SAFETY MANUAL

Termination Boards for Tricon & Tricon CX
TBE-D5016-TRI-0xx with xx from 01 to 12 except 10 and TBE-D5008-TRI-001

Reference must be made to the relevant sections within the instruction manual ISM0452, which contain basic guides for the installation of the equipment.
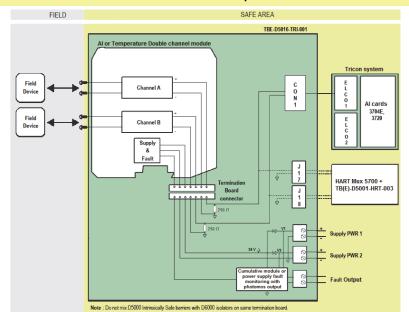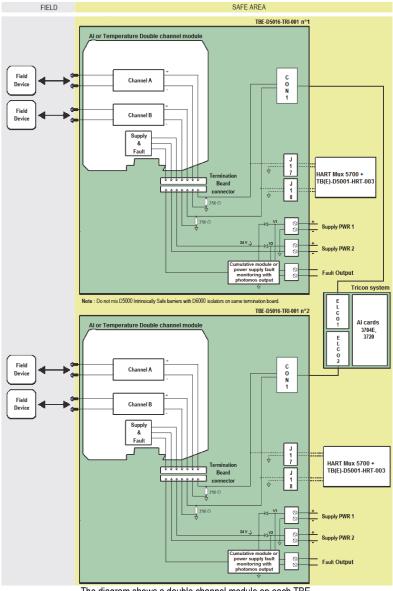
gmI
technology for safety

Index

This safety manual refers to the functional safety applications of the following termination boards that can be connected to the Tricon and Tricon CX systems:

Application of TBE-D5016-TRI-001 with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon system AI cards

The diagram shows a double channel module on TBE. On a single TBE-D5016-TRI-001 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

The diagram shows a double channel module on each TBE.
On two TBE-D5016-TRI-001 Termination Boards can be installed up to 16+16 double channel modules for a maximum of 64 channels.

Description: The TBE-D5016-TRI-001 Termination Board provides direct connection between the Tricon system AI cards 3704E or 3720 and GMI D5000 / D6000 series AI or Temperature double channel modules. In addition, this TBE has got HART® Multiplexing capability by connection to GMI HART® Mux 5700 + TB(E)-D5001-HRT-003.
The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is used to supply GMI D5000 / D6000 series bus powered modules by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Application of TBE-D5016-TRI-001 with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon system AI cards

Safety Function and Failure behavior:

For each TBE channel, the 4-20 mA module output current is converted (by 250 Ohm on TBE) to 1-5 V voltage signal, which is read by Tricon system AI cards.

The TBE-D5016-TRI-001 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.

For each TBE channel, the failure behaviour is described by the following definitions:

□ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with shutdown of AI or Temperature module and its related safety loop (that is 0 mA output current equal to 0 V converted signal). For the safety loop, the fail-safe state is also given when AI or Temperature module output current is 0 mA, that is 0 V converted signal.

□ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.

□ Fail Dangerous: failure mode that does not respond to a demand from the process, so that AI or Temperature module output current is deviated more than 5% (0.8 mA) of full span, that is converted voltage signal is deviated more than 5% (0.2 V) of full span.

□ Fail High: failure mode that causes AI or Temperature module output current value > 20 mA, that is converted voltage signal value > 5 V.
  Assuming that the application program in the safety logic solver is configured to detect High failure, this failure has been classified as a dangerous detected (DD) failure.

□ Fail Low: failure mode that causes AI or Temperature module output current value < 4 mA, that is converted voltage signal value < 1 V.
  Assuming that the application program in the safety logic solver is configured to detect Low failure, this failure has been classified as a dangerous detected (DD) failure.

□ Fail "No Effect": failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure.
  When calculating the SFF, this failure mode is not taken into account.

□ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is part of the circuit diagram and is listed for completeness.
  When calculating the SFF, this failure mode is not taken into account.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.14
λ_{du} = Total Dangerous Undetected failures	0.06
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.82
$\lambda_{tot\ safe}$ **= Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$**	**1.02**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**112˙302 years**
$\lambda_{no\ effect}$ = "No effect" failures	86.38
$\lambda_{not\ part}$ = "Not Part" failures	146.20
$\lambda_{tot\ device}$ **= Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$**	**233.60**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**489 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.82 FIT	0.14 FIT	0.06 FIT	94.10%

When a TBE-D5016-TRI-001 channel operates in Low Demand mode:

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing system contributes ≤10% of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 2.64E-07 Valid for **SIL 3**	PFDavg = 5.29E-06 Valid for **SIL 3**

When a TBE-D5016-TRI-001 channel operates in High Demand mode:

PFH = λ_{du} = 0.06 E-09 h^{-1} - Valid for SIL 3.

SC3: Systematic capability SIL 3.

Testing procedure at T-proof

Application of TBE-D5016-TRI-001 with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon system AI cards
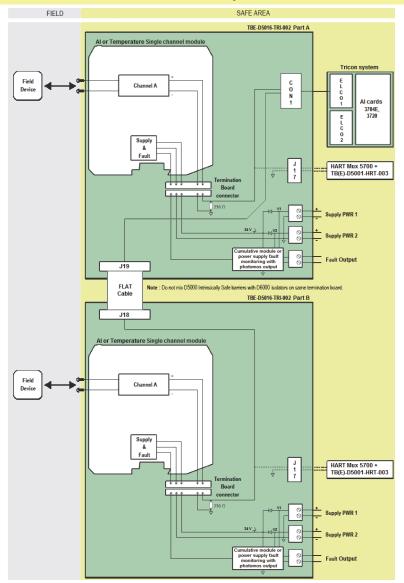
The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected fault, which have been noted during the FMEDA, can be revealed during proof test.

For each TBE channel, the 4-20 mA module output current is converted (by 250 Ohm on TBE) to 1-5 V voltage signal, which is read by Tricon system AI cards.

The Proof test consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	For each TBE channel, set the input current of AI module or the input signal of the Temperature module in order to go to high alarm module output current (> 20 mA) and verify that the converted output voltage signal of the TBE reaches a value > 5 V.
3	For each TBE channel, set the input current of AI module or the input signal of the Temperature module in order to go to low alarm module output current (< 4 mA) and verify that the converted output voltage signal of the TBE reaches a value < 1 V.
4	For each TBE channel, set the input current of AI module or the input signal of the Temperature module in order to impose some module output current values of the 4-20 mA range and verify that the correspondent converted output voltage signal values of the TBE are within the specified accuracy, that is less than 0.2 V respect to the correct values.
5	Restore each safety loop to full operation.
6	Remove the bypass from the safety-related PLC or restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the TBE.

Application of TBE-D5016-TRI-002 (Part A and Part B) with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon system AI cards

The diagram shows a single channel module on each TBE Part A or Part B.
On each TBE-D5016-TRI-002 Part A or Part B Termination Board can be installed up to 16 single channel modules for a maximum of 16 channels.
On a couple of TBE-D5016-TRI-002 Part A and Part B Termination Boards can be installed up to 16+16 single channel modules for a maximum of 32 channels.
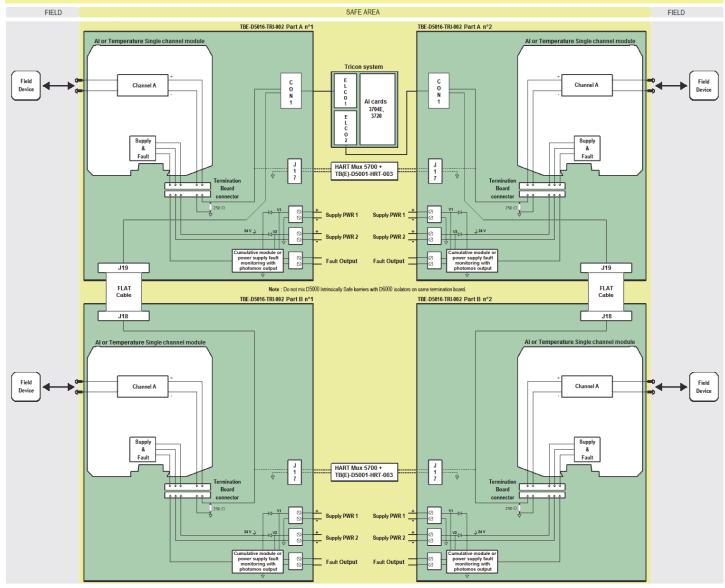
Application of TBE-D5016-TRI-002 (Part A and Part B) with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon system AI cards

The diagram shows a single channel module on each TBE Part A or Part B.
On each TBE-D5016-TRI-002 Part A or Part B Termination Board can be installed up to 16 single channel modules for a maximum of 16 channels.
On a double couple of TBE-D5016-TRI-002 Part A and Part B Termination Boards can be installed up to 2 x (16+16) single channel modules for a maximum of 64 channels.

Description:

The TBE-D5016-TRI-002 (Part A and Part B) Termination Boards provide direct connection between the Tricon system AI cards 3704E or 3720 and GMI D5000 / D6000 series AI or Temperature single channel modules. In addition, these TBE have got HART® Multiplexing capability by connection to GMI HART® Mux 5700 + TB(E)-D5001-HRT-003.
The 24 Vdc Power Supply of each TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is used to supply GMI D5000 / D6000 series bus powered modules by TB connectors. By these connectors, each TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

For each TBE Part A or Part B channel, the 4-20 mA module output current is converted (by 250 Ohm on TBE) to 1-5 V voltage signal, which is read by Tricon system AI cards.
The TBE-D5016-TRI-002 (Part A or Part B) is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.
For each TBE Part A or Part B channel, the failure behaviour is described by the following definitions:

□ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with shutdown of AI or Temperature module and its related safety loop (that is 0 mA output current equal to 0 V converted signal). For the safety loop, the fail-safe state is also given when AI or Temperature module output current is 0 mA, that is 0 V converted signal.

□ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.

□ Fail Dangerous: failure mode that does not respond to a demand from the process, so that AI or Temperature module output current is deviated more than 5% (0.8 mA) of full span, that is converted voltage signal is deviated more than 5% (0.2 V) of full span.

