HY-TTC 500

Safety Manual (SM)

Original Instructions

Author:	Dominik Langer
Security:	Public
Document number:	D-TTC5F-M-02-002
Version:	1.13.0
Date:	2021-04-28
Status:	Released
Windchill ID:	544450

TTControl GmbH

Schoenbrunner Str. 7, A-1040 Vienna, Austria, Tel. + 43 1 585 34 34-0, Fax +43 1 585 34 34-90, office@ttcontrol.com

Approval

Name	Function	Signature
Dominik Langer	Author	Dominik Langer
Kamil Schostok	Project Manager	Kamil
Christiana Seethaler	Department Head	
Fabian Rier	Configuration Manager	Rier Fabian
Ralph Hois	Quality Engineer	p.p. Roland Braun

Revision History

A revision is a new edition of the document and may affect all sections of this document.

	Date	Responsible Person	Modification
1.0.0	2015-01-15	OPR/SSE	initial version ready for review
1.0.1	2015-01-22	OPR	issue71686 - [SM] Describe system relevant IEC 61508 phases issue71690 - [SM] Number of possible safety functions per ECU issue71692 - [SM] Reference to I/O driver API's error type table issue71693 - [SM] Requirement for informing TTControl about safety-related incidents issue71729 - [SM] Requirement for current plausibility check
1.0.2	2015-01-26	OPR	issue71729 - [SM] Requirement for current plausibility check issue71878 - [PR-SM-1.0.1] - Typos issue71880 - [PR-SM-1.0.1] - References issue71881 - [PR-SM-1.0.1] - Acronyms issue71883 - [PR-SM-1.0.1] - General contents issue71959 - [SM] Update IEC 61508 and ISO 13849 failure metrics
1.0.3	2015-01-28	OPR	issue71883 - [PR-SM-1.0.1] - General contents issue71959 - [SM] Update IEC 61508 and ISO 13849 failure metrics
1.0.4	2015-02-03	OPR	issue72441 - [SM] Findings
1.1.0	2015-04-08	OPR	issue73121 - [SM] TTC 540 vs. TTC 580 issue73335 - [SM] Consistent usage of specific terms issue74521 - [SM] Update failure rates issue74870 - [SM] Cross references in section 7 issue75164 - [SM] Add user requirement for handling a safety switch runtime error issue75166 - [SM] Add user requirement for handling a safety switch startup error issue74079 - [SM] PWD and PWM failure reaction needs more time issue73440 - [SM] Failure reaction time formula is incorrect issue75636 - [SM] Application requirements for frequently changing DOUTs
1.2.0	2015-05-05	OPR	issue76056 - [SM] Correct heading indentation issue76248 - [SM] FIN/DigIn on HS PWM 28-35 in safety critical applications issue77151 - [SM] Explicitly forbid Codesys usage
1.3.0	2015-08-04	OPR	issue76833 - [SM] Power section leads to confusion issue76834 - [SM] Style of document does not clearly list requirements issue77475 - [SM] Req. for Temperature_Monitoring not clear issue77604 - [SM] Add user requirement for configuring the behavior for integer divisions by zero issue78473 - [SM] Update safety parameters and FMEDA values issue78794 - [SM] Only 6 "safe" inputs provided for 3 switch functions issue80883 - [SM] Clarify length of diagnostic PWM pulses

			issue81230 - [SM] Usage of open devices issue81241 - [SM] Add second invalid case to power section
1.3.1	2015-08-20	SSZ	issue77609 - Add universal timer mode for concurrent frequency/pulse width measurement and edge/incremental counter
1.3.2	2015-08-31	OPR	issue83922 - [SM] Review findings of recent document extension
1.4.0	2015-09-29	OPR	issue84150 - [SM] General calculation formula for MTTFd issue85441 - [SM] Rework tables in section "Failure Diagnostics" issue85463 - [SM] Minor findings during MATCH integration
1.4.1	2015-10-06	OPR	issue76833 - [SM] Power section leads to confusion issue84150 - [SM] General calculation formula for MTTFd issue82629 - [SM] No info about the response time of the external shut-off inputs issue85313 - [SM] IO_PWD_GetCurrent() needs to be called with safe current PWD inputs issue85441 - [SM] Rework tables in section "Failure Diagnostics" issue85567 - [SM] LS errors are just as fatal as HS errors issue85702 - [SM] Further review findings of recent document extension
1.4.2	2015-10-13	OPR	review183 - SM V1.4
1.4.3	2015-10-13	OPR	issue78473 - [SM] Update safety parameters and FMEDA values
1.5.0	2016-06-22	OPR	issue82427 - Added reference to chapter "Power Supply" to the requirement prohibiting nonstop operation (ID587497). issue86638 - Added description of safety mechanisms for encoder input mode (ID591419). issue86641 - Clarified that the system integrator is responsible for selecting DC values (ID920153). issue86643 - Corrected mapping within table of safety mechanisms for PWM High Side Stages (ID921278). issue86647 - Added description of safety mechanism "shut-off path test" (ID1194916). issue87688, issue91509 - Updated list of safe and unsafe components (ID590200 & ID590289). issue87864 - Provided clarification that the sensor supply outputs will not be switched of in the safe state (ID586823). issue87864 - Added FPGA bitstream to the safety platform's description (ID586811). issue87864 - Assigned new ID1195043 to requirement (old ID609547). issue89294 - Removed unncessary restrictions for PWM frequencies (ID592687 & ID592689) and initialization (deleted ID592697). issue90799 - Removed unncessary restrictions for periodically calling I/O task functions (deleted ID895043, ID895045, ID894954, ID894899, ID894973, ID895071 & ID895073). issue88196 - Modified comments to clarify the consequence of a failing safety switch (ID808085 & ID808549). issue93409 - Updated references to the TTC-Downloader release notes (ID592667 & ID591265). issue93413 - Added requirement for usage of TTC-Downloader or TTC-Downloader-DLL (ID1200803).

