 or PSD1220-098 modules, for ND output load and with single AC input supply



Description: in normal operation, four paralleled PSD1220 or PSD1220-098 modules are unpowered because of absence of AC input supply, which is connected to related terminal blocks, so that their green Power ON LEDs are turned off and ND output load (connected to external wiring paralleled outputs of all modules) is Normally De-energized (ND) (see functional diagram in the instruction manual ISM0370 for more information). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

In absence of AC input supply, all paralleled modules are shutdown (their fault relay contacts are open) and output load is normally de-energized. In presence of AC input supply, all paralleled modules are powered, their green Power ON LEDs are lit, their fault relay contacts are closed (if fault is absent) and output load is energized (Safe State).

Safety Function and Failure behavior:

Four paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 3+1 on output. The failure behavior of four paralleled modules for ND load is described as follows:

- □ Fail-Safe State: it is defined as the paralleled output going between 22 and 28 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 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 paralleled output voltage is blocked or oscillating between 0 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.
- □ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protection tries to limit paralleled output voltage < 28.5 Vdc, otherwise for paralleled output ≥ 29 Vdc internal crowbars trip, turning off failed 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 22 Vdc. This failure mode is dangerous, but internal diagnostics notify Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off failed power supply and to replace it with new one.
- □ 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	04.00
λ_{du} = Total Dangerous Undetected failures	50.77
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	6763.31
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**6818.08**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**16 years**
$\lambda_{not\ part}$ = "Not Part" failures	36.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	**6854.08**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**16 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.228E-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	6763.31 FIT	4.00 FIT	50.77 FIT	99.26%	0.00%	7.30%

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

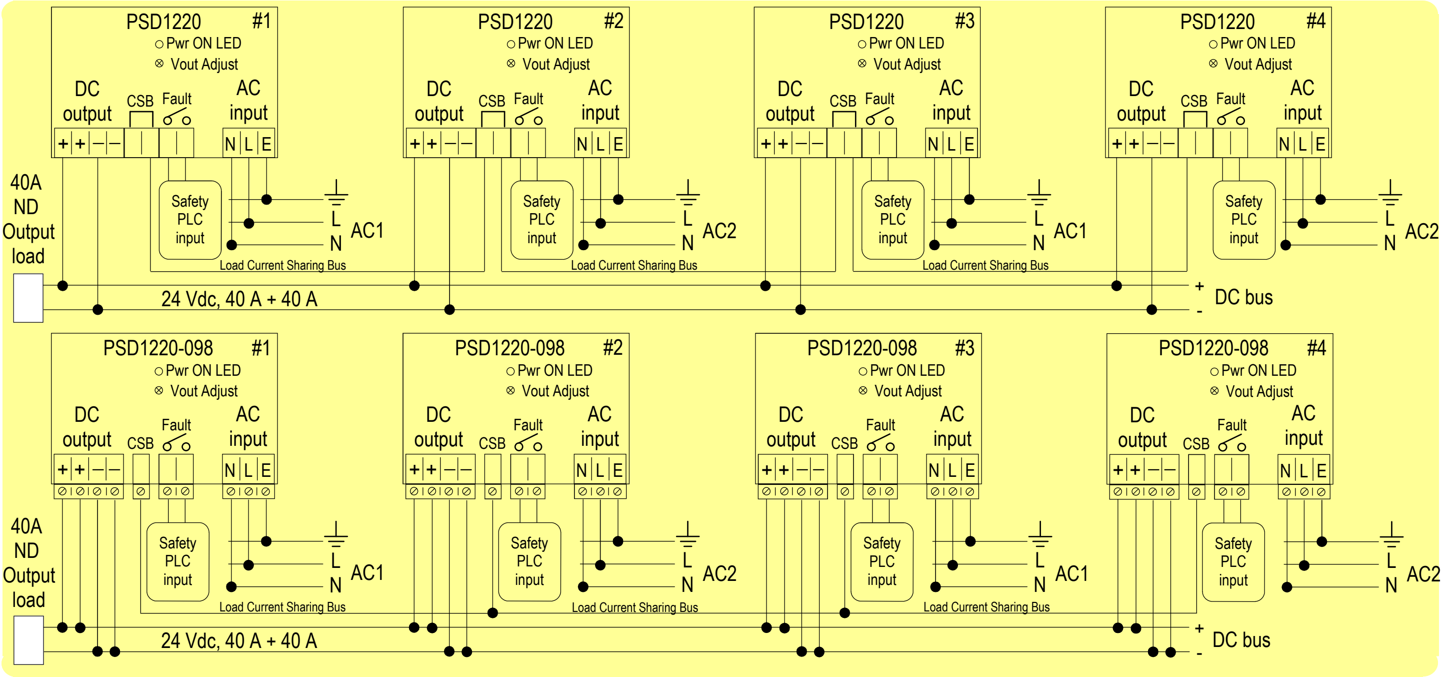
T[Proof] = 4 years	T[Proof] = 20 years
PFDavg = 8.91 E-04 - Valid for **SIL 2**	PFDavg = 4.46 E-03 - Valid for **SIL 1**

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] = 12 years
PFDavg = 2.67 E-03 - Valid for **SIL 2**

Systematic capability SIL 3.

M) Application (HFT=1) of four paralleled PSD1220 or PSD1220-098 modules, for ND output load and with double AC input supply



Description: in normal operation, four paralleled PSD1220 or PSD1220-098 modules are unpowered because of absence of double AC1 / AC2 input supply, which is connected to related terminal blocks, so that their green Power ON LEDs are turned off and ND output load (connected to external wiring paralleled outputs of all modules) is Normally De-energized (ND) (see functional diagram in the instruction manual ISM0370 for more information). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

In absence of both AC1 and AC2 input supplies, all paralleled modules are shutdown (their fault relay contacts are open) and output load is normally de-energized. In presence of both AC1 and AC2 input supplies, all paralleled modules are powered, their green Power ON LEDs are lit, their fault relay contacts are closed (if fault is absent) and output load is energized (Safe State). With double AC1 / AC2 input supply, there is input redundancy because in absence of one only input supply (AC1 or AC2), two modules are shutdown (their fault relay contacts are open) but the other ones operate in normal condition, so that output load is kept energized (Safe State).

