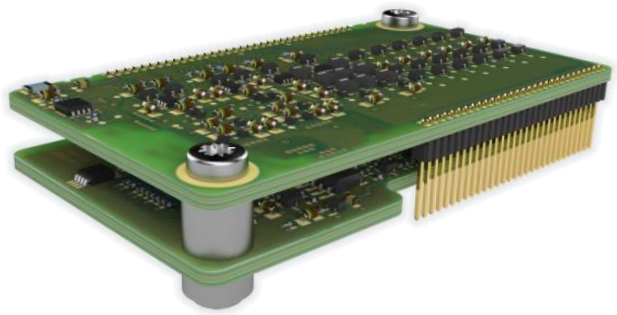
Safety Manual – Original Instructions

IXXAT Safe T100

Product Version 1.x



HMS Technology Center Ravensburg GmbH
Helmut-Vetter-Straße 2
88213 Ravensburg
Germany

Tel.: +49 751 56146-0
Fax: +49 751 56146-29
Internet: www.hms-networks.de
E-Mail: info-ravensburg@hms-networks.de

Support

In case of unsolvable problems with this product please contact HMS in written form by:

Fax: +49 751 56146-29
E-Mail: support@ixxat.de

Further international support contacts can be found on our webpage www.ixxat.com/support

Copyright

Registered trademarks

Document number: 1.04.0300.20000
Version: 2.8
Issue Date: 13.09.2016

1 Preface

When to Read and Use the Document

Whether you already have decided to develop an application with the IXXAT Safe T100 or not, you shall read this document as a first introduction on how to, as an integrator, make a safe hardware In-Design with the module or, as an end-user, use the T100 in a safety application. This safety manual also lists the necessary steps to be followed by the integrator (IDR-x) and the end-user (SAR-x) in order to get a simplified recertification of the safety functions of the T100 in a safety host and a safety application.

This document covers the generic implementation and use as well as the specific integration and use of the T100 running PROFIsafe with an Anybus CompactCom PROFINET module for example.

The Anybus CompactCom concept is further described in the Anybus CompactCom Software Design Guide and the Anybus CompactCom Hardware Design Guide (see section 1.2.1) which can be found at the support pages at www.anybus.com.

1.1 Important User Information

This document is intended to provide a good understanding of the generic properties of the IXXAT Safe T100 (T100). It contains information for the customer necessary for correct usage of the IXXAT Safe T100 in safety applications. It gives advice on how to integrate the IXXAT Safe T100 into a product with the target to get safe inputs and outputs and connect them to a system using for example PROFIsafe communication.

The reader of this document is expected to be familiar with hardware design and communication systems in general.

Knowledge of functional safety is required for the design, testing and certification process of the customer device.

Along with the information giving a better understanding of the T100,

this document contains safety relevant advice, that must be followed both by the integrator and by the end-user. These safety critical aspects are clearly marked with exclamation signs, ⚠ .

A full list of all safety advices can be found in appendix A and appendix B.

For more information, documentation etc., please visit the IXXAT web site, 'www.ixxat.com'.

1.1.1 T100 safety precautions

The T100 contains measures against a set of reasonably foreseeable misuse which is the use of a product, process or service in a way not intended by the supplier, but which may result from readily predictable human behavior. In addition the T100 is also prepared to deal with some malevolent or accidental misuse. As the end user is connecting sensors and actuators directly to the T100 there is a direct interaction and therefore a source of errors to be considered. The failures of IO modules are covered by measures described below in chapters “Digital Input, Semiconductor (DI-S)” (section 3.5.1.2), “Digital Input, Contact (DI-C)” (section 3.5.1.1) and “Digital Output (DO)” (section 3.5.3). Nevertheless, the Integrator and the end user has to think about all reasonably foreseeable misuse and malevolent or unauthorized actions that may result in his applications and check if the measures of the T100 are strong enough to detect and safely treat these error sources. [SC_344, SC_381]

1.1.2 Liability

Every care has been taken in the preparation of this manual. Please inform HMS Industrial Networks AB of any inaccuracies or omissions. The data and illustrations found in this document are not binding. We, HMS Industrial Networks AB, reserve the right to modify our products in line with our policy of continuous product development.

The information in this document is subject to change without notice and should not be considered as a commitment by HMS Industrial Networks AB. HMS Industrial Networks AB assumes no responsibility for any errors that may appear in this document.

There are many applications of this product. Those responsible for the use of this device must ensure that all the necessary steps have been taken to verify that the applications meet all performance and safety requirements including any applicable laws, regulations, codes, and standards.

HMS Industrial Networks AB will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features, timing, or functional side effects found outside the documented scope of this product. The effects caused by any direct or indirect use of such aspects of the product are undefined, and may include e.g. compatibility issues and stability issues.

The examples and illustrations in this document are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular implementation, HMS Industrial Networks AB cannot assume responsibility for actual use based on these examples and illustrations.

HMS will and cannot guarantee backwards compatibility for older applications, where not all recommendations, presented in the Anybus CompactCom Hardware Design Guide, have been followed.

1.1.3 Intellectual Property Rights

HMS Industrial Networks AB has intellectual property rights relating to technology embodied in the product described in this document. These intellectual property rights may include patents and pending patent applications in the US and other countries.

1.1.4 Trademark Acknowledgements

Anybus ® is a registered trademark of HMS Industrial Networks AB. All other trademarks are the property of their respective holders.

Warning: This is a class A product according to DIN EN 55022. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

ESD Note: This product contains ESD (Electrostatic Discharge) sensitive parts that may be damaged if ESD control procedures are not followed. Static control precautions are required when handling the product. Failure to observe this may cause damage to the product.

Warning: Improper handling of the T100 by the integrator can cause damage to the T100 and result in a loss of the safety functions. The T100 shall only be transported and handled in ESD protected areas, by specially trained personnel.

1.2 About This Document

For more information, documentation etc., please visit the HMS website, www.hms-networks.com.

1.2.1 Related and Additional Documents

Document	Doc. Id.	Author
Anybus CompactCom Hardware Design Guide	HMSI-168-31	HMS
Anybus CompactCom Software Design Guide	HMSI-168-97	HMS
Anybus CompactCom PROFINET User Manual	HMSI-168-49	HMS
PROFIsafe Profile Version 2.4	3.192b	PNO

A list of standards, relevant to this product, can be found in appendix C.

1.2.2 Document History

Revision	Date	Autor(s)	Chapter(s)	Description
2.5	2014-12-18	KrS	3.6.2, 9.1, 9.3, Appendix B	Integrated Review results of TÜV, Clarified SAR-5.4. Official Released document
2.6	2015-09-15	KrS	3.6.1, 4.1.5	Renamed chapter, clarified descriptions of IDR-4.1
2.8	2016-07-26	KrS	1.3.3	Added new valid product version and TÜV report. Replaced IXXAT GmbH by its legal successor HMS TC Ravensburg GmbH

1.2.3 Conventions & Terminology

The following conventions are used throughout this manual:

- The terms ‘T100’ or ‘module’ refer to the IXXAT Safe T100 in general which describes the safety-protocol independent properties.
- The term ‘T100/PS’ refers to the IXXAT Safe T100 module running the PROFIsafe (PS) safety protocol.
- The terms ‘host’ or ‘host application’ refer to the device that hosts the IXXAT Safe T100 and the Anybus CompactCom.

Danger - Violation of this precautionary measure leads to **severe injury, death or material-damage**.

Warning - Violation of this precautionary measure **probably** leads to **severe injury, death or material-damage**.

Attention - Violation of this precautionary measure **probably** leads to **minor injury or material-damage**.

- The terms ‘user’ or ‘end user’ refers to a person operating or handling the host to which the T100 is a subpart.
- The term integrator refers to a person, who integrates the T100 into a host and who is responsible for the safety certification of the entire host.
- In-design rules, marked with [IDR-x], shall be followed by the integrator when designing or integrating a safety device with the T100.
- Safety application rules marked with [SAR-x], shall be forwarded to the end- user by the integrator within its safety manual. [SAR-x] shall be

followed by the end user when operating the T100 within a safety application.

- Information necessary for the HMS-internal requirement tracking are labled with [PRS_x], [SC_x], [DR_x] or [HR_x].
- Numbered lists provide sequential steps.
- Bulleted lists provide information, not procedural steps.
- Hexadecimal values are written in the format NNNNh, where NNNN is the hexadecimal value.
-  This sign is used to mark safety relevant requirements or information which has to be fulfilled or considered by the host device.

In accordance with the ISO/IEC Directives, Part 2, Fifth Edition, 2004, the following verbal forms are used in this document with the following meanings:

- Requirements:

shall	is required
shall not	is not allowed, is not permitted

-Recommendations:

should	is recommended
should not	is not recommended

- Permissions:

may	is allowed
need not	is not required

- Possibility and capability:

can	is able, is possible
cannot	is not able, is not possible

1.2.4 Abbreviations

Word	Explanation
AIC	Anybus internal communication (protocol used to communicate between T100 and non-safe communication controller)
CDev	Customer Device – Device which integrates the T100 to fulfill a certain safety function
DI	Digital Input
DI-C	Digital Input – Contact
DIH	Digital Input High
DIL	Digital Input Low
DI-S	Digital Input – Semiconductor
DO	Digital Output
ESD	Electrostatic Discharge
FE	Functional Earth
FS	Fail-Safe
HFT	Hardware Fault Tolerance
I	Input
O	Output
PELV	Protected Extra Low Voltage
PL	Performance Level
PS	PROFIsafe
PSU	Power Supply Unit
PWR	Power
SC	Safety Controller
SELV	Safety Extra Low Voltage
SIL	Safety Integrity Level
T100	IXXAT Safe T100 (generic / protocol independent)
T100/PS	IXXAT Safe T100 for PROFIsafe
TO	Test Output
VSS	Negative supply voltage; equal to logic ground (GND) potential

1.3 Restrictions

1.3.1 Handling

This safety product shall be handled, operated, and maintained only by qualified personnel. Qualified personnel in the context of this safety manual are

- familiar with the basic safety concepts and regulations for safety and accident prevention.
- experienced in the field of safety applications to recognize or avoid dangerous situations.

1.3.2 Area of Application

The T100 shall only be used under the mechanical, electrical, and other environmental conditions described within this safety manual. A proper safe operation of the device is only given if all precautions for the T100 are considered during storage, transport, mounting, operation and maintenance.

Checking if specific safety sector norms are applicable for the use of the T100 shall be carried out by the integrator or end-user.

[IDR-1.1], [SAR-1.1] **Warning:** The T100 is designed to be used in the environment of industrial automation or process control systems. The T100 integrator and end-user shall check if the T100 is allowed to be used within the environment of the final application.

1.3.3 Validity of this Safety Manual

This safety manual is valid for the following HMS products:

- 1.01.0300.00000, IXXAT Safe T100/PS (Prototype – shall not be used for safety-related applications)
- 1.01.0300.00001, IXXAT Safe T100/PS Certified Product Version 1.0:
  Controller Board V1.3.1
  IO-Board V1.3.1
  Firmware V0.3.12 (Major SW Version: 0, Minor SW Version: 3, Build: 12)
  Bootloader V1.15
- 1.01.0300.00001, IXXAT Safe T100/PS Certified Product Version 1.1:
  Controller Board V1.3.1
  IO-Board V1.3.1
  Firmware V0.3.19 (Major SW Version: 0, Minor SW Version: 3, Build: 19)
  Bootloader V1.15

Other documents related to the integration of the T100 or the Anybus CompactCom as well as application notes can be found at www.hms-networks.com.

1.3.4 Service and Maintenance

The T100 itself does not contain any serviceable parts. Moreover it is not allowed to modify or repair the T100 in case of a hardware failure.

[IDR-1.2], [SAR-1.2] **Danger:** No repair or modification of the T100 is allowed.

[SAR-1.3] **Danger:** Safety critical T100 failures which do not lead to the safe state shall be reported to HMS/IXXAT immediately (see section 1.4).

1.3.5 End of Life

The maximum product life time (proof-test interval) of the T100, which allows a proper operation within the specified safety limits, is 20 years (see section 3.5). Please note the regulations for the disposal of electronic equipment after product end of life.

1.3.6 Disclaimer

HMS Industrial Networks is not liable and does not provide warranty for damages caused by

- violation of safety standards and rules
- non-observance of the safety notices described in this safety manual
- any modification to the T100 hardware device
- improper installation or use

1.4 Support

For more information on HMS and IXXAT products, FAQ lists and installation tips, please refer to the support area on the respective home pages, (http://www.hms-networks.com, http://www.ixxat.de).

There you will also find information on current product versions and available updates. For general contact information and where to find support, please refer to the contact and support pages at www.hms-networks.com or www.ixxat.de.

1.5 Returning Hardware

If it is necessary to return hardware, please download the relevant RMA form from the home page and follow the instructions on this form.

1.6 CE pre-testing

As the T100 is not considered to be a complete device or machine with respect to the machine directive, a CE compliance declaration is not possible. Anyway, the T100 was tested in an exemplary safety device to comply with the CE Rules.

Note: This equipment has been pre-tested and found to comply with the limits for a Class A digital device in accordance with DIN EN 55022. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in an industrial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

1.7 Information on EMC

The product is a class A device (DIN EN 55022) and therefore designed for the use in industrial environments only. If the product is used in office or home environment radio interference can occur under certain conditions.

For more details about the EMC-Test applied to the T100 refer to section 4.2.7 of this document.

1.8 Product change requests

Product change requests or any detected product error shall be reported to HMS using the contact form of the support web page under the URL www.ixxat.de/support.

2 General Description

2.1 Background

The need for safe transfer of data is steadily rising in large segments of the industry. Many companies are today looking into integrated safety which means that the standard non-safe communication network is also used for the safety-related data exchange. The demand for readymade solutions has grown, as not all customers have either the means or the time to develop solutions of their own.

2.2 IXXAT Safe T100

The IXXAT Safe T100 is a pre-certified embedded safety option module which provides device manufacturers with an easy and cost efficient way to integrate conformant safe I/O signals into standard automation devices. It connects via its serial black channel interface to an Anybus CompactCom module. The module provides digital safe I/O signals, controlled via the network and directly connected to the safety functions of an automation device.

The black channel is a transportation mechanism for safety related protocol extensions over a non-safe communication media. The safety layer performs safety related transmission functions and checks on the communication to ensure that the integrity of the link meets the requirement for use in a SIL 3 environment.

Figure 2-1 shows a typical example of an integrated safety communication solution. The black channel can be considered as a virtual link between the safety layers of the devices.

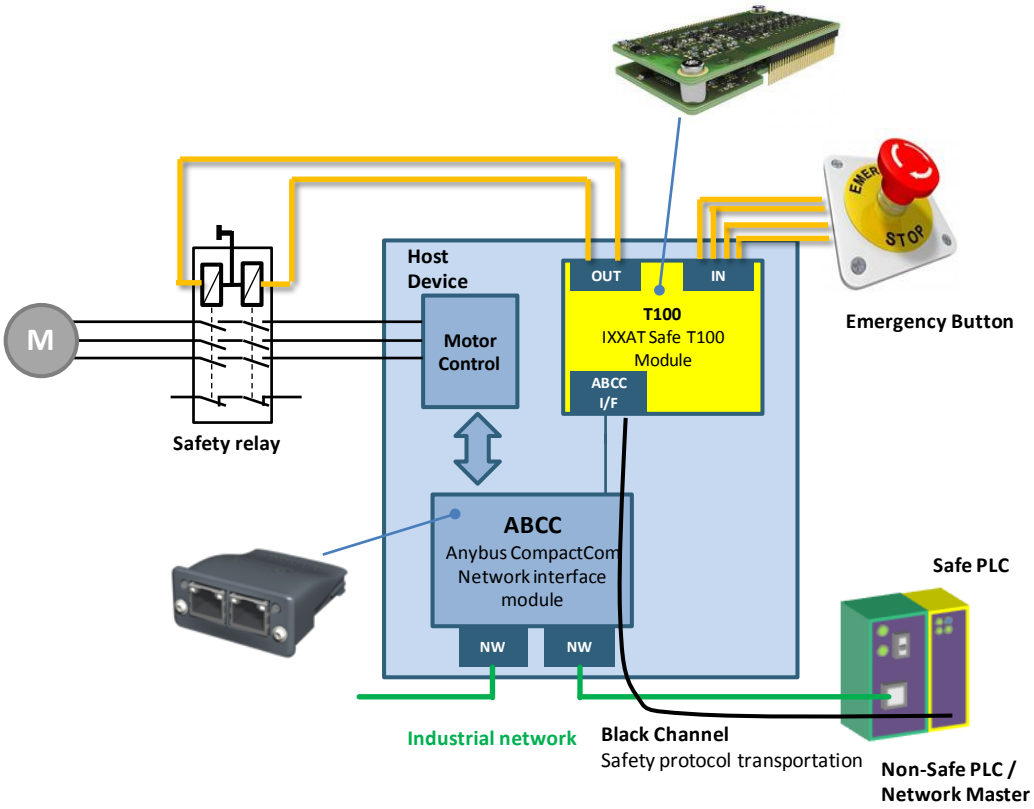


Figure 2-1: Architectural overview of a typical customer safety host device

- Safety: The IXXAT Safe T100 is developed in order to be suitable for use in applications up to Category 4 / PL e according to EN ISO 13849-1 and SIL 3 according to EN 62061 / IEC 61508.
- Mechanics: The IXXAT Safe T100 is an add-on PCB connected to the host device.
- Application: The IXXAT Safe T100 connects inputs and outputs in a safe way to the communication data bus.

In combination with other safe components and under the described conditions it is possible to obtain a certificate from a notified body for functional safety with limited efforts.

Features

- Safe communication protocol execution (e.g. PROFIsafe)
- Configurable 3 safe dual-channel (up to SIL 3, cat 4/PL e depending on configuration and external wiring) or 6 safe single-channel inputs (up to SIL 3, cat 2/PL d – depending on the configuration, external wiring and components)
- Configurable 1 safe dual-channel output (SIL 3, cat4/PL e, depending on configuration and external wiring)
- Possibility to connect active and / or passive inputs
- Compact size

2.3 The Black Channel Approach

It is possible to transmit safety messages on the existing standard bus cables in coexistence with the standard messages. Conventional and safety messages can be operated on one single bus cable including the use of standard PLCs with integrated but logically separated safety processing.

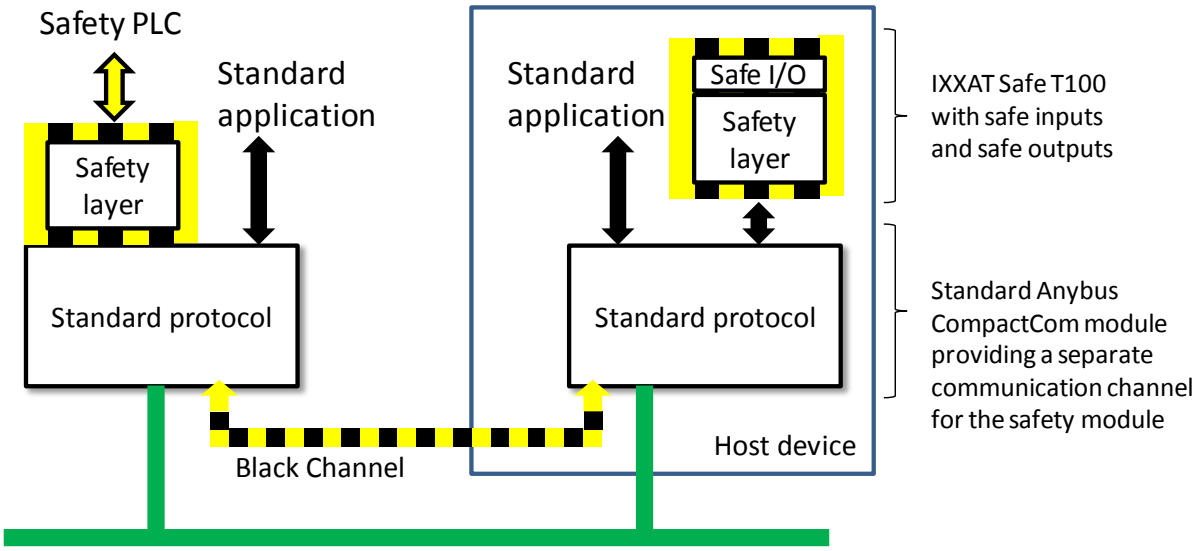


Figure 2-2: Black-channel approach

The safety protocol has no impact on the standard bus protocols. It doesn't matter what kind of physical transmission channel is used, nor transmission rates, nor error detection means. The message is embedded in a safety message and the safety protocol overtakes, for the users, the safety assessment of their individual backplane communication and also transmission paths beyond the original networks. It secures the whole path from the location where a safety signal originates to the location where it is processed and vice versa. The transmission channel acts as a Black Channel, where the user does not have to consider the underlying content.

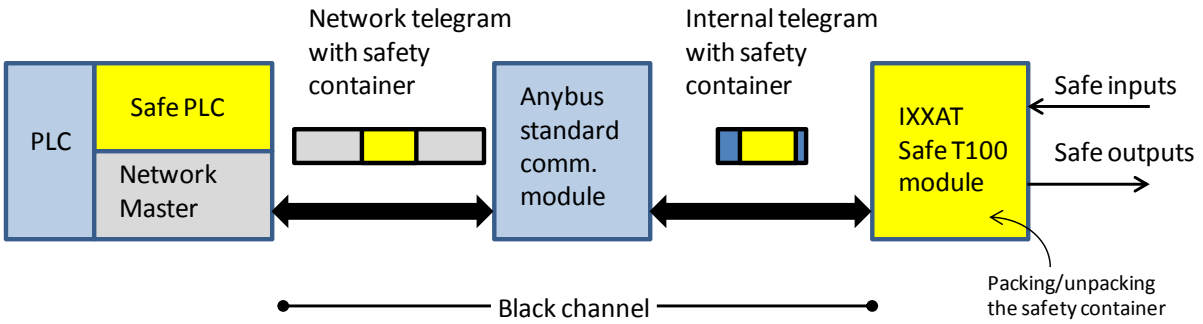


Figure 2-3: Safety container encapsulation

3 T100 operation

3.1 Overview

The T100 includes all necessary features in soft- and hardware to operate safe digital inputs and outputs. Beside a detailed FMEDA (Failure Mode Effect and Diagnosis Analysis) of the hardware during the design phase, a permanent checking of the digital input and output sections as well as of the processor units during runtime of the T100 takes place. Any fault detected during runtime will cause the T100 to enter the fail-safe state.

[SAR-3.1] **Attention:** There is no galvanic isolation between the digital inputs, the digital outputs and the T100 board electronic itself.

3.2 Safety Functions

1. The status of the digital inputs (DI-C, DI-S) is reported via a safety output telegram to the safe communication network. Only if the status of the input is “active” and no failure in the input circuit has been detected, the safety telegram to the PLC will report the input data as “active”.

2. The outputs (DO) of the T100 can be controlled via the safety communication network protocol. Only if the nominal value of the input telegram (to the T100) is "active" and no failure in the transfer of the safety telegram (F-telegram) from the PLC has been detected, the output (DO) may be set to active.

3. Any severe fault detected during runtime will cause the T100 to enter the fail-safe state and to turn off the digital outputs as well as to stop the communication via the safety fieldbus protocol. In case of channel-specific errors the T100 deactivates the channel, i.e. set the output to the inactive state or set the status of the input data reported via the safety fieldbus to inactive.

3.3 Pinning

The T100 is designed as an add-on module for easy integration into customer safety devices. The only electrical connectivity between the customer device and the T100 is done using a 30-Pin male connector (see Figure 3-1 and the table below).

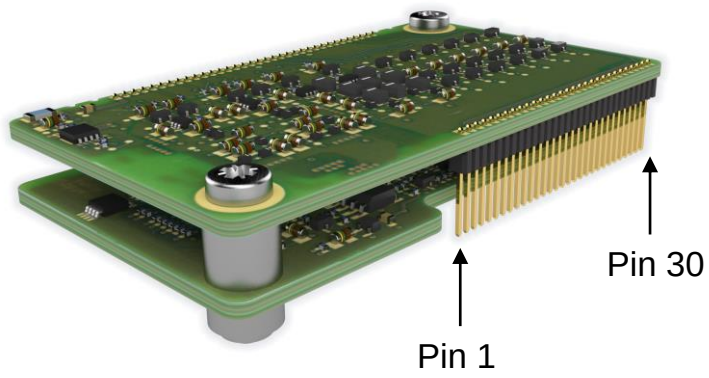


Figure 3-1: IXXAT Safe T100 Module

Pin No.	Signal Name	Type	Description
1,2	24V	PWR	24 V DC (SELV/PELV) power supply from external source
3,4	VSS	PWR	Power ground reference
5,6	DO 1	O	Digital Output 1
7,8	DO 2	O	Digital Output 2
9	VSS	PWR	Power ground reference
10	TO1	O	Test Output 1. Power supply provided by T100 to external sensors
11	TO2	O	Test Output 2. Power supply provided by T100 to external sensors
12	N.C.	PWR	External connection to VSS
13	DI1	I	Digital Input 1
14	N.C.	PWR	External connection to VSS
15	DI2	I	Digital Input 2
16	N.C.	PWR	External connection to VSS
17	DI3	I	Digital Input 3
18	N.C.	PWR	External connection to VSS
19	DI4	I	Digital Input 4
20	N.C.	PWR	External connection to VSS

21	DI5	I	Digital Input 5
22	N.C.	PWR	External connection to VSS
23	DI6	I	Digital Input 6
24	N.C.	PWR	External connection to VSS
25	EXT_0V	PWR	Communication bus interface ground
26	EXT_3V3	PWR	3.3 V DC power supply from external source for the communication bus interface and the reset line.
27	RX	I	Communication bus interface
28	Tx	O	Communication bus interface
29	N.C.	PWR	External connection to VSS
30	$\overline{\text{RST}}$	I	Reset (active low signal)

I: Input
O: Output
PWR: Power
N.C. Not connected

3.4 Power Supply

The following list shows the T100 connector pins relevant for the connection of the external power sources.