			issue98133 - Added requirement for usage of IO_PWM_ResolveOpenLoadShortCircuit() (ID1195152). issue86632, issue86635, issue86636, issue87864 - Corrected wording and spelling throughout several sections.
1.5.1	2016-07-01	OPR	issue86638 - Corrected description of safety mechanisms for encoder input mode (ID591419). issue86635 - Corrected wording and spelling.
1.5.2	2016-07-15	TGU	issue99057 - suspect traces removed - no changes with regard to contents (no textual change)
1.5.3	2016-08-02	SSZ	issue101093 - two comment items have been replaced (with same text) due to wrong references - no changes with regrad to contents (ID1244009, ID1244011, ID1244013)
1.6.0	2017-05-09	FWI	issue106526 - new variants HY-TTC 510 and HY-TTC 520 added (ID544461, ID590200, ID590289); hardware metrics separately listed for each variant and respective pins added (ID1534877, ID1534879, ID1534873, ID1534875, ID1534869, ID1534871, ID919185 replaced by ID1534713, ID919701 replaced by ID1534715); issue116787 - CAN Termination and CAN Interface 3-6 separately listed in the *Guideline on Hardware Metrics* (ID1534879, ID1534875, ID1534871, ID1534715); issue117070 - calculations and respective metrics corrected for functional blocks without any diagnostic measures (PVG Output, LIN Interface, RS232 Interface, CAN Interface 0-6, CAN Termination, Real Time Clock) and timer input 6-11 added which leads to an update of the PCB failure rate distribution and therefore in new metrics for nearly each functional block (ID1534879, ID1534875, ID1534871, ID1534715, ID590425, ID931802, ID931806, ID931808); issue116664 - overall safety information added (ID1543030)
1.6.1	2017-05-09	FWI	findings after formal review implemented (no functional change)
1.7.0	2017-11-08	FWI	issue124380 - Wrong DC values in section 'Core' ID894365 and 'PWM HS Stages' ID921278 corrected to cover recently updated FMEDA calculation (see Description for SM V1.6.0)
1.8.0	2018-03-07	FWI	issue129478 – Wrong FMEDA calculation for functional block ‘Core’ led to wrong and worse failure rate and diagnostic coverage. Values for ‘Core’ corrected in section ‘Guideline on Hardware Metrics Determination‘ (ID1534877, ID1534873, ID1534869, ID1534713, ID894365); Metrics for ‘Timer Input 6-11’ corrected due to inconsistency (ID1534879, ID1534875, ID1534871, ID1534715)
1.8.1	2018-11-26	FWI	issue133375 - External Watchdog Window Time (t_wd) corrected which implies an updated worst case failure reaction time (wc_frt_core) [ID813067, ID813591, ID813743, ID592663, ID717254]
1.9.0	2019-09-24	FWI	TTC500-414 - Description of Analog 2 Mode Input clarified [ID592229] TTC500-452 - Implement new variants HY-TTC 508, HY-TTC 590 and HY-TTC 590E and update existing once [ID544461, ID590200, ID590289, ID3276670, ID3276672, ID1534877, ID1534879, ID1534873, ID1534875, ID1534869, ID1534871,