Safety Function and Failure behavior:

Four paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 2+2 on output & input (because of double input supply). The failure behavior of four paralleled modules for ND load is described as follows:

- □ Fail-Safe State: it is defined as the paralleled output going between 22 and 28 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 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 paralleled output voltage is blocked or oscillating between 0 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.
- □ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protection tries to limit paralleled output voltage < 28.5 Vdc, otherwise for paralleled output ≥ 29 Vdc internal crowbars trip, turning off failed 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 22 Vdc. This failure mode is dangerous, but internal diagnostics notify Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off failed power supply and to replace it with new one.
- □ 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	04.00
λ_{du} = Total Dangerous Undetected failures	50.77
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	6763.31
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**6818.08**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**16 years**
$\lambda_{not\ part}$ = "Not Part" failures	36.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	**6854.08**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**16 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.228E-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	6763.31 FIT	4.00 FIT	50.77 FIT	99.26%	0.00%	7.30%

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

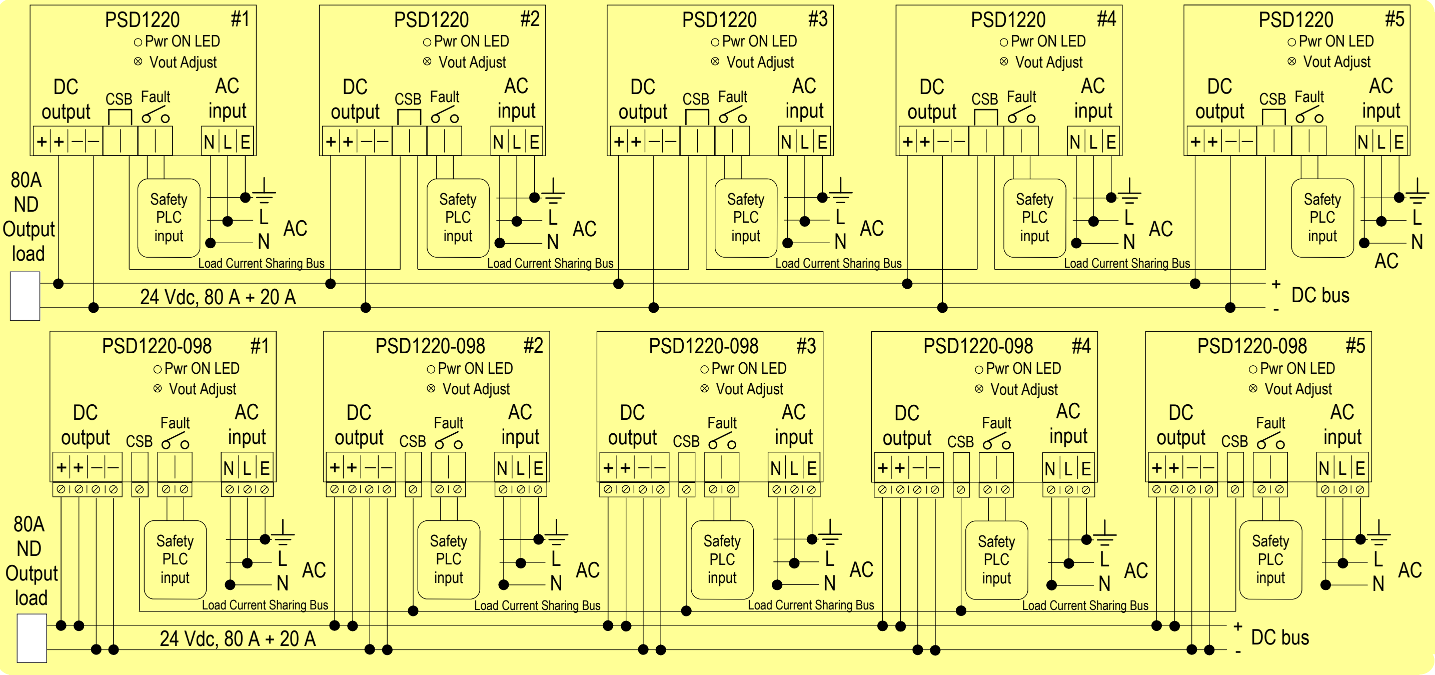
T[Proof] = 4 years	T[Proof] = 20 years
PFDavg = 8.91 E-04 - Valid for **SIL 2**	PFDavg = 4.46 E-03 - Valid for **SIL 1**

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] = 12 years
PFDavg = 2.67 E-03 - Valid for **SIL 2**

Systematic capability SIL 3.

N) Application (HFT=1) of five paralleled PSD1220 or PSD1220-098 modules, for ND output load and with single AC input supply



Description: in normal operation, five paralleled PSD1220 or PSD1220-098 modules are unpowered because of absence of AC input supply, which is connected to related terminal blocks, so that their green Power ON LEDs are turned off and ND output load (connected to external wiring paralleled outputs of all modules) is Normally De-energized (ND) (see functional diagram in the instruction manual ISM0370 for more information). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

In absence of AC input supply, all paralleled modules are shutdown (their fault relay contacts are open) and output load is normally de-energized. In presence of AC input supply, all paralleled modules are powered, their green Power ON LEDs are lit, their fault relay contacts are closed (if fault is absent) and output load is energized (Safe State).