□ Fail High: failure mode that causes AI or Temperature module output current value > 20 mA, that is converted voltage signal value > 5 V.
  Assuming that the application program in the safety logic solver is configured to detect High failure, this failure has been classified as a dangerous detected (DD) failure.

□ Fail Low: failure mode that causes AI or Temperature module output current value < 4 mA, that is converted voltage signal value < 1 V.
  Assuming that the application program in the safety logic solver is configured to detect Low failure, this failure has been classified as a dangerous detected (DD) failure.

□ Fail "No Effect": failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure.
  When calculating the SFF, this failure mode is not taken into account.

□ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is 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.

Functional Safety Manual and Applications

Application of TBE-D5016-TRI-002 (Part A and Part B) with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon system AI cards

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.14
λ_{du} = Total Dangerous Undetected failures	0.06
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.82
$\lambda_{tot\ safe}$ = **Total Failure Rate (Safety Function)** = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**1.02**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**112˙302 years**
$\lambda_{no\ effect}$ = "No effect" failures	86.38
$\lambda_{not\ part}$ = "Not Part" failures	143.00
$\lambda_{tot\ device}$ = **Total Failure Rate (Device)** = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**230.40**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**495 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.82 FIT	0.14 FIT	0.06 FIT	94.10%

When a TBE-D5016-TRI-002 Part A or Part B channel operates in Low Demand mode:
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing system contributes ≤10% of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 2.64E-07 Valid for **SIL 3**	PFDavg = 5.29E-06 Valid for **SIL 3**

When a TBE-D5016-TRI-002 Part A or Part B channel operates in High Demand mode:
PFH = λ_{du} = 0.06 E-09 h^{-1} - **Valid for SIL 3.**

SC3: Systematic capability SIL 3.

Testing procedure at T-proof

Application of TBE-D5016-TRI-002 (Part A and Part B) with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon system AI cards
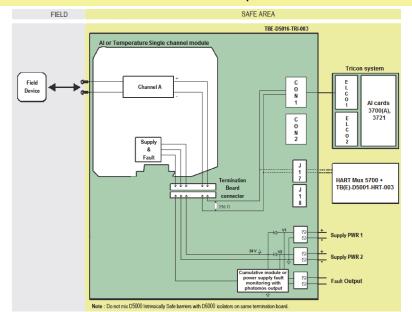
The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected fault, which have been noted during the FMEDA, can be revealed during proof test.
For each TBE channel, the 4-20 mA module output current is converted (by 250 Ohm on TBE) to 1-5 V voltage signal, which is read by Tricon system AI cards.
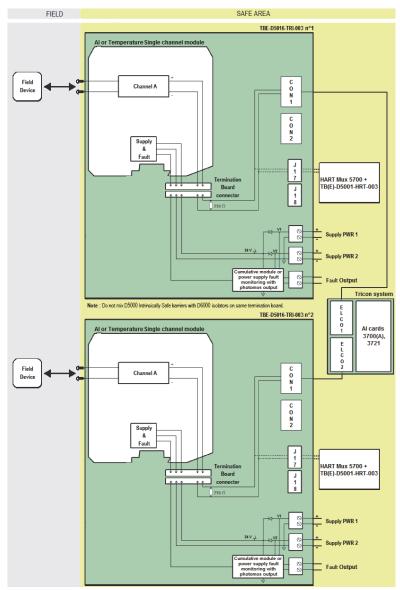**The Proof test** consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	For each TBE channel, set the input current of AI module or the input signal of the Temperature module in order to go to high alarm module output current (> 20 mA) and verify that the converted output voltage signal of the TBE reaches a value > 5 V.
3	For each TBE channel, set the input current of AI module or the input signal of the Temperature module in order to go to low alarm module output current (< 4 mA) and verify that the converted output voltage signal of the TBE reaches a value < 1 V.
4	For each TBE channel, set the input current of AI module or the input signal of the Temperature module in order to impose some module output current values of the 4-20 mA range and verify that the correspondent converted output voltage signal values of the TBE are within the specified accuracy, that is less than 0.2 V respect to the correct values.
5	Restore each safety loop to full operation.
6	Remove the bypass from the safety-related PLC or restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the TBE.

Application of TBE-D5016-TRI-003 with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon system AI cards
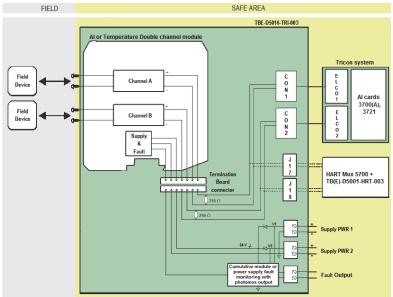

The diagram shows a single channel module on TBE. On a single TBE-D5016-TRI-003 Termination Board can be installed up to 16 single ch. modules for a maximum of 16 channels.

The diagram shows a single channel Module on each TBE.
On two TBE-D5016-TRI-003 Termination Boards can be installed up to 16+16 single channel modules for a maximum of 32 channels.

Application of TBE-D5016-TRI-003 with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon system AI cards

The diagram shows a double channel module on TBE. On a single TBE-D5016-TRI-003 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

Description:

The TBE-D5016-TRI-003 Termination Board provides direct connection between the Tricon system AI cards 3700, 3700A or 3721 and GMI D5000 / D6000 series AI or Temperature single or double channel modules. In addition, this TBE has got HART® Multiplexing capability by connection to GMI HART® Mux 5700 + TB(E)-D5001-HRT-003.

The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is used to supply GMI D5000 / D6000 series bus powered modules by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

For each TBE channel, the 4-20 mA module output current is converted (by 250 Ohm on TBE) to 1-5 V voltage signal, which is read by Tricon system AI cards.

The TBE-D5016-TRI-003 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.

For each TBE channel, the failure behaviour is described by the following definitions:

□ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with shutdown of AI or Temperature module and its related safety loop (that is 0 mA output current equal to 0 V converted signal). For the safety loop, the fail-safe state is also given when AI or Temperature module output current is 0 mA, that is 0 V converted signal.

□ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.

□ Fail Dangerous: failure mode that does not respond to a demand from the process, so that AI or Temperature module output current is deviated more than 5% (0.8 mA) of full span, that is converted voltage signal is deviated more than 5% (0.2 V) of full span.

□ Fail High: failure mode that causes AI or Temperature module output current value > 20 mA, that is converted voltage signal value > 5 V.
  Assuming that the application program in the safety logic solver is configured to detect High failure, this failure has been classified as a dangerous detected (DD) failure.

□ Fail Low: failure mode that causes AI or Temperature module output current value < 4 mA, that is converted voltage signal value < 1 V.
  Assuming that the application program in the safety logic solver is configured to detect Low failure, this failure has been classified as a dangerous detected (DD) failure.

□ Fail "No Effect": failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure.
  When calculating the SFF, this failure mode is not taken into account.

□ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is part of the circuit diagram and is listed for completeness.
  When calculating the SFF, this failure mode is not taken into account.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.26
λ_{du} = Total Dangerous Undetected failures	0.06
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.82
$\lambda_{tot\ safe}$ = **Total Failure Rate (Safety Function)** = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**1.14**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**100˙445 years**
$\lambda_{no\ effect}$ = "No effect" failures	86.26
$\lambda_{not\ part}$ = "Not Part" failures	152.40
$\lambda_{tot\ device}$ = **Total Failure Rate (Device)** = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**239.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**476 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.82 FIT	0.26 FIT	0.06 FIT	94.72%

When a TBE-D5016-TRI-003 channel operates in Low Demand mode:
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing system contributes ≤10% of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 2.65E-07 Valid for **SIL 3**	PFDavg = 5.31E-06 Valid for **SIL 3**

When a TBE-D5016-TRI-003 channel operates in High Demand mode:
PFH = λ_{du} = 0.06 E-09 h⁻¹ - Valid for SIL 3.

SC3: Systematic capability SIL 3.

Application of TBE-D5016-TRI-003 with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon system AI cards
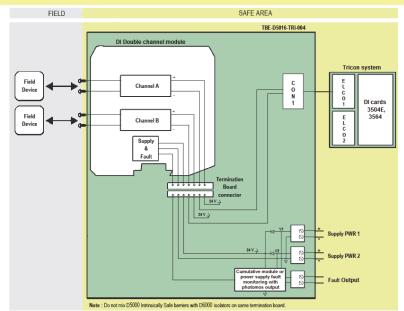
The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected fault, which have been noted during the FMEDA, can be revealed during proof test.

For each TBE channel, the 4-20 mA module output current is converted (by 250 Ohm on TBE) to 1-5 V voltage signal, which is read by Tricon system AI cards.
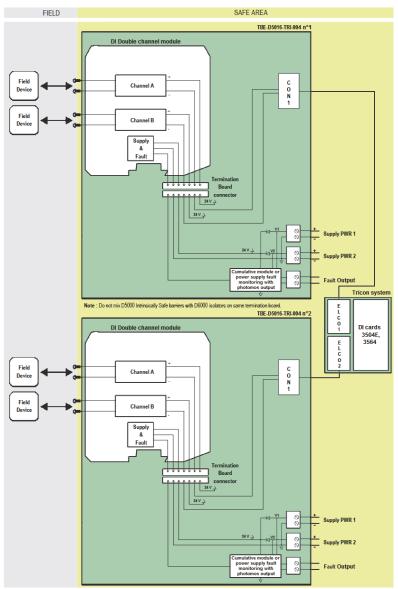
The Proof test consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	For each TBE channel, set the input current of AI module or the input signal of the Temperature module in order to go to high alarm module output current (> 20 mA) and verify that the converted output voltage signal of the TBE reaches a value > 5 V.
3	For each TBE channel, set the input current of AI module or the input signal of the Temperature module in order to go to low alarm module output current (< 4 mA) and verify that the converted output voltage signal of the TBE reaches a value < 1 V.
4	For each TBE channel, set the input current of AI module or the input signal of the Temperature module in order to impose some module output current values of the 4-20 mA range and verify that the correspondent converted output voltage signal values of the TBE are within the specified accuracy, that is less than 0.2 V respect to the correct values.
5	Restore each safety loop to full operation.
6	Remove the bypass from the safety-related PLC or restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the TBE.