			ID1534713, ID1534715, ID3276664, ID3276666, ID894365, ID921278] TTC500-536 - Useful lifetime added [ID3065953, ID3065955]
1.9.1	2019-10-01	FRR	TTC500-982 - Convert SM PTC tables to HTML [ID591167, ID3400585, ID3400587, ID3400593, ID3400595, ID3276670, ID3276672, ID1534877, ID1534879, ID1534873, ID1534875, ID1534869, ID1534871, ID1534713, ID1534715, ID3276664, ID3276666, ID894365, ID920236, ID920909, ID920350, ID591419, ID959339, ID921278, ID894367, ID894369, ID924869]. TTC500-1077 - add HW V6 to metrics [ID591167, ID3407546, ID3404454] TTC500-1079 - Allow higher compiler versions than V5.1.6 in SM [ID3407524, ID3407534, ID3407526, ID3407528, ID3407530, ID717023] TTC500-656 - Clarify usage of debug functionality [ID590289, (deleted ID717647)]
1.10.0	2019-10-04	FRR	TTC500-1096 Wrong hardware metrics caused by framework bug [ID3400585, ID3400587, ID3400593, ID3400595, ID3276670, ID3276672, ID1534877, ID1534879, ID1534873, ID1534875, ID1534869, ID1534871, ID1534713, ID1534715, ID3276664, ID3276666, ID894365]
1.11.0	2020-03-31	FRR	TTC500-1441 Post mortem EEPROM [ID590311, ID4133883, ID609585] TTC500-1448 Mixed criticality for applications [ID3832760, ID3832766, ID3832772, ID4106044, ID410603, ID4105505, ID4106230, ID4106267, ID4106271, ID4106341, ID718454, ID718579, ID718472] TTC500-1462 MPU must not deny read access [ID3832766, ID3832772, ID3832760, ID4115538, ID4115931, ID4115889, ID4115852, ID4115848]
1.11.1	2020-04-01	FRR	Update after formal review
1.11.2	2020-04-02	FRR	Update after formal review
1.12.0	2020-05-06	FRR	TTC500-1643 IEC SM: Reference to 26262 in DC Tables [ID920236, ID920909, ID920350, ID591419, ID959339, ID921278, ID894367, ID894369, ID9244869] TTC500-644 SM has to point out relevant parts of ISO 25119[ID4217706, ID4217708, ID4217740, D591187, ID592451, ID920236, ID920909, ID920350, ID591419, ID959339, ID921278, ID894367, ID894369, ID9244869 ID586702, ID4189062, ID4189060, ID586714, ID3073813, ID3073809, ID586716, ID586807, ID586813, 586827, 894081] TTC500-1712 Hardware metrics update [ID3276670, ID3276672, ID1534877, ID1534879, ID1534873, ID1534875, ID1534869, ID534871, ID1534713, ID1534715, ID3276664, ID3276666, ID894365, ID921278, ID3400585]
1.12.1	2020-07-01	FRR	TTC500-1847 Generic SM needs to refer to ISO 26262 Addon [ID 586702 , ID 4494995]
1.12.2	2020-07-03	FRR	TTC500-1847 Generic SM needs to refer to ISO 26262 Addon [ID 586702]
1.12.3	2020-07-07	FWI	TTC500-1913 Statement regarding mixed criticality added [ID4572941, ID4572481]

1.13.0	2021-04-28	langer	TTC500-2069 Possible reentrance into EEPROM/RTC functions from notification callbacks [ID 609585] TTC500-2068 Extern "C" in header files I/O driver and SafeRTOS integration added [ID 5707591] TTC500-2095 Check compiler and linker for known bugs added [ID 5732724] TTC500-2055 Activation of the Safe State by the CPU can be unreliable [ID 813067, ID 813591, ID 813743, ID 592663, ID 717254, ID 590311, ID 4133883 (deleted), ID 723224] TTC500-2166 Formal delta review of SM1.13.0

Table 1

Table of Contents

1 Introduction 11
1.1 Purpose 11
1.2 Scope 11
1.3 Terminology and Notation 12
1.3.1 Definitions 12
1.3.2 Typographic Conventions 12
1.4 Safety Information 12
2 Safety Lifecycle 15
2.1 IEC 61508 15
2.2 ISO 13849 15
2.3 ISO 25119 16
3 Safety Concept Overview 18
3.1 Safety Parameters 19
3.1.1 Safety Function 19
3.1.2 Definition of the Safe State 19
3.1.3 Safety-critical System Components 20
3.1.4 Failure Reaction in Case of Errors 22
3.1.5 Failure Reaction Time 23
3.1.6 Probabilistic Failure Rate 29
4 Safety Measures of the HY-TTC 500 Platform 33
4.1 Power Supply 33
4.2 Input Stages 36
4.2.1 Timer Inputs 36
4.2.2 Analog Inputs 38
4.3 Power Stages 40
4.3.1 PWM High Side Stages 40
4.3.2 Digital High Side Stages 43
4.3.3 Digital Low Side Stages 44
4.3.4 Memory Protection Unit 45
5 Application Interface 47
5.1 Initialization 48
5.2 Generic 49
5.3 Runtime 50
5.4 Failure Diagnostics 51
5.5 Safe State 54
5.5.1 Application Callbacks 54
5.6 C-driver Examples 57
6 Development Environment 58
6.1 Compiler & Linker 58
6.2 Application Download 61
7 Information for Use 62
8 Guideline on Hardware Metrics Determination 63
8.1 MTTFd Values of Functional Blocks 63
8.1.1 Hardware Metrics HY-TTC 508 63
8.1.2 Hardware Metrics HY-TTC 510 65
8.1.3 Hardware Metrics HY-TTC 520 66
8.1.4 Hardware Metrics HY-TTC 540 67
8.1.5 Hardware Metrics HY-TTC 580 69
8.1.6 Hardware Metrics HY-TTC 590/HY-TTC 590E 70
8.2 Failure Diagnostics 71
8.2.1 Combined Safety Mechanisms 72