Safety Function and Failure behavior:

Five paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 4+1 on output. The failure behavior of five paralleled modules for ND load is described as follows:

□ Fail-Safe State: it is defined as the paralleled output going between 22 and 28 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 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 paralleled output voltage is blocked or oscillating between 0 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.

□ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protection tries to limit paralleled output voltage < 28.5 Vdc, otherwise for paralleled output ≥ 29 Vdc internal crowbars trip, turning off failed 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 22 Vdc. This failure mode is dangerous, but internal diagnostics notify Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off failed power supply and to replace it with new one.

□ 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	05.00
λ_{du} = Total Dangerous Undetected failures	51.72
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	8465.88
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**8522.60**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**13 years**
$\lambda_{not\ part}$ = "Not Part" failures	45.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	**8567.60**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**13 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.27E-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	8465.88 FIT	5.00 FIT	51.72 FIT	99.39%	0.00%	8.82%

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

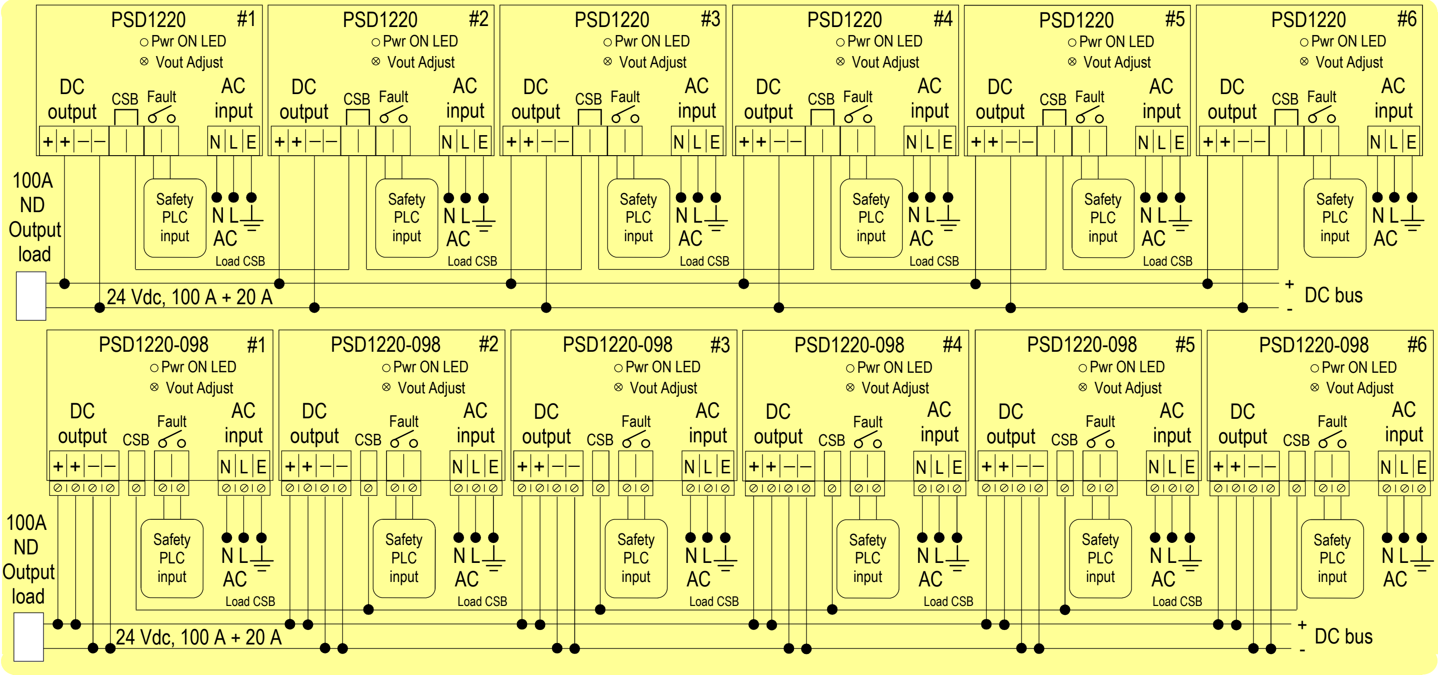
T[Proof] = 4 years	T[Proof] = 20 years
PFDavg = 9.08 E-04 - Valid for **SIL 2**	PFDavg = 4.54 E-03 - Valid for **SIL 1**

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] = 12 years
PFDavg = 2.72 E-03 - Valid for **SIL 2**

Systematic capability SIL 3.

O) Application (HFT=1) of six paralleled PSD1220 or PSD1220-098 modules, for ND output load and with single AC input supply



Description: in normal operation, six paralleled PSD1220 or PSD1220-098 modules are unpowered because of absence of AC input supply, which is connected to related terminal blocks, so that their green Power ON LEDs are turned off and ND output load (connected to external wiring paralleled outputs of all modules) is Normally De-energized (ND) (see functional diagram in the instruction manual ISM0370 for more information). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

In absence of AC input supply, all paralleled modules are shutdown (their fault relay contacts are open) and output load is normally de-energized. In presence of AC input supply, all paralleled modules are powered, their green Power ON LEDs are lit, their fault relay contacts are closed (if fault is absent) and output load is energized (Safe State).

Safety Function and Failure behavior:

Six paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 5+1 on output. The failure behavior of six paralleled modules for ND load is described as follows:

□ Fail-Safe State: it is defined as the paralleled output going between 22 and 28 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 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 paralleled output voltage is blocked or oscillating between 0 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.

□ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protection tries to limit paralleled output voltage < 28.5 Vdc, otherwise for paralleled output ≥ 29 Vdc internal crowbars trip, turning off failed 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 22 Vdc. This failure mode is dangerous, but internal diagnostics notify Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off failed power supply and to replace it with new one.