Application of TBE-D5016-TRI-004 with GMI D5000/D6000 series DI modules for connection to Tricon system DI cards

The diagram shows a double channel module on TBE. On a single TBE-D5016-TRI-004 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

The diagram shows a double channel module on each TBE.
On two TBE-D5016-TRI-004 Termination Boards can be installed up to 16+16 double channel modules for a maximum of 64 channels.

Description:

The TBE-D5016-TRI-004 Termination Board provides direct connection between the Tricon system DI cards 3504E or 3564 and GMI D5000 / D6000 series DI double channel modules. The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is used to supply GMI D5000 / D6000 series bus powered modules by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Application of TBE-D5016-TRI-004 with GMI D5000/D6000 series DI modules for connection to Tricon system DI cards

Safety Function and Failure behavior:
For each TBE channel, the output voltage signal, read by Tricon system DI cards, can be:
1) high: about 24 Vdc;
2) low: 0 Vdc.
The TBE-D5016-TRI-004 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.
For each TBE channel, the failure behaviour is described by the following definitions:

▢ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with shutdown of DI module and its related safety loop (that is 0 V output signal).
About the safety loop, the fail-safe state is also 0 V output signal.

▢ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.

▢ Fail Dangerous: failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined Fail-Safe state), so that output voltage signal value is blocked to about 24 Vdc.

▢ Fail "No Effect": failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure.
When calculating the SFF, this failure mode is not taken into account.

▢ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is part of the circuit diagram and is listed for completeness.
When calculating the SFF, this failure mode is not taken into account.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.00
λ_{du} = Total Dangerous Undetected failures	0.00
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.82
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = λ_{dd} + λ_{du} + λ_{sd} + λ_{su}	**0.82**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**139'810 years**
$\lambda_{no\ effect}$ = "No effect" failures	86.38
$\lambda_{not\ part}$ = "Not Part" failures	140.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{no\ effect}$ + $\lambda_{not\ part}$	**227.20**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**502 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.82 FIT	0.00 FIT	0.00 FIT	100.00%

When a TBE-D5016-TRI-004 channel operates in Low Demand mode:
the **PFDavg (T[Proof] = 1 year) = 0**, considering λ_{du} and λ_{dd} absence.
Therefore, a TBE-D5016-TRI-004 channel has **SIL 3 level for product lifetime of 20 years.**

When a TBE-D5016-TRI-004 channel operates in High Demand mode:
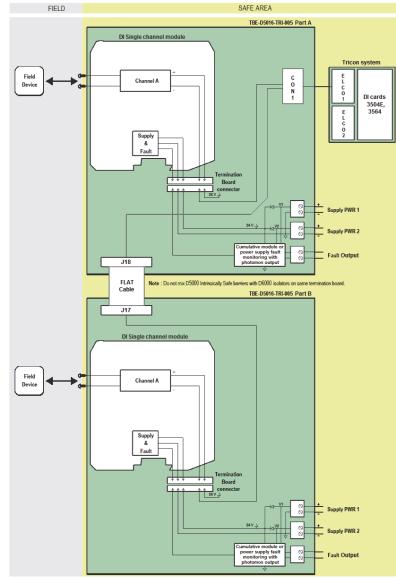the **PFH = 0 h^{-1} - Valid for SIL 3**, considering λ_{du} absence.

SC3: Systematic capability SIL 3.

Testing procedure at T-proof

Application of TBE-D5016-TRI-004 with GMI D5000/D6000 series DI modules for connection to Tricon system DI cards
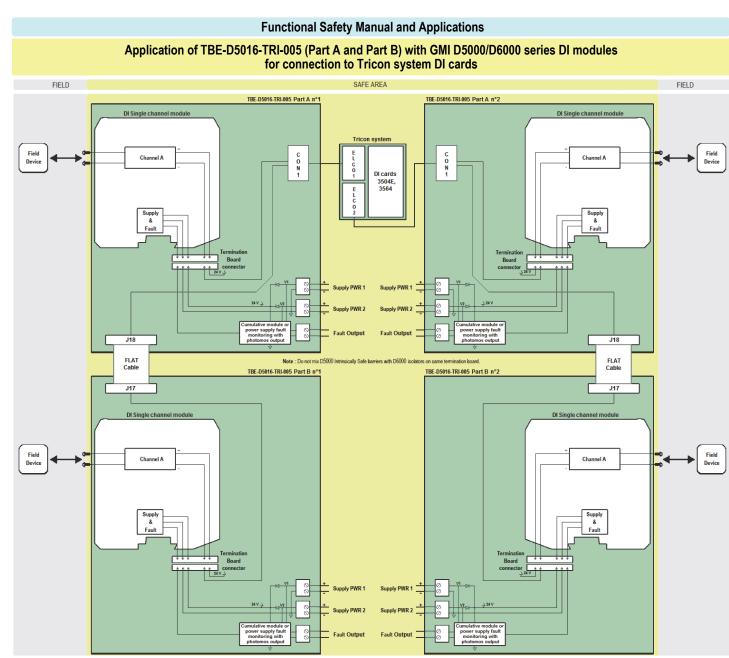
Since no dangerous undetected failures have been noted during the FMEDA analysis, there is no need to perform a proof test to reveal dangerous faults.

Application of TBE-D5016-TRI-005 (Part A and Part B) with GMI D5000/D6000 series DI modules for connection to Tricon system DI cards

The diagram shows a single channel module on each TBE Part A or Part B.
On each TBE-D5016-TRI-005 Part A or Part B Termination Board can be installed up to 16 single channel modules for a maximum of 16 channels.
On a couple of TBE-D5016-TRI-005 Part A and Part B Termination Boards can be installed up to 16+16 single channel modules for a maximum of 32 channels.

Application of TBE-D5016-TRI-005 (Part A and Part B) with GMI D5000/D6000 series DI modules for connection to Tricon system DI cards

The diagram shows a single channel module on each TBE Part A or Part B.
On each TBE-D5016-TRI-005 Part A or Part B Termination Board can be installed up to 16 single channel modules for a maximum of 16 channels.
On a double couple of TBE-D5016-TRI-005 Part A and Part B Termination Boards can be installed up to 2 x (16+16) single channel modules for a maximum of 64 channels.

Description:

The TBE-D5016-TRI-005 (Part A and Part B) Termination Boards provide direct connection between the Tricon system DI cards 3504E or 3564 and GMI D5000 / D6000 series DI single channel modules. The 24 Vdc Power Supply of each TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is used to supply GMI D5000 / D6000 series bus powered modules by TB connectors. By these connectors, each TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

For each TBE Part A or Part B channel, the output voltage signal, read by Tricon system DI cards, can be:
1) high: about 24 Vdc;
2) low: 0 Vdc.
The TBE-D5016-TRI-005 (Part A or Part B) is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.
For each TBE Part A or Part B channel, the failure behaviour is described by the following definitions:
☐ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with shutdown of DI module and its related safety loop (that is 0 V output signal).
  About the safety loop, the fail-safe state is also 0 V output signal.
☐ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.
☐ Fail Dangerous: failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined Fail-Safe state), so that output voltage signal value is blocked to about 24 Vdc.
☐ Fail "No Effect": failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure.
  When calculating the SFF, this failure mode is not taken into account.
☐ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is 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.

Functional Safety Manual and Applications

Application of TBE-D5016-TRI-005 (Part A and Part B) with GMI D5000/D6000 series DI modules for connection to Tricon system DI cards

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.00
λ_{du} = Total Dangerous Undetected failures	0.00
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.82
$\lambda_{tot\ safe}$ = **Total Failure Rate (Safety Function)** = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**0.82**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	139'810 years
$\lambda_{no\ effect}$ = "No effect" failures	86.38
$\lambda_{not\ part}$ = "Not Part" failures	140.00
$\lambda_{tot\ device}$ = **Total Failure Rate (Device)** = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**227.20**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**502 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.82 FIT	0.00 FIT	0.00 FIT	100.00%

When a TBE-D5016-TRI-005 Part A or Part B channel operates in Low Demand mode:
the **PFDavg (T[Proof] = 1 year) = 0**, considering λ_{du} and λ_{dd} absence.
Therefore, a TBE-D5016-TRI-005 channel has **SIL 3 level for product lifetime of 20 years.**

When a TBE-D5016-TRI-005 Part A or Part B channel operates in High Demand mode:
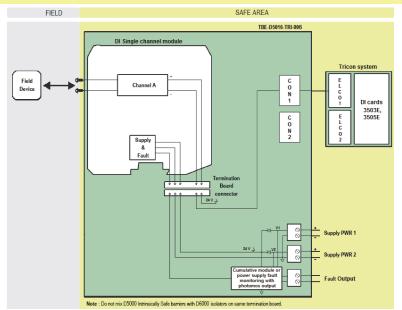the **PFH = 0 h^{-1} - Valid for SIL 3**, considering λ_{du} absence.

SC3: Systematic capability SIL 3.

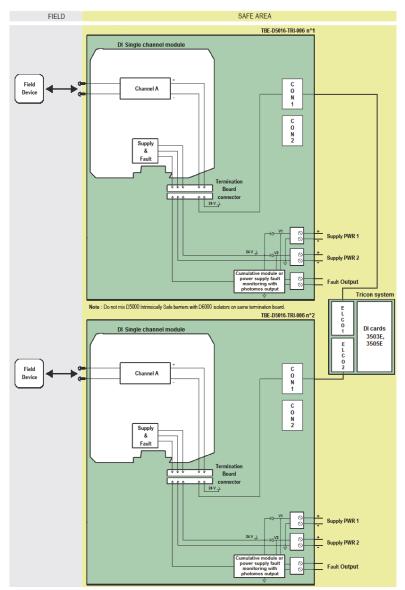## Testing procedure at T-proof

Application of TBE-D5016-TRI-005 (Part A and Part B) with GMI D5000/D6000 series DI modules for connection to Tricon system DI cards

Since no dangerous undetected failures have been noted during the FMEDA analysis, there is no need to perform a proof test to reveal dangerous faults.