Signal Name	Type	Pin No.	Description
24V	PWR	1,2	24 V DC (SELV/PELV) power supply from external source
VSS	PWR	3,4,9	Power ground reference
EXT_3V3	PWR	26	3.3 V DC power supply from external source for the communication bus and the reset line.
EXT_0V	PWR	25	communication bus interface ground
N.C.	PWR	12,14, 16,18,20,22, 24,29	Must be externally connected to power ground reference VSS

[IDR-3.1] **Attention:** The unconnected pins (N.C.) of the T100 connector shall be connected to the SELV/PELV ground VSS.

3.4.1 Voltage Levels and Power Consumption, 24V

The T100 has to be supplied by a 24V DC SELV/PELV[1] supply voltage [HR_90]. According to IEC61131-2 the supply voltage shall be 24V DC -20%/+25% [HR_158]. Reference levels for the external power supply (24V) are given below [2].

Parameter	Unit	Min	Typ.	Max
Power supply (24V) DC	V	19.2	24	30
P_{tot}	W	1.5	30	60

[1]See EN60950-1, §2.2. The voltage must not exceed 60V DC under normal and single-fault conditions.

A SELV circuit must have protective-separation (reinforced insulation or protective screening) from all circuits other than SELV/PELV and a simple separation from other SELV/PELV systems and ground.

A PELV circuit requires protective-separation from all circuits other than SELV/PELV (i.e., all circuits that might carry higher voltages), but it may have connections to other PELV systems and ground.

[2] EN 61131-2, table 6

The IXXAT Safe T100 internal power consumption at 24 V does not exceed 1.5 W. Note that a destructive fuse limits the T100 internal current to a maximum of 2 A. The digital outputs and the test outputs of the T100 are directly driven from the (non-fused) 24V SELV/PELV input.
The external power consumption for each of the digital outputs shall not exceed the following ratings when being connected to external devices:

- I_{max_DO} = 500 mA (see section 3.5.3)
- P_{max_DO} = 15 W

The test outputs shall not exceed

- I_{max_TO} = 100 mA (see section 3.5.2)

[IDR-3.2] **Warning:** The 24V signal shall be connected to pin 1 and 2 of the T100 connector.

[IDR-3.3] **Danger:** The VSS signal (24V ground) shall be connected to pin 3, 4 and 9 of the T100 connector. [HR_342]

[IDR-3.4] **Warning:** The VSS signal (24V ground) shall be connected to pin 12, 14, 16, 18, 20, 22, 24 and 29 of the T100 connector to detect connector errors (cross-connections between neighbor signal pins).

[IDR-3.5], [SAR-3.2] **Danger:** The T100 shall be supplied by a 24V SELV/PELV power supply according to EN60950-1 [DR_C_HW_POW, DR_I_POW] which limits the maximum voltage in case of a failure to 60V. [PRS_107], [HR_158]

[IDR-3.6], [SAR-3.3] **Warning:** The maximum constant supply voltage of 30V shall not be exceeded in order to avoid permanent damage of the T100.

No specific buffer capacitors at the 24V input are necessary to guarantee the safe operation of the T100. Upon power loss, under voltage or power dips the T100 enters automatically the fail-safe state.

3.4.2 Reverse Battery Protection, 24V

The T100 **does not** include a reverse battery protection. Therefore an external protection circuit as shown in Figure 3-2 shall be implemented on the customer device. The reverse battery protection circuit itself needs not to be considered and designed as a safety critical circuit. Nevertheless, it prevents the T100 to get irreversibly damaged in case of reverse battery connection.

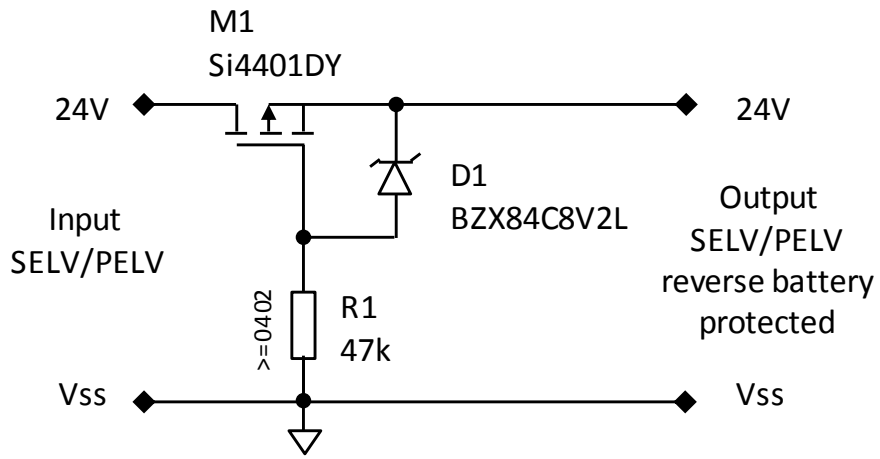


Figure 3-2: Reverse battery protection circuit example

[IDR-3.7] **Warning:** The customer device shall include a reverse battery protection circuit if the CDev does not generate the 24V DC supply internally. [SC_425]
[Reverse power connection can be excluded by design when using an internal power supply as no change to the internal power supply chain is assumed to be done in the field]

[SAR-3.4] **Danger:** The proper operation of the reverse battery protection circuit shall be tested whenever the power supply chain of the T100 is changed. This test shall be part of the initial safety machine operation tests where all safety functions shall be tested at least once. Changes to the power supply during runtime are not allowed without explicit re-testing of the overall safety function.

3.4.3 EMC Protection, 24V

3.4.3.1 Clamp Diode

To withstand the enhanced EMC requirements for safety devices, an external suppressor diode shall be placed between the 24V and the VSS signal of the T100 on the customer device. It is recommended that this suppressor diode shall be a 5 KW type such as 5.0SMDJ33CA for example.

[IDR-3.8] **Warning:** An external suppressor diode shall be present on the customer device between 24V and VSS. To withstand the EMC tests of the entire customer device at least a 5KW type shall be chosen.

3.4.3.2 HF filter

To increase the immunity against ESD distortions coming from the T100 power supply connection, special coupling capacitors shall be added to the CDev.

[IDR-3.9] **Warning:** The CDev shall provide a functional earth (FE) connection.

[IDR-3.10] **Warning:** To dissipate high frequent ESD pulses a 1,5 nF (10%, 2kV) capacitor shall be placed between the 24V SELV/PELV and the FE connection as well as between the VSS and the FE connection on the CDev.

Figure 3-3 shows an example circuit which can be used to protect the T100 from reverse battery powering and which gives protection against increased EMC levels at the power supply pins of the T100.

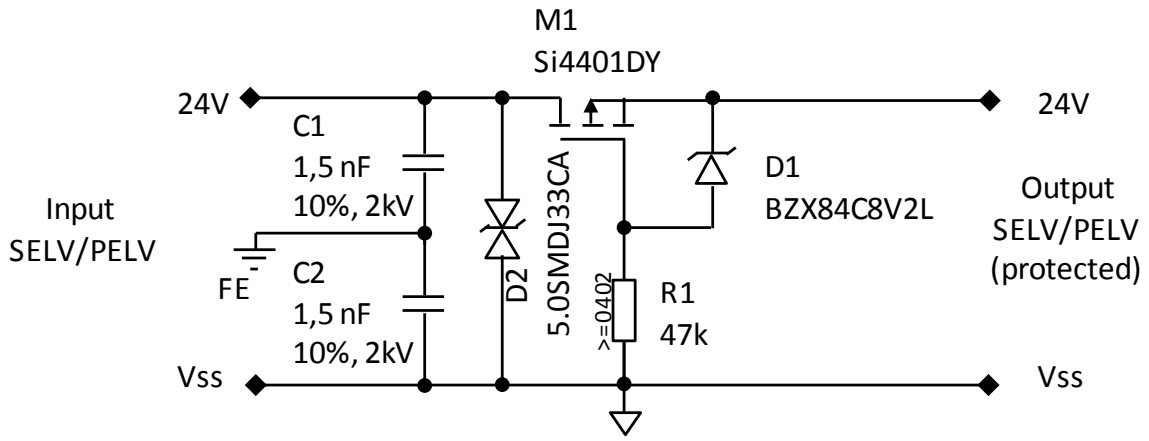


Figure 3-3: Complete CDev power supply protection circuits

3.4.4 Voltage Levels and Power Consumption, EXT_3V3

The external voltage EXT_3V3 for the communication bus has to be provided by the host device [HR_90]. This voltage source is used for the communication interface and the external reset signal only.

Parameter	**Unit**	**Min**	**Typ.**	**Max**
Power supply (3.3 V) DC	V	2.5	3.3	3.4
Current consumption	mA	-	11	25

A destructive fuse limits the current to a maximum of 50 mA.

3.4.5 Ground Concept

[IDR-3.11] **Warning:** All input and output signals of the T100 refer to the ground Signal VSS. The ground VSS is not supplied to the output loads by the T100, i.e. the inputs and outputs must be connected with low impedance externally to the VSS ground level. [SC_406], [HR_225]

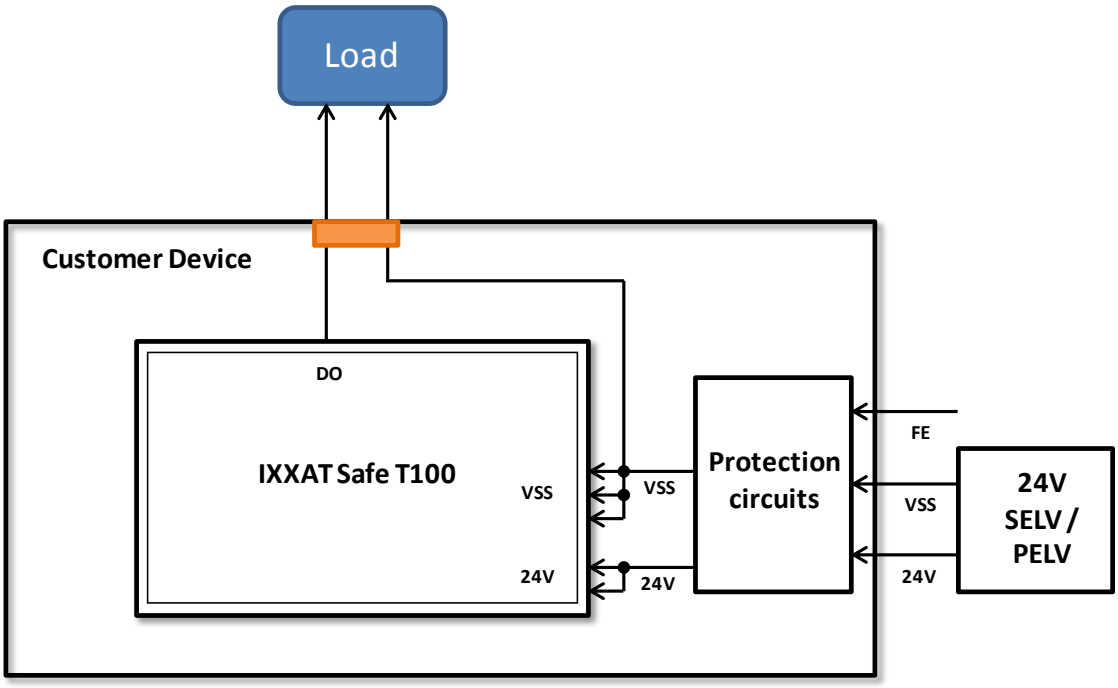


Figure 3-4: DO load ground connection

Pin 25, providing ground signal to the communication interface, is not connected internally to the other ground signals. To provide consistent grounding all the signals of the T100 connector have to be connected externally in the customer device (see Figure 3-5). [SC_410]

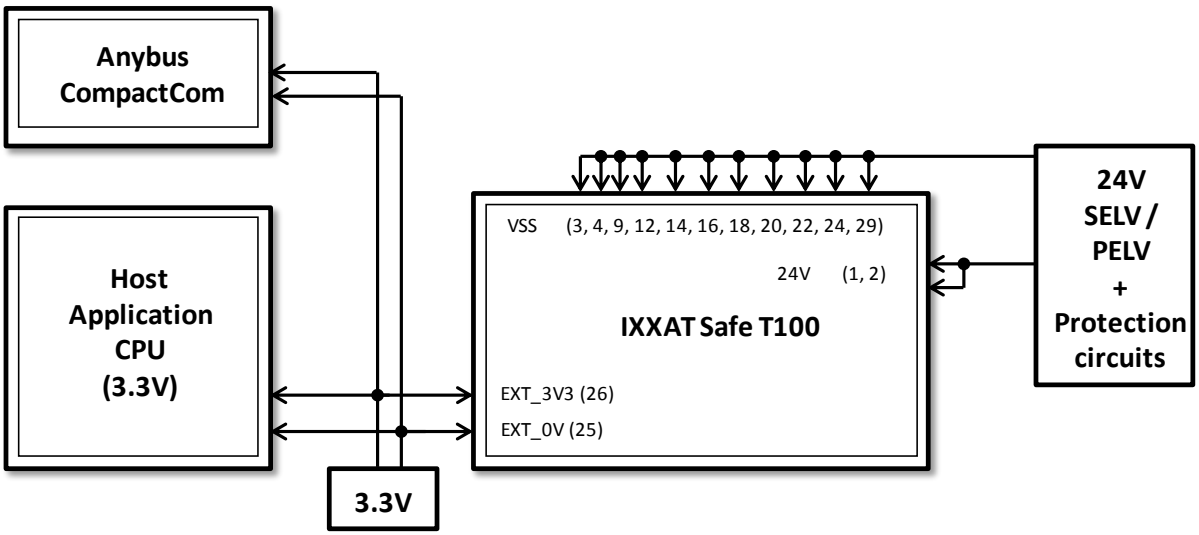


Figure 3-5: T100 ground concept

The pads around the mounting holes of the T100 as well as the standoffs between the two PCBs of the T100 are not connected to the ground Signal VSS.

3.4.6 Galvanic isolation

Only the communication interface (pin 27 and 28) and the reset signal (pin 30) are galvanic isolated from the T100 electronics.

There is no galvanic isolation between the digital inputs, the digital outputs, the test outputs and the T100 board electronic itself.

3.4.7 Integrated I/O protection circuits

The T100 I/O signals are tested to withstand the increased EMC levels as defined in IEC 61326-3-1. The necessary clamping diodes are already integrated on the T100. There is no need for additional protection circuits at the I/O pins of the T100 module.

3.5 Safe Operation

To achieve SIL-3 and Cat.4 / PLe the T100 uses a 1oo2d (one out of two with diagnosis) safety architecture. With this dual-channel processing of input- and output signals the T100 achieves a calculated proof-test interval of 20 years for the given PFH. The internal diagnosis test interval is 1h [SC_323].

[SAR-3.5] **Danger:** The maximum operation time (proof-test interval) of the T100 shall not exceed 20 years. When reaching the proof-test limit the T100 shall be replaced and put permanently out of order.

The proof test interval starts with the final integration test of the end device done by the integrator of the T100.

[IDR-3.12], [SAR-3.6] **Danger:** The manufacturer of the end device must clearly note and supply the date of the integration test of the T100. This marks the earliest beginning of the proof-test interval the end user or system integrator has to consider to keep the T100 operation time within the calculated 20 year proof-test interval.

3.5.1 Safe Digital Inputs

The digital inputs of the T100 are conformant to EN 61131 Type 1 (see EN 61131-2, figure 4 and table 8 with Ue=DC 24V).

Signal Name	Type	Pin No.	Description
DI[1..6]	I	13, 15, 17, 19, 21, 23	Digital Input

Reference levels for digital inputs with respect to EN 61131-2
(with Ue = 24V DC, Type 1)

Parameter	Unit	Min	Typ.	Max
V_{DIH}[a]	V	15	24	30
V_{DIL}[b]	V	-3	0	5
I_{DIH}	mA	2	5	15
I_{DIL}	mA	0[c]		15[d]
F_{max} (Dependant on filter settings)	Hz	-	-	62,5

[a] DIH: Digital Input High

[b] DIL: Digital Input Low

[c] This value is not defined by the standard, but can be assumed to be 0 mA due to the reverse current protection

[d] Requirement from standard

In general, the digital inputs switch to active mode, when an input signal of at least 15V is connected. All inputs use the same VSS connection.

The digital inputs can be configured for the support of different operation modes. In the dual-channel mode two inputs are grouped together to one safe input channel to obtain the SIL 3 or PL e Cat 4 rating. In addition a debounce and a consistency filter can be configured for each input group. Further details about the possible configuration settings of the digital inputs can be found in section 5 of this document.

[SAR-3.7] **Danger:** Two inputs have to be configured as one dual channel safe input to obtain SIL 3, PL e Cat 4. If two identical sensors are connected to the dual inputs one of the dual sensors shall be connected to input 1, 3 or 5.
The other shall be connected to input 2, 4 or 6.
Additional measures for wiring fault exclusion or using certified components might be necessary.

An unconnected input channel input does not influence the safety function of the T100.

[SAR-3.8] **Danger:** Single-channel inputs of the T100 shall be used for safety applications only under special precautions. The safe operation of a single channel input always requires additional safety measures or fault exclusions which must be considered in the overall safety system design.

The safe input state from the T100 point of view is a “low” signal. Therefore sensors connected to the T100 shall use the low signal to indicate a safe state request.

[SAR-3.9] **Attention:** Unconnected digital inputs in dual channel mode will cause the T100 to signal the inactive safe state for the input pair.

Besides the dual-channel and the filter modes, the digital inputs can also be configured for the use with passive contact inputs (DI-C) such as emergency buttons or active semiconductor inputs (DI-S) such as light curtains.

3.5.1.1 DI-C Contact inputs

Safety sensors connected to a DI-C input typically need to be powered by the T100 as they can only drive simple safety contacts. The T100 therefore needs to detect possible cabling or sensor errors on its own to achieve the SIL 3 or PL e Cat. 4 rating. For this reason the T100 has two test pulse outputs (see section 3.5.2 of this document) which can power up to two different groups of

digital inputs. In combination with the dual-channel input mode these test pulses allow to detect the following error sources:

- Stuck at 24 V
- Stuck at VSS
- Cross-connection of input lines
- Broken connection at one digital input (only in dual-channel when one input is set high)

An external short over the sensor cannot be detected in DI-C mode.

[IDR-3.13], [SAR-3.10] **Warning:** External short over the sensor in DI-C mode has to be prevented by fulfilling certain rules when developing the host device or cabling the sensors such as distances between lines or pins as described in the standard EN 60664 [SC_55, SC_370]. Which failure is excluded by which rule, has to be documented, see “Layout Rules, Host Device” in section 4.2.1 of this document.
Product- or application specific safety regulations which might apply for the CDev regarding external sensors and cabling shall be considered as well.

[SAR-3.11] **Warning:** When using the DI-C input mode the T100 test outputs shall be used as power source for the external sensor for proper error detection by the T100. The test pulse length shall be configured to a value different than “Always High” (see section 5.2). [PRS_97]

3.5.1.2 DI-S Semiconductor input

In contrast to the DI-C input mode, the DI-S input is used to connect active safety output devices to the T100 inputs. When configured to DI-S, an input channel does not check for external cabling faults as the T100 TO signal is not expected to be looped-back into the DI-S input.

[SAR-3.12] **Warning:** An active sensor, connected to a semiconductor input, must use the same ground level VSS than the IXXAT Safe T100.

[IDR-3.14], [SAR-3.13] **Warning:** If an input is configured as type DI-S, the following failures cannot be detected by the IXXAT Safe T100 [DR_I_DIS], [SC_319, SC_320, SC_321]:

- external short over sensor
- external short to 24 V
- external short between dual channel DI lines

These failures have to be prevented by fulfilling certain rules when developing the host device, e.g. distance between signal lines or pins as described in the standard. Which failure is excluded by which rule, has to be documented[3].

A set of rules for the signal routing and protection can be found in sections 4.2.1 and 4.2.5 of this document.

3.5.1.3 Input wiring examples

Example 1

This example shows an emergency stop button, connected to dual inputs of type DI-C. When using safety certified or compliant components (e.g. E-Stop Button) and proper external wiring, maximum SIL 3 or Category 4 / PLe can be achieved for the input function. A valid T100 configuration can be found in section 5.4.1.

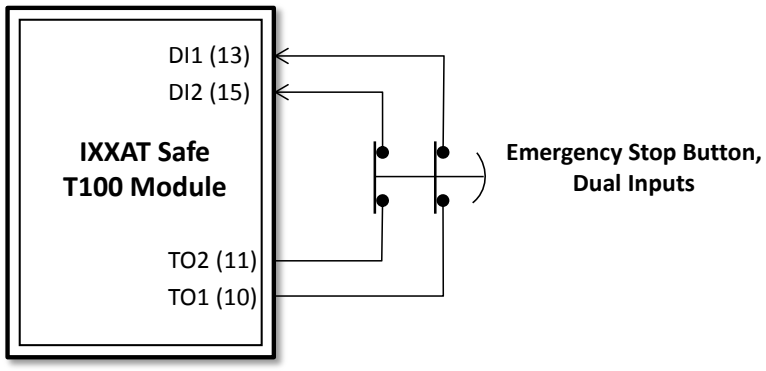


Figure 3-6: Passive sensor with dual-inputs

[3] EN 62061 §6.7.6.1c) and 6.7.7 require that "failure exclusions have to be justified and documented". For justification §3.3 and table D.5 - D.8 in EN ISO 13849-2 may be used.

Example 2

This example shows active sensors with external power supply (SELV/PELV), connected to dual inputs of type DI-S. When using safety certified or compliant components (e.g. active Sensors with safe outputs) and proper external wiring, maximum SIL 3 or Category 4 / PLe can be achieved for the input function. A valid T100 configuration for this application can be found in section 5.4.2.

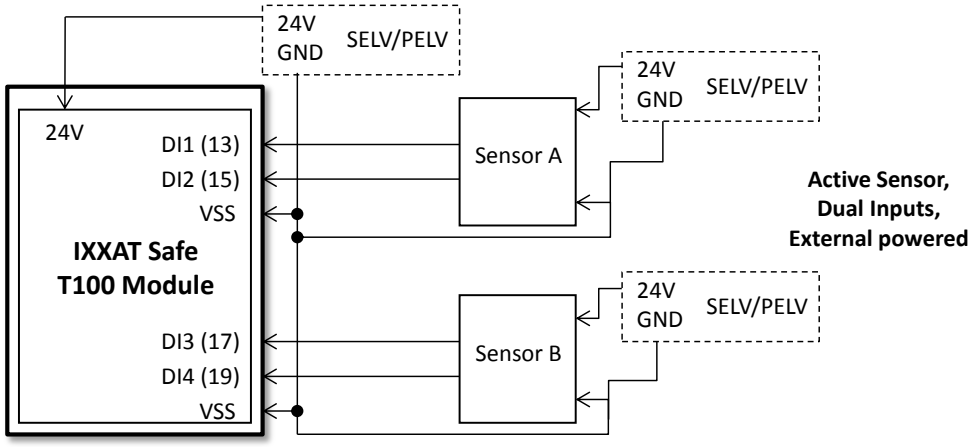


Figure 3-7: Active sensor, external powered

3.5.1.4 Digital input diagnosis and safe state

The T100 continually executes internal self-tests of the CPU RAM and ROM as well as hardware tests to detect potential errors. The internal self-test interval of the T100 is 1h which means that the complete internal tests are executed within this time. In addition the HW self-tests of the dedicated input circuits are run whenever an input or output signal changes. The maximum time interval between an input signal change and the detection of an error is 5 ms. The safe state of the DIs is “low” or “inactive”.

3.5.1.5 Safe application DI reaction time

Forwarding a change of the DIs to the safety protocol is one of the main tasks of the T100. This data exchange takes place within the safe application reaction time. Depending on the configured input filtering and the number of configured safety inputs, the minimum achievable safe application reaction time is 6 ms for a single input channel state change.

[SAR-3.15] **Warning:** The minimum time between the change of a single safe digital input and the transmission to the safety fieldbus is 6 ms. In case of an input level change at all 6 safe digital inputs at the same time, the maximum safe application reaction time is 16 ms (approx. 2 ms processing time per changed input).

3.5.1.6 DI diagnostic test interval

The diagnostic test interval for the DIs is the time span to detect an accumulation of errors at a certain input. The T100 internally does a self-test with every activation of a safe input to detect any kind of internal hardware errors as soon as possible. In addition the clock signal provided by the test outputs (see 3.5.2) can be used in DI-C mode to detect external cabling faults. The test pattern applied to the test outputs has a repetition rate of 1 second. This allows detecting an external cabling fault within less or equaling than 1 second. In dual-channel mode it can be additionally assumed that a single external error does not lead to a safety critical input state and the second error at the input (accumulation of errors) only arises after the diagnostic test interval of 1 hour.

[SAR-3.16] **Warning:** The diagnostic test interval for dual-channel DI-C inputs is 1 hour [SC_323].

3.5.1.7 Reliability block diagram

The safe digital inputs of the T100 in dual channel mode are equivalent with the reliability block diagrams as shown in Figure 3-8 and Figure 3-6.