□ 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	06.00
λ_{du} = Total Dangerous Undetected failures	52.67
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	10168.45
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**10227.12**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**11 years**
$\lambda_{not\ part}$ = "Not Part" failures	54.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	**10281.12**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**11 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.312E-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	10168.45 FIT	6.00 FIT	52.67 FIT	99.49%	0.00%	10.23%

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

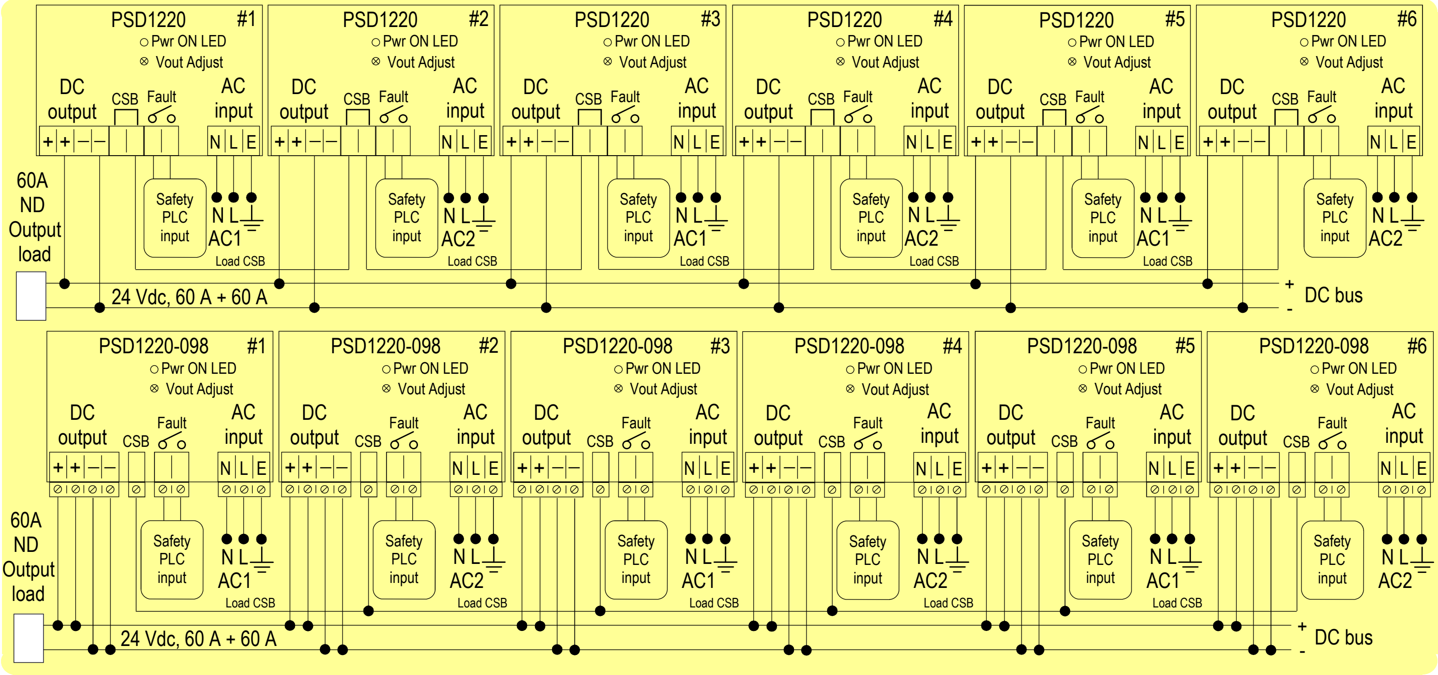
T[Proof] = 4 years	T[Proof] = 20 years
PFDavg = 9.25 E-04 - Valid for **SIL 2**	PFDavg = 4.62 E-03 - Valid for **SIL 1**

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] = 12 years
PFDavg = 2.77 E-03 - Valid for **SIL 2**

Systematic capability SIL 3.

P) Application (HFT=1) of six paralleled PSD1220 or PSD1220-098 modules, for ND output load and with double AC input supply



Description: in normal operation, six paralleled PSD1220 or PSD1220-098 modules are unpowered because of absence of double AC1 / AC2 input supply, which is connected to related terminal blocks, so that their green Power ON LEDs are turned off and ND output load (connected to external wiring paralleled outputs of all modules) is Normally De-energized (ND) (see functional diagram in the instruction manual ISM0370 for more information). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

In absence of both AC1 and AC2 input supplies, all paralleled modules are shutdown (their fault relay contacts are open) and output load is normally de-energized. In presence of both AC1 and AC2 input supplies, all paralleled modules are powered, their green Power ON LEDs are lit, their fault relay contacts are closed (if fault is absent) and output load is energized (Safe State). With double AC1 / AC2 input supply, there is input redundancy because in absence of one only input supply (AC1 or AC2), three modules are shutdown (their fault relay contacts are open) but the other ones operate in normal condition, so that output load is kept energized (Safe State).

Safety Function and Failure behavior:

Six paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 1 or redundant configuration 3+3 on output & input (because of double input supply). The failure behavior of six paralleled modules for ND load is described as follows:

- □ Fail-Safe State: it is defined as the paralleled output going between 22 and 28 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 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 paralleled output voltage is blocked or oscillating between 0 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.
- □ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protection tries to limit paralleled output voltage < 28.5 Vdc, otherwise for paralleled output ≥ 29 Vdc internal crowbars trip, turning off failed 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 22 Vdc. This failure mode is dangerous, but internal diagnostics notify Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off failed power supply and to replace it with new one.
- □ 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	06.00
λ_{du} = Total Dangerous Undetected failures	52.67
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	10168.45
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**10227.12**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**11 years**
$\lambda_{not\ part}$ = “Not Part” failures	54.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	**10281.12**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**11 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.312E-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	10168.45 FIT	6.00 FIT	52.67 FIT	99.49%	0.00%	10.23%