Application of TBE-D5016-TRI-006 with GMI D5000/D6000 series DI modules for connection to Tricon system DI cards
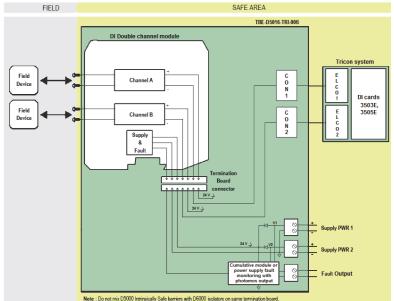

The diagram shows a single channel module on TBE. On a single TBE-D5016-TRI-006 Termination Board can be installed up to 16 single ch. modules for a maximum of 16 channels.

The diagram shows a single channel module on each TBE.
On two TBE-D5016-TRI-006 Termination Boards can be installed up to 16+16 single channel modules for a maximum of 32 channels.

Application of TBE-D5016-TRI-006 with GMI D5000/D6000 series DI modules for connection to Tricon system DI cards

The diagram shows a double channel module on TBE. On a single TBE-D5016-TRI-006 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

Description:

The TBE-D5016-TRI-006 Termination Board provides direct connection between the Tricon system DI cards 3503E or 3505E and GMI D5000 / D6000 series DI single or double channel modules. The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is used to supply GMI D5000 / D6000 series bus powered modules by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

For each TBE channel, the output voltage signal, read by Tricon system DI cards, can be:
1) high: about 24 Vdc;
2) low: 0 Vdc.
The TBE-D5016-TRI-006 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.
For each TBE channel, the failure behaviour is described by the following definitions:
 □ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with shutdown of DI module and its related safety loop (that is 0 V output signal).
   About the safety loop, the fail-safe state is also 0 V output signal.
 □ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.
 □ Fail Dangerous: failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined Fail-Safe state), so that output voltage signal value is blocked to about 24 Vdc.
 □ Fail "No Effect": failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure.
   When calculating the SFF, this failure mode is not taken into account.
 □ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is part of the circuit diagram and is listed for completeness.
   When calculating the SFF, this failure mode is not taken into account.
Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.00
λ_{du} = Total Dangerous Undetected failures	0.00
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.82
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**0.82**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**139'810 years**
$\lambda_{no\ effect}$ = "No effect" failures	86.18
$\lambda_{not\ part}$ = "Not Part" failures	140.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**227.00**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**503 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.82 FIT	0.00 FIT	0.00 FIT	100.00%

When a TBE-D5016-TRI-006 channel operates in Low Demand mode:
the **PFDavg (T[Proof] = 1 year) = 0**, considering λ_{du} and λ_{dd} absence.
Therefore, a TBE-D5016-TRI-006 channel has **SIL 3 level for product lifetime of 20 years.**

When a TBE-D5016-TRI-006 channel operates in High Demand mode:
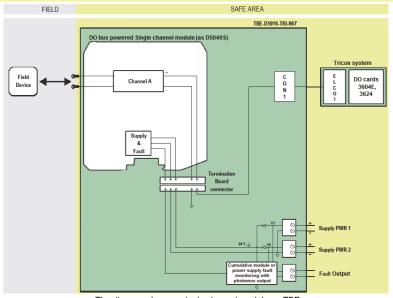the **PFH = 0 h^{-1} - Valid for SIL 3**, considering λ_{du} absence.

SC3: Systematic capability SIL 3.

Testing procedure at T-proof

Application of TBE-D5016-TRI-006 with GMI D5000/D6000 series DI modules for connection to Tricon system DI cards
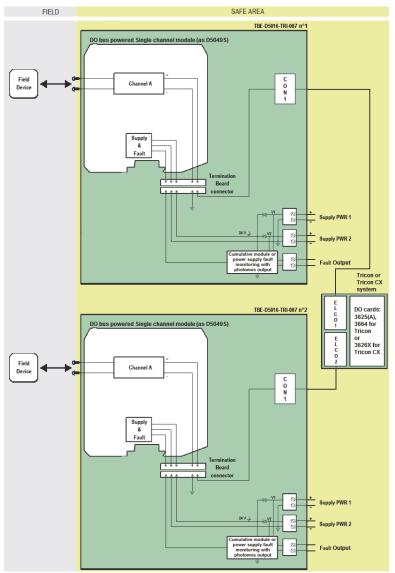
Since no dangerous undetected failures have been noted during the FMEDA analysis, there is no need to perform a proof test to reveal dangerous faults.

Application of TBE-D5016-TRI-007 with GMI D5000 series DO bus powered modules (as D5049S) for connection to Tricon or Tricon CX system DO cards, considering DTT safety loops

The diagram shows a single channel module on TBE.
When Tricon system DO card 3604E or 3624 is used, on a single TBE-D5016-TRI-007 Termination Board can be installed up to 16 single ch. modules for a maximum of 16 channels.

The diagram shows a single channel module on each TBE.
When Tricon system DO card 3625 or 3625A or 3664 is used or Tricon CX system DO card 3626X is used, on two TBE-D5016-TRI-007 Termination Boards can be installed up to 16+16 single channel modules for a maximum of 32 channels.

Functional Safety Manual and Applications

Application of TBE-D5016-TRI-007 with GMI D5000 series DO bus powered modules (as D5049S) for connection to Tricon or Tricon CX system DO cards, considering DTT safety loops

Description:

The TBE-D5016-TRI-007 Termination Board provides direct connection between the Tricon system DO cards 3604E or 3624 or 3625 or 3625A or 3664 *or* the Tricon CX system DO card 3626X and GMI D5000 series DO bus powered single channel modules (as D5049S). The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is used to supply GMI D5000 series bus powered modules by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

The TBE-D5016-TRI-007 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.

For each TBE channel or GMI D5000 series DO (as D5049S) bus powered module channel with DTT De-energized To Trip or DTS De-energized To Safe condition,

the failure behaviour is described by the following definitions:

□ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with shutdown of DO module and its related DTT safety loop.

□ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.

□ Fail Dangerous: failure mode that does not respond to a demand from the process, so that DO module output to remains energized.

□ Fail "No Effect": failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure. When calculating the SFF, this failure mode is not taken into account.

□ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is part of the circuit diagram and is listed for completeness. When calculating the SFF, this failure mode is not taken into account.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.00
λ_{du} = Total Dangerous Undetected failures	0.00
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.82
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**0.82**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**139`810 years**
$\lambda_{no\ effect}$ = "No effect" failures	86.18
$\lambda_{not\ part}$ = "Not Part" failures	134.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**221.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**515 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.82 FIT	0.00 FIT	0.00 FIT	100.00%

When a TBE-D5016-TRI-007 channel operates in Low Demand mode:

the **PFDavg (T[Proof] = 1 year) = 0**, considering λ_{du} and λ_{dd} absence.

Therefore, a TBE-D5016-TRI-007 channel has **SIL 3 level for product lifetime of 20 years.**

When a TBE-D5016-TRI-007 channel operates in High Demand mode:

the **PFH = 0 h^{-1} - Valid for SIL 3**, considering λ_{du} absence.
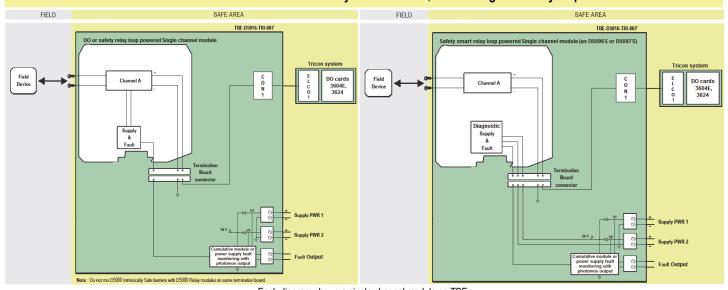
SC3: Systematic capability SIL 3.
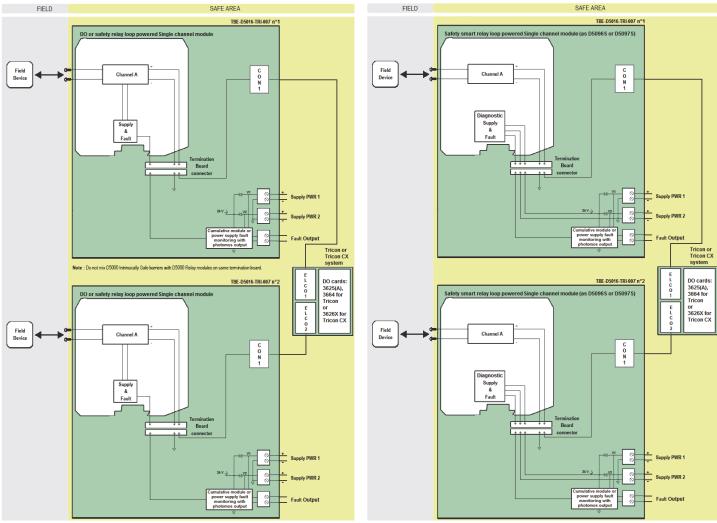
Testing procedure at T-proof

Application of TBE-D5016-TRI-007 with GMI D5000 series DO bus powered modules (as D5049S) for connection to Tricon or Tricon CX system DO cards, considering DTT safety loops

Since no dangerous undetected failures have been noted during the FMEDA analysis, there is no need to perform a proof test to reveal dangerous faults.

Application of TBE-D5016-TRI-007 with GMI D5000 series DO or safety relay loop powered modules for connection to Tricon or Tricon CX system DO cards, considering DTT safety loops

Each diagram shows a single channel module on TBE.
When Tricon system DO card 3604E or 3624 is used, on a single TBE-D5016-TRI-007 Termination Board can be installed up to 16 single ch. modules for a maximum of 16 channels.

Each diagram shows a single channel module on each TBE.
When Tricon system DO card 3625 or 3625A or 3664 is used or Tricon CX system DO card 3626X is used,
on two TBE-D5016-TRI-007 Termination Boards can be installed up to 16+16 single channel modules for a maximum of 32 channels.