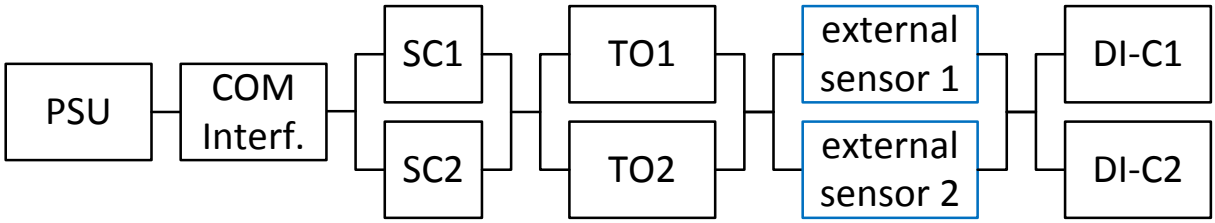


Figure 3-8: Reliability block diagram of inputs in dual-channel DI-C mode

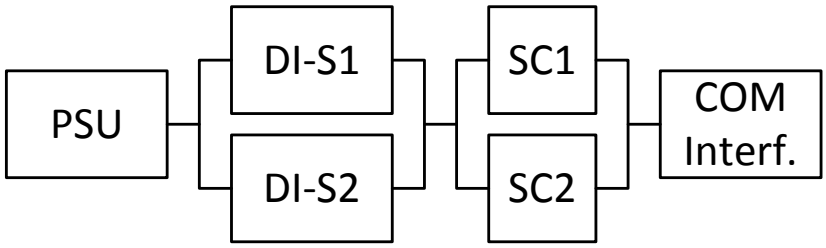


Figure 3-9: Reliability block diagram of inputs in dual-channel DI-S mode

Lengend:

COM Interf.:	Communication interface (RS232)
DI-Cx:	Digital inputs (contact) of controller x
DI-Sx:	Digital inputs (semiconductor) of controller x
PSU:	Power supply unit
SCx:	Safety Controller
TOx:	Test output logic

3.5.2 Test Outputs

The test outputs of the T100 are conformant to EN 61131-2, table 10 (with I_e=0.5 A) and table 6 (with U_e= 24V DC). In contrast to the EN 61131-2 the maximum permanent output current shall not exceed 100 mA. As the T100 does not monitor the output current, an overload of the output will not be detected. Only in case of a short to VSS a thermal shut down will be issued by the T100 automatically. [HR_131]

Signal Name	Type	Pin No.	Description
TO[1,2]	O	10, 11	Test Output. Can be used as power supply provided by the IXXAT Safe T100 to passive sensors.

Parameter	Unit	Min	Typ.	Max
V_{TOH}[a]	V	19.2	24	30
V_{TOL}[b]	V	-	High Z	-
I_{DOH}	mA		100	100
I_{DOL}	mA	-	-	0.5
I_{SCp}[c]	A	9	17	28

[a] TOH: Test Output High

[b] TOL: Test Output Low

[c] SCp: Shortcut peak

The test outputs can be used to generate a dynamic signal to detect cabling and sensor failures of connected devices in DI-C mode. As the test outputs are operated by a high-side switch, loads can only be switched to 24V DC and not to VSS.

The configurable test output signal timings are described in section 5.2 of this document.

Note that the test outputs are only operated if at least one of the T100 input channels is configured to DI-C mode.

[SAR-3.17] **Warning:** Do not deactivate the test pulse outputs (set pulse-length to 0 or “Always High”) in the configuration when using the digital inputs in DI-C mode.

[SAR-3.18] **Attention:** The test output signals are not isolated and use all the same ground potential VSS.

[SAR-3.19] **Warning:** The maximum constant output current at the test output pins of 0.1A shall not be exceeded to avoid damage of the T100 hardware [PRS_433], [HR_131]. It must be ensured that only devices consuming a total current of less than 0.1A are connected to the TO or technical measures such as protective fuses are in place on the CDev.

[IDR-3.15] **Warning:** Short-circuit of the TO to VSS will activate the thermal protection circuit of the output driver. The shut-down temperature of this component is given with 150°C. In case of a TO short to GND parts of the T100 PCB will heat up to 150°C which shall be considered in the design of the overall safety device housing.

3.5.3 Safe Digital Outputs

The IXXAT Safe T100 has two digital outputs which in combination can be used as one safe output to obtain safety level SIL 3, PL e Cat 4. The module checks the incoming safety telegram. If the telegram was correct, the outputs will be set according to the message.

The digital outputs of the T100 are conformant to EN 61131-2, table 10 (with Ie=0,5A) and table 6 with Ue= 24V DC. In contrast to the EN 61131-2 the maximum permanent output current shall not exceed 500 mA each.

The digital outputs are powered directly from the T100 connector pins 1 and 2.

[SAR-3.20] **Warning**: The maximum output current at the digital output pins shall not exceeded 500 mA to avoid damage of the T100 hardware.

The maximum output current is not supervised by the IXXAT Safe T100. A thermal cutoff for over current or short circuit is implemented internally. The digital outputs are using N-Channel high side switches and are thermal short circuit protected.

[SAR-3.21] **Attention:** In case of a short circuit of the digital outputs a thermal shut down into the safe state will be issued by the T100 automatically.

[IDR-3.16], [SAR-3.22] **Warning:** When turned off (safe-state), the output signal is not pulled actively to VSS.

[PRS_106]

Signal Name	**Type**	**Pin No.**	**Description**
DO[1..2]	O	(5, 6)[a] , (7,8)[b]	Digital Output

[a] Pins 5 and 6 must be connected to DO1
[b] Pins 7 and 8 must be connected to DO2

Parameter	**Unit**	**Min**	**Typ.**	**Max**
V_{DOH}[a]	V	19.2	24	30
I_{DOH}	mA			500
I_{DOL}[b]	mA			0.5
I_{SCp}[c]	A	2	5	8
Inductive load	H			0.5
Capacitive load	µF			1
Minimum output level change time (time between reception of safety fieldbus	ms		5	7.7

message and operation of output pin)				

[a] DOH: Digital Output High – active state

[b] DOL: Digital Output Low – inactive (safe) state

[c] SCp: Shortcut peak

The digital output states are defined by output currents in EN 61131-2. Each current level below 500 µA applies as low level.

[SAR-3.23] **Warning:** The safe state of the T100 digital outputs is “off” (high impedance). Therefore it is not allowed to connect an external safety device or function (like a valve or break) which needs a “High” level to keep the safe state.

The digital outputs of the T100 only achieve safety level SIL 3, PL e Cat 4 when used in dual-channel mode. This means that a safety critical action shall not be controlled by the T100 by just using one digital output connection.

[SAR-3.24] **Warning:** To achieve SIL 3, PL e Cat 4 the digital outputs of the T100 shall be operated and connected in dual-channel mode [SC_75], [SC_76].

3.5.3.1 Digital output diagnosis and DO diagnostic test interval

To detect hardware faults in the digital output section of the T100, the outputs are cyclically disabled when they are in active state. This test pulse length can be configured as described in section 5.3 of this document.

[SAR-3.25] **Warning:** Safety devices like actors or brakes connected to the T100 digital outputs must be robust against the configured T100 output test pulses. [SC_324]

[IDR-3.17] **Warning:** Safety outputs shall be connected to the T100 connector always using both output pins per output channel (DO1: Pin 5 and 6, DO2: Pin 7 and 8).

The diagnostic test interval of the digital outputs is the maximum time between the occurrence of a potential safety critical error and the transition of the digital output into the safe state (inactive state). The output control circuits are tested with an interval of 1 second when being in active state. Nevertheless, all other safety critical errors will be checked and detected within the self-test interval of 1h only.

[SAR-3.26] **Warning:** The diagnostic test interval for the DOs is 1h. [SC_323]

The T100 design of the safety digital outputs in dual-channel mode complies to a hardware fault tolerance (HFT) of 1. Therefore a single point of failure detected in the T100 will lead to the safe state of the output. Nevertheless, it is assumed by the safety calculations of the T100 that after the diagnostic test interval of 1h a second failure can happen which in turn can lead to a safety critical output state again.

[SAR-3.27] **Danger:** After detection of a safety critical error, the T100 shall not be kept in fail-safe state for more than 1h [DR_I_DO].

3.5.3.2 Loss of ground at DO

The return current from the load has to be directed to the CDev at a separate VSS ground connection. This connection must be hardwired (without possible loss of connection) to the VSS input of the T100 so any loss of external ground does not cause dangerous situations.

[IDR-3.18], [SAR-3.28] **Danger:** A loss of ground of the load connected to the T100 DO shall be prevented by means of a hardwired ground connection to the VSS input of the T100.

3.5.3.3 Safe application DO reaction time

The DO state is controlled by the safety fieldbus protocol. The safe application reaction time for the DOs is therefore defined as the time between receiving a safety telegram on the T100 and setting of the corresponding output. The maximum safe application reaction time is 7.7 ms.

[SAR-3.29] **Warning:** The maximum time between the reception of a safety telegram and setting the corresponding safe digital output is 7.7 ms.

3.5.4 Output wiring examples

Example 1

This example shows the allowed wiring of a safety relay using the dual outputs of the T100 for an application up to SIL 3 PL e Cat. 4. The diagnosis read-back line of the safety relay is required to detect failures of the safety relay itself within an adequate period of time. The matching configuration can be found in section 5.4.3.

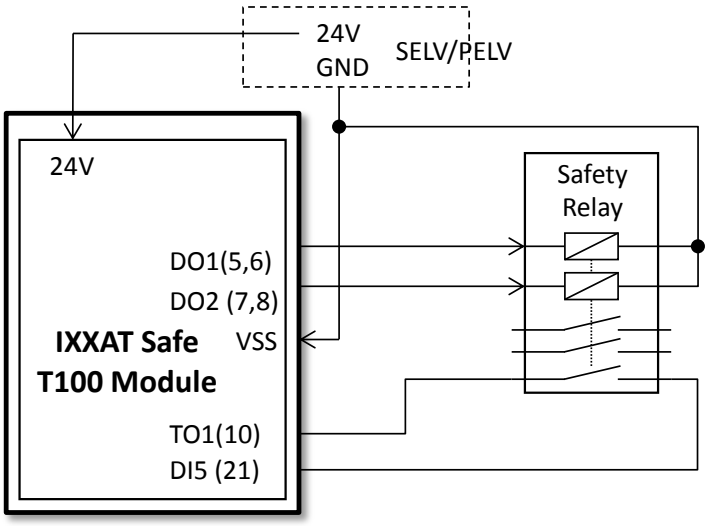


Figure 3-10: Dual-channel output wiring of a safety relay

Example 2

Figure 3-11 shows a wiring example which is **not allowed** to be used for SIL 3, PL e Cat. 4 applications

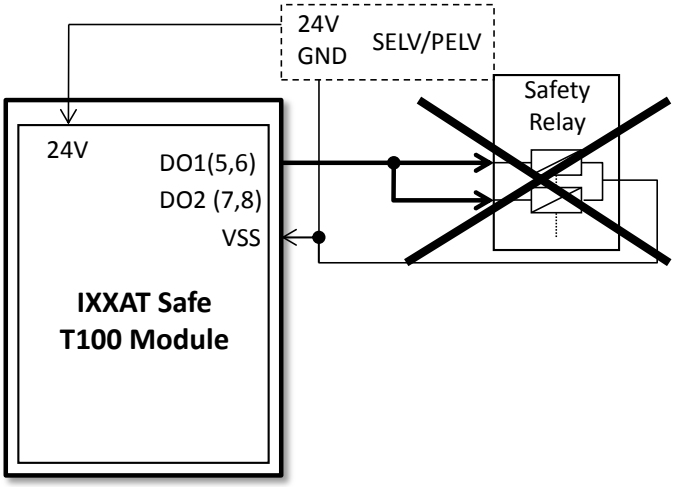


Figure 3-11: Single-channel output wiring

Example 3

An improper connected safety relay is shown in Figure 3-12. This kind of wiring error can happen upon a “ground loss” fault for example.

[SAR-3.30] **Warning:** Proper grounding and measures against an external ground loss shall be applied to safety devices connected to the T100.

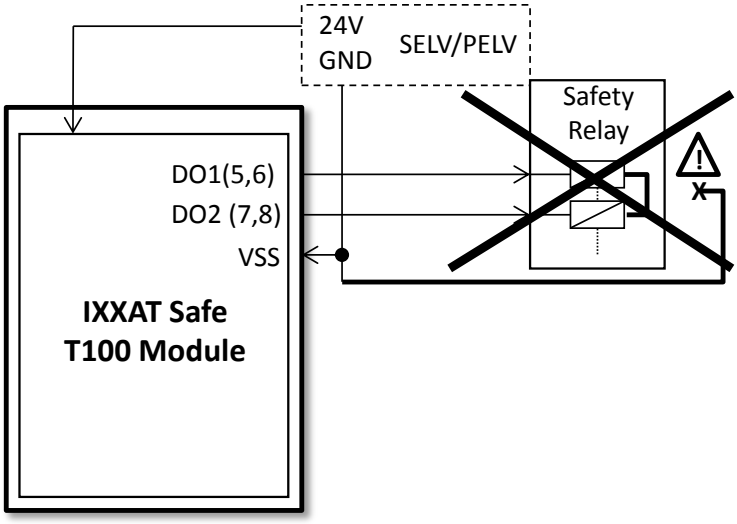


Figure 3-12: Improper connected safety relay

3.5.5 Reliability block diagram

Figure 3-13 shows the reliability block diagram of the digital outputs of the T100.

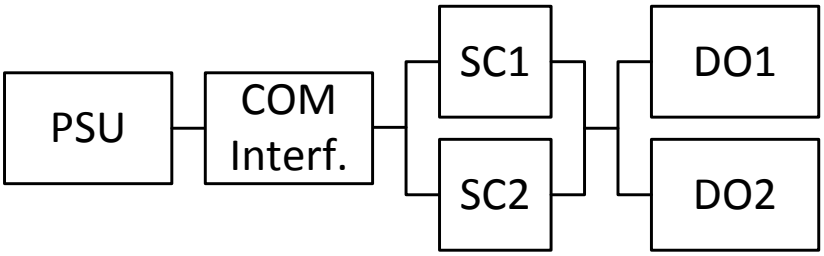


Figure 3-13: Reliability block diagram digital output

3.6 Safe State and Reaction times

The T100 permanently checks its hard- and software execution. These self-tests are cyclically executed within an interval of 1h. Any failure detected leads to the global fail-safe state of the T100.

In the global fail-safe state:

- The IXXAT Safe T100 does not execute safety fieldbus communication such as PROFIsafe for example.
- All DOs are inactive, i.e. high impedance output.

During global fail-safe state the IXXAT Safe T100 continues to communicate non-safe data with the Anybus CompactCom module in order to transfer error information but the T100 does no longer react on received messages from the Anybus CompactCom. If possible the previous state and the reason for the transition to fail-safe state will be recorded in non-volatile memory of the T100. In addition the T100 sends out cyclically a message indicating the fail-safe error code on the serial interface to the Anybus module.

The fatal error serial message has the following setup:

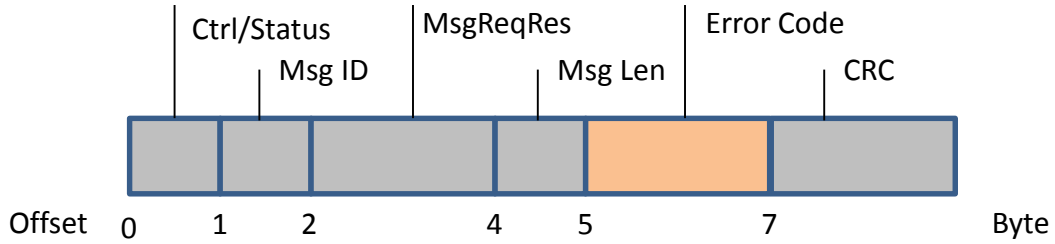


Figure 3-14: Setup of global fail-safe error message

Byte	Name	Size (Bytes)	Description
0	Ctrl/Status	1	Control and Status information Bit 0..3: 0 - State Boot 1 - State Init 2 - State Parametrization 3 - State Run 4 - State Stopped 0x0F - State Error
1	Msg ID	1	Message identifier Value = 0
2	MsgReqRes	2	Message Request / Response Value: 0x4000 - Fatal Error Request
4	Msg Len	1	Message data length Value = 2

5	Error Code	2	See Table 3-1
7	CRC	2	16-Bit Message CRC

Depending on the error, different actions can be performed.
Global fail-safe errors lead to a complete stop of the T100 module. This global fail-safe state can only be left with an external reset.

Input- or output channel specific errors do not lead to a complete stop of the T100 module. The fail-safe mode of a channel-specific error can be left after receiving an error acknowledge message from the ABCC or via the safety fieldbus protocol. See section 0 for more details about the channel specific errors and their protocol specific treatment.

The IXXAT Safe T100 leaves the global fail-safe state and resets the microcontrollers only when receiving a reset signal from the host device (pin RST).

After restart the T100 hardware tests will be repeated which will detect persistent hardware faults.

A T100 module indicating a permanent global fail-safe state shall be replaced immediately. In this situation subsequent faults inside the T100 may lead to a dangerous state

[SAR-3.31] **Danger:** Replace a malfunctioning T100 immediately.

[SAR-3.32] **Danger:** The T100 shall not be operated more than 8h outside the RUN state (see section 3.10) in order to make sure that all relevant tests are executed within the safe reaction time. [SC_379, SC_373, SC_423]

Detected Error	**Error Code**	**Global fail-safe**	**Channel fail-safe**	**Error recovery**
ROM test error	0x830B	X		External reset
RAM test error	0x84C0	X		External reset
RAM startup test error	0x8557	X		External reset
Stack under-/overflow	0x8679	X		External reset
Opcode test failure	0x87EE	X		External reset
SFR test error	0x8878	X		External reset
Core register test error	0x89EF	X		External reset
Program-Flow error	0x8AC1	X		External reset
Safety container CRC error	0x8B56	X		External reset
Safety Handler timeout	0x8C9D	X		External reset
Safety Variable error	0x8D0A	X		External reset
NMI error	0x8E24	X		External reset
Hard Fault error	0x8FB3	X		External reset
Memory Management Fault	0x909F	X		External reset
Bus Fault	0x9108	X		External reset
Usage Fault	0x9226	X		External reset
SVC Fault	0x93B1	X		External reset
Debug Monitor Fault	0x947A	X		External reset
Pending SV Fault	0x93B1	X		External reset
Systick failure	0x96C3	X		External reset
Initialization Fault	0x9754	X		External reset
IPC Sync Fault	0x98C2	X		External reset
IPC CRC Fault	0x9955	X		External reset
Controller ID Fault	0x9A7B	X		External reset
IPC ID Fault	0x9BEC	X		External reset
IPC return code error	0x9C27	X		External reset
IPC timeout	0x9DB0	X		External reset
Configuration mismatch	0x9E9E	X		External reset
Invalid parameter	0x9F09	X		External reset
Invalid pointer	0xA0C6	X		External reset
ADC timeout	0xA151	X		External reset
ADC calibration error	0xA27F	X		External reset
PROFIsafe hard error	0xA3E8	X		External reset
Cyclic iPar CRC check	0xA423	X		External reset

error				
Cyclic fPar CRC error check error	0xA5B4	X		External reset
Under-/Over-Temperature	0xA69A	X		External reset
Sync. Fault with ABCC	0xA70D	X		External reset
DO diagnostic error	0xA89B	X		External reset
DI diagnostic error	0xA90C	X		External reset
Clock control failure	0xAA22	X		External reset
Scheduler timeout	0xABBB5	X		External reset
Main-loop timeout	0xAC7E	X		External reset
No failure	0xADE9			
Under-/Over-Voltage (without fuse blown)		(X)		Automatic restart when reaching valid power level
Safety fieldbus protocol timeout			X	Safety fieldbus communicatio n restart
DO short to VSS or 24V			X	Channel reset command + setting output low before reactivation
DI consistency error			X	Channel reset command
DI-C input errors (external short or cross-connections)			X	Channel reset command

Table 3-1: Serial black-channel error codes and error classes

3.7 Hardware interfaces to non-safe components

The T100 has got a bi-directional UART connection as well as a reset input line as non-safe hardware interfaces which are galvanic isolated from the non-safe Anybus CompactCom communication interface and the host CPU. The isolation circuits on the T100 must be powered from an additional 3.3 Volt input (see section 3.2).

Signal Name	Type	Pin No.	Description
Rx	I	27	Serial UART (Rx/Tx) Default Baudrate: 1020 kBaud (+/- 0.5%) [HR_321, PRS_434]
Tx	O	28	
$\overline{\text{RST}}$	I	30	Low-active reset signal

Parameter		Unit	Min	Typ.	Max
Rx	High level input voltage	V	2	3.3	EXT_3V3+0.5
	Low level input voltage	V	-0.3	0	0.8
Tx	High level output voltage (I_{OH} = -4mA)	V	2.2	3.3	EXT_3V3
	Low level output voltage (I_{OL} = 4mA)	V	-0.3	0	0.8
$\overline{\text{RST}}$	High level input voltage (V_{IH})	V	2	3.3	5.5
	Low level input voltage (V_{IL})	V		0	0.8

For the Rx, Tx and RST pins it is guaranteed that any overvoltage up to 60 VDC will not lead to a safety-critical error of the IXXAT Safe T100. Nevertheless, an Rx signal level above 3.3 V will damage or destroy the serial interface driver of the T100 board permanently. [DR_C_HW_COMM]

3.7.1 T100 Hardware Reset conditions

The reset of the T100 becomes active when applying a logic low signal to the RST pin. [HR_282]

The IXXAT Safe T100 does not feature any internal reset regulation, which means that the host application is solely responsible for resetting the IXXAT Safe T100. Nevertheless an integrated power brown-out is used inside the T100 to shut down the safety CPUs properly while the T100 outputs are kept in the safe state.

There is no Schmitt Trigger circuitry on the RST signal line, which means that the module requires a fast RST rise time, preferably equal to the slew rate of typical logical circuits. Stable operation is not guaranteed unless RST slews from logic 0 (low, zero) to 1 (high, one) within 50 µs. A simple RC-circuit is not sufficient to achieve this slew rate. Instead a dedicated reset controller or host controller output pin shall be used to initiate the reset of the T100.

3.7.1.1 Powerup Reset

During startup, the RESET signal must be held low as shown in Figure 3-15 at least until the power supply has reached a stable value.

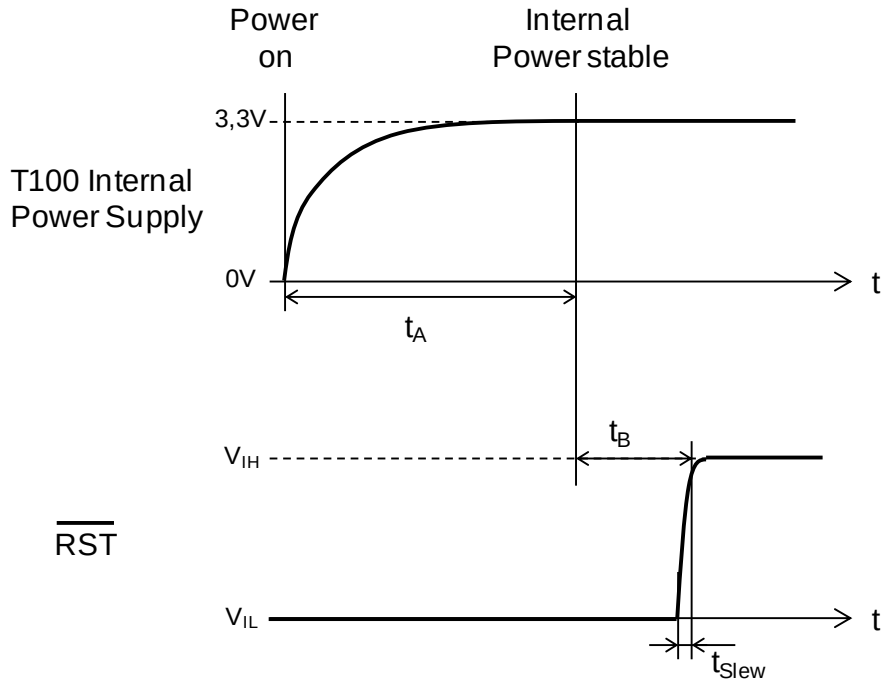


Figure 3-15: Powerup reset

Parameter	Unit	Min	Typ.	Max	Definition
t_A	ms	-	-	50	Power supply rise time (0.1 V_{DD} to 0.9 V_{DD})
t_B	ms	100	-	-	Safety margin wait time
t_{Slew}	µs	-	-	50	Signal slew rate

3.7.1.2 Restart Reset

The reset pulse duration must be at least 100 µs in order for the module to properly recognize a reset (see Figure 3-16). Attention this restart reset shall not be mixed up with the reintegration reset necessary to re-enable the safe digital inputs and outputs after a channel specific fail-safe error. The restart reset is intended to restart the T100 when it has entered the global fail-safe state.