8.2.2 Core ... 72
8.2.3 5 V Sensor Supplies ... 73
8.2.4 Analog 3 Mode Inputs ... 74
8.2.5 Analog 2 Mode Inputs ... 78
8.2.6 Timer Inputs (IO_PWD_00 ... IO_PWD_05) ... 79
8.2.7 Timer Inputs (IO_PWD_06 ... IO_PWD_11) ... 83
8.2.8 PWM High Side Stages ... 84
8.2.9 Digital High Side Stages ... 88
8.2.10 Digital Low Side Stages ... 92
8.2.11 High Side Digital / PVG / VOUT Output ... 95
9 Guideline on Sensor Selection ... 99
9.1 Analog Sensors ... 99
9.1.1 Usage of Redundant Sensors ... 99
9.1.2 Potentiometric Analog Sensors ... 100
9.1.3 Current Loop Sensors ... 101
9.2 Digital Sensors ... 102
9.2.1 PWM Position Sensors ... 102
9.2.2 RPM Sensors ... 103
9.2.3 Digital Switches ... 103
9.3 External Short Circuit Check ... 104
10 Glossary ... 105
11 Acronyms ... 107
12 References ... 108

Category:	Comment	ID:	544457

LEGAL DISCLAIMER

THE INFORMATION GIVEN IN THIS DOCUMENT IS GIVEN AS SUPPORT FOR THE USAGE OF THE ECU AND SHALL NOT BE REGARDED AS ANY DESCRIPTION OR WARRANTY OF A CERTAIN FUNCTIONALITY, CONDITION OR QUALITY OF THE ECU. THE RECIPIENT OF THIS DOCUMENT MUST VERIFY ANY FUNCTION DESCRIBED HEREIN IN THE REAL APPLICATION.

THIS DOCUMENT WAS MADE TO THE BEST OF TTCONTROL’S KNOWLEDGE. NEVERTHELESS AND DESPITE GREATEST CARE, IT CANNOT BE EXCLUDED THAT MISTAKES COULD HAVE CREPT IN. TTCONTROL PROVIDES THE DOCUMENT FOR THE ECU "AS IS" AND WITH ALL FAULTS AND HEREBY DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ACCURACY OR COMPLETENESS, OR OF RESULTS TO THE EXTENT PERMITTED BY APPLICABLE LAW. THE ENTIRE RISK, AS TO THE QUALITY, USE OR PERFORMANCE OF THE DOCUMENT, REMAINS WITH THE RECIPIENT. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW TTCONTROL SHALL IN NO EVENT BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOSS OF DATA, DATA BEING RENDERED INACCURATE, BUSINESS INTERRUPTION OR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF THE USE OR INABILITY TO USE THE DOCUMENT EVEN IF TTCONTROL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IF THE ECU IS MARKED AS “PROTOTYPE”, THE DELIVERED ECU IS A DEVELOPMENT SAMPLE (“SAMPLE”). THE RECIPIENT ACKNOWLEDGES THAT HE IS ALLOWED TO USE THE SAMPLE ONLY IN A LABORATORY FOR THE PURPOSE OF DEVELOPMENT. IN NO EVENT IS HE ALLOWED TO USE THE SAMPLE FOR THE PURPOSE OF SERIES MANUFACTURING.

TTCONTROL PROVIDES NO WARRANTY FOR ITS PRODUCTS OR ITS SAMPLES, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW DISCLAIMS ALL LIABILITIES FOR DAMAGES RESULTING FROM OR ARISING OUT OF THE APPLICATION OR USE OF THESE PRODUCTS OR SAMPLES.

THE EXCLUSION OF LIABILITY DOES NOT APPLY IN CASES OF INTENT AND GROSS NEGLIGENCE. MOREOVER, IT DOES NOT APPLY TO DEFECTS WHICH HAVE BEEN DECEITFULLY CONCEALED OR WHOSE ABSENCE HAS BEEN GUARANTEED, NOR IN CASES OF CULPABLE HARM TO LIFE, PHYSICAL INJURY AND DAMAGE TO HEALTH. CLAIMS DUE TO STATUTORY PROVISIONS OF PRODUCT LIABILTY SHALL REMAIN UNAFFECTED.