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

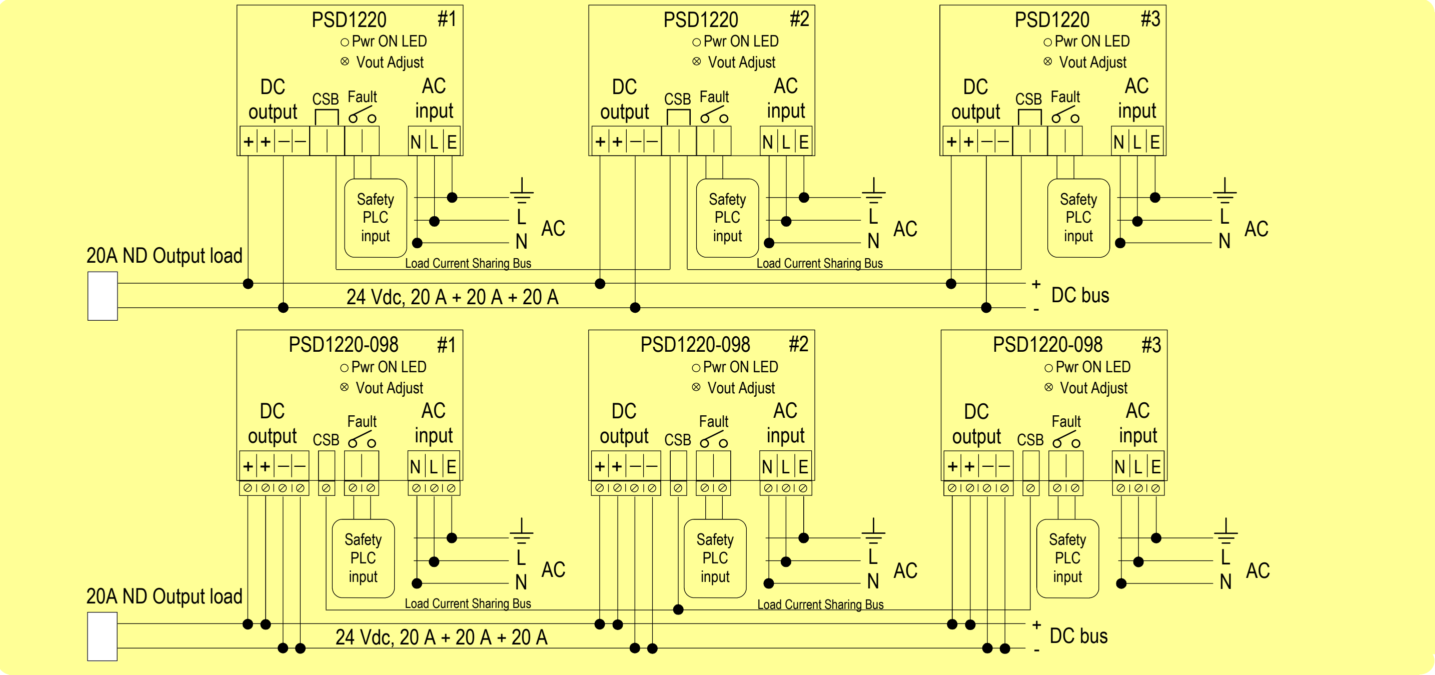
T[Proof] = 4 years	T[Proof] = 20 years
PFDavg = 9.25 E-04 - Valid for **SIL 2**	PFDavg = 4.62 E-03 - Valid for **SIL 1**

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] = 12 years
PFDavg = 2.77 E-03 - Valid for **SIL 2**

Systematic capability SIL 3.

Q) Application (HFT=2) of three paralleled PSD1220 or PSD1220-098 modules, for ND output load and with single AC input supply



Description: in normal operation, three paralleled PSD1220 or PSD1220-098 modules are unpowered because of absence of AC input supply, which is connected to related terminal blocks, so that their green Power ON LEDs are turned off and ND output load (connected to external wiring paralleled outputs of all modules) is Normally De-energized (ND) (see functional diagram in the instruction manual ISM0370 for more information). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

In absence of AC input supply, all paralleled modules are shutdown (their fault relay contacts are open) and output load is normally de-energized. In presence of AC input supply, all paralleled modules are powered, their green Power ON LEDs are lit, their fault relay contacts are closed (if fault is absent) and output load is energized (Safe State).

Safety Function and Failure behavior:

Three paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 2 or redundant configuration 1+(1+1) = 1+2 on output. The failure behavior of three paralleled modules for ND load is described as follows:

□ Fail-Safe State: it is defined as the paralleled output going between 22 and 28 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 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 paralleled output voltage is blocked or oscillating between 0 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.

□ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protection tries to limit paralleled output voltage < 28.5 Vdc, otherwise for paralleled output ≥ 29 Vdc internal crowbars trip, turning off failed 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 22 Vdc. This failure mode is dangerous, but internal diagnostics notify Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off failed power supply and to replace it with new one.

□ 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	03.00
λ_{du} = Total Dangerous Undetected failures	49.82
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	5060.74
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**5113.56**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**22 years**
$\lambda_{not\ part}$ = "Not Part" failures	27.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	**5140.56**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**22 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.186E-04**