**Application of TBE-D5016-TRI-007 with GMI D5000 series DO or safety relay loop powered modules
for connection to Tricon or Tricon CX system DO cards, considering DTT safety loops**

Description:

The TBE-D5016-TRI-007 Termination Board provides direct connection between the Tricon system DO cards 3604E or 3624 or 3625 or 3625A or 3664 *or* the Tricon CX system DO card 3626X and GMI D5000 series DO or safety relay loop powered single channel modules (or safety smart relay loop powered single channel modules as D5096S or D5097S).
The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is NOT used to supply GMI D5000 series DO or safety relay loop powered modules, but the 24 Vdc is only used to supply internal diagnostic circuits of the GMI D5000 series safety smart relay loop powered modules (as D5096S or D5097S) by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

The TBE-D5016-TRI-007 is considered a Type A system.
A shutdown of the TBE redundant power supply due to TBE internal component failures cannot influence each TBE channel or GMI D5000 series DO or safety (smart) relay loop powered module channel with DTT De-energized To Trip or DTS De-energized To Safe condition. Indeed, GMI D5000 series DO or safety relay loop powered modules are not supplied by the 24 Vdc Power Supply of the TBE. Instead, the internal diagnostic circuits of the GMI D5000 series safety smart relay loop powered modules (as D5096S or D5097S) are supplied by the 24 Vdc Power Supply of the TBE but the internal diagnostic circuits cannot influence on DTT safety loops of safety smart relay channels, therefore in case of shutdown of the TBE redundant power supply the internal diagnostic circuits are turned off but DTT safety loops are not influenced.
Finally, TBE internal component failures are only considered "Not Part" failures, described by the following definition:
□ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is part of the circuit diagram and is listed for completeness.
  When calculating the SFF, this failure mode is not taken into account.
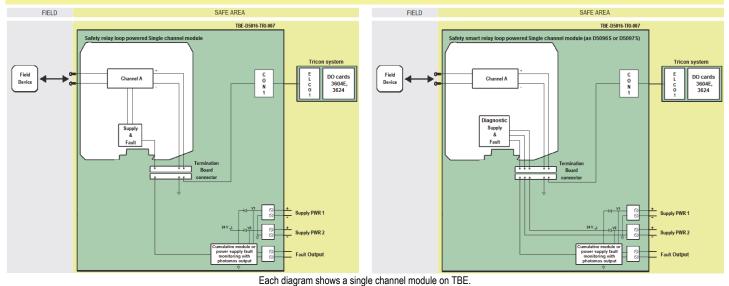Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

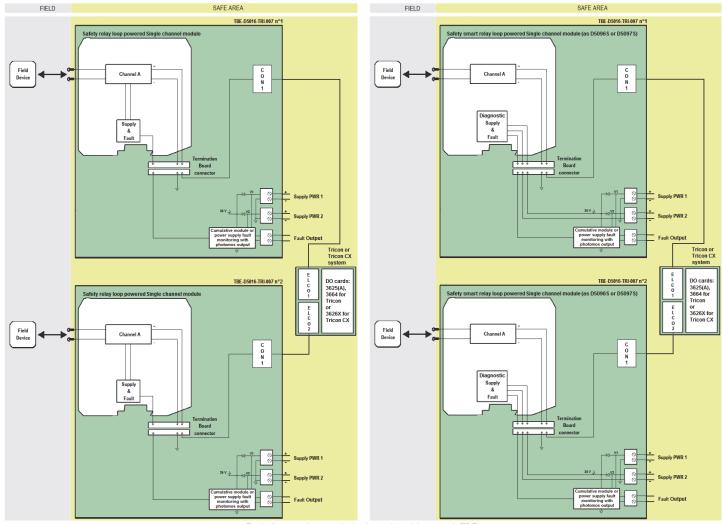| Failure category	Failure rates (FIT)
$\lambda_{not\ part}$ = "Not Part" failures	221.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{no\ effect}$ + $\lambda_{not\ part}$	**221.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**515 years**

Testing procedure at T-proof

**Application of TBE-D5016-TRI-007 with GMI D5000 series DO or safety relay loop powered modules
for connection to Tricon or Tricon CX system DO cards, considering DTT safety loops**

Since only no dangerous undetected failures have been noted during the FMEDA analysis, there is no need to perform a proof test to reveal dangerous faults.

Application of TBE-D5016-TRI-007 with GMI D5000 series safety relay loop powered modules for connection to Tricon or Tricon CX system DO cards, considering ETT safety loops

Each diagram shows a single channel module on TBE.
When Tricon system DO card 3604E or 3624 is used, on a single TBE-D5016-TRI-007 Termination Board can be installed up to 16 single ch. modules for a maximum of 16 channels.

Each diagram shows a single channel module on each TBE.
When Tricon system DO card 3625 or 3625A or 3664 is used or Tricon CX system DO card 3626X is used, on two TBE-D5016-TRI-007 Termination Boards can be installed up to 16+16 single channel modules for a maximum of 32 channels.

**Application of TBE-D5016-TRI-007 with GMI D5000 series safety relay loop powered modules
for connection to Tricon or Tricon CX system DO cards, considering ETT safety loops**

Description:

The TBE-D5016-TRI-007 Termination Board provides direct connection between the Tricon system DO cards 3604E or 3624 or 3625 or 3625A or 3664 *or* the Tricon CX system DO card 3626X and GMI D5000 series safety relay loop powered single channel modules (or safety smart relay loop powered single channel modules as D5096S or D5097S). The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is NOT used to supply GMI D5000 series safety relay loop powered modules, but the 24 Vdc is only used to supply internal diagnostic circuits of the GMI D5000 series safety smart relay loop powered modules (as D5096S or D5097S) by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

The TBE-D5016-TRI-007 is considered a Type A system.

A shutdown of the TBE redundant power supply due to TBE internal component failures cannot influence each TBE channel or GMI D5000 series safety (smart) relay loop powered module channel with ETT Energized To Trip or ETS Energized To Safe condition. Indeed, GMI D5000 series safety relay loop powered modules are not supplied by the 24 Vdc Power Supply of the TBE. Instead, the internal diagnostic circuits of the GMI D5000 series safety smart relay loop powered modules (as D5096S or D5097S) are supplied by the 24 Vdc Power Supply of the TBE but the internal diagnostic circuits cannot influence on ETT safety loops of safety smart relay channels, therefore in case of shutdown of the TBE redundant power supply the internal diagnostic circuits are turned off but ETT safety loops are not influenced.

Finally, TBE internal component failures are only considered "Not Part" failures, described by the following definition:

□ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is part of the circuit diagram and is listed for completeness.
   When calculating the SFF, this failure mode is not taken into account.

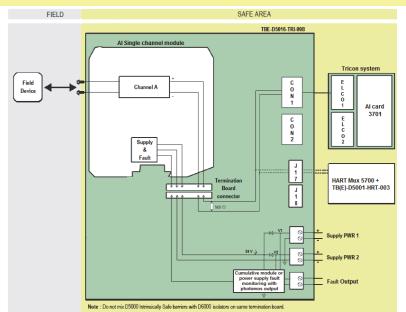Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

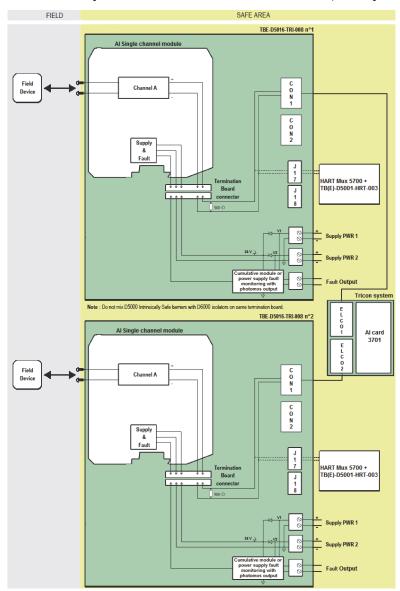| Failure category	Failure rates (FIT)
$\lambda_{not\ part}$ = "Not Part" failures	221.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{no\ effect}$ + $\lambda_{not\ part}$	**221.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**515 years**

Testing procedure at T-proof

**Application of TBE-D5016-TRI-007 with GMI D5000 series safety relay loop powered modules
for connection to Tricon or Tricon CX system DO cards, considering ETT safety loops**

Since only no dangerous undetected failures have been noted during the FMEDA analysis, there is no need to perform a proof test to reveal dangerous faults.

Application of TBE-D5016-TRI-008 with GMI D5000/D6000 series AI modules for connection to Tricon system AI cards
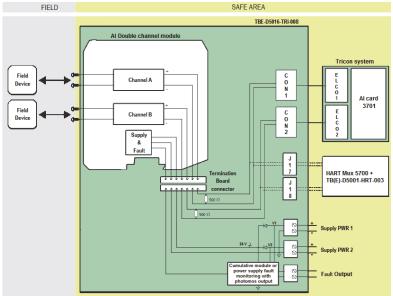

The diagram shows a single channel module on TBE. On a single TBE-D5016-TRI-008 Termination Board can be installed up to 16 single ch. modules for a maximum of 16 channels.

The diagram shows a single channel module on each TBE.
On two TBE-D5016-TRI-008 Termination Boards can be installed up to 16+16 single channel modules for a maximum of 32 channels.

Application of TBE-D5016-TRI-008 with GMI D5000/D6000 series AI modules for connection to Tricon system AI cards

The diagram shows a double channel module on TBE. On a single TBE-D5016-TRI-008 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

Description:

The TBE-D5016-TRI-008 Termination Board provides direct connection between the Tricon system AI card 3701 and GMI D5000 / D6000 series AI single or double channel modules. In addition, this TBE has got HART® Multiplexing capability by connection to GMI HART® Mux 5700 + TB(E)-D5001-HRT-003.

The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is used to supply GMI D5000 / D6000 series bus powered modules by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

For each TBE channel, the 4-20 mA module output current is converted (by 500 Ohm on TBE) to 2-10 V voltage signal, which is read by Tricon system AI cards.

The TBE-D5016-TRI-008 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.

For each TBE channel, the failure behaviour is described by the following definitions:

□ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with shutdown of AI module and its related safety loop (that is 0 mA output current equal to 0 V converted signal). For the safety loop, the fail-safe state is also given when AI module output current is 0 mA, that is 0 V converted signal.

□ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.

□ Fail Dangerous: failure mode that does not respond to a demand from the process, so that AI module output current is deviated more than 5% (0.8 mA) of full span, that is converted voltage signal is deviated more than 5% (0.4 V) of full span.