Category:	Comment	ID:	1244009

Legal Notice

The information contained in this document does not affect or change any General Terms and Conditions of TTControl and/or any agreements existing between TTControl and the recipient regarding the product or Sample concerned.

The reader acknowledges that this document may not be reproduced, stored in a retrieval system, transmitted, changed, or translated, in whole or in part, without the express prior written consent of TTControl.

The reader acknowledges that any and all of the copyrights, trademarks, trade names, patents (whether registrable or not) and other intellectual property rights embodied in or in connection with this document are and will remain the sole property of TTControl or the respective right holder. Nothing contained in this legal notice, the document or in any TTControl web site shall be construed as conferring to the recipient any license under any intellectual property rights, whether explicit, by estoppel, implication, or otherwise.

Please note that based on the current state of the art in science and technology, it is impossible to develop software that is free of defects in all applications.

Category:	Comment	ID:	586833

We Listen to Your Comments

Is there any information in this document that you feel is wrong, unclear or missing?
Your feedback will help us to continuously improve the quality of this document. Please contact TTControl support if you have questions, change requests or suggestions for improvement related to the product or documentation. TTControl support can be reached via the following e-mail address: support@ttcontrol.com.

1 Introduction

Category:	Comment	ID:	1244013
TTControl has taken care and attention in order to develop the HY-TTC 500 platform with extraordinary diligence. However, the system integrator is advised to immediately contact TTControl, if malfunctioning or uncertainties regarding the HY-TTC 500 platform arise contrary to specifications.			

1.1 Purpose

Category:	Comment	ID:	544461
This document represents the manual for integration of the HY-TTC 500 platform into safety-critical systems. The HY-TTC 500 family's variants (i.e. HY-TTC 508, HY-TTC 510, HY-TTC 520, HY-TTC 540, HY-TTC 580, HY-TTC 590 and HY-TTC 590E) only differ in their I/O and partly memory sets, while featuring the same safety mechanisms with regards to functional safety. Consequently, this Safety Manual is valid for the variants HY-TTC 508, HY-TTC 510, HY-TTC 520, HY-TTC 540, HY-TTC 580, HY-TTC 590 and HY-TTC 590E equally, otherwise it is stated in the respective requirement/comment. For a detailed description of the ECU variants, please refer to the HY-TTC 500 System Manual [TTC500-SysM], Part I: Hardware Description. For simplification, all HY-TTC 500 family variants will be called HY-TTC 500 throughout this document, after the product family of safety-certified user-programmable ECUs. This document frequently refers to the "system integrator". The system integrator is the person who is responsible for the integration of the HY-TTC 500 into a safety-related system. The system integrator is responsible for the integration of the HY-TTC 500 into the overall functional safety concept of the integrated system. This means that the requirements described by this document have to be fulfilled by the system integrator to reach the specified level of safety integrity. The system integrator is able to check whether the HY-TTC 500 platform is suitable for the intended functional safety concept of the integrated system by analyzing • the overall system's safety requirements • the Safety Manual (this document).			

1.2 Scope

Category:	Comment	ID:	586688
This document includes: • Requirements that have to be met by the system in which the HY-TTC 500 is integrated. Other requirements and restrictions that have to be observed are listed in the HY-TTC 500 Hardware System Manual [TTC500-SysM]. • Abbreviations and Acronyms containing definitions of terms used throughout this document. • References listing all related documents including their exact identification.			

1.3 Terminology and Notation

1.3.1 Definitions

Category:	Comment	ID:	586694

The **HY-TTC 500 platform** provides a user programmable general purpose ECU, intended for usage in safety-critical environments. It consists of:

- the HY-TTC 500 hardware platform
- the bootloader containing the start-up code for the Main CPU
- Diagnostic software executed by the Main CPU
- I/O drivers for reading sensor data and controlling actuators

The term **system** refers to the final system (e.g. vehicle, machine …) in which the HY-TTC 500 platform is integrated.

The term **safety-critical system** refers to a system whose failure or malfunction may result in death or injury.

The **system integrator** defines and develops the system and integrates the HY-TTC 500 into the system. The system integrator is responsible for the safe operation of the full system.

The term **application software** refers to the software part developed by the system integrator that is executed on the Main CPU of the HY-TTC 500 platform and based on the provided I/O drivers.

1.3.2 Typographic Conventions

Category:	Comment	ID:	586698

This Safety Manual uses the following typographic conventions:

- Attributes that have to be fulfilled by the system and/or the application software are expressed as *Requirements* and shaded in red.
- Additional information on requirements, whose content is nonbinding, is expressed as *Comment*.

1.4 Safety Information

Category:	Requirement	Label:		ID:	1543030
Related To:			Related To':		

The system integrator **shall** carefully read the System Manual [TTC500-SysM] before using, integrating or operating the HY-TTC 500 platform.
This safety manual is just valid in combination with the System Manual [TTC500-SysM].