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

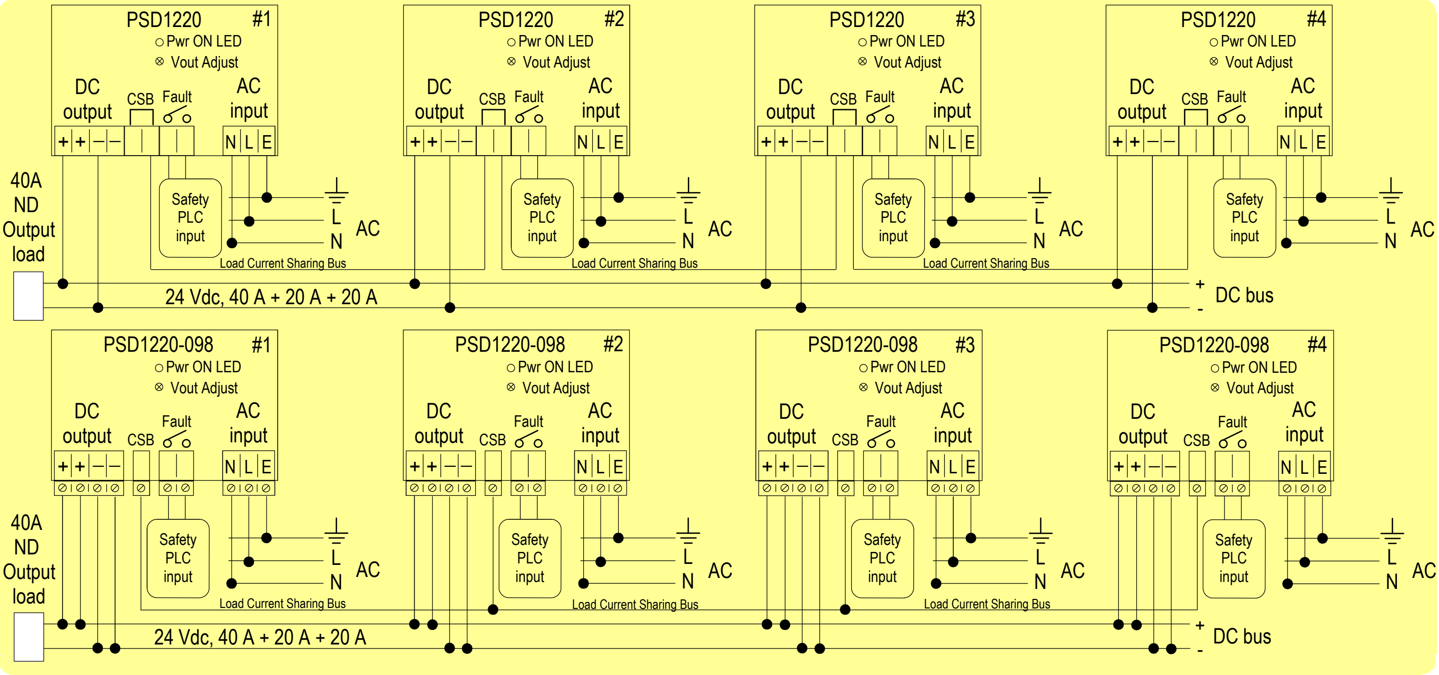
λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	5060.74 FIT	3.00 FIT	49.82 FIT	99.03%	0.00%	5.68%

PFDavg vs T[Proof] table (assuming Proof Test coverage of 90%), with determination of SIL supposing module contributes ≤25% of total SIF dangerous failures:

T[Proof] = 1 year
PFDavg = 2.19 E-04 - Valid for **SIL 3**

Systematic capability SIL 3.

R) Application (HFT=2) of four paralleled PSD1220 or PSD1220-098 modules, for ND output load and with single AC input supply



Description: in normal operation, four paralleled PSD1220 or PSD1220-098 modules are unpowered because of absence of AC input supply, which is connected to related terminal blocks, so that their green Power ON LEDs are turned off and ND output load (connected to external wiring paralleled outputs of all modules) is Normally De-energized (ND) (see functional diagram in the instruction manual ISM0370 for more information). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

In absence of AC input supply, all paralleled modules are shutdown (their fault relay contacts are open) and output load is normally de-energized. In presence of AC input supply, all paralleled modules are powered, their green Power ON LEDs are lit, their fault relay contacts are closed (if fault is absent) and output load is energized (Safe State).

Safety Function and Failure behavior:

Four paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 2 or redundant configuration 2+(1+1) = 2+2 on output. The failure behavior of four paralleled modules for ND load is described as follows:

□ Fail-Safe State: it is defined as the paralleled output going between 22 and 28 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 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 paralleled output voltage is blocked or oscillating between 0 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.

□ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protection tries to limit paralleled output voltage < 28.5 Vdc, otherwise for paralleled output ≥ 29 Vdc internal crowbars trip, turning off failed 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 22 Vdc. This failure mode is dangerous, but internal diagnostics notify Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off failed power supply and to replace it with new one.

□ 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	04.00
λ_{du} = Total Dangerous Undetected failures	50.77
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	6763.31
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = λ_{dd} + λ_{du} + λ_{sd} + λ_{su}	**6818.08**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**16 years**
$\lambda_{not\ part}$ = “Not Part” failures	36.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{not\ part}$	**6854.08**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**16 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.228E-04**