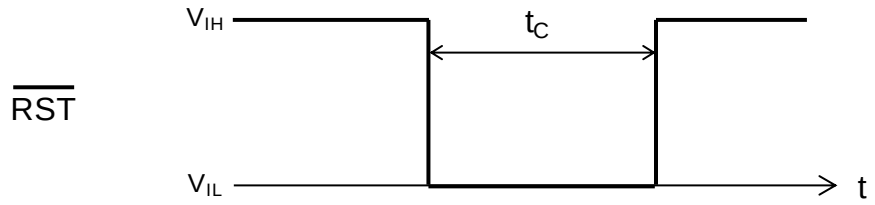


Figure 3-16: Restart reset

Parameter		**Unit**	**Min.**	**Typ.**	**Max**
t_C	Reset pulse width	µs	100	-	-

3.7.2 Wiring example

The Anybus CompactCom module is connected via the serial or parallel interface to the host application CPU. Information about the serial or parallel interface can be found in the Anybus CompactCom Hardware Design Guide.

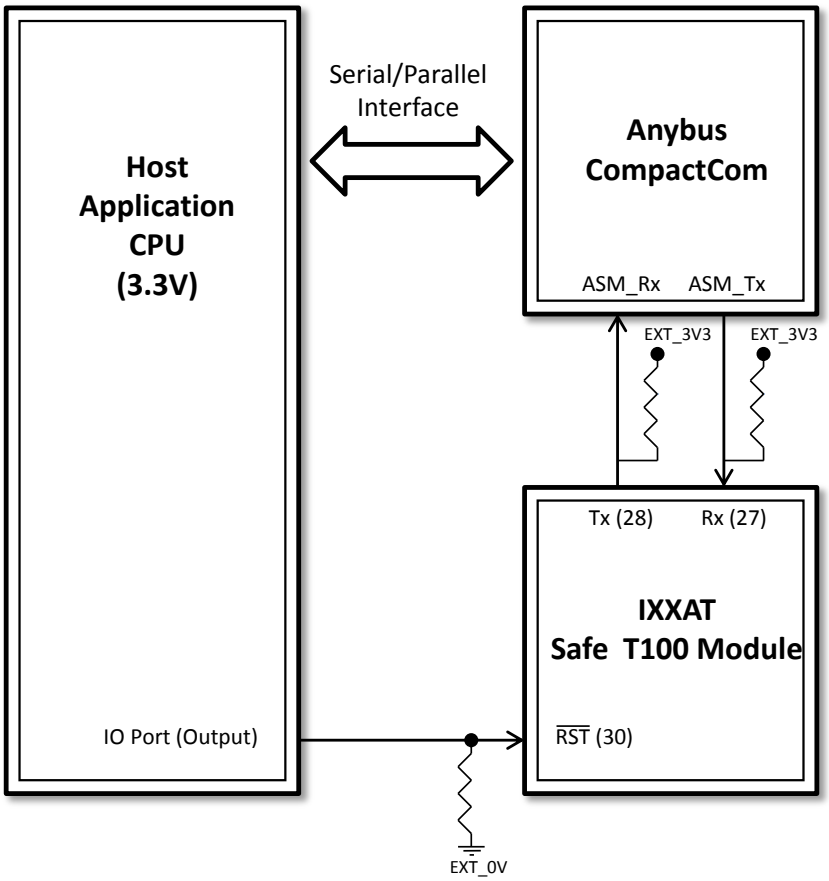


Figure 3-17: T100 wiring example, non-safe interfaces

[IDR-3.19] **Attention:** A 2.2 kOhm pull-up resistor shall be placed on the CDev to the Rx and the Tx signal line.

[IDR-3.20] **Attention:** There shall be a 4.7 kOhm pull-down resistor placed on the CDev to the RST line.

3.8 T100 Firmware update

The T100 module offers a firmware update possibility via the black-channel interface. This update is secured by a CRC check to detect transfer or flash storage errors. In case of an improper update the T100 will stay in the safe state.

[IDR-3.21], [SAR-3.33] **Warning:** Only use officially released and approved T100 firmware files from HMS for the T100 firmware update. Software not approved by HMS can cause damage to the T100 or lead to non-safe behavior of the T100.

Approved and released firmware update files are available directly from IXXAT on request (www.ixxat.de/support) together with the corresponding release history, approval report and handling precautions). The steps to do a T100 firmware update in combination with an ABCC module are described in the release information file shipped along with the updated T100 firmware.

Typically an updated safety module needs to be logged in the safety logbook of a machine in case the update was done in a running machine by the end-user. Integrators may keep track of updated modules by means of a safety configuration management plan.

[SAR-3.34] **Attention:** Updated T100 modules shall be tracked or clearly marked by the integrator or end-user to indicate modules with a firmware version different to the one originally shipped by HMS.

In general, a reassessment of the safety function of a device is necessary from the safety point of view which requires an impact analysis and detailed regression tests with the CDev. This is vital to prove that the updated T100 firmware works also as expected from the safety application point of view.

[SAR-3.37] **Warning:** The firmware update of the T100 shall not be performed during operation in the field. [SC_434]

[SAR-3.35] **Warning:** After a proper firmware update the safety function shall be checked by the integrator or end-user and documented properly.

3.9 T100 Module identification

The T100 transmits the module identifier within the Startup-Telegram via the black-channel interface to the non-safe communication controller (e.g. ABCC) [PRS_364]. Depending on the safety fieldbus protocol or the non-safe communication controller application the T100 module identification may be stored and read out also at a later time. Note, that there is no dedicated read-out function for this ID implemented in the black-channel interface layer of the T100 to the non-safe communication controller.

Module identifier:

Bit	**Name**	**Description**
0-7	Sub-Division	Type-specific sub-division of safe I/Os as shown in table below
8-15	Type	Type specifier: 0x01 – Dual channel digital input/output

Sub-Division for type 1 modules:

Bit	**Name**	**Description**
0-3	Input	Number of dual-channel digital inputs 0 to 15
8-15	Type	Number of dual-channel digital outputs 0 to 15

Example: The T100 with 3 dual channel inputs and one dual channel output will have the module identifier 0x0113.

3.10 Operating states

After power-on the T100 passes several internal states before the normal operation mode is entered where the safe input and output data exchange takes place. As some of the state changes require either an active acknowledge, data or command from the remote safety controller, a restart or re-enabling of the T100 outputs upon a local Reset for example cannot be automatically done by the local T100 firmware. This always require a valid safety fieldbus communication with the safety controller.

1. **Boot**
   checking of proper T100 firmware in internal Flash of µC1 and µC2 and channel opened to update T100 firmware via black-channel (AIC) interface. All DO's remain in fail-safe or inactive mode – no safety fieldbus communication possible.
2. **Init**
   Initialization of uC peripherals and software modules. All DO's remain in fail-safe or inactive mode. No safety fieldbus communication possible.
3. **Selftest**
   Complete internal self-test on µC1 and µC2. All DO's remain in fail-safe or inactive mode. No safety fieldbus communication possible.
4. **Parametrization**
   Initialization of black-channel AIC communication with non-safe communication controller (e.g. Anybus CompactCom) by Startup message, wait for Parameters, receive and check Parameters. All DO's remain in fail-safe or inactive mode.
5. **Run**
   Communication via safety fieldbus is started. Setting of DO's according to received fieldbus telegrams. Processing of DIs and forwarding to safety fieldbus. Cyclic error and Watchdog checking started.
6. **FAIL_SAFE**
   Both µCs enter a safe state after a fatal error has occurred. Before entering FAIL_SAFE state, a message is sent (cyclically) via AIC, containing the error ID and the error ID is programmed into the flash. All DOs remain in safe state, no communication via safety fieldbus and black-channel AIC is possible.

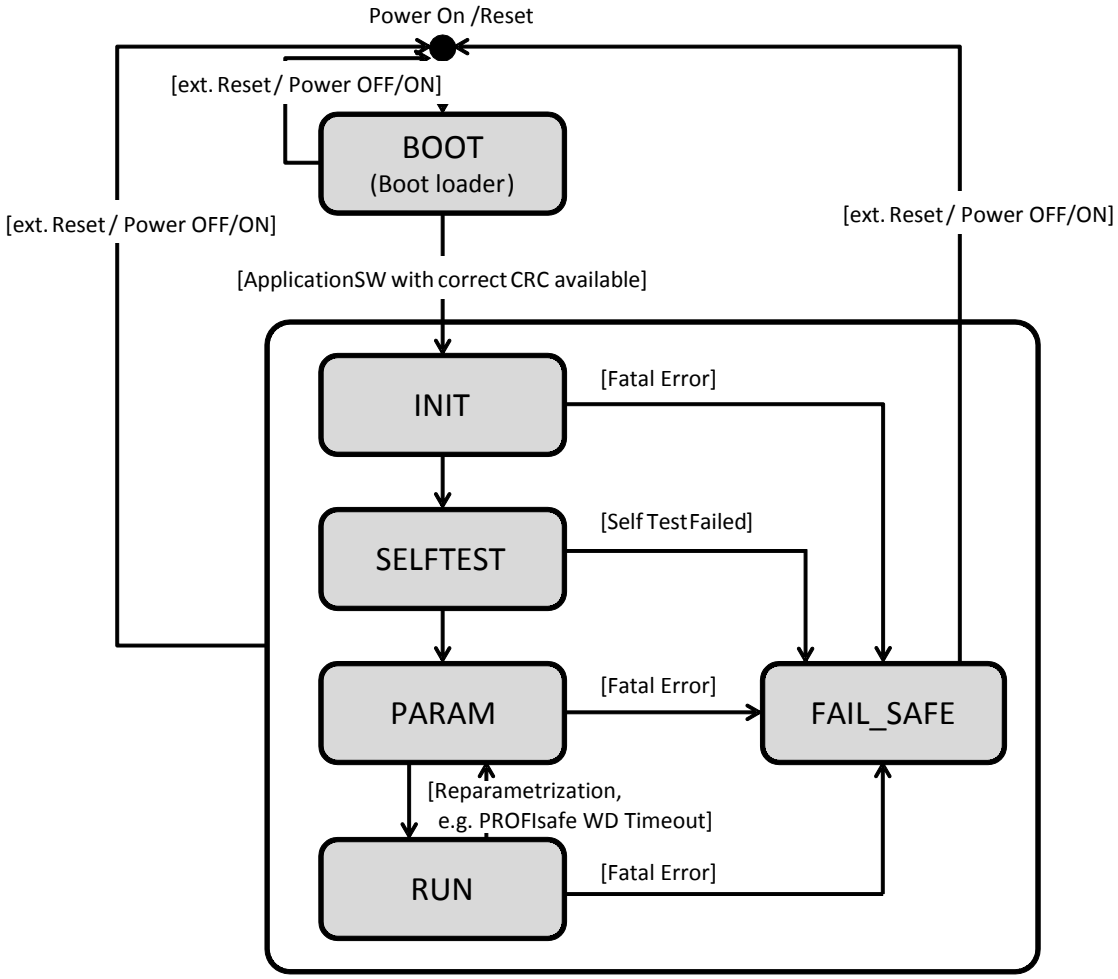


Figure 3-18: T100 state-machine

[SAR-3.36] **Danger:** If the T100 module is powered on and does not enter properly the RUN state within a maximum of 8 hours, the module shall be restarted via a power-cycle. Afterwards it shall be checked by trained safety service personal for a proper safety operation. [SC_379]

4 In-Design

4.1 Mechanical Specification

4.1.1 T100 dimensions

The size of the IXXAT Safe T100 is 70mm x 40mm x 12.6mm. It consists of two stacked PCBs as shown in Figure 4-1.

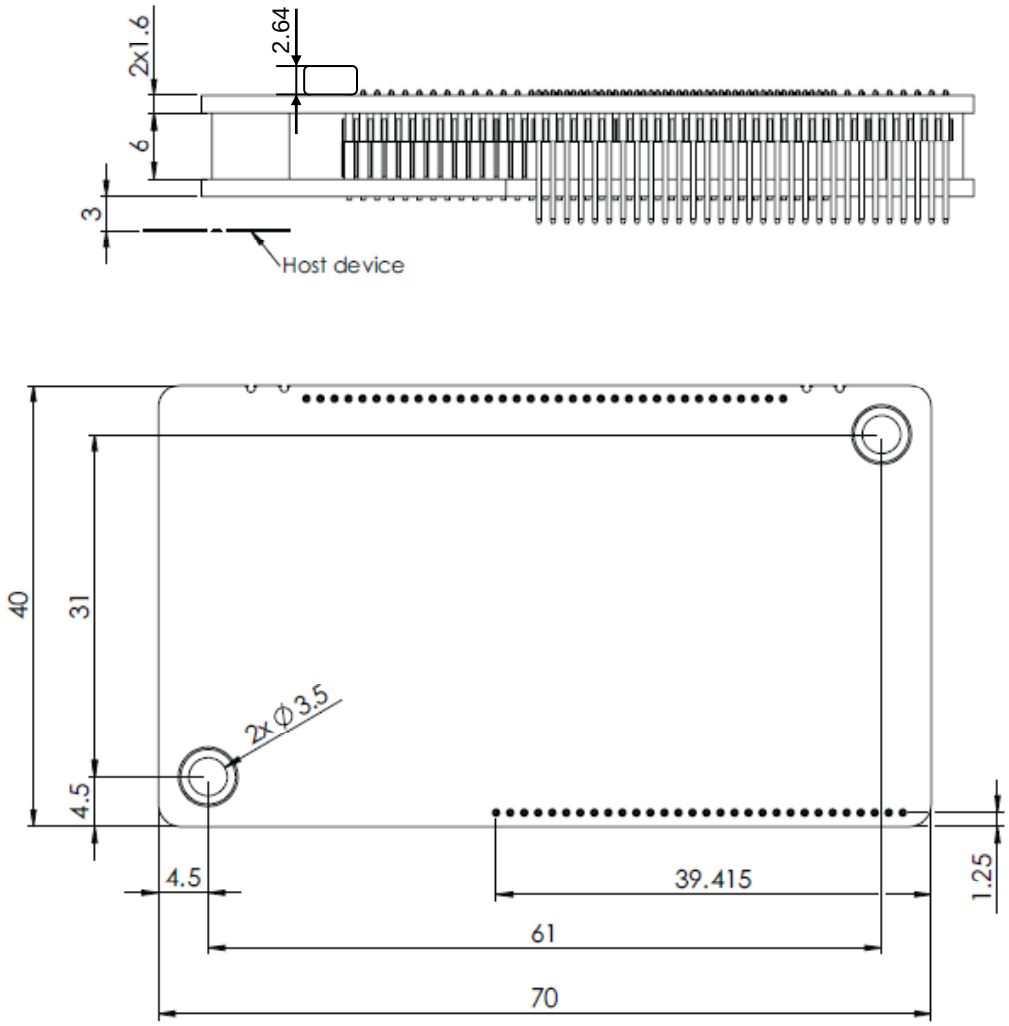


Figure 4-1: T100 dimensions

The dimensions shown in Figure 4-1 have a tolerance of +/- 0.1 mm unless otherwise stated. The distance between the IXXAT Safe T100 and the host device shall be at least 3 mm.

4.1.2 Connection to host board

The T100 uses a 30-Pin male connector to interface to the host board. This connector shall have a pitch of 1.27 mm and be capable of picking up squared

pins with a diameter of 0.4x0.4 mm. The minimum clamping depth shall be 2 mm to ensure a proper contact to the T100 and a mechanical limit to stabilize the T100 board when connected (see Figure 4-2).

[HR_253]

Host connector requirements			
Connector	Number of pins	30	pins
	Pin pitch	1.27	mm
	Pin dimension	0.4x0.4	mm
	Minimum clamping depth	2	mm

4.1.3 Mounting recommendations

For a proper mounting of the T100 the two mounting screws shall be tightened with a torque of minimum 0,4 Nm and a maximum of 0,8 Nm to avoid damage of the T100 PCB itself. It is recommended to use a washer and, if necessary, an additional spring washer to secure the T100 module on the hosting board.

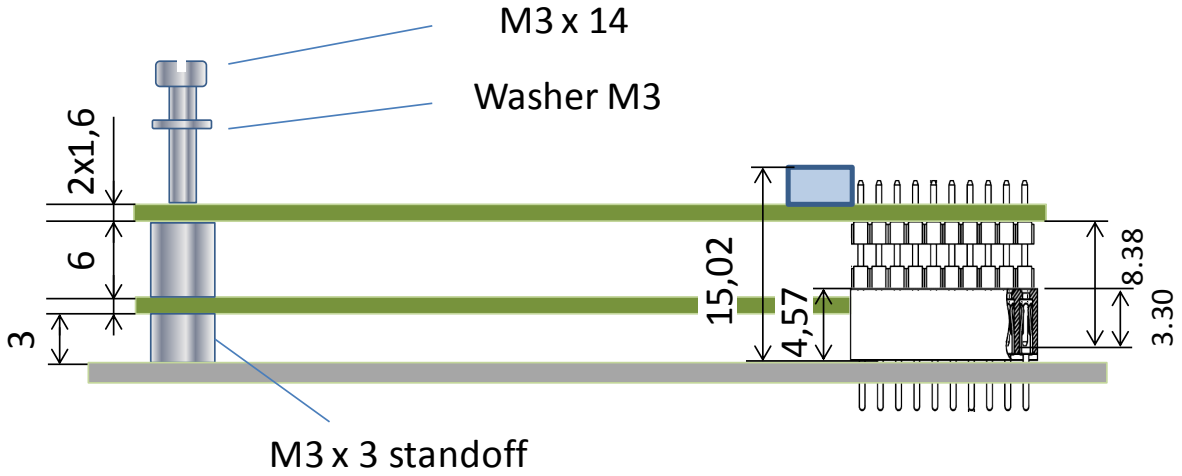


Figure 4-2: T100 mounting example

4.1.4 Mechanical mounting set recommendations

Host board standoff:

- 3 mm standoff with integrated M3 thread

Example type: Colly SMTSO-M3-3

Host board T100 connector:

- 30-Pin, female single row connector with 1.27 mm pitch

Example type: Samtec SLM-130-01-L-S

4.1.5 Clearances

To safely separate the T100 module from other parts of the host board, a minimum mechanical clearance of 3 mm on each side of the T100 shall be ensured by the integrator (measured between host board or housing and top most point of the T100). In order to keep the 3 mm clearance at all places, care has to be taken on the top side of the T100 PCB where components with a height of up to 2.64 mm are assembled.

[IDR-4.1] **Warning:** The minimum clearance around the T100 should be 3 mm. On the top side this should be measured from the top face of the components, on all other sides measured from nearest point on the PCB surface. The clearance above the highest component on the top face should measure 5.64 mm above the surface of the PCB.

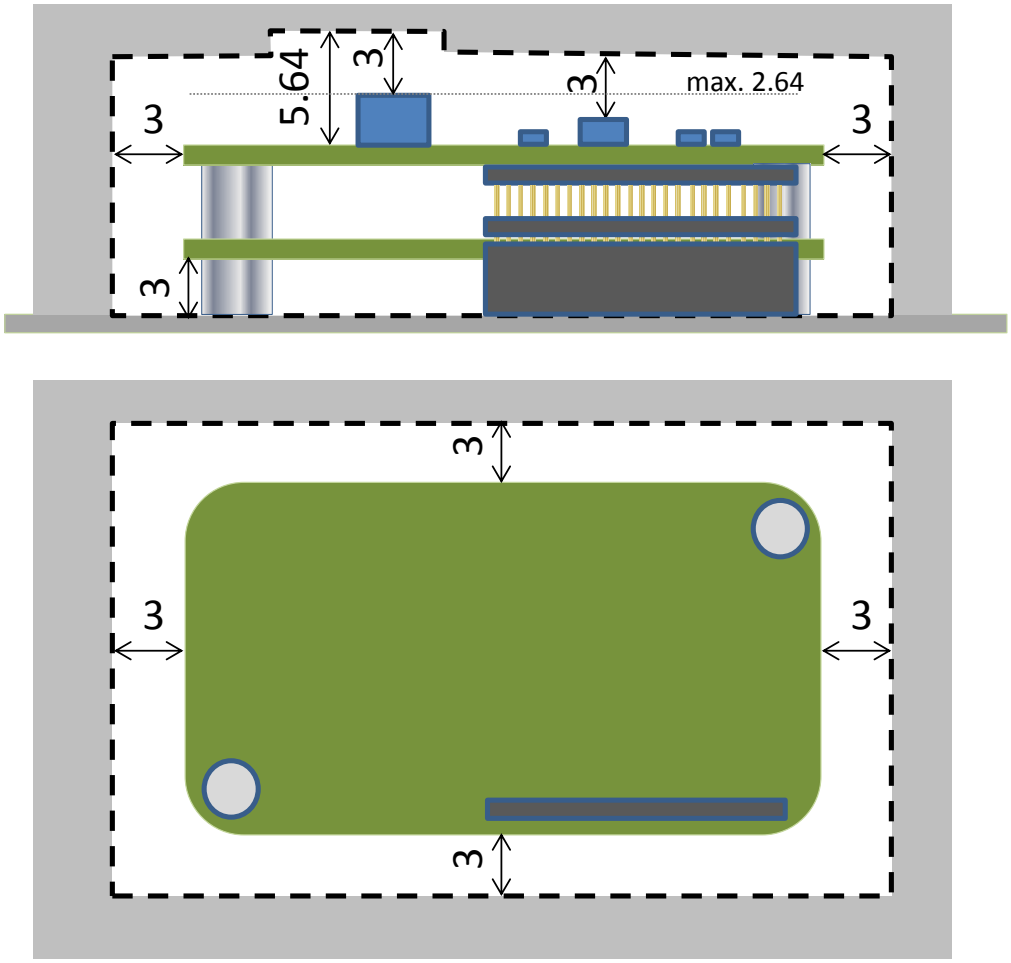


Figure 4-3: Mechanical clearance around the T100 (all values given in mm)

[IDR-4.2] **Warning:** When using conductive spacers and screws to mount the T100 on the base board, there must be at least 3 mm space to any conductive elements on the base board as well. Connecting the mounting points to ground or any other potential is not allowed.

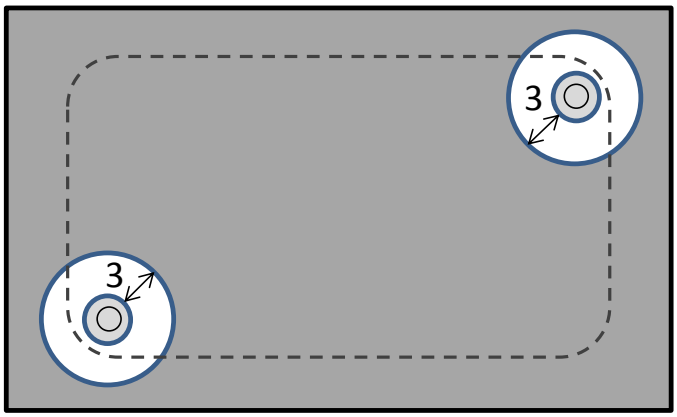


Figure 4-4: Clearance around the T100 mounting points (all values given in mm)

4.1.6 Allowed mounting positions

When keeping the above described clearances around the T100 there are no restrictions on the mounting position of the T100. Due to convection cooling effects there might be differences in the maximum possible environmental operating temperature as the T100 temperature sensors might detect over-temperatures earlier in different mounting positions. Nevertheless it is required according to the In-Design rules given in section 4.2.2 that the T100 is tested and verified in the exact mounting and operating position within the CDev and under the maximum operating conditions given for the CDev.

4.1.7 Labeling of safety signals

[IDR-4.3]: **Attention:** If the safety inputs or outputs of the T100 are routed to a user terminal, the provided signals shall be clearly marked according to DIN EN 61310.

4.2 Environmental considerations

4.2.1 Layout rules

When routing the T100 signals on the PCB of the host device, certain limits and conditions must be kept to ensure a safe operation of the T100 and its input- and output signals.

[IDR-4.4] **Danger:** The PCB of the host device shall fulfill EN 60664 with a minimum clearance of 0.2 mm at least for the T100 signals and T100 SELV/PELV power supply [DR_C_LO_POW]. This value is given under the assumption of over voltage category I with a nominal voltage of 330V r.m.s. [DR_C_LO_DIO], [SC_140], [HR_320].

[IDR-4.5] **Danger:** The minimum creepage distance between the T100 signals on the host PCB shall be 0.063 mm assuming 63 V r.m.s. effective voltage for all isolators except IIIb according to EN 60664 [DR_C_LO_DIO].

[IDR-4.6] **Warning:** To protect conducting lines (power, input and output) of the T100 on the PCB of the host device a non-aging lacquer shall be used [DR_C_LO_LAC], [SC_141], [HR_201]. Special coating is not required.

[IDR-4.7], [SAR-4.1] **Warning:** Routing of dual-channel input signal lines to the final input terminal as well as cabling of the external sensors to the T100 inputs shall be done in a way that adjacent signal lines or input terminals are using different test output signals.

[IDR-4.8] **Attention:** The interface connection between the IXXAT Safe T100 and the Anybus CompactCom module has to be able to handle a data transfer speed of 1020 kbit/s [DR_C_LO_COMM].

4.2.2 Temperature

The T100 does not require an active or convection cooling.

[PRS_339], [PRS_343], [HR_343]

Parameter	Unit	Min	Typ.	Max
Storage temperature	°C	-40	-	+85
Fail-safe entry ambient temperature	°C	-30	-	+68

Table 4-1: Maximum temperature ratings

[IDR-4.10] **Attention:** The maximum temperature rise produced by the T100 within the CDev under normal operation is 22 Kelvin. In case of TO output short-circuits, the internal temperature rise will be higher (see IDR-3.15).

[IDR-4.11] **Attention:** The T100 shall not be mounted in direct neighborhood of temperature hot-spots or convection cooling paths of the host device to avoid local over- or under-temperatures within the T100.

The T100 has a build-in temperature surveillance. When detecting critical temperatures, the T100 enters the fail-safe state. The last message sent by T100 before entering the FAIL_SAFE state, contains the error state and ID.