Category:	Requirement	Label:	Read_Doc	ID:	586704
Related To:	411160		Related To':		

This document contains requirements for the integration of the HY-TTC 500 platform in safety-critical applications and **shall** be read carefully before use.

Category:	Comment	ID:	586706

This manual is written for experienced hardware, software and functional safety engineers, responsible for integration of the HY-TTC 500 into the overall system.

Category:	Requirement	Label:		ID:	3065953
Related To:			Related To':		

To guarantee proper safety integrity the device **shall** not be used after the maximum lifetime of 20 years.

Category:	Comment	ID:	3065955

After a lifetime of 20 years, the device's probabilistic metrics cannot be seen as constant anymore (failure rates, PFH) and therefore the targeted Performance (PL) and Safety Integrity Level (SIL) cannot be guaranteed. For this reason, operating a device in a safety critical application after 20 years is in full responsibility of the system integrator.

Category:	Requirement	Label:	Contact_Support	ID:	729965
Related To:			Related To':		

The system integrator **shall** contact TTControl support (support@ttcontrol.com) if safety-related incidents occur during the integration or operation of the HY-TTC 500 platform.

Category:	Comment	ID:	586708

For the electrical specification of the HY-TTC 500, please refer to the HY-TTC 500 System Manual [TTC500-SysM], Part I: Hardware Description. The knowledge of the electrical specification, especially the characteristics and maximum ratings of the I/Os is required for the integration into a safety-critical system.

For the documentation of the I/O drivers, including information on how to use these drivers in safety related applications, refer to the HY-TTC 500 System Manual [TTC500-SysM], Part II: Software Description. Check the release notes for known issues and their impact on the ECU's functions.

The HY-TTC 500 platform cannot guarantee safe operation of the system as a whole. Therefore, certain requirements and constraints have to be fulfilled by the application software as described in this document. Also, a functional safety assessment has to be conducted for the final system according to the system's applicable standards and norms.

Category:	Comment	ID:	586702

The HY-TTC 500 platform fulfills the requirements of the following safety standards and their assigned safety/performance levels:

- ISO 13849 Category 2, Performance Level d.
- IEC 61508 Safety Integrity Level 2.
- ISO 25119 AgPL d/SRL 2.

The HY-TTC 500 platform may also fulfill the requirements of the ISO 26262 series of standards, however this Safety Manual alone does **NOT** cover all necessary requirements to use the platform in an ISO 26262 related environment. If the platform will be used in an ISO 26262 related environment the customer needs to fulfil the requirements in this Safety Manual and the ISO 26262 Safety Manual [TTC500-SM-26262] addon.

Category:	Comment	ID:	4572941

The HY-TTC 500 platform allows the system integrator to realize mixed criticality applications (applications containing safe and unsafe code).

Therefore, mechanisms for temporal and spatial separation have been considered during development. Temporal separation is already ensured by design, but spatial separation needs to be implemented by the application software (see section '*Memory Protection Unit*').

For further information regarding mixed criticality please contact TTControl support (support@ttcontrol.com).

Category:	Requirement	Label:		ID:	4572481
Related To:			Related To':		

The system integrator **shall** use the Memory Protection Unit (MPU) in case of realizing a mixed criticality application.

Category:	Requirement	Label:		ID:	4494995
Related To:			Related To':		

The system integrator **shall** consider the requirements in the ISO 26262 Safety Manual addon [TTC500-SM-26262] , in case compliance to ISO 26262 is required.

2 Safety Lifecycle

Category:	Comment	ID:	586714
Due to the HY-TTC 500 platform's nature of being a generic control unit for diverse safety-critical applications, the execution of the IEC 61508, ISO 13849 and ISO 25119 safety lifecycle phases are based on specific assumptions for the overall system. These assumptions are listed within the following document and need to be considered by the system integrator.			

Category:	Comment	ID:	3074044
The following subsections list the corresponding safety lifecycle phases and/or activities partly (e.g. overall system phases only applied on ECU level, ...) or completely considered in the course of the HY-TTC 500 platform development. Caused by the platforms nature, only a subset of phases/activities have been applied to the HY-TTC 500 which means all other lifecycle phases/activities have to be considered in the course of the system development by the system integrator. Although a phase/activity has already been considered on HY-TTC 500 ECU level, it does not mean that it is not also relevant for the system integrator on system level.			