□ Fail High: failure mode that causes AI module output current value > 20 mA, that is converted voltage signal value > 10 V.
Assuming that the application program in the safety logic solver is configured to detect High failure, this failure has been classified as a dangerous detected (DD) failure.

□ Fail Low: failure mode that causes AI module output current value < 4 mA, that is converted voltage signal value < 2 V.
Assuming that the application program in the safety logic solver is configured to detect Low failure, this failure has been classified as a dangerous detected (DD) failure.

□ Fail "No Effect": failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure.
When calculating the SFF, this failure mode is not taken into account.

□ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is part of the circuit diagram and is listed for completeness.
When calculating the SFF, this failure mode is not taken into account.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.28
λ_{du} = Total Dangerous Undetected failures	0.12
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.82
$\lambda_{tot\ safe}$ = **Total Failure Rate (Safety Function)** = λ_{dd} + λ_{du} + λ_{sd} + λ_{su}	**1.22**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**93'839 years**
$\lambda_{no\ effect}$ = "No effect" failures	86.18
$\lambda_{not\ part}$ = "Not Part" failures	152.40
$\lambda_{tot\ device}$ = **Total Failure Rate (Device)** = $\lambda_{tot\ safe}$ + $\lambda_{no\ effect}$ + $\lambda_{not\ part}$	**239.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**476 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.82 FIT	0.28 FIT	0.12 FIT	90.14%

When a TBE-D5016-TRI-008 channel operates in Low Demand mode:

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing system contributes ≤10% of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 5.29E-07 Valid for **SIL 3**	PFDavg = 1.06E-05 Valid for **SIL 3**

When a TBE-D5016-TRI-008 channel operates in High Demand mode:
PFH = λ_{du} = 0.12 E-09 h^{-1} - Valid for SIL 3.

SC3: Systematic capability SIL 3.

Testing procedure at T-proof

Application of TBE-D5016-TRI-008 with GMI D5000/D6000 series AI modules for connection to Tricon system AI cards
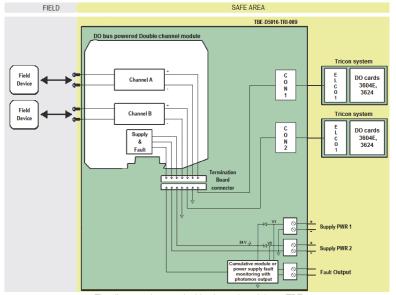
The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected fault, which have been noted during the FMEDA, can be revealed during proof test.

For each TBE channel, the 4-20 mA module output current is converted (by 500 Ohm on TBE) to 2-10 V voltage signal, which is read by Tricon system AI cards.

The Proof test consists of the following steps:

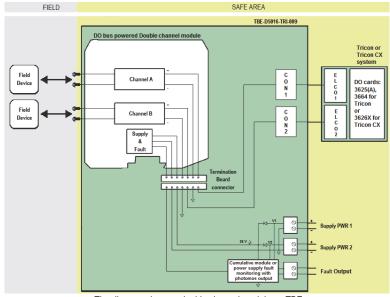| Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	For each TBE channel, set the input current of AI module in order to go to high alarm module output current (> 20 mA) and verify that the converted output voltage signal of the TBE reaches a value > 10 V.
3	For each TBE channel, set the input current of AI module in order to go to low alarm module output current (< 4 mA) and verify that the converted output voltage signal of the TBE reaches a value < 2 V.
4	For each TBE channel, set the input current of AI module in order to impose some module output current values of the 4-20 mA range and verify that the correspondent converted output voltage signal values of the TBE are within the specified accuracy, that is less than 0.4 V respect to the correct values.
5	Restore each safety loop to full operation.
6	Remove the bypass from the safety-related PLC or restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the TBE.

Application of TBE-D5016-TRI-009 with GMI D5000 series DO bus powered modules for connection to Tricon or Tricon CX system DO cards, considering DTT safety loops

The diagram shows a double channel module on TBE.

When Tricon system DO cards 3604E or 3624 are used, on a single TBE-D5016-TRI-009 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

The diagram shows a double channel module on TBE.

When Tricon system DO card 3625 or 3625A or 3664 is used or Tricon CX system DO card 3626X is used, on a single TBE-D5016-TRI-009 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

Description:

The TBE-D5016-TRI-009 Termination Board provides direct connection between the Tricon system DO cards 3604E or 3624 or 3625 or 3625A or 3664 *or* the Tricon CX system DO card 3626X and GMI D5000 series DO bus powered double channel modules. The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is used to supply GMI D5000 series bus powered modules by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

The TBE-D5016-TRI-009 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.

For each TBE channel or GMI D5000 series DO bus powered module channel with DTT De-energized To Trip or DTS De-energized To Safe condition,

the failure behaviour is described by the following definitions:

- □ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with shutdown of DO module and its related DTT safety loop.
- □ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.
- □ Fail Dangerous: failure mode that does not respond to a demand from the process, so that DO module output to remains energized.
- □ Fail "No Effect": failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure.
  When calculating the SFF, this failure mode is not taken into account.
- □ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is 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.

**Application of TBE-D5016-TRI-009 with GMI D5000 series DO bus powered modules
for connection to Tricon or Tricon CX system DO cards, considering DTT safety loops**

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.00
λ_{du} = Total Dangerous Undetected failures	0.00
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.82
$\lambda_{tot\ safe}$ = **Total Failure Rate (Safety Function)** = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**0.82**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**139'810 years**
$\lambda_{no\ effect}$ = "No effect" failures	86.18
$\lambda_{not\ part}$ = "Not Part" failures	134.80
$\lambda_{tot\ device}$ = **Total Failure Rate (Device)** = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**221.80**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**515 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.82 FIT	0.00 FIT	0.00 FIT	100.00%

When a TBE-D5016-TRI-009 channel operates in Low Demand mode:
the **PFDavg (T[Proof] = 1 year) = 0**, considering λ_{du} and λ_{dd} absence.
Therefore, a TBE-D5016-TRI-009 channel has **SIL 3 level for product lifetime of 20 years.**

When a TBE-D5016-TRI-009 channel operates in High Demand mode:
the **PFH = 0 h^{-1} - Valid for SIL 3**, considering λ_{du} absence.
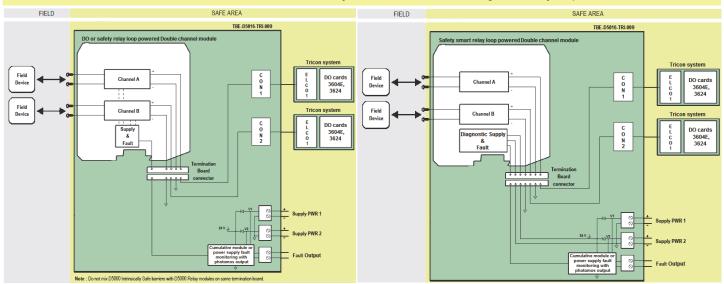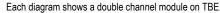
SC3: Systematic capability SIL 3.

Testing procedure at T-proof

**Application of TBE-D5016-TRI-009 with GMI D5000 series DO bus powered modules
for connection to Tricon or Tricon CX system DO cards, considering DTT safety loops**
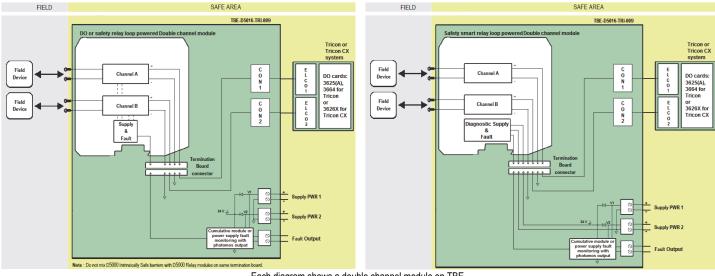
Since no dangerous undetected failures have been noted during the FMEDA analysis, there is no need to perform a proof test to reveal dangerous faults.

Application of TBE-D5016-TRI-009 with GMI D5000 series DO or safety relay loop powered modules for connection to Tricon or Tricon CX system DO cards, considering DTT safety loops

Each diagram shows a double channel module on TBE.
When Tricon system DO cards 3604E or 3624 are used, on a single TBE-D5016-TRI-009 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

Each diagram shows a double channel module on TBE.
When Tricon system DO card 3625 or 3625A or 3664 is used or Tricon CX system DO card 3626X is used, on a single TBE-D5016-TRI-009 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

Description: The TBE-D5016-TRI-009 Termination Board provides direct connection between the Tricon system DO cards 3604E or 3624 or 3625 or 3625A or 3664 **or** the Tricon CX system DO card 3626X and GMI D5000 series DO or safety relay loop powered double channel modules (or safety smart relay loop powered double channel modules). The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is NOT used to supply GMI D5000 series DO or safety relay loop powered modules, but the 24 Vdc is only used to supply internal diagnostic circuits of the GMI D5000 series safety smart relay loop powered modules by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:
The TBE-D5016-TRI-009 is considered a Type A system.
A shutdown of the TBE redundant power supply due to TBE internal component failures cannot influence each TBE channel or GMI D5000 series DO or safety (smart) relay loop powered module channel with DTT De-energized To Trip or DTS De-energized To Safe condition. Indeed, GMI D5000 series DO or safety relay loop powered modules are not supplied by the 24 Vdc Power Supply of the TBE. Instead, the internal diagnostic circuits of the GMI D5000 series safety smart relay loop powered modules are supplied by the 24 Vdc Power Supply of the TBE but the internal diagnostic circuits cannot influence on DTT safety loops of safety smart relay channels, therefore in case of shutdown of the TBE redundant power supply the internal diagnostic circuits are turned off but DTT safety loops are not influenced.
Finally, TBE internal component failures are only considered "Not Part" failures, described by the following definition:
  □ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is 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.
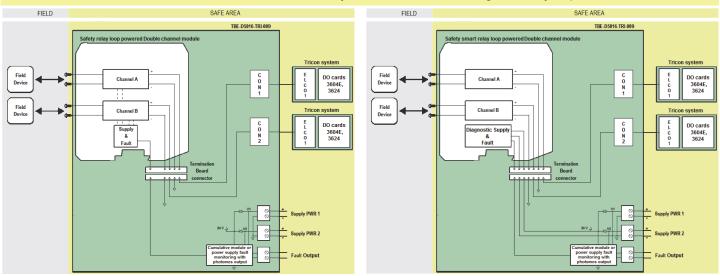
Failure rate table:

Failure category	Failure rates (FIT)
$\lambda_{not\ part}$ = "Not Part" failures	221.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{no\ effect}$ + $\lambda_{not\ part}$	221.80
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	515 years

Testing procedure at T-proof

Application of TBE-D5016-TRI-009 with GMI D5000 series DO or safety relay loop powered modules for connection to Tricon or Tricon CX system DO cards, considering DTT safety loops
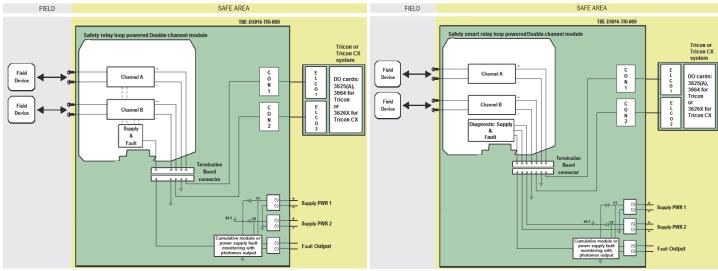
Since only no dangerous undetected failures have been noted during the FMEDA analysis, there is no need to perform a proof test to reveal dangerous faults.