To release the fail-safe condition, the T100 must be set into a valid temperature range and a local reset of the T100 needs to be done before the normal operation can take place again.

Due to self-heating, component variations and drift effects, the effective ambient temperature leading into the fail-safe state of the T100 is different from the maximum allowed device temperature of -40°C or +85°C. To keep some safety margins, the T100 enters the fail-safe state when reaching ambient temperatures below -30°C or above +68°C.

When detecting the fail-safe temperature internally, it is guaranteed that still all components of the T100 are within their valid operation temperature range and will not be damaged.

4.2.2.1 Temperature verification inside CDev

To approve that the maximum temperature ratings given above for the T100 are kept in the final mounting position and under the maximum operating conditions of the CDev, the integrator has to measure the most critical temperature inside the T100 during the CDev environmental tests. Figure 4-5 shows the proper location of the temperature sensor to measure the internal environmental temperature of the T100.

Note that the temperature sensor shall be electrical non-conductive at the surface to avoid damage of the T100 during the tests.

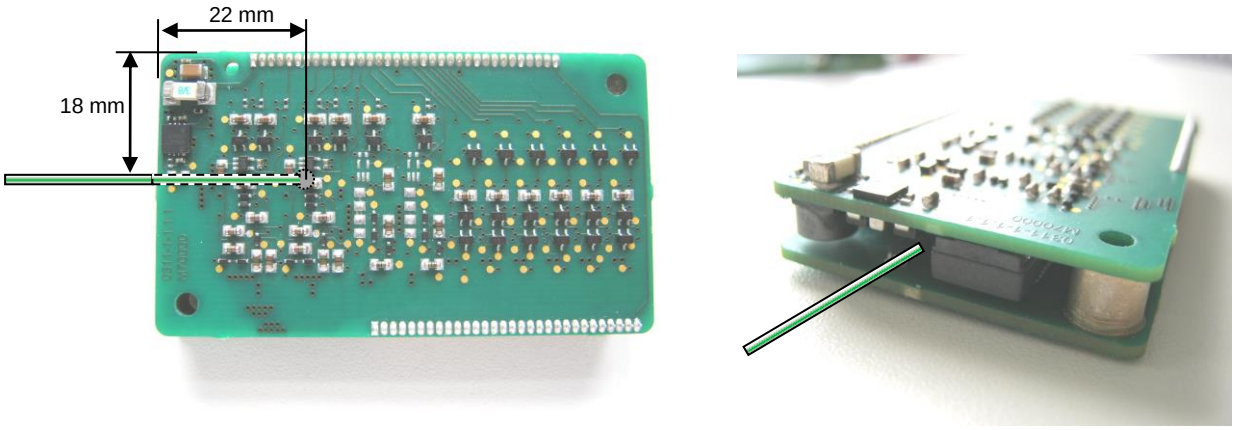


Figure 4-5: Recommended placement of temperature sensor

[IDR-4.9] **Attention:** It must be verified e.g. by test, that under worst case load and mounting position conditions inside the CDev the temperature of the IXXAT Safe T100 is always within the specified limits as listed in Table 4-1. [DR_C_ENV_TEMP], [PRS_481]

4.2.3 Shock / Vibration

The T100 is rated and tested to be used up to the following shock and vibrations limits [PRS_345]:

- Shock test, operating IEC 60068-2-27 half-sine 30g, 11 ms, 3 positive and 3 negative shocks in each of three mutually perpendicular directions.
- Shock test, operating IEC 60068-2-27 half-sine 50g, 11 ms, 3 positive and 3 negative shocks in each of three mutually perpendicular directions.
- Sinusoidal vibration, operating IEC 60068-2-6 10-500 Hz, 0.35 mm, 5g, 1oct/min., 10 double-sweep in each of three mutually perpendicular directions.

[IDR-4.12], [SAR-4.2] **Warning:** The vibration and shock limits of the final host device shall not exceed the values given in section 4.2.3 of this safety manual [PRS_345]. The limits given by IEC 60068-2-27 and IEC 60068-2-6 or a higher product standard shall be approved by tests within the final CDev.

4.2.4 Humidity and Pollution level

[IDR-4.13] **Danger:** The T100 is designed and tested to comply with IEC 60068-2-30 for a relative humidity of 5% to 95% non-condensing [PRS_344)]. Environmental tests with the integrated T100 shall be done to approve that the specified humidity levels are kept in the end device.

[IDR-4.14], [SAR-4.3] **Danger:** The storage and operating environment of the T100 shall be in the limits of pollution level 2 according to EN 60664.

4.2.5 Intrusion protection

A direct coincident contact with conducting parts of the T100 PCB shall be avoided by intrusion protection mechanisms of the end device.

[IDR-4.15] **Danger:** The intrusion protection for the T100 in the end device shall be equal or better than IP 54.

4.2.6 Maximum operation altitude

[SAR-4.4] **Danger:** The maximum operation altitude of 2000m shall not be exceeded.

4.2.7 EMC

EMC tests (electromagnetic compatibility) have to be performed on the final application together with the T100. With increased test levels (as defined in EN EN 61326-3-1) it must be verified that the safety functions of the IXXAT Safe T100 do not fail if triggered under test conditions, and that the safe state of an output channel (digital output or communication telegram) is withheld.

Application	Phenomenon	Basic Standard	EN 61326-3-1	Crit.[1]
Enclosure port	Electrostatic discharge (ESD) [2]	EN 61000-4-2	6 kV/8 kV contact/air	FS
	Electromagnetic field (EM)	EN 61000-4-3	20 V/m (80 MHz to 1 GHz) 10 V/m (1,4 GHz to 2 GHz) 3 V/m (2 GHz to 2,7 GHz)	FS
	Rated power frequency magnetic field[2]	EN 61000-4-8	30 A/m	FS
DC power ports	Burst	EN 61000-4-4	3 kV (5/50 ns, 5 kHz)	FS
	Surge	EN 61000-4-5	1 kV line to line / 2 kV line to ground	FS
	Conducted RF	EN 61000-4-6	10V (150 kHz – 80 MHz)	FS
	Voltage dips[2]	EN 61000-4-29	40% U_T for 10 ms	FS
	Short interruptions[2]	EN 61000-4-29	0% U_T for 20 ms	FS
I/O signal/ control ports	Burst	EN 61000-4-4	2 kV (5/50ns, 5 kHz)	FS
	Surge	EN 61000-4-5	2 kV	FS
	Conducted RF	EN 61000-4-6	10V (150 kHz – 80 MHz)	FS
	Conducted common mode voltage[2]	EN 61000-4-16	1,5 kHz to 15 kHz 1 V to 10 V, 20 dB/Dec. 15 kHz to 150 kHz, 10 V DC, 16 2/3 Hz, 50/60 Hz 10 V continuous 100 V short duration (1 s) 150/180 Hz, 10 V continuous	FS

[1] Criteria: FS – Fail-Safe

[2] Not pre-tested or applicable for the raw T100 module

Table 4-2: EMC ratings according to EN61326-3-1

Application	Phenomenon	Basic Standard	EN 61326-1	Crit.[1]
Enclosure port	Electrostatic discharge (ESD) [2]	EN 61000-4-2	4 kV/8 kV contact/air	B
	Electromagnetic field (EM)	EN 61000-4-3	10 V/m (80 MHz to 1 GHz) 3 V/m (1,4 GHz to 2 GHz) 1 V/m (2 GHz to 2,7 GHz)	A
	Rated power frequency magnetic field[2]	EN 61000-4-8	30 A/m	A
DC power ports	Burst	EN 61000-4-4	2 kV (5/50 ns, 5 kHz)	B
	Surge	EN 61000-4-5	1 kV line to line / 2 kV line to ground	B
	Conducted RF	EN 61000-4-6	3V (150 kHz – 80 MHz)	A
I/O signal/ control ports	Burst	EN 61000-4-4	1 kV (5/50ns, 5 kHz)	B
	Surge	EN 61000-4-5	1 kV	B
	Conducted RF	EN 61000-4-6	3V (150 kHz – 80 MHz)	A

[1] Criteria: A – no effect, B – reversible degradation,
[2] Not pre-tested or applicable for the raw T100 module

Table 4-3: EMC ratings according to EN61326-1

[IDR-4.16] **Warning:** The EMC ratings given in Table 4-2 shall not be exceeded at the mounting location of the T100 in the end device. The proper operation of the T100 safety functions shall be verified during the EMC tests of the final host device with increased test levels in accordance with IEC 61326-3-1 where applicable. Safe functions shall not fail if triggered and the safe state of the outputs shall be kept. [DR_C_ENV_EMC], [PRS_150]

4.2.7.1 T100 radiated Emission

The radiated emission of the T100 is below the limit class A given by EN55011:2009 + A1:2010 as shown in Figure 4-6. Nevertheless, the total radiated emissions of the final CDev need to be measured and checked to comply with EN 55022 or a higher product norm when applicable.

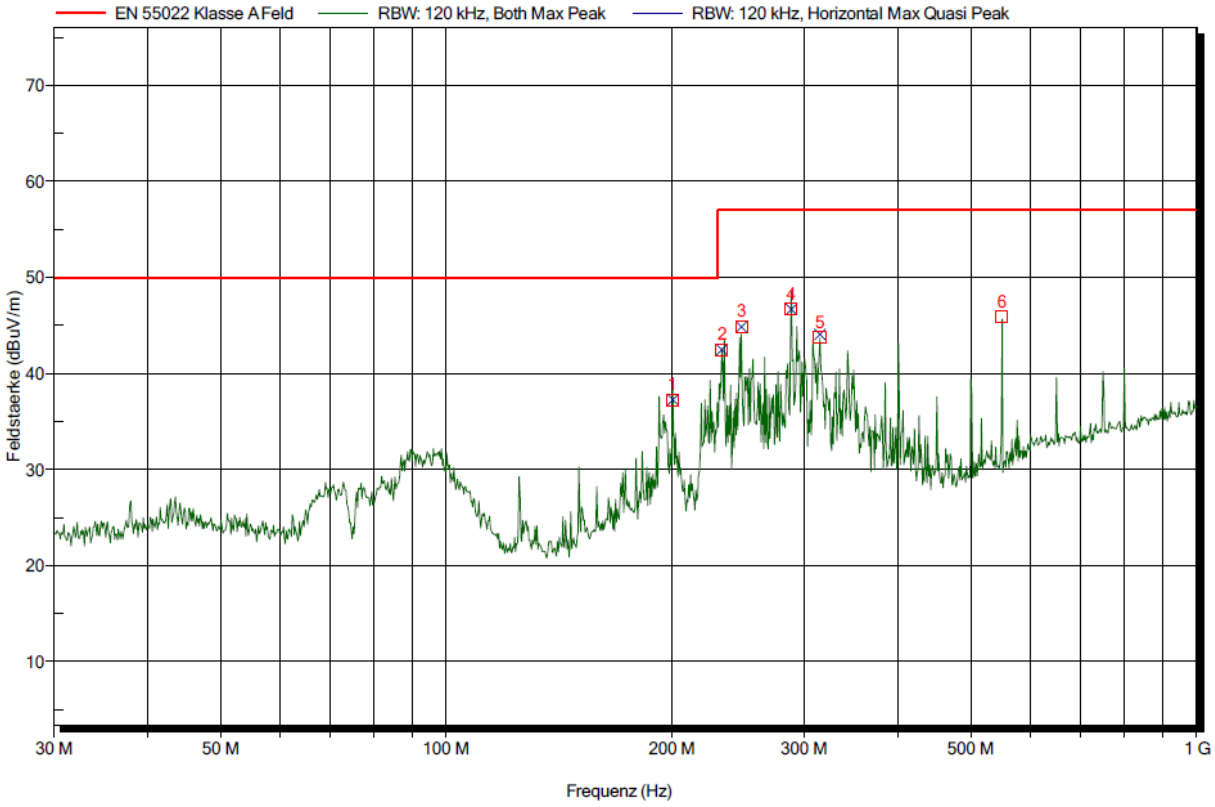


Figure 4-6: Measured radiated emission of the T100

5 Configuration and Programming

The configuration of the T100 safety Input- and Output parameters is a safety-relevant task. It has to be carried out by trained safety engineers and thoroughly verified as an improper configuration of the safety I/Os may lead to unexpected and non-safe behavior in the final application. To ensure the proper transfer of the configuration data between the safety master and the T100, CRCs are used to detect falsification of data. Note, that the CRCs for a certain configuration need to be safely calculated and transferred to the T100 using the appropriate mechanisms of the safety fieldbus protocol.

[SAR-5.1] **Danger:** Use a safe configuration tool, a specific review processes (or a combination of both) to verify that the configuration of the T100 safe I/Os are matching the safe applications' needs [SC_100].

[SAR-5.2] **Danger:** Only use a safe configuration tool to calculate the configuration CRC for the T100 or use the pre-tested configurations with the approved CRCs as listed in section 5.4 of this safety manual [SC_101].

The actually applied configuration mechanism or encapsulation protocol depends on the supported safety fieldbus protocol. Section 6.1.1.3 for example shows the description of the configuration parameters when using PROFIsafe. The actual representation and configuration tasks are depending on the configuration tool itself and can therefore not be described in general within this safety manual.

5.1 Configuration of safety inputs

The behavior of the T100 safety inputs can be configured in order to fit best for the user application. The configuration of the inputs is safety relevant and is therefore using a secured configuration process.

A series of input filters and modes can be set for each group of input signals.

Figure 5-1 gives an overview to the possible input control and filter sections.

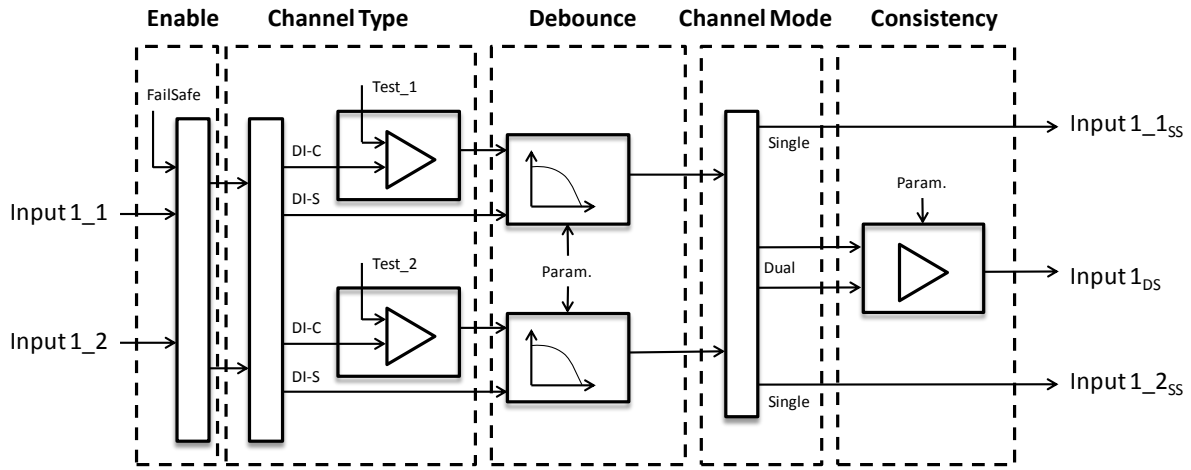


Figure 5-1: Safety input configuration and filter sections

5.1.1 Enable

Each input group can be individually enabled or disabled. When disabled, the inputs are internally considered to be in the safe state (signal level: low). When being enabled, the physical input signals of the corresponding input pins are used for further processing within the T100.

Parameter	Size	Value
Input Enable	1 Bit	0: disabled (input group reports safe state: 0/low) 1: enabled

5.1.2 Channel Type

Depending on the type of device connected to the T100 safe inputs the expected input type can be selected between contact inputs (DI-C) and semiconductor inputs (DI-S). The major difference between the two input types is the expected test-pulse pattern which is used in DI-C mode to be able to detected external wiring faults (see SAR-3.10 or IDR-3.13). In DI-S mode no test pulses are expected at the inputs which requires to observe the rules SAR-3.13 or IDR-3.14 externally. The type and parameters of the test pulses for the DI-C input settings can be configured as described in section 5.2 of this manual.

Parameter	Size	Value
Channel input type	1 Bit	0: DI-S 1: DI-C

Refer to section 3.5.1 of this manual for further details of the digital inputs of the T100.

5.1.3 Debounce Filter

The debounce filter can be configured in order to filter out short input signal drops as caused by mechanical contacts when being opened or closed or to be robust against external test pulses generated by a safety compliant output device for example. The input debounce filter time value specifies a time window (t_D) in which transient signal level changes may happen but do not affect the output state. At the end of the time window the input signal is being considered as stable and is forwarded to the T100 software logic for further processing steps (see Figure 5-2).

The T100 module applies a fix basic filter mechanism to each of the safe inputs which requires that an input signal is kept high for at least 1,2 ms to be properly detected.

The input debounce filter time can be set to prolong the fixed basic filtering with a granularity of 400µs.

Parameter	Size	Unit	Min	Typ.	Max
Input debounce filter time extension (x * 400 µs)	8 Bit	-	0 (Off)	-	255 (102 ms)

[SAR-5.3] **Warning:** Depending on the selected input debounce filter time value the input response time (i.e. the safe application time) will be increased by the given debounce filter time. [DR_I_DI]

The input response time can be calculated by the following equation:

$$6\ ms + (2\ ms * (n - 1)) + t_D$$

n: number of changed Inputs at a given point of time

t_D: Selected debounce filter time extension

Note that the debounce filter is applied to the input signal when being turned on as well as when being turned off. Therefore the input debounce filtering at the time a signal is turned on delays the transmission of the input signal change to the safety network. At the time the input signal is physically turned off again, the input debounce filter delays the forwarding of the “off” state to the safety network again.

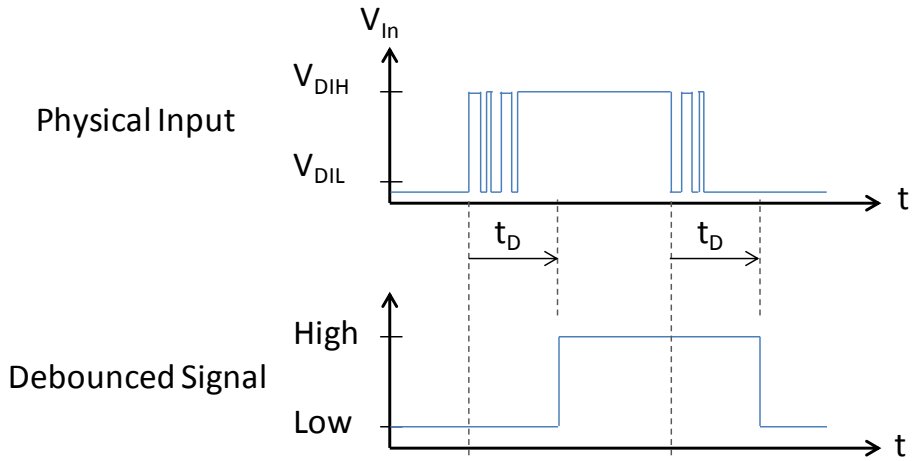


Figure 5-2: Input debounce filter

5.1.4 Channel Mode

Note: To achieve the SIL 3 and PL e Cat 4 rating, two digital inputs (Input X_1_{SS} and Input X_2_{SS}) need to be combined to one safety digital input (Input X_{DS}).

To achieve HFT=1 (hardware fault tolerance 1) each of the two digital input signals is processed by one of the two safety CPUs of the T100. In single-channel mode each channel is treated separately by the T100 which achieves HFT=0 in the end.
The following input signals are combined in dual-channel mode:

Input Group	Input Name	Input Pin
Group 1	DI 1	13
	DI 2	15
Group 2	DI 3	17
	DI 4	19
Group 3	DI 5	21
	DI 6	23

The T100 offers the parameter “Input Channel Mode” to be set for each of the three input groups above to either single channel or dual channel mode.

Parameter	Size	Value
Input channel mode	1 Bit	0: single channel input 1: dual-channel input

Note: To achieve SIL 3, PLe Cat 4 rating of the digital inputs the dual-channel mode for the inputs shall be activated.

5.1.5 Consistency Filter

In dual-channel mode each safe input has to carry identical input signals for a specified time span (t_C) in order to interpret the input is valid active. The consistency filter is used to supervise this time span.

Whenever the two channels of one dual channel input differ for a time > tc, the safe state is reported for this input channel pair.

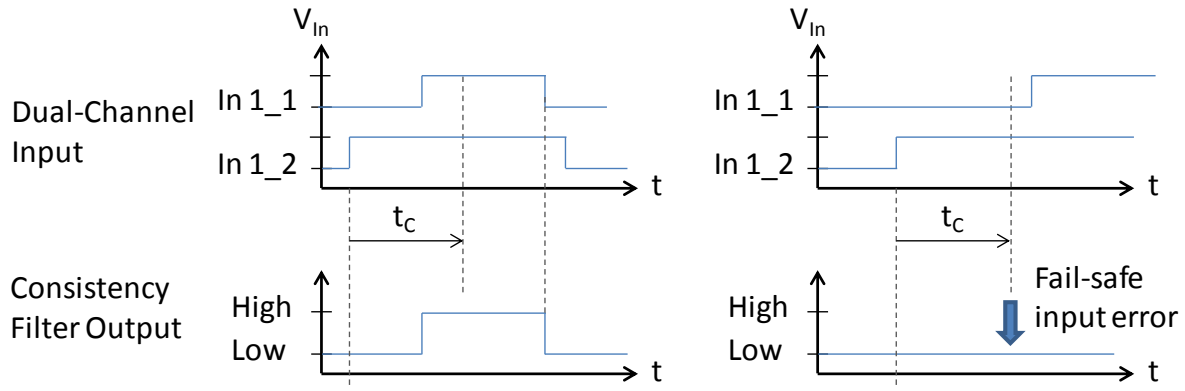


Figure 5-3: Consistency filter outputs

The consistency filter is only operated in dual channel input mode and can be individually set for the predefined input groups.

The minimum granularity of the input consistency filter time setting is 400µs.

Parameter	Size	Unit	Min	Typ.	Max
Input consistency filter time (x * 400 µs)	16 Bit	-	0 (off)	-	65535 (26,2 s)

[SAR-5.4] **Warning:** Deactivation of the consistency filter in dual-channel mode must be done in accordance with the safety application as stuck-at errors in Dual-Channel DI-S mode or short over sensor in Dual-Channel DI-C mode at one input line for example are not detected and will therefore not lead to a fail-safe input error signaling.

In general the consistency filter operation shall only take place after the input signals have reached a stable input level, i.e. the debounce time has elapsed.

[SAR-5.9] **Warning:** For a proper operation of the consistency filter, the filter time parameter shall be set to a value which is larger than the input debounce filter time parameter (see section 5.1.3).

5.1.6 Reset of Input Errors

Input errors like missing test pulses or consistency mismatches of dual-channel inputs result in a “Not-Active” or “Fail-safe” state of the affected T100 inputs channel which is also reported via the safety network protocol. To leave this channel error state a special reset action is required (see section 0). Either the error reset flag within the safety protocol data part shall be set or the AIC message “Error Confirmation” shall be sent via the serial interface from the non-safe communication controller (e.g. ABCC).

Note: Do not mix up the error reset with the T100 reset input signal RST which resets the entire T100 hard- and software. The T100 reset is only required if a global fail-safe error was detected (see section 3.6)

Parameter	**Size**	**Value**
Input reset type	1 Bit	0: manual 1: automatic – not supported; will be treated as “manual”

5.1.7 Non-safe read access

The T100 provides the filtered and processed input state of the safe inputs and outputs via the black-channel protocol to the non-safe communication module. In addition the error status flags for each safe input and output can be read as well. As this data is transferred in a non-safe way, it shall not be used to issue safe actions via the network. The safety input- and output- data is read-only on the non-safe side and can be accessed with non-safe fieldbus specific services. See section 6.1.2 for more details how to access the safe input and output data from the PROFINET side for example.

Note that in Dual-Channel mode only the combined safety input value from a channel group can be accessed on the non-safe side.

5.2 Configuration of test outputs

The test output signal can be used to detect cabling issues with external sensors in DI-C mode or to power external sensors depending on the test output signal configuration (see section 3.5.2 of this manual for further details). Detecting cross connections of sensor cables within an input group is possible by using two different test pulse patterns with a dedicated phase shift and a fixed allocation to one of the inputs of the input group as shown in Figure 5-4 and Figure 5-5.

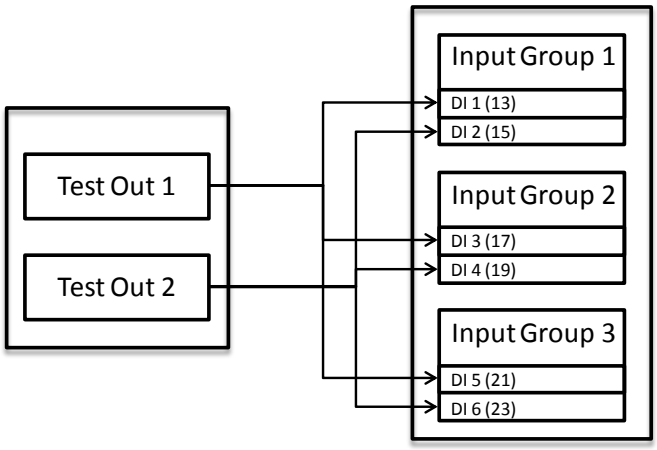


Figure 5-4: Test output allocation to input groups

The test output signal pulse length can be configured in 5 steps to an effective duration t_P of 627µs to 2847µs (HW_Delay+configured test pulse duration). The repetition time t_R = 1s and the phase shift t_S between the two test outputs are constant values. Alternatively the test output signal can be set to permanent on (24V) or permanent off (high impedance).