2.1 IEC 61508

Category:	Comment	ID:	729253
The following IEC 61508 safety lifecycle phases were conducted on ECU level during the development of the HY-TTC 500 platform. The system integrator is, however, required to evaluate those assumptions that have been made during the execution: • Management of functional safety (part 1, clause 6) • Overall safety requirements (part 1, clause 7.5) • Overall safety requirements allocation (part 1, clause 7.6) • E/E/PE system safety requirements specification (part 1, clause 7.10) • E/E/PE safety related system: realization (part 1, clause 7.11) • Overall installation and commissioning (part 1, clause 7.13) • Overall operation, maintenance and repair (part 1, clause 7.15) • Overall modification and retrofit (part 1, clause 7.16) • Verification (part 1, clause 7.18) • Functional safety assessment (part 1, clause 8)			

2.2 ISO 13849

Category:	Comment	ID:	3074037
The following ISO 13849 safety lifecycle activities were conducted on ECU level during the development of the HY-TTC 500 platform. The system integrator is, however, required to evaluate those assumptions that have been made during the execution:			

- Design of SRP/CS (part 1, clause 4.4)
- Evaluation of the achieved PL (part 1, clause 4.5)
- Software safety requirements (part 1, clause 4.6)
- Verification that achieved PL meets PLr (part 1, clause 4.7)
- Ergonomic aspects of design (part 1, clause 4.8)
- Safety functions (part 1, clause 5)
- Categories and their relations to MTTFD of each channel, DCavg and CCF (part 1, clause 1.6)
- Fault consideration, fault exclusion (part 1, clause 1.7)
- Validation (part 1, clause 1.8)
- Maintenance (part 1, clause 1.9)

2.3 ISO 25119

Category:	Comment	ID:	4189060

The following ISO 25119 safety lifecycle activities were conducted on ECU level during the development of the HY-TTC 500 platform. The system integrator is, however, required to evaluate those assumptions that have been made during the execution:

- Quality Management System (part 1, clause 5)
- Management during complete safety lifecycle (part 1, clause 6)
- Assessment of functional safety (part 1, clause 7)
- Functional safety management activities after start of production (part1, clause 8)
- Plan for production and installation of safety-related systems (part1, clause 9)

Category:	Requirement	Label:		ID:	3073813
Related To:	855075		Related To':		

The system integrator **shall** conduct all lifecycle phases not or only partly applicable on HY-TTC 500 ECU level for the overall safety-related system depending on their required standard (IEC 61508 and/or ISO 13849 and/or ISO 25119).

Category:	Requirement	Label:		ID:	3073809
Related To:	855075		Related To':		

The system integrator **shall** evaluate the assumptions that have been made for the lifecycle phases/activities applicable on HY-TTC 500 ECU level related the overall safety-related system depending on their required standard (IEC 61508 and/or ISO 13849 and/or ISO 25119).

Category:	Comment	ID:	729351

Regardless of the HY-TTC 500 platform's development, it is the responsibility of the system integrator to follow the appropriate process for the overall system's development and integration with regards to the applicable standards and norms.

Category:	Requirement	Label:	Staff_Training	ID:	586716
Related To:		Related To':			

All persons involved in any lifecycle activity at the system integrator, including management activities, **shall** have the appropriate training, technical knowledge, experience and qualification relevant to the specific duties they have to perform. For details, see IEC 61508-1 [IEC 61508], section 6 and ISO 25119-1 [ISO 25119], section 6.4.

Category:	Requirement	Label:	HaR_Analysis	ID:	586718
Related To:	283858	Related To':			

The system integrator **shall** perform a hazard and risk analysis for the system and verify that the system requirements and the overall safety requirements derived from the hazard and risk analysis match the properties of the HY-TTC 500 platform (e.g. performance level, reaction times …).

Category:	Requirement	Label:	Safety_Parameters	ID:	586803
Related To:	411160	Related To':			

The system integrator **shall** verify that the safety requirements of the system (as derived from the hazard and risk analysis) match the safety parameters of the HY-TTC 500, e.g.

- Safety function
- Process safety time
- Proof test interval
- Safety integrity level or performance level

Category:	Comment	ID:	586805

For a definition of these parameters please refer to section *Safety Parameters*.
If the safety lifecycle is followed and the system integrator can demonstrate that all constraints are fulfilled by the system, safety integrity level 2 (SIL 2) and performance level d (PL d) can be achieved with the HY-TTC 500 platform.

Category:	Requirement	Label:	System_Eval	ID:	586807
Related To:	283808,627432	Related To':			

The system's safety functions, with respect to the required safety integrity level and performance level, respectively, **shall** be evaluated by the system integrator for the whole system—including the application software developed by the system integrator—according to the methods described in IEC 61508 [IEC 61508], ISO 25119 [ISO 25119] and ISO 13849 [ISO 13849].

3 Safety Concept Overview

Category:	Comment	ID:	586811

Special hardware and software functions are integrated into the HY-TTC 500 platform that allow the use in safety-critical applications.