Application of TBE-D5016-TRI-009 with GMI D5000 series safety relay loop powered modules for connection to Tricon or Tricon CX system DO cards, considering ETT safety loops

Each diagram shows a double channel module on TBE.

When Tricon system DO cards 3604E or 3624 are used, on a single TBE-D5016-TRI-009 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

Each diagram shows a double channel module on TBE.

When Tricon system DO card 3625 or 3625A or 3664 is used or Tricon CX system DO card 3626X is used, on a single TBE-D5016-TRI-009 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

Description: The TBE-D5016-TRI-009 Termination Board provides direct connection between the Tricon system DO cards 3604E or 3624 or 3625 or 3625A or 3664 *or* the Tricon CX system DO card 3626X and GMI D5000 series safety (smart) relay loop powered double channel modules. The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is NOT used to supply GMI D5000 series safety relay loop powered modules, but the 24 Vdc is only used to supply internal diagnostic circuits of the GMI D5000 series safety smart relay loop powered modules by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

The TBE-D5016-TRI-009 is considered a Type A system.

A shutdown of the TBE redundant power supply due to TBE internal component failures cannot influence each TBE channel or GMI D5000 series safety (smart) relay loop powered module channel with ETT Energized To Trip or ETS Energized To Safe condition. Indeed, GMI D5000 series safety relay loop powered modules are not supplied by the 24 Vdc Power Supply of the TBE. Instead, the internal diagnostic circuits of the GMI D5000 series safety smart relay loop powered modules are supplied by the 24 Vdc Power Supply of the TBE but the internal diagnostic circuits cannot influence on ETT safety loops of safety smart relay channels, therefore in case of shutdown of the TBE redundant power supply the internal diagnostic circuits are turned off but ETT safety loops are not influenced.

Finally, TBE internal component failures are only considered "Not Part" failures, described by the following definition:

□ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is 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.
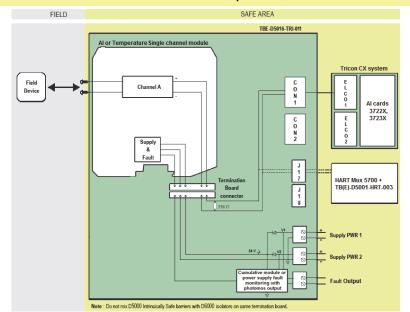
Failure rate table:

Failure category	Failure rates (FIT)
$\lambda_{not\ part}$ = "Not Part" failures	221.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe}$ + $\lambda_{no\ effect}$ + $\lambda_{not\ part}$	221.80
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	515 years

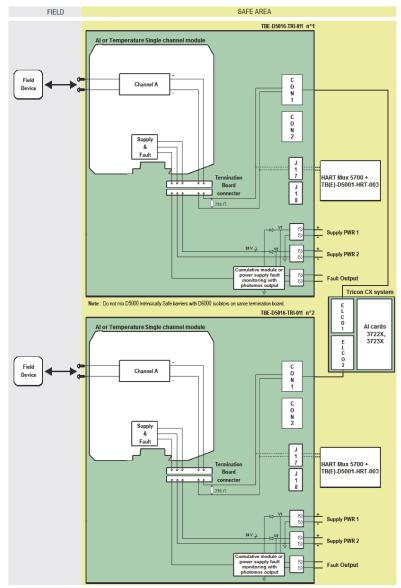### Testing procedure at T-proof

Application of TBE-D5016-TRI-009 with GMI D5000 series safety relay loop powered modules for connection to Tricon or Tricon CX system DO cards, considering ETT safety loops

Since only no dangerous undetected failures have been noted during the FMEDA analysis, there is no need to perform a proof test to reveal dangerous faults.

Application of TBE-D5016-TRI-011 with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon CX system AI cards
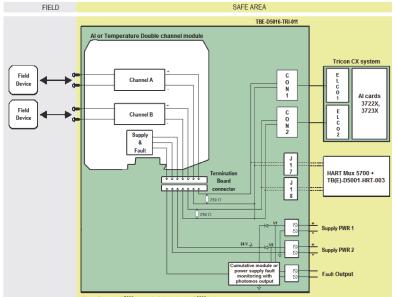

The diagram shows a single channel module on TBE. On a single TBE-D5016-TRI-011 Termination Board can be installed up to 16 single ch. modules for a maximum of 16 channels.

The diagram shows a single channel module on each TBE.
On two TBE-D5016-TRI-011 Termination Boards can be installed up to 16+16 single channel modules for a maximum of 32 channels.

Application of TBE-D5016-TRI-011 with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon CX system AI cards

The diagram shows a double channel module on TBE. On a single TBE-D5016-TRI-011 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

Description:

The TBE-D5016-TRI-011 Termination Board provides direct connection between the Tricon CX system AI cards 3722X or 3723X and GMI D5000 / D6000 series AI or Temperature single or double channel modules. In addition, this TBE has got HART® Multiplexing capability by connection to GMI HART® Mux 5700 + TB(E)-D5001-HRT-003.
The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is used to supply GMI D5000 / D6000 series bus powered modules by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

For each TBE channel, the 4-20 mA module output current is converted (by 250 Ohm on TBE) to 1-5 V voltage signal, which is read by Tricon CX system AI cards.
The TBE-D5016-TRI-011 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.
For each TBE channel, the failure behaviour is described by the following definitions:
  □ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with shutdown of AI or Temperature module and its related safety loop (that is 0 mA output current equal to 0 V converted signal). For the safety loop, the fail-safe state is also given when AI or Temperature module output current is 0 mA, that is 0 V converted signal.
  □ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.
  □ Fail Dangerous: failure mode that does not respond to a demand from the process, so that AI or Temperature module output current is deviated more than 5% (0.8 mA) of full span, that is converted voltage signal is deviated more than 5% (0.2 V) of full span.
  □ Fail High: failure mode that causes AI or Temperature module output current value > 20 mA, that is converted voltage signal value > 5 V.
    Assuming that the application program in the safety logic solver is configured to detect High failure, this failure has been classified as a dangerous detected (DD) failure.
  □ Fail Low: failure mode that causes AI or Temperature module output current value < 4 mA, that is converted voltage signal value < 1 V.
    Assuming that the application program in the safety logic solver is configured to detect Low failure, this failure has been classified as a dangerous detected (DD) failure.
  □ Fail "No Effect": failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure.
    When calculating the SFF, this failure mode is not taken into account.
  □ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is part of the circuit diagram and is listed for completeness.
    When calculating the SFF, this failure mode is not taken into account.
Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.26
λ_{du} = Total Dangerous Undetected failures	0.06
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.82
$\lambda_{tot\ safe}$ = **Total Failure Rate (Safety Function)** = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**1.14**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**100`445 years**
$\lambda_{no\ effect}$ = "No effect" failures	86.26
$\lambda_{not\ part}$ = "Not Part" failures	158.60
$\lambda_{tot\ device}$ = **Total Failure Rate (Device)** = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**246.00**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**464 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.82 FIT	0.26 FIT	0.06 FIT	94.72%

When a TBE-D5016-TRI-011 channel operates in Low Demand mode:
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing system contributes ≤10% of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 2.65E-07 Valid for **SIL 3**	PFDavg = 5.31E-06 Valid for **SIL 3**

When a TBE-D5016-TRI-011 channel operates in High Demand mode:
PFH = λ_{du} = 0.06 E-09 h^{-1} - Valid for SIL 3.

SC3: Systematic capability SIL 3.

Testing procedure at T-proof

Application of TBE-D5016-TRI-011 with GMI D5000/D6000 series AI or Temperature modules for connection to Tricon CX system AI cards
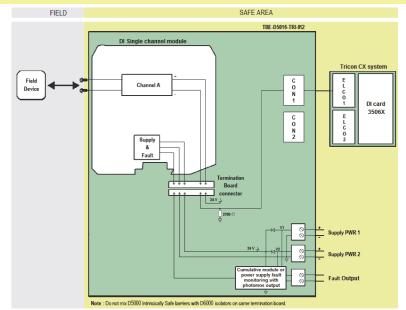
The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected fault, which have been noted during the FMEDA, can be revealed during proof test.

For each TBE channel, the 4-20 mA module output current is converted (by 250 Ohm on TBE) to 1-5 V voltage signal, which is read by Tricon CX system AI cards.