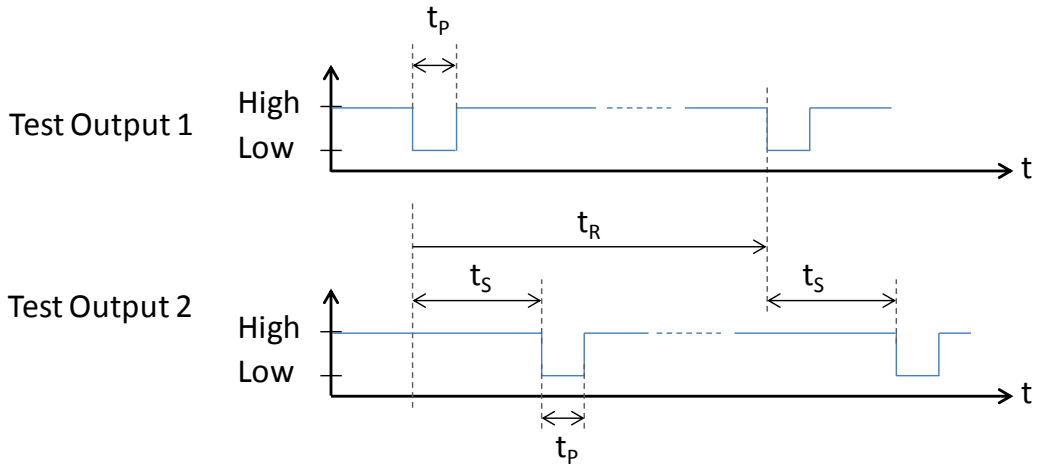


Figure 5-5: Test output signal pulse timings

Parameter	Size	Value
Test output Signal	3 Bit	000: test pulse duration 400µs + HW_Delay 001: test pulse duration 800µs + HW_Delay 010: test pulse duration 1200µs + HW_Delay 011: test pulse duration 1600µs + HW_Delay 100: test pulse duration 2000µs + HW_Delay 101: test pulse duration 2400µs + HW_Delay 110: Always low (high impedance) 111: Always high

The HW_Delay depends on the overall DI and DO processing and varies between 227 µs and 447 µs.

The test output signals are only operated in DI-C mode of the input ports. If none of the T100 input ports is configured to DI-C mode, the test outputs are typically disabled (high-impedance) regardless of the test output settings.

[SAR-5.5] **Attention:** Due to hardware limitations the T100 with 3 dual-channel inputs and one dual-channel output has only one configurable TO pair. This TO pair is configured via the test output signal configuration parameters of input group 1. Modifying TO parameters of input group 2 or 3 will have no effect.

[SAR-5.8] **Attention:** The test pulse duration of 400µs shall be used with an external Test Output load of <= 2 kOhm.

5.3 Configuration of safety outputs

The safety outputs of the T100 can be configured with the control blocks as shown in Figure 5-6 for each available output group. An output group consists of two single output lines which can be controlled separately in single-channel mode or together in dual-channel mode. The configuration is set identical for all outputs of the same output group.

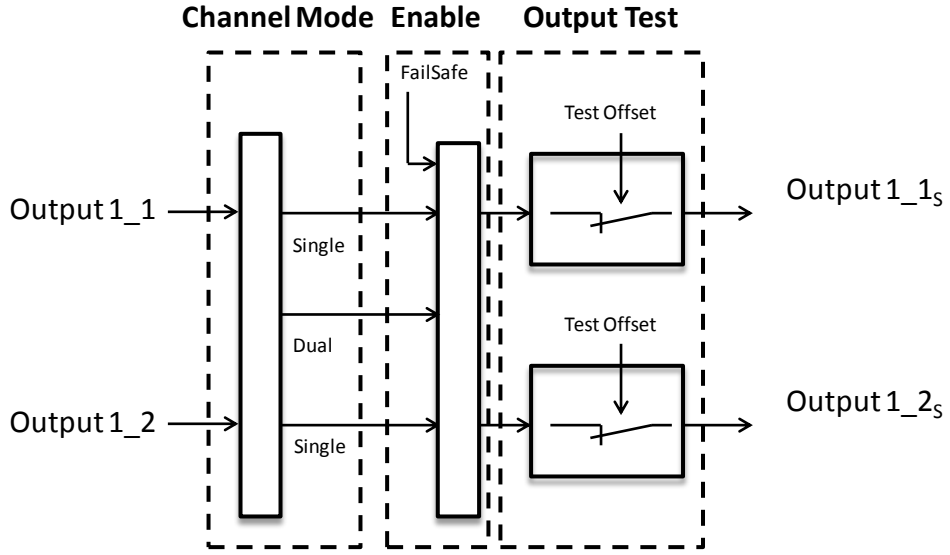


Figure 5-6: Output control blocks

5.3.1 Channel Mode

Note: To achieve the SIL 3 or PL e Cat 4 rating for the T100 outputs, the dual-channel mode shall be activated as described in section 3.5.3.

When activating the single-channel mode, each T100 output can be controlled by an individual output data bit received via the safety network. In this case the achievable SIL level or performance level strongly depends on the overall safety system design. In dual-channel mode, only one safety input bit is used to control both T100 outputs at the same time but also faults detected in one channel will lead to a deactivation of the other channel automatically by the T100.

Parameter	Size	Value
Output Channel Mode	1 Bit	0: Single Channel 1: Dual-channel

5.3.2 Enable

With the Enable parameter the output group can be either enabled or disabled. In the enabled state, the output can be controlled by the data received via the safety network. When disabled, each output of the output group is set to the fail-safe (low) value. Due to the used high-side switches, the fail-safe low-state is a high impedance floating level.

Parameter	Size	Value
Output Enable	1 Bit	0: Disabled 1: Enabled

5.3.3 Output test

The safe operation of the T100 outputs is checked in an interval t_{Repeat} of 1 second when being activated. During the output test, the T100 turns off the output high-side switch and first waits for a drop-down of the output signal for at least t_{Wait}. Afterwards the T100 issues an internal discharge to force a complete drop-down of the output signal before it checks for a proper low-level of the output (see Figure 5-7). If the proper low-level is not reached, the T100 sets the output channel into the fail-safe state. In dual-channel mode all channels of an output group are set to their fail-safe state if the output test of at least one channel fails. In single-channel mode only the output detecting the error will be set to fail-safe state. Any output error is reported also via the safety network.
The output test pulse length is typically 1,2 ms [SC_324]. The safe actor connected to the T100 output pins therefore has to be tolerant against these output test pulses. Within this test-pulse sequence internal output circuit errors but also short-circuits to VSS will be detected which leads to the fail-safe state of the output or output group.

In some applications it might be necessary to use the pulses generated by the T100 outputs on the input device side again to check for a safe connection or to allow larger discharge times at the output. If necessary, the 1,2 ms test pulse length of the T100 can be prolonged using the configuration parameter “Output Test Offset (extension)”.

Parameter	Size	Value
Output Test Offset (extension)	4 Bit	0: No Offset 1..15 extension of 1,2 ms test output signal in steps of x * 400µs

[SAR-5.6] **Warning:** Output test pulses are only generated if the output is set active / high. In safe-state (low, high-impedance) no test pulses are generated.

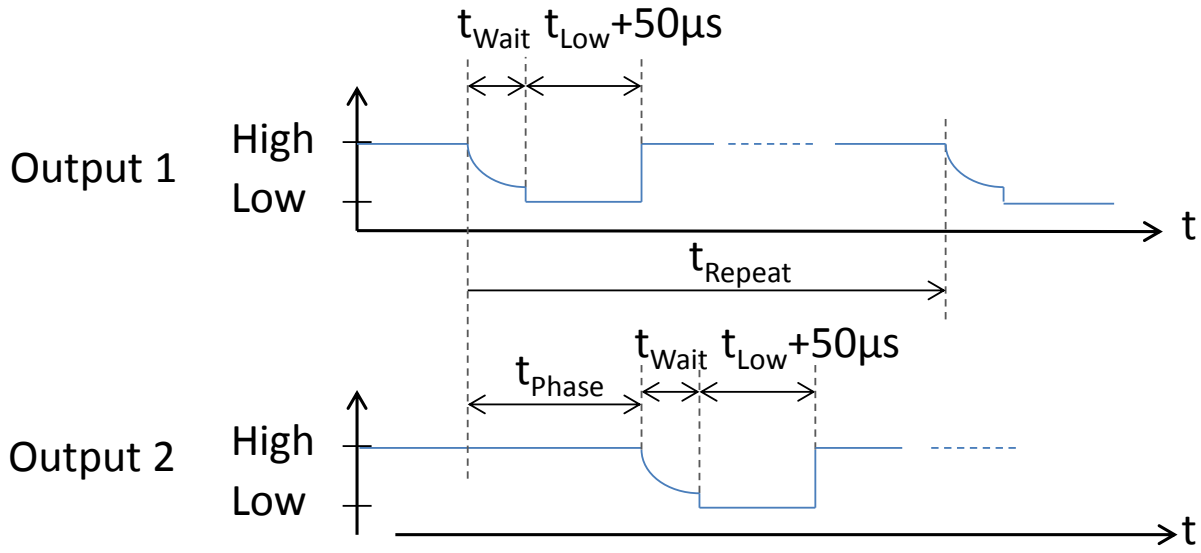


Figure 5-7: Output test pulse timing

Parameter	Unit	Min	Typ.	Max
t_{Wait}	ms	-	0,3	-
t_{Low} ($t_{Low, min}$ + t_{Offset})	ms	0,9	-	6,95

t_{Phase} is a constant value which is always set internally larger than t_{Wait} + t_{Low} in order to keep at least one output on during a single channel DO test.

Due to other internal tests of the DO circuits up to three test pulses with a minimum length of 1,2 ms are visible at each output within the overall 1 Hz test repetition frequency.

5.3.4 Output Error Reset

Whenever the T100 detects an error that leads to a fail-safe state, the outputs are set to their fail-safe values. To re-enable the outputs either an automatic or a manual error reset is required. Note that only channel-specific errors such as short circuits at the output will cause a fail-safe state of the output channel. A global T100 fail-safe state leads to a permanent DO disabling which requires a hard reset of the T100 to recover.

[SAR-5.7] **Attention:** If manual output error reset is configured, any output error will be reset, when receiving a valid safety network message containing the appropriate error reset bit transition [PRS_141].

The output error reset shall not be mixed up with the T100 reset signal RST which resets the entire T100 soft- and hardware. Nevertheless, this hardware reset also forces to leave the T100 fail-safe state and to perform a complete self-test of the T100 soft- and hardware.

Parameter	**Size**	**Value**
Output Reset Type	1 Bit	0: manual 1: automatic – not supported; same behavior than manual

5.4 Pre-tested configurations

The above described configuration settings allow a large number of parameter variations. In the following sections, a list of pre-tested configurations is given together with their approved configuration iPar CRC values.

[SAR-5.10] **Warning:** Using any other configuration than the ones listed in section 5.4.1, 5.4.2 or 5.4.3 requires a functional validation on application level to approve the proper operation of the overall safety function.

5.4.1 Dual-Channel DI-C

Parameter	Dual-Channel DI-C
CH1/2: Input Enabled	Enable
CH1/2: Input Channel Mode	Dual Channel
CH1/2: Input Type	DIC
CH1/2: Input Reset Type	Manual
CH1/2: Input Test Output Signal	800us
CH1/2: Input Debounce Filter Time (400us steps)	125
CH1/2: Input Consistency Filter Time (400us steps)	625
CH3/4: Input Enabled	Enable
CH3/4: Input Channel Mode	Dual Channel
CH3/4: Input Type	DIC
CH3/4: Input Reset Type	Manual
CH3/4: Input Test Output Signal	800us
CH3/4: Input Debounce Filter Time (400us steps)	125
CH3/4: Input Consistency Filter Time (400us steps)	625
CH5/6: Input Enabled	Enable
CH5/6: Input Channel Mode	Dual Channel
CH5/6: Input Type	DIC
CH5/6: Input Reset Type	Manual
CH5/6: Input Test Output Signal	800us
CH5/6: Input Debounce Filter Time (400us steps)	125
CH5/6: Input Consistency Filter Time (400us steps)	625
CH1/2: Output Enabled	Enable
CH1/2: Output Channel Mode	Dual Channel
CH1/2: Output Reset Type	Manual
CH1/2: Output Test Offset (extension)	No Offset
iPar CRC	**0x3807E28D**

5.4.2 Dual-Channel DI-S

Parameter	Dual-Channel DI-S
CH1/2: Input Enabled	Enable
CH1/2: Input Channel Mode	Dual Channel
CH1/2: Input Type	DIS
CH1/2: Input Reset Type	Manual
CH1/2: Input Test Output Signal	800us
CH1/2: Input Debounce Filter Time (400us steps)	0
CH1/2: Input Consistency Filter Time (400us steps)	25
CH3/4: Input Enabled	Enable
CH3/4: Input Channel Mode	Dual Channel
CH3/4: Input Type	DIS
CH3/4: Input Reset Type	Manual
CH3/4: Input Test Output Signal	800us
CH3/4: Input Debounce Filter Time (400us steps)	0
CH3/4: Input Consistency Filter Time (400us steps)	25
CH5/6: Input Enabled	Enable
CH5/6: Input Channel Mode	Dual Channel
CH5/6: Input Type	DIS
CH5/6: Input Reset Type	Manual
CH5/6: Input Test Output Signal	800us
CH5/6: Input Debounce Filter Time (400us steps)	0
CH5/6: Input Consistency Filter Time (400us steps)	25
CH1/2: Output Enabled	Enable
CH1/2: Output Channel Mode	Dual Channel
CH1/2: Output Reset Type	Manual
CH1/2: Output Test Offset (extension)	No Offset
iPar CRC	**0x72245A9D**

5.4.3 Mixed DI-C Dual/Single Channel

Parameter	Mixed DI-C Dual/Single
CH1/2: Input Enabled	Enable
CH1/2: Input Channel Mode	Dual Channel
CH1/2: Input Type	DIC
CH1/2: Input Reset Type	Manual
CH1/2: Input Test Output Signal	800us
CH1/2: Input Debounce Filter Time (400us steps)	125
CH1/2: Input Consistency Filter Time (400us steps)	625
CH3/4: Input Enabled	Enable
CH3/4: Input Channel Mode	Dual Channel
CH3/4: Input Type	DIC
CH3/4: Input Reset Type	Manual
CH3/4: Input Test Output Signal	800us
CH3/4: Input Debounce Filter Time (400us steps)	125
CH3/4: Input Consistency Filter Time (400us steps)	625
CH5/6: Input Enabled	Enable
CH5/6: Input Channel Mode	Single Channel
CH5/6: Input Type	DIC
CH5/6: Input Reset Type	Manual
CH5/6: Input Test Output Signal	800us
CH5/6: Input Debounce Filter Time (400us steps)	125
CH5/6: Input Consistency Filter Time (400us steps)	0
CH1/2: Output Enabled	Enable
CH1/2: Output Channel Mode	Dual Channel
CH1/2: Output Reset Type	Manual
CH1/2: Output Test Offset (extension)	0us
iPar CRC	**0x35B02548**

6 Safety fieldbus communication

6.1 PROFIsafe

The T100 version supporting the PROFIsafe protocol is named „IXXAT Safe T100/PS" or just "T100/PS". The currently supported PROFIsafe profile version is V2.4.

Basically the T100/PS runs the PROFIsafe slave communication protocol software which is used to transfer input- and output data from and to a PROFIsafe PLC, also called "F-Host". Beside this cyclic safe data exchange, also parameterization data shall be transferred from the F-Host to the T100/PS. This data is acyclically exchanged and uses the standard PROFINET services on the lower communication layers. Independent transfer channels and checksums ensure the proper and safe data exchange in the field.

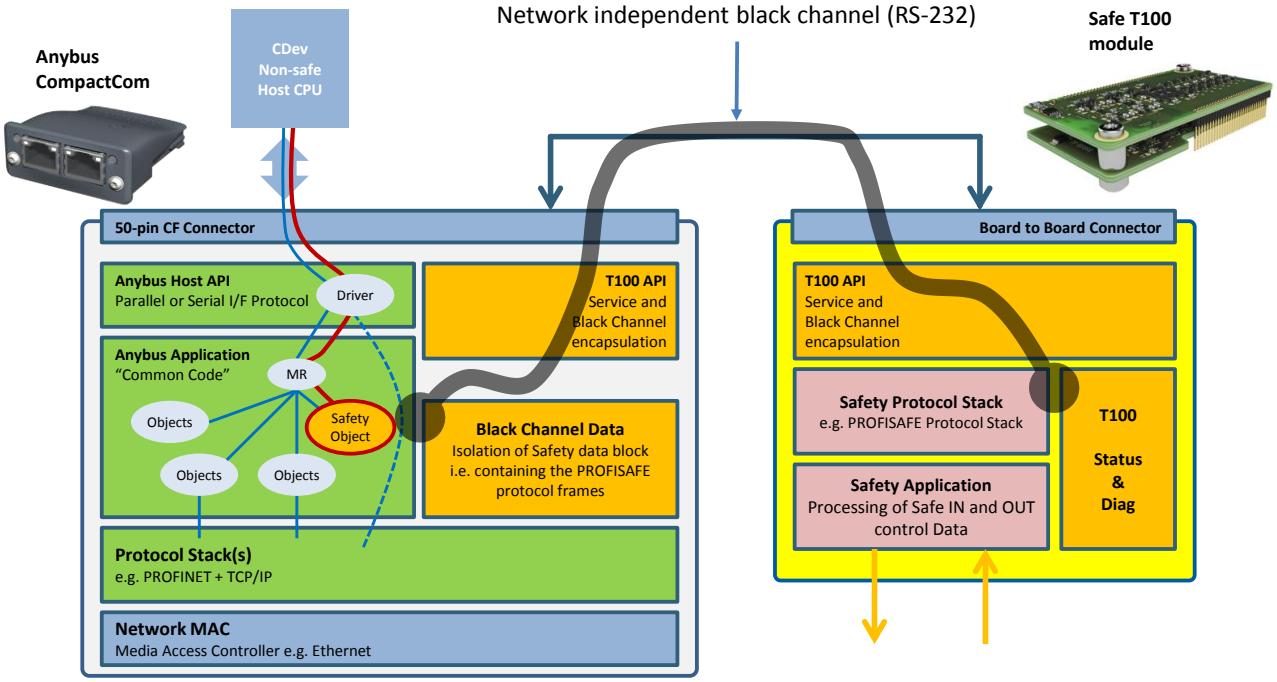


Figure 6-1: Block diagram of PROFINET/PROFIsafe Anybus CompactCom and T100/PS

6.1.1 PROFIsafe configuration sequence

The following configuration sequence describes the PROFIsafe configuration steps to be done when using the SIEMENS Step7 or TIA Portal Engineering tools.

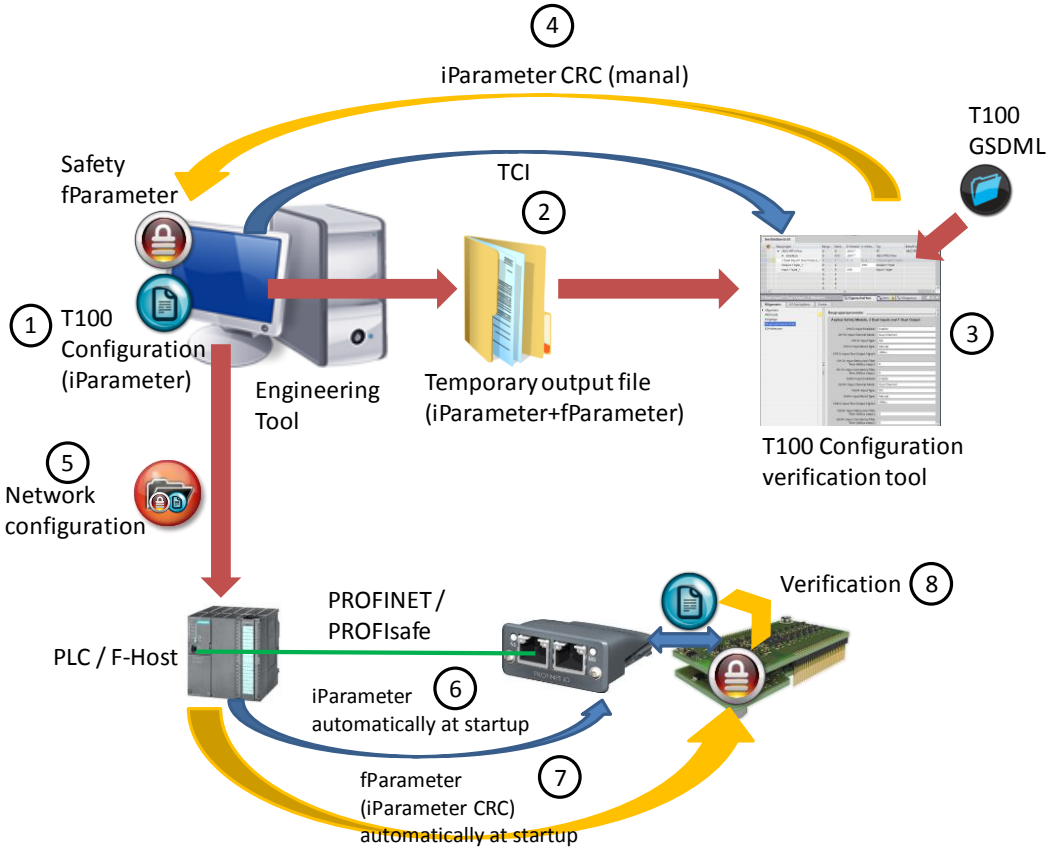


Figure 6-2: PROFIsafe configuration sequence

Step	Description
1	Setup of non-safe and safe parameters within the PLC engineering tool
2	Export of safe and non-safe configuration parameters for the T100/PS and its non-safe communication controller (e.g. ABCC running PROFINET)
3	T100/PS configuration check and CRC calculation tool is invoked (see section 6.1.1.4). The tool checks the proper configured values for plausibility and calculates the iParameter CRC
4	The calculated iParameter CRC is copied into the fParameter block within the PLC engineering tool
5	The PLC engineering tool stores the iParameter and fParameter of the entire network (including the T100/PS) within the F-Host
6	At startup the F-Host transfers the iParameter to the non-safe communication module (using the ABCC safety object instance)

	which forwards the data to the T100/PS using AIC channel messages
7	In addition the fParameters are transferred from the F-Host to the non-safe communication module. There the fParameter data is forwarded to the T100/PS again via the AIC channel.
8	Based on the iParameter set received, the T100/PS calculates the expected iParameter CRC and compares it against the received iParameter CRC within the fParameter data block. Only if both iParameter CRCs match, the T100/PS will start up correctly

6.1.1.1 F-Parameter setup

The following fParameter are necessary to be set and transferred to the T100/PS by the non-safe communication module according to the PROFIsafe profile. When using the Anybus CompactCom device, these parameters can be found in the safety object instance.

Parameter	**Data length**	**Value range**	**Description**
F-Source Address	16 Bit	1 .. 65534	Unique source address of a PROFIsafe message
F-Destination Address	16 Bit	1 .. 65534	Unique destination address; must be equal to locally set F-Address of the T100/PS
Watchdog Time	16 Bit	20 .. 10000	PROFIsafe connection watchdog time in ms
Parameter Flag 1	8 Bit	0 .. 255	Parameter Flags
Parameter Flag 2	8 Bit	0 .. 255	Parameter Flags
iParameter CRC	32 Bit	1 .. 2^{32}	iParameter CRC built across the iParameter set by a configuration tool for example
fParameter CRC	16 Bit	0 .. 65535	fParameter CRC build across the above fParameter values by the engineering tool

In the following sections the most important fParameters for the T100/PS operation are described in more detail.

6.1.1.1.1 F-Address

The F-Address data is used by the F-Host and the F-Devices (e.g. T100/PS) to uniquely identify a safe data connection. At startup (during Init-state, see 3.10) the locally set F-Address on the T100/PS is used to initialize the PROFIsafe communication software (see document HMSI-168-49 section 10.5, Instance

#20 attribute how to set the F-address). Once the F-Destination address is received during Parametrization-state (see 3.10) as part of the fParameter data block, the T100/PS checks if the two addresses match. Only if the local F-Address is equal to the F-Destination address received, the T100/PS is allowed to continue its startup.

6.1.1.1.2 Watchdog time

The PROFIsafe watchdog time shall not be mixed up with the T100/PS internal HW watchdogs which trigger the safe state of the entire module. The PROFIsafe Watchdog time received within the fParameter data block is used to monitor the cyclic PROFIsafe communication. If no new PROFIsafe message with valid content is received within the configured Watchdog time, the T100/PS will set the DO and DI values to their fail-safe values and will wait for a restart of the PROFIsafe communication.

The Watchdog time shall take the T100/PS acknowledge time as well as the Bus transfer times and the F-Host processing times into consideration. For more details, please refer to the PROFIsafe profile specification V2.4 section 9.3.3.

6.1.1.1.3 iParameter CRC

The iParameter CRC is used by the T100/PS to check the proper reception of the iParameter data. After complete reception of the iParameter data, the T100/PS locally calculates the CRC value out of this data set. Once the fParameter data block is received, the transferred (expected) iParameter CRC can be extracted by the T100/PS and checked against the locally calculated one. Only in case of a match of the two CRC values, the T100/PS will be able to enter the Run-state (see section 3.10).