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

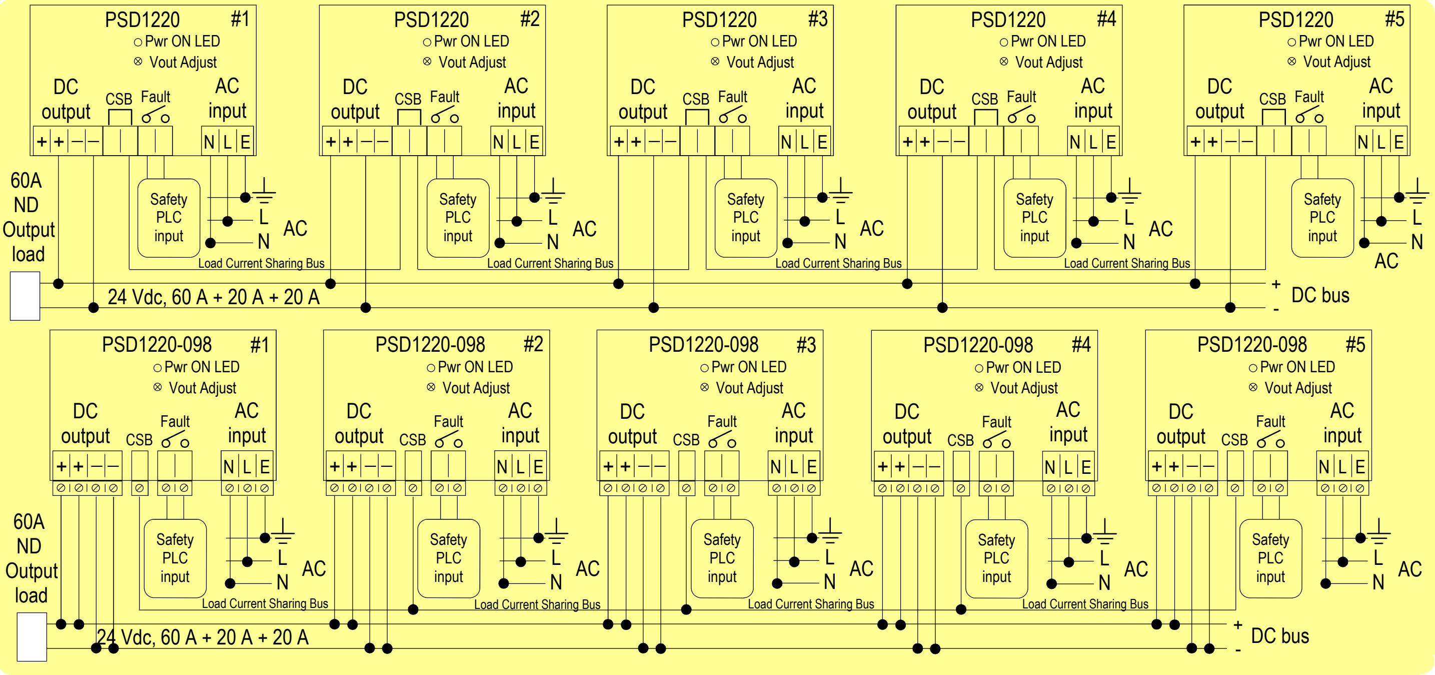
λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	6763.31 FIT	4.00 FIT	50.77 FIT	99.26%	0.00%	7.30%

PFDavg vs T[Proof] table (assuming Proof Test coverage of 90%), with determination of SIL supposing module contributes ≤25% of total SIF dangerous failures:

T[Proof] = 1 year
PFDavg = 2.23 E-04 - Valid for **SIL 3**

Systematic capability SIL 3.

S) Application (HFT=2) of five paralleled PSD1220 or PSD1220-098 modules, for ND output load and with single AC input supply



Description: in normal operation, five paralleled PSD1220 or PSD1220-098 modules are unpowered because of absence of AC input supply, which is connected to related terminal blocks, so that their green Power ON LEDs are turned off and ND output load (connected to external wiring paralleled outputs of all modules) is Normally De-energized (ND) (see functional diagram in the instruction manual ISM0370 for more information). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

In absence of AC input supply, all paralleled modules are shutdown (their fault relay contacts are open) and output load is normally de-energized. In presence of AC input supply, all paralleled modules are powered, their green Power ON LEDs are lit, their fault relay contacts are closed (if fault is absent) and output load is energized (Safe State).

Safety Function and Failure behavior:

Five paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 2 or redundant configuration 3+(1+1) = 3+2 on output. The failure behavior of five paralleled modules for ND load is described as follows:

□ Fail-Safe State: it is defined as the paralleled output going between 22 and 28 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 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 paralleled output voltage is blocked or oscillating between 0 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.

□ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protection tries to limit paralleled output voltage < 28.5 Vdc, otherwise for paralleled output ≥ 29 Vdc internal crowbars trip, turning off failed 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 22 Vdc. This failure mode is dangerous, but internal diagnostics notify Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off failed power supply and to replace it with new one.

□ 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	05.00
λ_{du} = Total Dangerous Undetected failures	51.72
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	8465.88
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = λ_{dd} + λ_{du} + λ_{sd} + λ_{su}	**8522.60**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**13 years**
$\lambda_{not\ part}$ = "Not Part" failures	45.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{not\ part}$	**8567.60**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**13 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.27E-04**