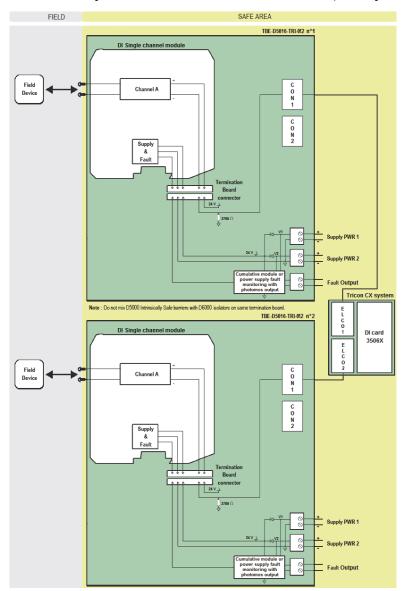**The Proof test** consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	For each TBE channel, set the input current of AI module or the input signal of the Temperature module in order to go to high alarm module output current (> 20 mA) and verify that the converted output voltage signal of the TBE reaches a value > 5 V.
3	For each TBE channel, set the input current of AI module or the input signal of the Temperature module in order to go to low alarm module output current (< 4 mA) and verify that the converted output voltage signal of the TBE reaches a value < 1 V.
4	For each TBE channel, set the input current of AI module or the input signal of the Temperature module in order to impose some module output current values of the 4-20 mA range and verify that the correspondent converted output voltage signal values of the TBE are within the specified accuracy, that is less than 0.2 V respect to the correct values.
5	Restore each safety loop to full operation.
6	Remove the bypass from the safety-related PLC or restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the TBE.

Application of TBE-D5016-TRI-012 with GMI D5000/D6000 series DI modules for connection to Tricon CX system DI cards
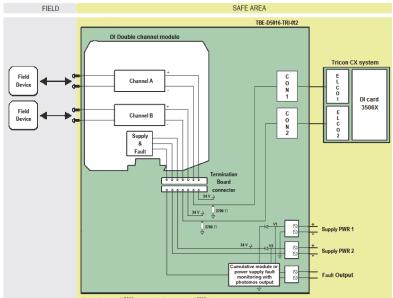

The diagram shows a single channel module on TBE. On a single TBE-D5016-TRI-012 Termination Board can be installed up to 16 single ch. modules for a maximum of 16 channels.

The diagram shows a single channel module on each TBE.
On two TBE-D5016-TRI-012 Termination Boards can be installed up to 16+16 single channel modules for a maximum of 32 channels.

Application of TBE-D5016-TRI-012 with GMI D5000/D6000 series DI modules for connection to Tricon CX system DI cards

The diagram shows a double channel module on TBE. On a single TBE-D5016-TRI-012 Termination Board can be installed up to 16 double ch. modules for a maximum of 32 channels.

Description:

The TBE-D5016-TRI-012 Termination Board provides direct connection between the Tricon CX system DI cards 3506X and GMI D5000 / D6000 series DI single or double channel modules. The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is used to supply GMI D5000 / D6000 series bus powered modules by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

For each TBE channel, the output voltage signal (on 2.7 kOhm), read by Tricon CX system DI cards, can be:
1) high: about 24 Vdc for generic DI module **OR** about 24 Vdc * (2.7 kOhm/(2.7 kOhm + RL)) for D5038**, D5039**, D6038** and D6039** modules;
2) low: 0 Vdc for generic DI module **OR** about 24 Vdc * (2.7 kOhm/(2.7 kOhm + RH)) for D5038**, D5039**, D6038** and D6039** modules.
The TBE-D5016-TRI-012 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.
For each TBE channel, the failure behaviour is described by the following definitions:
□ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with shutdown of DI module and its related safety loop (that is 0 V output signal).
   About the safety loop, the fail-safe state is also:
   1) 0 V output signal for generic DI module or for D5038**, D5039**, D6038** and D6039** modules;
   2) 24 Vdc for D5038**, D5039**, D6038** and D6039** modules.
   For D5038**, D5039**, D6038** and D6039** modules, the Tricon CX system DI card must monitor each safety loop in order to detect 0 V or 24 V output signal.
□ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.
□ Fail Dangerous: failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined Fail-Safe state), so that output voltage signal value is blocked to: 1) about 24 Vdc for generic DI module; 2) about 24 Vdc * (2.7 kOhm/(2.7 kOhm + RL)) for D5038**, D5039**, D6038** and D6039** modules.
□ Fail "No Effect": failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure.
   When calculating the SFF, this failure mode is not taken into account.
□ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is part of the circuit diagram and is listed for completeness.
   When calculating the SFF, this failure mode is not taken into account.
Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.00
λ_{du} = Total Dangerous Undetected failures	0.09
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.93
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**1.02**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**112'501 years**
$\lambda_{no\ effect}$ = "No effect" failures	86.39
$\lambda_{not\ part}$ = "Not Part" failures	152.40
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**239.81**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**476 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.93 FIT	0.00 FIT	0.09 FIT	91.18%

When a TBE-D5016-TRI-012 channel operates in Low Demand mode:
PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing system contributes ≤10% of total SIF dangerous failures:

T[Proof] = 1 year	T[Proof] = 20 years
PFDavg = 3.95E-07 Valid for **SIL 3**	PFDavg = 7.90E-06 Valid for **SIL 3**

When a TBE-D5016-TRI-012 channel operates in High Demand mode:
PFH = λ_{du} = 0.09 E-09 h^{-1} - Valid for SIL 3.

SC3: Systematic capability SIL 3.

Application of TBE-D5016-TRI-012 with GMI D5000/D6000 series DI modules for connection to Tricon CX system DI cards

The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected fault, which have been noted during the FMEDA, can be revealed during proof test.

For each TBE channel, the output voltage signal (on 2.7 kOhm), read by Tricon CX system DI cards, can be:

1) high: about 24 Vdc for generic DI module *OR*

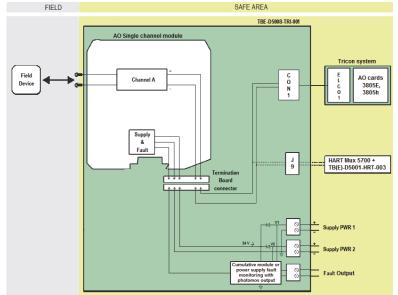about 24 Vdc * (2.7 kOhm/(2.7 kOhm + RL)) for D5038**, D5039**, D6038** and D6039** modules;

2) low: 0 Vdc for generic DI module *OR*

about 24 Vdc * (2.7 kOhm/(2.7 kOhm + RH)) for D5038**, D5039**, D6038** and D6039** modules.

The Proof test consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	For each TBE channel, vary the state conditions of the DI module input (for example open / closed input) in order to change correspondently the DI module output (for example open / closed output) and verify that the converted output voltage signal of the TBE reaches the correspondent value (for example 1)low / 2)high voltage as previously defined).
5	Restore each safety loop to full operation.
6	Remove the bypass from the safety-related PLC or restore normal operation.

This test will detect approximately 99 % of possible Dangerous Undetected failures in the TBE.

Application of TBE-D5008-TRI-001 with GMI D5000/D6000 series AO modules for connection to Tricon system AO cards

The diagram shows a single channel module on TBE. On a single TBE-D5008-TRI-001 Termination Board can be installed up to 8 single ch. modules for a maximum of 8 channels.

Description: The TBE-D5008-TRI-001 Termination Board provides direct connection between the Tricon system AO cards 3805E or 3805h and GMI D5000 / D6000 series AO single channel modules. In addition, this TBE has got HART® Multiplexing capability by connection to GMI HART® Mux 5700 + TB(E)-D5001-HRT-003.

The 24 Vdc Power Supply of the TBE is given by OR-ing diode mixing of two supply sources (PWR1 & PWR2) with related plug-in terminal blocks, for a redundant power supply with fault monitoring. The 24 Vdc is used to supply GMI D5000 / D6000 series bus powered modules by TB connectors. By these connectors, the TBE reads fault signals of modules and use them to give a cumulative module fault signalling, which is added to power supply fault monitoring to give a cumulative fault signal by a photomos fault output (normally closed in absence of fault, while open in presence of fault on PWR1 or PWR2 or at least a module).

Safety Function and Failure behavior:

The TBE-D5008-TRI-001 is considered a Type A system, having Hardware Fault Tolerance (HFT) = 0.

For each TBE channel, the failure behaviour is described by the following definitions:

- □ Fail-Safe State: it is defined as the redundant power supply going to 0 Vdc, with shutdown of AO module and its related safety loop (that is 0 mA output current).
- □ Fail Safe: failure mode that causes the system to go to the defined Fail-Safe state without a demand from the process.
- □ Fail Dangerous: failure mode that does not respond to a demand from the process, so that AO module output current is deviated more than 5% (0.8 mA) of full span.
- □ Fail High: failure mode that causes AO module output current value > 20 mA. This mode is considered a Dangerous Undetected failure.
- □ Fail Low: failure mode that causes AO module output current value < 4 mA. Assuming that the field I/P safety converter is configured to detect Low failure, this failure has been classified as a dangerous detected (DD) failure.
- □ Fail "No Effect": failure mode of a component that plays a part in implementing the Safety Function but that is neither a safe failure nor a dangerous failure. When calculating the SFF, this failure mode is not taken into account.
- □ Fail "Not part": failure mode of a component that is not part of the Safety Function but that is part of the circuit diagram and is listed for completeness. When calculating the SFF, this failure mode is not taken into account.

Failure rate data: taken from Siemens Standard SN29500.

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	0.00
λ_{du} = Total Dangerous Undetected failures	0.00
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.82
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**0.82**
MTBF (safety function, each channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**139'810 years**
$\lambda_{no\ effect}$ = "No effect" failures	86.18
$\lambda_{not\ part}$ = "Not Part" failures	140.00
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**227.00**
MTBF (device) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**503 years**

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

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF
0.00 FIT	0.82 FIT	0.00 FIT	0.00 FIT	100.00%

When a TBE-D5008-TRI-001 channel operates in Low Demand mode:

the **PFDavg (T[Proof] = 1 year) = 0**, considering λ_{du} and λ_{dd} absence.

Therefore, a TBE-D5008-TRI-001 channel has **SIL 3 level for product lifetime of 20 years.**

When a TBE-D5008-TRI-001 channel operates in High Demand mode:

the **PFH = 0 h^{-1} - Valid for SIL 3**, considering λ_{du} absence.

SC3: Systematic capability SIL 3.

Testing procedure at T-proof

Application of TBE-D5008-TRI-001 with GMI D5000/D6000 series AO modules for connection to Tricon system AO cards

Since no dangerous undetected failures have been noted during the FMEDA analysis, there is no need to perform a proof test to reveal dangerous faults.