The iParameter CRC mismatch can be caused by the following errors:

- iParameter falsification during transfer.
- Engineering tool iParameter set mismatch.
- Missing update of iParameter CRC within the fParameter data block after changes in the iParameter set.
- iParameter CRC contains the main SW revision of the T100/PS firmware. In case of incompatible configuration values with future T100/PS firmware version, the iParameter CRC check will report an error.

6.1.1.2 iParameter setup

The application configuration is done offline using first of all the PLC engineering tool to set up the non-safe and safe functionality by accessing the corresponding safe and non-safe input- and output memory areas of the T100/PS. During this process the safety-relevant fParameters of the T100/PS must be set up as well within the engineering tool.

In order to verify and confirm the configured safety-relevant parameters of the T100/PS a diverse redundant approach is used by invoking a special configuration check and CRC calculation tool [DR_C_CFG_CRC]. Within this tool the configuration done for the T100/PS within the engineering tool is displayed again for manual inspection and release. If the configuration is rated to be safe, the tool generates the 32-Bit iParameter CRC which allows detection of data falsification on the way between the F-Host and the T100/PS.

The configuration data transfer of the safe digital inputs and outputs as described in section 5 is based on the PROFINET iParameter service. This service allows the asynchronous transfer of configuration data at startup of the PROFINET communication prior to the start of the PROFIsafe communication protocol. The non-safe communication controller (e.g. ABCC running PROFINET) has to provide an iParameter object which can be used by the F-Host to write the application specific configuration parameters to. Via the AIC protocol received iParameter data has to be written from the non-safe communication controller to the T100/PS.

iParameters are neither stored by the T100/PS nor the ABCC. Typically these parameters are transferred by the F-Host to the F-Device (ABCC and T100/PS) and validated within the T100/PS at each startup. In case of a mismatch between the CRC calculated from the received iParameter data and the CRC received via the fParameter service, the outputs of the T100/PS will stay in the safe state and a configuration error message is sent. [SC_101].

Note that the T100/PS does not support the iPar Server functionality.

Invalid configurations for a certain soft- or hardware version of the T100/PS are detected by including the T100/PS SW major revision (see section 1.3.3) and its module identifier (see section 3.9) into the calculation of the iParameter CRC.

[SAR-6.1] **Warning**: Documentation (and Review) of the configured iParameter for a certain safe application is mandatory and requires the safe generation and storage of the iParameter data set as supplement for the safety assessor of the entire safety system. [SC_100, DR_C_CFG_DEF]

The following iParameter values need to be configured and transferred to the T100/PS for a proper operation:

Parameter		**Size**	**Description / value**
Input 1,2			
	Enabled	1 Bit	0: disabled 1: enabled
	Channel Mode	1 Bit	0: single channel 1: dual-channel
	Channel Type	1 Bit	0: DI-S 1: DI-C
	Reset Type	1Bit	0: manual 1: automatic - not supported
	Test Output Signal	3 Bit	Test-pulse duration 0 .. 5: pulse extension by x*400µs 6: TO always off 7: TO always on
	Reserved	1 Bit	
	Input Debounce filter time	8 Bit	Debounce filter time in 400µs steps 0 .. 255
	Input Consistency filter time	16 Bit	Consistency check time in dual-channel mode given in x*400µs 0: consistency check deactivated 1 .. 2^{16} : x*400µs
Input 3,4			
	Enabled	1 Bit	0: disabled 1: enabled
	Channel Mode	1 Bit	0: single channel 1: dual-channel
	Channel Type	1 Bit	0: DI-S 1: DI-C
	Reset Type	1Bit	0: manual 1: automatic - not supported
	Test Output Signal	3 Bit	Test-pulse duration 0 .. 5: pulse extension by x*400µs 6: TO always off 7: TO always on
	Reserved	1 Bit	
	Input Debounce filter time	8 Bit	Debounce filter time in 400µs steps 0 .. 255
	Input	16 Bit	Consistency check time in dual-

	Consistency filter time		channel mode given in x*400µs 0: consistency check deactivated 1 .. 2^{16} : x*400µs
Input 5,6			
	Enabled	1 Bit	0: disabled 1: enabled
	Channel Mode	1 Bit	0: single channel 1: dual-channel
	Channel Type	1 Bit	0: DI-S 1: DI-C
	Reset Type	1Bit	0: manual 1: automatic - not supported
	Test Output Signal	3 Bit	Test-pulse duration 0 .. 5: pulse extension by x*400µs 6: TO always off 7: TO always on
	Reserved	1 Bit	
	Input Debounce filter time	8 Bit	Debounce filter time in 400µs steps 0 .. 255
	Input Consistency filter time	16 Bit	Consistency check time in dual-channel mode given in x*400µs 0: consistency check deactivated 1 .. 2^{16} : x*400µs
Output 1,2			
	Enabled	1 Bit	0: disabled 1: enabled
	Channel Mode	1 Bit	0: single channel 1: dual-channel
	Reset Type	1 Bit	0: manual 1: automatic - not supported
	Reserved	1 Bit	
	Output Test Offset	4 Bit	Output test pulse length in x*400µs 0 .. 15

6.1.1.3 GSD file

The available and valid iParameter and fParameter values of the T100/PS are described within the GSD (General Station Description) file of the T100/PS or the non-safe communication controller offering the iParameter object.

```
<RecordDataList>
  <ParameterRecordDataItem Index="28673" Length="15">
    <Name TextId="T_ID_PROFILE_T100_3DIN1DOUT_IPAR"/>
    <Const Data="0x03,0x01,0x07,0x00,0x00,0x00,0x07,0x00,0x00,0x00,0x07,0x00,
                 0x00,0x00,0x03"/>
    <Ref ValueItemTarget="V_ID_T100_ENABLE" ByteOffset="2" DataType="Bit"
                          BitOffset="0" DefaultValue="1"
                          TextId="T_ID_T100_3DIN1DOUT_IN_1_ENABLE"/>
    <Ref ValueItemTarget="V_ID_T100_INOUT_CHANNEL_MODE" ByteOffset="2"
                          DataType="Bit" BitOffset="1" DefaultValue="1"
                          TextId="T_ID_T100_3DIN1DOUT_IN_1_CHANNEL_MODE"/>
    <Ref ValueItemTarget="V_ID_T100_INTYPE" ByteOffset="2" DataType="Bit"
                          BitOffset="2" DefaultValue="1"
                          TextId="T_ID_T100_3DIN1DOUT_IN_1_TYPE"/>
    <Ref ValueItemTarget="V_ID_T100_IN_RES_TYPE" ByteOffset="2" DataType="Bit"
                          BitOffset="3" DefaultValue="0"
                          TextId="T_ID_T100_3DIN1DOUT_IN_1_RES_TYPE"/>
    <Ref ValueItemTarget="V_ID_T100_IN_TEST_OUT" DataType="BitArea"
                          ByteOffset="2" BitOffset="4" BitLength="3"
                          DefaultValue="0" AllowedValues="0..7" Changeable="true"
                          Visible="true"
                          TextId="T_ID_T100_3DIN1DOUT_IN_1_TEST_OUT"/>
    <Ref DataType="Unsigned8" ByteOffset="3" DefaultValue="0"
                          AllowedValues="0..255"
                          TextId="T_ID_T100_3DIN1DOUT_IN_1_CONS_DEBOUNCE"/>
    <Ref DataType="Unsigned16" ByteOffset="4" DefaultValue="0"
                          AllowedValues="0..65535"
                          TextId="T_ID_T100_3DIN1DOUT_IN_1_CONS_FILTER"/>
    <Ref ValueItemTarget="V_ID_T100_ENABLE" ByteOffset="6" DataType="Bit"
                          BitOffset="0" DefaultValue="1"
                          TextId="T_ID_T100_3DIN1DOUT_IN_2_ENABLE"/>
    <Ref ValueItemTarget="V_ID_T100_INOUT_CHANNEL_MODE" ByteOffset="6"
                          DataType="Bit" BitOffset="1" DefaultValue="1"
                          TextId="T_ID_T100_3DIN1DOUT_IN_2_CHANNEL_MODE"/>
    <Ref ValueItemTarget="V_ID_T100_INTYPE" ByteOffset="6" DataType="Bit"
                          BitOffset="2" DefaultValue="1"
                          TextId="T_ID_T100_3DIN1DOUT_IN_2_TYPE"/>
    <Ref ValueItemTarget="V_ID_T100_IN_RES_TYPE" ByteOffset="6" DataType="Bit"
                          BitOffset="3" DefaultValue="0"
                          TextId="T_ID_T100_3DIN1DOUT_IN_2_RES_TYPE"/>
    <Ref ValueItemTarget="V_ID_T100_IN_TEST_OUT" DataType="BitArea"
                          ByteOffset="6" BitOffset="4" BitLength="3"
                          DefaultValue="0" AllowedValues="0..7" Changeable="true"
                          Visible="true"
                          TextId="T_ID_T100_3DIN1DOUT_IN_2_TEST_OUT"/>
    <Ref DataType="Unsigned8" ByteOffset="7" DefaultValue="0"
                          AllowedValues="0..255"
                          TextId="T_ID_T100_3DIN1DOUT_IN_2_CONS_DEBOUNCE"/>
```

```
    <Ref DataType="Unsigned16" ByteOffset="8" DefaultValue="0"
                         AllowedValues="0..65535"
                         TextId="T_ID_T100_3DIN1DOUT_IN_2_CONS_FILTER"/>
    <Ref ValueItemTarget="V_ID_T100_ENABLE" ByteOffset="10" DataType="Bit"
                         BitOffset="0" DefaultValue="1"
                         TextId="T_ID_T100_3DIN1DOUT_IN_3_ENABLE"/>
    <Ref ValueItemTarget="V_ID_T100_INOUT_CHANNEL_MODE" ByteOffset="10"
                         DataType="Bit" BitOffset="1" DefaultValue="1"
                         TextId="T_ID_T100_3DIN1DOUT_IN_3_CHANNEL_MODE"/>
    <Ref ValueItemTarget="V_ID_T100_INTYPE" ByteOffset="10" DataType="Bit"
                         BitOffset="2" DefaultValue="1"
                         TextId="T_ID_T100_3DIN1DOUT_IN_3_TYPE"/>
    <Ref ValueItemTarget="V_ID_T100_IN_RES_TYPE" ByteOffset="10" DataType="Bit"
                         BitOffset="3" DefaultValue="0"
                         TextId="T_ID_T100_3DIN1DOUT_IN_3_RES_TYPE"/>
    <Ref ValueItemTarget="V_ID_T100_IN_TEST_OUT" DataType="BitArea"
                         ByteOffset="10" BitOffset="4" BitLength="3"
                         DefaultValue="0" AllowedValues="0..7" Changeable="true"
                         Visible="true"
                         TextId="T_ID_T100_3DIN1DOUT_IN_3_TEST_OUT"/>
    <Ref DataType="Unsigned8" ByteOffset="11" DefaultValue="0"
                         AllowedValues="0..255"
                         TextId="T_ID_T100_3DIN1DOUT_IN_3_CONS_DEBOUNCE"/>
    <Ref DataType="Unsigned16" ByteOffset="12" DefaultValue="0"
                         AllowedValues="0..65535"
                         TextId="T_ID_T100_3DIN1DOUT_IN_3_CONS_FILTER"/>
    <Ref ValueItemTarget="V_ID_T100_ENABLE" ByteOffset="14" DataType="Bit"
                         BitOffset="0" DefaultValue="1"
                         TextId="T_ID_T100_3DIN1DOUT_OUT_1_ENABLE"/>
    <Ref ValueItemTarget="V_ID_T100_INOUT_CHANNEL_MODE" ByteOffset="14"
                         DataType="Bit" BitOffset="1" DefaultValue="1"
                         TextId="T_ID_T100_3DIN1DOUT_OUT_1_CHANNEL_MODE"/>
    <Ref ValueItemTarget="V_ID_T100_IN_RES_TYPE" ByteOffset="14" DataType="Bit"
                         BitOffset="2" DefaultValue="0"
                         TextId="T_ID_T100_3DIN1DOUT_OUT_1_RES_TYPE"/>
    <Ref ValueItemTarget="V_ID_T100_OUT_TEST_OUT_OFFSET" DataType="BitArea"
                         ByteOffset="14" BitOffset="4" BitLength="4"
                         DefaultValue="0" AllowedValues="0..10" Changeable="true"
                         Visible="true"
                         TextId="T_ID_T100_3DIN1DOUT_OUT_1_TEST_OUT_OFFSET"/>
  </ParameterRecordDataItem>

  <F_ParameterRecordDataItem Index="28672" F_ParamDescCRC="59655">
    <F_Check_iPar DefaultValue="NoCheck" Visible="false" Changeable="false"/>
    <F_SIL DefaultValue="SIL2" AllowedValues="SIL2 SIL3" Visible="true"
                        Changeable="true"/>
    <F_CRC_Length DefaultValue="3-Byte-CRC" Visible="true"/>
    <F_Block_ID DefaultValue="1" AllowedValues="1" Changeable="false"/>
    <F_Par_Version/>
    <F_Source_Add AllowedValues="1..65534"/>
    <F_Dest_Add AllowedValues="1..65534"/>
    <F_WD_Time DefaultValue="150" AllowedValues="20..10000"/>
    <F_Par_CRC DefaultValue="25685"/>
    <F_iPar_CRC DefaultValue="66651370"/>
  </F_ParameterRecordDataItem>
</RecordDataList>
```

[IDR-6.1] **Attention:** The final GSD file of the CDev shall contain the iParameter and fParameter block of the T100/PS. This block can be copied from the reference GSD file provided with the T100/PS and shall not be modified [PRS_227].

6.1.1.4 iParameter CRC calculation tool

The iParameter CRC is calculated based on the iParameter described in section 6.1.2. Additionally the major software version of the T100/PS firmware and the module identifier (see section 3.9) is considered by the iParameter CRC to make sure that the CRC calculated by the offline configuration tool for a certain T100/PS is only valid for the given configuration data and T100/PS version.

The safe iParameter CRC calculation tool is available as download from the T100 product webpage under www.ixxat.de. More information such as a user manual for this tool can be found there as well.

6.1.2 F-Data exchange

The IXXAT Safe T100/PS checks the digital inputs. If they are active and no error has been detected, the status “active” will be reported via a PROFIsafe telegram. If any error was detected, T100/PS reports the input as “inactive” via PROFIsafe. Additionally a qualifier bit indicates that the corresponding input or output is in fail-safe state. Depending on the error type (see section 3.6) an error message as described in section 0 may be transferred additionally.

The T100/PS checks the received PROFIsafe telegrams. Only if the telegram is ok, the T100/PS sets the digital outputs according the message. If the telegram was not ok or any other failure occurred the outputs are set to “inactive”. All the T100/PS input and output data as well as the qualifier bits can be accessed in a non-safe way for reading by e.g. the local non-safe CDev host processor.

6.1.2.1 Input process image

The input process image contains the data and status collected from the local digital inputs of the T100/PS as well as the PROFIsafe frame elements which are to be transported via PROFINET from the T100/PS to the F-Host.

	Bit 0	**Bit 1**	**Bit 2**	**Bit 3**	**Bit 4**	**Bit 5**	**Bit 6**	**Bit 7**
Byte 0	DI_1	DI_2	DI_3	DI_4	DI_5	DI_6	Res.	Res.
Byte 1	QDI_1	QDI_2	QDI_3	QDI_4	QDI_5	QDI_6	Res.	Res.
Byte 2	QDO_1	QDO_2	Res.	Res.	Res.	Res.	Res.	Res.
Byte 3	PROFIsafe Control Byte							
Byte 4	PROFIsafe CRC2							
Byte 5								
Byte 6								

Configuration	**Dual-Channel**	**Single-Channel**
DI_1, DI_3, DI_5	Current state of the Dual-Channel Inputs	Current state of the inputs located at µC1
DI_2, DI_4, DI_6	Unused / Current state of the Dual-Channel Inputs	Current state of the inputs located at µC2
QDI_1, QDI_3, QDI_5	Qualifier of the Dual-Channel Inputs	Qualifier of the inputs located at µC1
QDI_2, QDI_4, QDI_6	Unused / Qualifier of the Dual-Channel Inputs	Qualifier of the inputs located at µC2
QDO_1	Qualifier of the Dual-Channel Output	Qualifier of the output located at µC1
QDO_2	Unused / Qualifier of the Dual-Channel Output	Qualifier of the output located at µC2

The qualifier bits QDI_x indicate whether a fail-safe error was detected at the corresponding input or output channel of the T100/PS. If set to 0, the input or output state is “fail-safe”, i.e. the input data contains the fail-safe values or the output is locally set to the fail-safe value by the T100/PS. A qualifier with the value 1 indicates that the input or output is operated without any fail-safe errors. Note, that the input- and output channel qualifiers are operated individually, i.e. the qualifiers show the error state only for the corresponding channel or channel group. Other channels may still operate correctly.

Bit	Value	Description
DI_x	0	Input channel inactive (safe state)
	1	Input channel active
QDI_x	0	Input channel status “error” (see section 3.6 for possible errors). DI_x set to inactive / safe state
	1	Input channel normal operation. DI_x reflects physical input value
QDO_x	0	Output channel status “error”. DO_x is set to safe state / inactive
	1	Output channel normal operation. DO_x can be set/reset via safety fieldbus protocol

6.1.2.2 Output process image

The output process image of the T100/PS contains all the safety-relevant data sent from the F-Host to the T100/PS. The data of the output process image is used on the one hand to control the safe digital output states of the T100/PS and on the other hand to send the fail-safe error acknowledge data for the digital inputs and outputs of the T100/PS (see section 0 and 5.3.4 of this document for further details)

	Bit 0	**Bit 1**	**Bit 2**	**Bit 3**	**Bit 4**	**Bit 5**	**Bit 6**	**Bit 7**
Byte 0	DO_1	DO_2	Res.	Res.	Res.	Res.	Res.	Res.
Byte 1	ERDI_1	ERDI_2	ERDI_3	ERDI_4	ERDI_5	ERDI_6	Res.	Res.
Byte 2	ERDO_1	ERDO_2	Res.	Res.	Res.	Res.	Res.	Res.
Byte 3	PROFIsafe Control Byte							
Byte 4	PROFIsafe CRC2							
Byte 5								
Byte 6								

Configuration	**Dual-Channel**	**Single-Channel**
DO_1	Requested value for dual-channel output group	Requested value for DO1 located at T100/PS Pin 5/6
DO_2	Unused / Ignored	Requested value for DO2 located at T100/PS Pin 7/8
ERDI_1, ERDI_3, ERDI_5	Error-Reset Bits of the dual-channel inputs	Error-Reset Bits of the inputs DI1, DI3, DI5, DI7
ERDI_2, ERDI_4, ERDI_6	Unused / Ignored	Error-Reset Bits of the inputs DI2, DI4, DI6, DI8
ERDO_1	Error-Reset Bits of the dual-channel outputs	Error-Reset Bits of the output DO1
ERDO_2	Unused / Ignored	Error-Reset Bits of the output DO2

Bit	**Value**	**Description**
DO_x	0	Output channel inactive (safe state, low)
	1	Output channel active (high)
ERDI_x	0	Input channel error reset not requested
	1	Input channel error reset requested
ERDO_x	0	Output channel error reset not requested
	1	Output channel error reset requested

At startup (power-up or reset) the outputs are set to the safe state. Only in the state “RUN” (see section 3.10) where the PROFIsafe data communication takes places the outputs can be safely operated.

In case of a communication loss, the configured PROFIsafe watchdog will elapse. In this case, the outputs are all reset to their safe value (i.e. turned off).

The safe outputs are reset to the safe state whenever the output provider status is set to “Bad”. Refer to the PROFIsafe profile specification for more details.

6.1.3 Error Handling

As already described in section 3.6, the T100/PS detects various internal and external errors which lead into either a channel-specific or a global fail-safe state of the T100/PS. If possible internally detected faults are reported via PROFINET Alarm messages so the main (non-safe) controller receives more detailed information about the detected error. The error codes reported via the Alarm messages can be found in Table 3-1.

Note that in case of a T100/PS global fail-safe error (e.g. over-temperature) the PROFIsafe communication is no longer possible. In this case the fail-safe error information cannot be sent out by the T100/PS anymore even though the T100/PS inputs or outputs have correctly entered the fail-safe state.

[SAR-6.2] **Danger:** Error-Bits reported by the T100/PS via PROFIsafe shall not be used to trigger the safety function of a device or system.

Table 6-1 lists the PROFIsafe specific errors detected by the T100/PS as well as the issued error reaction.

Error	Severity	Handling	Description
F-Destination address mismatch	Parameter Error	Reported to F-Host. T100/PS stays in Parameter state	Locally configured F-Address and F-Destination address in fParameter block do not match
iParameter CRC mismatch	Parameter Error	Reported to F-Host. T100/PS stays in Parameter state	Locally calculated iParameter CRC and iParameter CRC in fParameter block do not match
PROFIsafe protocol Watchdog expired	Communication Error	T100/PS stops PROFIsafe data transmission and waits for restart of PROFIsafe reception	Expected cyclic PROFIsafe message did not arrive (in time).

Table 6-1: PROFIsafe specific errors

6.1.4 T100/PS temperature sensor data access

The T100/PS temperature sensor data can be read out using PROFINET services. When using the ABCC as non-safe PROFINET communication interface, the temperature sensor data can be read from the safety input module with the record index 7002_h. The temperature value is returned as 2 Byte raw ADC sensor value (ADC_{VAL}) and 1 Byte “In Range” information.

Byte	0	1	2
	ADC raw data		In Range

The ADC sensor value can be converted into a real temperature by the following equation:

$T100_{Temp} = -40°C+((ADC_{VAL}-164)/16,384)°C$

The “In Range” value is set to “0” if the valid operating temperature range of the T100/PS is left or an error within the internal T100/PS temperature sensor data processing was detected. Any value different from “0” indicates a valid temperature.

[SAR-6.4] Warning: The T100/PS internal temperature can only be read out in a non-safe way and shall therefore not be used to control any safe action on the Safety controller side.

6.1.5 Device replacement

As there is no storage of the iParameter data inside the T100/PS, the parameter set is transferred from the (Safe-) PLC to the T100/PS at every startup. The T100/PS itself also checks the parameter set completely at every startup. This procedure allows a very simple replacement of a broken T100/PS in a system without the need to reconfigure the (Safe-) PLC or the T100/PS with a special programming tool. Nevertheless, a broken or improper working T100/PS shall be replaced only by properly trained personnel as a broken device could indicate a systematic error. Additionally the component or the entire machine needs to be run through a complete re-testing of all safety functions after replacement of a safety component.

[SAR-6.3] Warning: Replacement of a broken T100 is only allowed by authorized and properly instructed persons as the T100 is typically only a sub-part of a machine or device integrated by a device or system integrator. After replacement a re-testing and re-validation of all safety functions of the CDev is necessary.

6.1.6 PROFIsafe certification

Any CDev based on the T100/PS needs to be tested to proof the PROFIsafe compliance at an accredited test lab. During these tests the PROFINET and the PROFIsafe parts of the CDev are tested to comply with the PROFINET and PROFIsafe standards.

[SAR-6.5] Attention: Any CDev using the T100/PS shall be tested for PROFINET and PROFIsafe compliance within an accredited test lab.

7 Re-Certification steps

7.1 General CDev integration and re-certification steps

Integrators using the T100 module to design-in safety I/O functionality to a specific device always have to certify the end device (CDev) according to the safety regulations. Even though the T100 has already been approved by TUV as a compliant item with the safety regulations IEC 61508 Parts 1-7:2010, EN 62061:2005 + AC:2010 +A1:2013 and EN ISO 13849-1:2008 + AC:2009, the end device has to achieve these approvals as well.

To simplify the re-certification of a CDev using the T100, all In-Design steps marked with [IDR-x] must be followed by the T100 integrator. Deviations from the in-design rules given within this safety manual have to be thoroughly discussed with the certification authority chosen by the integrator for his CDev.

Appendix A lists the In-Design Rules to be followed which are given within this safety manual.

Beside the in-design rules safety application rules [SAR-x] are listed in this safety manual. These safety rules must be provided to the end-user of the CDev using the T100 for the safety function.

The general steps for a proper re-certification of a CDev based on the T100 can be summarized as follows:

1. Set up a proper safe development process and safety product lifecycle with the required safety documentation for the CDev on integrator side. It is highly recommended to already start the concept phase of the CDev together with the final certification authority.
2. Follow all IDR-X In-Design rules. Fulfillment shall be recorded as part of the safety development documentation of the CDev and must be provided to the certification authority in the end.
3. Provide all SAR-X Safety Application rules to the end-user which are relevant for the usage of the T100 safety functions within the CDev. This is typically done within the CDev safety manual which has to be provided by the CDev integrator.
4. Parts of the IDR-X rules are environmental tests which shall be fulfilled by the end CDev. Therefore temperature tests, EMC and ESD tests, shock/vibration tests and humidity tests shall be done with the T100 integrated into the CDev under the maximum CDev operating conditions.
5. Follow the additional product regulations for the CDev which might be applicable to achieve certain product group compliance (e.g. ESD tests with increased levels according to IEC 61131).
6. Do the non-safe and safe fieldbus compliance tests and provide the test results to the certification authority.

7. Do the fully planned and documented verification and validation tests with the CDev especially regarding the safety function. It must be approved by tests that under all valid operating conditions of the CDev the safety functions are not degraded.