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

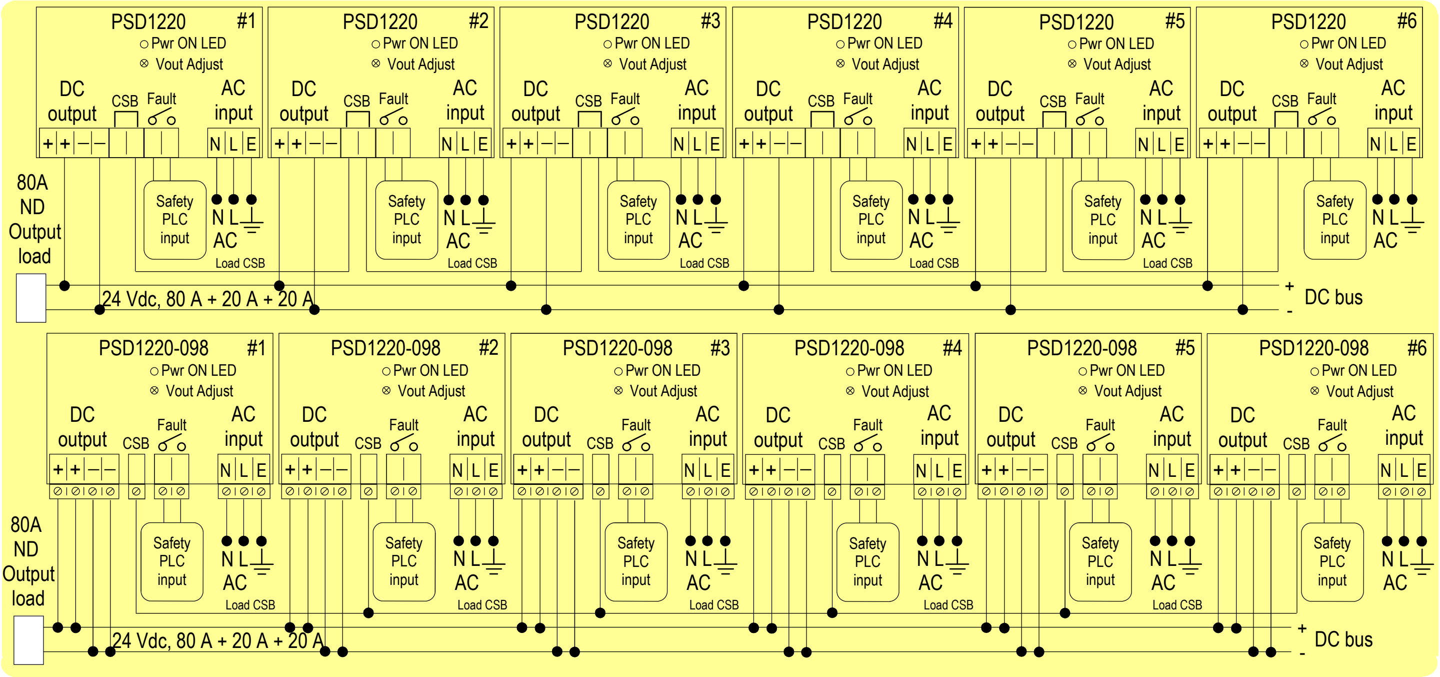
λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	8465.88 FIT	5.00 FIT	51.72 FIT	99.39%	0.00%	8.82%

PFDavg vs T[Proof] table (assuming Proof Test coverage of 90%), with determination of SIL supposing module contributes ≤25% of total SIF dangerous failures:

T[Proof] = 1 year
PFDavg = 2.27 E-04 - Valid for **SIL 3**

Systematic capability SIL 3.

T) Application (HFT=2) of six paralleled PSD1220 or PSD1220-098 modules, for ND output load and with single AC input supply



Description: in normal operation, six paralleled PSD1220 or PSD1220-098 modules are unpowered because of absence of AC input supply, which is connected to related terminal blocks, so that their green Power ON LEDs are turned off and ND output load (connected to external wiring paralleled outputs of all modules) is Normally De-energized (ND) (see functional diagram in the instruction manual ISM0370 for more information). For load current sharing operation, all modules must have their current sharing bus CSB terminal blocks connected together by external wiring (see functional diagram in the instruction manual ISM0370 for more information). For each module, the fault relay contact must be connected to Safety PLC or logic solver because power supply internal diagnostic uses this contact to notify over voltage faults to logic solver, which can require to turn off failed power supply and to replace it with new one. In absence of fault the relay contact is closed, while in presence of fault the relay contact is open.

In absence of AC input supply, all paralleled modules are shutdown (their fault relay contacts are open) and output load is normally de-energized. In presence of AC input supply, all paralleled modules are powered, their green Power ON LEDs are lit, their fault relay contacts are closed (if fault is absent) and output load is energized (Safe State).

Safety Function and Failure behavior:

Six paralleled PSD1220 or PSD1220-098 modules are operating in Low Demand mode, as Type A modules, having Hardware Fault Tolerance (HFT) = 2 or redundant configuration 4+(1+1) = 4+2 on output. The failure behavior of six paralleled modules for ND load is described as follows:

- □ Fail-Safe State: it is defined as the paralleled output going between 22 and 28 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 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 paralleled output voltage is blocked or oscillating between 0 and 22 Vdc or above 28 Vdc, and all internal diagnostics cannot detect and notify faults to logic solver.
- □ Fail High - Overvoltage: failure mode that causes the paralleled output to go above 28 Vdc. Internal overvoltage protection tries to limit paralleled output voltage < 28.5 Vdc, otherwise for paralleled output ≥ 29 Vdc internal crowbars trip, turning off failed 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 22 Vdc. This failure mode is dangerous, but internal diagnostics notify Low fail to logic solver, which cannot convert this failure to the fail-safe state but it can only require to turn off failed power supply and to replace it with new one.
- □ 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	06.00
λ_{du} = Total Dangerous Undetected failures	52.67
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	10168.45
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**10227.12**
MTBF (safety function) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**11 years**
$\lambda_{not\ part}$ = “Not Part” failures	54.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{not\ part}$	**10281.12**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**11 years**
PFDavg (TI = 1 year) = λdu * (0.5*8760 + 8)h + λdd * 8h	**2.312E-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	10168.45 FIT	6.00 FIT	52.67 FIT	99.49%	0.00%	10.23%

PFDavg vs T[Proof] table (assuming Proof Test coverage of 90%), with determination of SIL supposing module contributes ≤25% of total SIF dangerous failures:

T[Proof] = 1 year
PFDavg = 2.31 E-04 - Valid for **SIL 3**

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 PSD1220 or PSD1220-098** 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 input line of PSD1220 or PSD1220-098. This action does not affect output load operating, which holds normally energized because of redundant configuration on output (paralleling connection implies high availability) of the Functional Safety application. The power supply module turn off time lasts some seconds (typically 10 to 15 sec). During this time, the power supply module output voltage goes below 22 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 input line of PSD1220 or PSD1220-098. After about 2 seconds the power supply module operates correctly in load 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	Use an AC true rms voltmeter and connect its probes to DC (+ / -) power supply 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 300 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.

This test reveals 90% of all possible Dangerous Undetected failures in the PSD1220 or PSD1220-098 power supply module, when the output load is NE type.