8 Characteristics

[DR_I_FIG]

Safety Integrity Level according to IEC 61508	
- Dual-Channel DI	SIL 3
- Dual-Channel DO	SIL 3
- Single-Channel DI	SIL 3 (requires additional external safety measures – see 3.5.1)
- Single-Channel DO	SIL 1 (not recommended to be used without additional external safety measures)
Performance Level according to EN ISO 13849-1	
- Dual-Channel DI	PL e / Cat. 4
- Dual-Channel DO	PL e / Cat. 4
- Single-Channel DI	PL d / Cat. 2 (requires additional external safety measures – see 3.5.1)
- Single-Channel DO	PL c / Cat. 1 (not recommended to be used without additional external safety measures)
Hardware Fault Tolerance (HFT) in dual-channel mode	1
Hardware Fault Tolerance (HFT) in single-channel mode	0
Proof-test interval	20 years
Self-test interval	1 hour
Probability of failure PFH (high demand mode)	
- Dual-Channel input DI-S	$2.44 * 10^{-9}$ 1/h
- Dual-Channel input DI-C	$2.44 * 10^{-9}$ 1/h
- Dual-Channel Output	$2.46 * 10^{-9}$ 1/h
- Single-Channel input DI-S	$4.47 * 10^{-9}$ 1/h
- Single-Channel Output	$1.89 * 10^{-7}$ 1/h
Diagnostic Coverage DC	> 90%

$MTTF_d$ Dual-Channel DI and DO	>100 years
Safe Failure Fraction (SFF) - Dual-Channel input DI-S - Dual-Channel input DI-C - Dual-Channel Output - Single channel input DI-S - Single-Channel Output	 99.60 % 99.60 % 99.63 % 99.67 % 79.78 %

9 Compliance

9.1 CE

Since the IXXAT Safe T100 is considered a component for embedded applications, it cannot be CE-marked as an end product. However, the IXXAT Safe T100 is pre-compliance tested in a typical installation.

Note that a valid CE conformance declaration for the complete CDev is necessary in any way which will be simplified possible with the pre-tested T100. [PRS_288]

9.2 UL

Under preparation.

9.3 IEC 61508 and EN ISO 13849

The IXXAT Safe T100 is considered to be a component for embedded applications. Thus it is certified as a compliant item type B according to IEC 61508. However, the IXXAT Safe T100 is designed in accordance to IEC 61508 SIL 3 and EN ISO 13849-1:2008 Cat. 4 PL e and is certified as part of a typical safety host device by TÜV Rheinland.

The type approval of the IXXAT Safe T100 module was done by

TÜV Rheinland Industrie Service GmbH
Am Grauen Stein
51105 Köln / Germany

Tel.: +49 221 806-1790,
Fax: +49 221 806-1539,
E-Mail: industrie-service@de.tuv.com

The type approval (report number 968/EL 724.01/14 and 968/EL 724.02/16) of the IXXAT Safe T100 came to the result that the specified product is suitable to fulfill the requirements according to EN ISO 13849-1:2008 Cat. 4 PL e and SIL 3 according to EN 62061 / IEC 61508 when being integrated following the rules defined in this safety manual.

9.4 PROFIsafe

The PROFIsafe implementation used within the T100 complies with the PROFIsafe Profile V2.4 from March 2007. The PROFIsafe compliance was tested in an accredited test lab (ComDeC) with the test report number PS081-1. The PROFINET and PROFIsafe compliance was granted within the certificate numbers Z10891 and Z20137.

9.5 RoHS

All components of the IXXAT Safe T100 are RoHS compliant.

9.6 EMC

EMC measurements were done with the T100 in accordance with the increased test levels for functional safety devices given by EN 61326-3-1 (see section 4.2.7).

Appendix

A Safety Integration Rules

[IDR-1.1] Warning: The T100 is designed to be used in the environment of industrial automation or process control systems. The T100 integrator and end-user shall check if the T100 is allowed to be used within the environment of the final application.

[IDR-1.2] Danger: No repair or modification of the T100 is allowed.

[IDR-3.1] Attention: The unconnected pins (N.C.) of the T100 connector shall be connected to the SELV/PELV ground VSS.

[IDR-3.2] Warning: The 24V signal shall be connected to pin 1 and 2 of the T100 connector.

[IDR-3.3] Danger: The VSS signal (24V ground) shall be connected to pin 3, 4 and 9 of the T100 connector.

[IDR-3.4] Warning: The VSS signal (24V ground) shall be connected to pin 12, 14, 16, 18, 20, 22, 24 and 29 of the T100 connector to detect connector errors (cross-connections between neighbor signal pins).

[IDR-3.5] Danger: The T100 shall be supplied by a 24V SELV/PELV power supply according to EN60950-1 [DR_C_HW_POW, DR_I_POW] which limits the maximum voltage in case of a failure to 60V. [PRS_107], [HR_158]

[IDR-3.6] Warning: The maximum constant supply voltage of 30V shall not be exceeded in order to avoid permanent damage of the T100.

[IDR-3.7] Warning: The customer device shall include a reverse battery protection circuit if the CDev does not generate the 24V DC supply internally. [Reverse power connection can be excluded by design when using an internal power supply as no change to the internal power supply chain is assumed to be done in the field]

[IDR-3.8] Warning: An external suppressor diode shall be present on the customer device between 24V and VSS. To withstand the EMC tests of the entire customer device at least a 5KW type shall be chosen.

[IDR-3.9] Warning: The CDev shall provide a functional earth (FE) connection.

[IDR-3.10] Warning: To dissipate high frequent ESD pulses a 1,5 nF (10%, 2kV) capacitor shall be placed between the 24V SELV/PELV and the FE connection as well as between the VSS and the FE connection on the CDev.

[IDR-3.11] Warning: All input and output signals of the T100 refer to the ground Signal VSS. The ground VSS is not supplied to the output loads by the T100, i.e. the inputs and outputs must be connected with low impedance externally to the VSS ground level. [SC_406], [HR_225]

[IDR-3.12] Danger: The manufacturer of the end device must clearly note and supply the date of the integration test of the T100. This marks the earliest

beginning of the proof-test interval the end user or system integrator has to consider to keep the T100 operation time within the calculated 20 year proof-test interval.

[IDR-3.13] Warning: External short over the sensor in DI-C mode has to be prevented by fulfilling certain rules when developing the host device or cabling the sensors such as distances between lines or pins as described in the standard EN 60664 [SC_55, SC_370] . Which failure is excluded by which rule, has to be documented, see “Layout Rules, Host Device” in section 4.2.1 of this document. Product- or application specific safety regulations which might apply for the CDev regarding external sensors and cabling shall be considered as well.

[IDR-3.14] Warning: If an input is configured as type DI-S, the following failures cannot be detected by the IXXAT Safe T100 [DR_I_DIS], [SC_319, SC_320, SC_321]:

- external short over sensor

- external short to 24 V

- external short between dual channel DI lines

These failures have to be prevented by fulfilling certain rules when developing the host device, e.g. distance between signal lines or pins as described in the standard. Which failure is excluded by which rule, has to be documented.

[IDR-3.15] Warning: Short-circuit of the TO to VSS will activate the thermal protection circuit of the output driver. The shut-down temperature of this component is given with 150°C. In case of a TO short to GND parts of the T100 PCB will heat up to 150°C which shall be considered in the design of the overall safety device housing.

[IDR-3.16] Warning: When turned off (safe-state), the output signal is not pulled actively to VSS.

[IDR-3.17] Warning: Safety outputs shall be connected to the T100 connector always using both output pins per output channel (DO1: Pin 5 and 6, DO2: Pin 7 and 8).

[IDR-3.18] Danger: A loss of ground of the load connected to the T100 DO shall be prevented by means of a hardwired ground connection to the VSS input of the T100.

[IDR-3.19] Attention: A 2.2 kOhm pull-up resistor shall be placed on the CDev to the Rx and the Tx signal line.

[IDR-3.20] Attention: There shall be a 4.7 kOhm pull-down resistor placed on the CDev to the RST line.

[IDR-3.21] Warning: Only use officially released and approved T100 firmware files from HMS for the T100 firmware update. Software not approved by HMS can cause damage to the T100 or lead to non-safe behavior of the T100.

[IDR-4.1] Warning: The minimum clearance around the T100 should be 3 mm. On the top side this should be measured from the top face of the components, on all other sides measured from nearest point on the PCB surface. The clearance above the highest component on the top face should measure 5.64 mm above the surface of the PCB.

[IDR-4.2] Warning: When using conductive spacers and screws to mount the T100 on the base board, there must be at least 3 mm space to any conductive elements on the base board as well. Connecting the mounting points to ground or any other potential is not allowed.

[IDR-4.3]: Attention: If the safety inputs or outputs of the T100 are routed to a user terminal, the provided signals shall be clearly marked according to DIN EN 61310.

[IDR-4.4] Danger: The PCB of the host device shall fulfill EN 60664 with a minimum clearance of 0.2 mm at least for the T100 signals and T100 SELV/PELV power supply [DR_C_LO_POW]. This value is given under the assumption of over voltage category I with a nominal voltage of 330V r.m.s. [DR_C_LO_DIO], [SC_140].

[IDR-4.5] Danger: The minimum creepage distance between the T100 signals on the host PCB shall be 0.063 mm assuming 63 V r.m.s. effective voltage for all isolators except IIIb according to EN 60664 [DR_C_LO_DIO].

[IDR-4.6] Warning: To protect conducting lines (power, input and output) of the T100 on the PCB of the host device a non-aging lacquer shall be used [DR_C_LO_LAC],[SC_141]. Special coating is not required.

[IDR-4.7] Warning: Routing of dual-channel input signal lines to the final input terminal as well as cabling of the external sensors to the T100 inputs shall be done in a way that adjacent signal lines or input terminals are using different test output signals.

[IDR-4.8] Attention: The interface connection between the IXXAT Safe T100 and the Anybus CompactCom module has to be able to handle a data transfer speed of 1020 kbit/s [DR_C_LO_COMM].

[IDR-4.9] Attention: It must be verified e.g. by test, that under worst case load and mounting position conditions inside the CDev the temperature of the IXXAT Safe T100 is always within the specified limits as listed in Table 4-1. [DR_C_ENV_TEMP]

[IDR-4.10] Attention: The maximum temperature rise produced by the T100 within the CDev under normal operation is 22 Kelvin. In case of TO output short-circuits, the internal temperature rise will be higher (see IDR-3.15).

[IDR-4.11] Attention: The T100 shall not be mounted in direct neighborhood of temperature hot-spots or convection cooling paths of the host device to avoid local over- or under-temperatures within the T100.

[IDR-4.12] Warning: The vibration and shock limits of the final host device shall not exceed the values given in section 4.2.3 of this safety manual [PRS_345]. The limits given by IEC 60068-2-27 and IEC 60068-2-6 or a higher product standard shall be approved by tests within the final host device.

[IDR-4.13] Danger: The T100 is designed and tested to comply with IEC 60068-2-30 for a relative humidity of 5% to 95% non-condensing [PRS_344)]. Environmental tests with the integrated T100 shall be done to approve that the specified humidity levels are kept in the end device.

[IDR-4.14] Danger: The storage and operating environment of the T100 shall be in the limits of pollution level 2 according to EN 60664.

[IDR-4.15] Danger: The intrusion protection for the T100 in the end device shall be equal or better than IP 54.

[IDR-4.16] Warning: The EMC ratings given in Table 4-2 shall not be exceeded at the mounting location of the T100 in the end device. The proper operation of the T100 safety functions shall be verified during the EMC tests of the final host device with increased test levels in accordance with IEC 61326-3-1. Safe functions shall not fail if triggered and the safe state of the outputs shall be kept. [DR_C_ENV_EMC]

[IDR-6.1] Attention: The final GSD file of the CDev shall contain the iParameter and fParameter block of the T100/PS. This block can be copied from the reference GSD file provided with the T100/PS and shall not be modified [PRS_227].

B Safety Application Rules

[SAR-1.1] Warning: The T100 is designed to be used in the environment of industrial automation or process control systems. The T100 integrator and end-user shall check if the T100 is allowed to be used within the environment of the final application.

[SAR-1.2] Danger: No repair or modification of the T100 is allowed.

[SAR-1.3] Danger: Safety critical T100 failures which do not lead to the safe state shall be reported to HMS/IXXAT immediately (see section 1.4).

[SAR-3.1] Attention: There is no galvanic isolation between the digital inputs, the digital outputs and the T100 board electronic itself.

[SAR-3.2] Danger: The T100 shall be supplied by a 24V SELV/PELV power supply according to EN60950-1 [DR_C_HW_POW, DR_I_POW] which limits the maximum voltage in case of a failure to 60V. [PRS_107], [HR_158]

[**SAR-3.3] Warning:** The maximum constant supply voltage of 30V shall not be exceeded in order to avoid permanent damage of the T100.

[SAR-3.4] Danger: The proper operation of the reverse battery protection circuit shall be tested whenever the power supply chain of the T100 is changed. This test shall be part of the initial safety machine operation tests where all safety functions shall be tested at least once. Changes to the power supply during runtime are not allowed without explicit re-testing of the overall safety function.

[SAR-3.5] Danger: The maximum operation time (proof-test interval) of the T100 shall not exceed 20 years. When reaching the proof-test limit the T100 shall be replaced and put permanently out of order.

[SAR-3.6] Danger: The manufacturer of the end device must clearly note and supply the date of the integration test of the T100. This marks the earliest beginning of the proof-test interval the end user or system integrator has to consider to keep the T100 operation time within the calculated 20 year proof-test interval.

[SAR-3.7] Danger: Two inputs have to be configured as one dual channel safe input to obtain SIL 3, PL e Cat 4. If two identical sensors are connected to the dual inputs one of the dual sensors shall be connected to input 1, 3 or 5. The other shall be connected to input 2, 4 or 6. Additional measures for wiring fault exclusion or using certified components might be necessary.

[SAR-3.8] Danger: Single-channel inputs of the T100 shall be used for safety applications only under special precautions. The safe operation of a single channel input always required additional safety measures or fault exclusions which must be considered in the overall safety system design.

[SAR-3.9] Attention: Unconnected digital inputs in dual channel mode will cause the T100 to signal the inactive safe state for the input pair.

[SAR-3.10] Warning: External short over the sensor in DI-C mode has to be prevented by fulfilling certain rules when developing the host device or cabling the sensors such as distances between lines or pins as described in the standard EN 60664 [SC_55, SC_370] . Which failure is excluded by which rule, has to be documented, see “Layout Rules, Host Device” in section 4.2.1 of this document. Product- or application specific safety regulations which might apply for the CDev regarding external sensors and cabling shall be considered as well.

[SAR-3.11] Warning: When using the DI-C input mode the T100 test outputs shall be used as power source for the external sensor for proper error detection by the T100. The test pulse length shall be configured to a value different than “Always High” (see section 5.2). [PRS_97]

[SAR-3.12] Warning: An active sensor, connected to a semiconductor input, must use the same ground level VSS than the IXXAT Safe T100.

[SAR-3.13] Warning: If an input is configured as type DI-S, the following failures cannot be detected by the IXXAT Safe T100 [DR_I_DIS], [SC_319, SC_320, SC_321]:

- external short over sensor

- external short to 24 V

- external short between dual channel DI lines

These failures have to be prevented by fulfilling certain rules when developing the host device, e.g. distance between signal lines or pins as described in the standard. Which failure is excluded by which rule, has to be documented.

[SAR-3.15] Warning: The minimum time between the change of a single safe digital input and the transmission to the safety fieldbus is 6 ms. In case of an input level change at all 6 safe digital inputs at the same time, the maximum safe application reaction time is 16 ms (approx. 2 ms processing time per changed input).

[SAR-3.16] Warning: The diagnostic test interval for dual-channel DI-C inputs is 1 hour [SC_323].

[SAR-3.17] Warning: Do not deactivate the test pulse outputs (set pulse-length to 0 or “Always High”) in the configuration when using the digital inputs in DI-C mode.

[SAR-3.18] Attention: The test output signals are not isolated and use all the same ground potential VSS.

[SAR-3.19] Warning: The maximum constant output current at the test output pins of 0.1A shall not be exceeded to avoid damage of the T100 hardware. It must be ensured that only devices consuming a total current of less than 0.1A are connected to the TO or technical measures such as protective fuses are in place on the CDev.

[SAR-3.20] Warning: The maximum output current at the digital output pins shall not exceeded 500 mA to avoid damage of the T100 hardware

[SAR-3.21] Attention: In case of a short circuit of the digital outputs a thermal shut down into the safe state will be issued by the T100 automatically.

[SAR-3.22] Warning: When turned off (safe-state), the output signal is not pulled actively to VSS.

[SAR-3.23] Warning: The safe state of the T100 digital outputs is “off” (high impedance). Therefore it is not allowed to connect an external safety device or function (like a valve or break) which needs a “High” level to keep the safe state.

[SAR-3.24] Warning: To achieve SIL 3, PL e Cat 4 the digital outputs of the T100 shall be operated and connected in dual-channel mode [SC_75].

[SAR-3.25] Warning: Safety devices like actors or brakes connected to the T100 digital outputs must be robust against the configured T100 output test pulses. [SC_324]

[SAR-3.26] Warning: The diagnostic test interval for the DOs is 1h [SC_323]

[SAR-3.27] Danger: After detection of a safety critical error, the T100 shall not be kept in fail-safe state for more than 1h [DR_I_DO].

[SAR-3.28] Danger: A loss of ground of the load connected to the T100 DO shall be prevented by means of a hardwired ground connection to the VSS input of the T100.

[SAR-3.29] Warning: The maximum time between the reception of a safety telegram and setting the corresponding safe digital output is 7.7 ms.

[SAR-3.30] Warning: Proper grounding and measures against an external ground loss shall be applied to safety devices connected to the T100.

[SAR-3.31] Danger: Replace a malfunctioning T100 immediately.

[SAR-3.32] Danger: The T100 shall not be operated more than 8h outside the RUN state (see section 3.10) in order to make sure that all relevant tests are executed within the safe reaction time. [SC_379, SC_373]

[SAR-3.33] Warning: Only use officially released and approved T100 firmware files from HMS for the T100 firmware update. Software not approved by HMS can cause damage to the T100 or lead to non-safe behavior of the T100.

[SAR-3.34] Attention: Updated T100 modules shall be tracked or clearly marked by the integrator or end-user to indicate modules with a firmware version different to the one originally shipped by HMS.

[SAR-3.35] Warning: After a proper firmware update the safety function shall be checked by the integrator or end-user and documented properly.

[SAR-3.36] Danger: If the T100 module is powered on and does not enter properly the RUN state within a maximum of 8 hours, the module shall be restarted via a power-cycle. Afterwards it shall be checked by trained safety service personal for a proper safety operation. [SC_379]

[SAR-3.36] Warning: The firmware update of the T100 shall not be performed during operation in the field. [SC_434]

[SAR-4.1] Warning: Routing of dual-channel input signal lines to the final input terminal as well as cabling of the external sensors to the T100 inputs shall be done in a way that adjacent signal lines or input terminals are using different test output signals.

[SAR-4.2] Warning: The vibration and shock limits of the final host device shall not exceed the values given in section 4.2.3 of this safety manual [PRS_345]. The limits given by IEC 60068-2-27 and IEC 60068-2-6 or a higher product standard shall be approved by tests within the final host device.

[SAR-4.3] Danger: The storage and operating environment of the T100 shall be in the limits of pollution level 2 according to EN 60664.

[SAR-4.4] Danger: The maximum operation altitude of 2000m shall not be exceeded.

[SAR-5.1] Danger: Use a safe configuration tool or a specific review processes (or a combination of both) to verify that the configuration of the T100 safe I/Os are matching the safe applications' needs [SC_100].

[SAR-5.2] Danger: Only use a safe configuration tool to calculate the configuration CRC for the T100 or use the pre-tested configurations with the approved CRCs as listed in section 5.4 of this safety manual [SC_101].

[SAR-5.3] Warning: Depending on the selected iput debounce filter time value the input response time (i.e. the safe application time) will be increased by the given debounce filter time. [DR_I_DI]

[SAR-5.4] Warning: Deactivation of the consistency filter in dual-channel mode must be done in accordance with the safety application as stuck-at errors in Dual-Channel DI-S mode or short over sensor in Dual-Channel DI-C mode at one input line for example will not lead to a fail-safe input error signaling.

[SAR-5.5] Attention: Due to hardware limitations the T100 with 3 dual-channel inputs and one dual-channel output has only one configurable TO pair. This TO pair is configured via the test output signal configuration parameters of input group 1. Modifying TO parameters of input group 2 or 3 will have no effect.

[SAR-5.6] Warning: Output test pulses are only generated if the output is set active / high. In safe-state (low, high-impedance) no test pulses are generated.

[SAR-5.7] Attention: If manual output error reset is configured, any output error will be reset, when receiving a valid safety network message containing the appropriate error reset bit transition [PRS_141].

[SAR-5.8] Attention: The test pulse duration of 400µs shall to be used with an external Test Output load of <= 2 kOhm.

[SAR-5.9] Warning: For a proper operation of the Consistency filter, the filter time parameter shall be set to a value which is larger than the input debounce filter time parameter.

[SAR-5.10] Warning: Using any other configuration than the ones listed in section 5.4.1, 5.4.2 or 5.4.3 requires a functional validation on application level to approve the proper operation of the overall safety function.

[SAR-6.1] Warning: Documentation (and Review) of the configured iParameter for a certain safe application is mandatory and requires the safe generation and storage of the iParameter data set as supplement for the safety assessor of the entire safety system. [SC_100, DR_C_CFG_DEF]

[SAR-6.2] Danger: Error-Bits reported by the T100/PS via PROFIsafe shall not be used to trigger the safety function of a device or system.

[SAR-6.3] Warning: Replacement of a broken T100 is only allowed by authorized and properly instructed persons as the T100 is typically only a sub-part of a machine or device integrated by a device or system integrator. After replacement a re-testing and re-validation of all safety functions of the CDev is necessary.

[SAR-6.4] Warning: The T100/PS internal temperature can only be read out in a non-safe way and shall therefore not be used to control any safe action on the Safety controller side.

[SAR-6.5] Attention: Any CDev using the T100/PS shall be tested for PROFINET and PROFIsafe compliance within an accredited test lab.

C Applicable Standards

IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1 – Part 7
EN ISO 13849-1:2008 + AC:2009 Safety of machinery - Safety-related parts of control systems General principles for design
EN ISO 13849-2:2012 Safety of machinery - Safety-related parts of control systems Validation
EN 62061:2005 + AC:2010 + A1:2013 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
IEC 61131 Programmable controllers IEC 61131-1:2003 General information IEC 61131-2:2007 Equipment Requirements and tests
IEC 61326 Electrical equipment for measurement, control, and laboratory use - EMC requirements IEC 61326-3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications
IEC 61000 Electromagnetic compatibility (EMC) IEC61000-4-2:2009 Testing and measurement techniques - Electrostatic discharge immunity test EN 61000-4-3:2006 +A1:2008 Störfestigkeit gegen hochfrequente elektromagnetische Felder EN 61000-4-4:2013 Testing and measurement techniques – Electrical fast transient/burst immunity test EN 61000-4-5:2006 Testing and measurement techniques – Surge immunity test EN 61000-4-6:2010 Immunity to conducted disturbances, induced by radio-frequency fields IEC61000-4-11:2010 Voltage dips, short interruptions and voltage variations immunity tests IEC 61000-6-2:2005 Immunity for industrial environments IEC 61000-6-4:2011 Generic standards – Emission standard for industrial environments
IEC 61784-3-3 Industrial communication networks – Profiles – Part 3-3: Functional safety fieldbuses – Additional specifications for CFP 3

PROFIsafe – Profile for Safety Technology on PROFIBUS DP and PROFINET IO Version 2.4 “PROFIsafe-Profile_3192b_V24_Mar07.pdf”
SIMATIC PROFIsafe driver V2.1 for F-Slaves - Manual Edition 01 / 2009 “HB_PST_2009_01_ENU.pdf”
IEC 60068-2-6:2007 Environmental Testing -Part 2-6: Tests – Test Fc: Vibration (sinusoidal)
IEC 60068-2-27:2008 Environmental Testing - Part 2-27: Tests – Test Ea and guidance: Shock
IEC 60068-2-30:2005 Environmental Testing - Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle)

D Declaration of incorporation

Note: The safe operation of a machine or device incorporating the T100 is not allowed until the conformity of the complete machine or device to the Machinery Directive 2006/42/EC has been approved.

HMS Industrial Networks AB, Stationsgatan 37, SE-30250 Halmstad represented by its subsidiary HMS Technology Center Ravensburg GmbH in Helmut-Vetter-Strasse 2, D-88213 Ravensburg declares, that the

documentation of the product: **IXXAT Safe T100**
with the article number: **1.01.0300.00001**

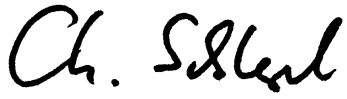
complies with the rules of the **Machinery Directive 2006/42/EC Appendix VII B**

Additionally applied harmonized standards for the development:

EN 62061:2005 +
AC:2010+A1:2013
EN 13849-1:2008 +
AC:2009
EN 13849-2:2012
EN 61326-1:2013
EN 61326-3-1:2008

On substantiated requests of governmental authorities the documentation of the T100 will be handed over to these authorities in electronic form.

26.07.2016, Dipl.-Ing. Christian Schlegel, Managing Director



HMS Technology Center Ravensburg GmbH
Helmut-Vetter-Strasse 2
88213 Ravensburg