The following hardware and software components are part of the safety platform:

- **ECU hardware:** The HY-TTC 500 is equipped with a Main CPU and a Safety Companion acting as external watchdog. For a detailed I/O description, characteristics and maximum ratings refer to the HY-TTC 500 System Manual [TTC500-SysM], Part I: Hardware Description.
- **Bootloader:** The bootloader will be executed after reset, performing application software download, checking and starting the application software.
- **Board support package (BSP):** Start-up code for the Main CPU that needs to be linked to the application software and linker command files (containing addresses and size of RAM, Flash and stack area).
- **FPGA bitstream:** The HY-TTC 500 features an additional logic IC that is used for obtaining certain feedback values of safety-critical outputs. The FPGA's function can be updated by flashing a separate FPGA bitstream to the ECU. This bitstream is part of the HY-TTC 500 platform's software release package.
- **I/O driver library:** The I/O drivers are delivered to the system integrator in form of a C library and header files. The I/O drivers include:
    - software functions allowing to access the HY-TTC 500 interfaces and I/Os from the application software (e.g. controlling the PWM outputs, reading the analog inputs, communicating over the CAN interface)
    - diagnostic modules that perform various I/O and CPU-internal tests at start-up and at runtime (e.g. RAM-tests, short circuit tests).

The interface between the application software and the HY-TTC 500 safety platform is the I/O driver API as specified by the HY-TTC 500 System Manual [TTC500-SysM], Part II: Software Description.

Category:	Requirement	Label:	3rd-Party_SW	ID:	586813
Related To:		Related To':			

Other software modules (e.g. additional libraries for CANopen Safety protocol implementations or CODESYS runtimes) are not part of the HY-TTC 500 safety platform. Therefore, if such modules are used with safety-critical applications, these modules **shall** either be classified as 'proven in use' according to the requirements of IEC 61508 [IEC 61508], ISO 25119 [ISO 25119] and ISO 13849 [ISO 13849] or verified and validated by the system integrator according to the requirements of the associated performance level. This verification and validation also applies to generated C or object code by tools used during application development.

Category:	Requirement	Label:	HW_Modification	ID:	586815
Related To:	283996	Related To':			

The HY-TTC 500 electronics **shall** not be modified in any part by the system integrator if used for safety-critical applications.

Category:	Requirement	Label:		ID:	924760
Related To:			Related To':		

In safety-critical environment, the system integrator **shall** only utilize HY-TTC 500 ECU variants with closed housing.

Category:	Requirement	Label:	SW_Modification	ID:	586817
Related To:			Related To':		

The I/O driver library and the header files as delivered by TTControl **shall** not be modified in any way by the system integrator.

Category:	Requirement	Label:	Env_Conditions	ID:	586819
Related To:	284157		Related To':		

The HY-TTC 500 **shall** only be used under the environmental conditions (e.g. temperature, vibration) as specified in the HY-TTC 500 System Manual [TTC500-SysM], Part I: Hardware Description.

Category:	Requirement	Label:	IO_Characteristics	ID:	717434
Related To:	284159		Related To':		

The HY-TTC 500 platform's I/Os **shall** only be used according to the characteristics and maximum ratings specified in the HY-TTC 500 System Manual [TTC500-SysM], Part I: Hardware Description.

3.1 Safety Parameters

3.1.1 Safety Function

Category:	Comment	ID:	587503

The following safety function is performed by the HY-TTC 500:

Execution of the user-programmed application (i.e. control the outputs in accordance with the control function and the input values) in a fail-safe principle.

3.1.2 Definition of the Safe State

Category:	Comment	ID:	586823

In the safe state, no current will be applied to the safety-critical outputs of the ECU, i.e. in case of an error the safety-critical outputs will be switched off.
One has to keep in mind, however, that the outputs are equipped with pull-up resistors to 5 V for diagnostic reasons. As this pull-up characteristic will not be disabled in the safe state, a minimal diagnostic current may flow through connected loads even in the safe state. The typical diagnostic

currents are specified in the corresponding output's section within the HY-TTC 500 System Manual [TTC500-SysM], Part I: Hardware Description.

Category:	Comment	ID:	1194971

For diagnostic reasons, the ECU's sensor supply outputs are not automatically switched off when entering the safe state. It is therefore not recommended to use the sensor supply outputs as a power source that should be disabled immediately, in case of a safe state transition.

Category:	Comment	ID:	587485

For diagnostic reasons, a minimum duty cycle is always applied to the safety-critical PWM stages as long as the CPU is in the state *Main*. This is the case, even if the application deliberately deactivates the corresponding outputs. For details see section *PWM High Side Stages*.

Category:	Comment	ID:	590202

The HY-TTC 500 platform's PWM stages are allocated to three different shut-off groups that feature separate shut-off paths, each. Thus—in case of certain failures—the application software can de-energize the one group with the erroneous PWM output, while keeping the remaining two groups operational. That way, the system integrator may implement a limp-home function which allows the system to run in a reduced mode, e.g. for returning to the workshop for repair.

Category:	Requirement	Label:	Shutoff_Allocation	ID:	590192
Related To:	320067		Related To':		

If the system integrator independently controls the separate shut-off groups in case of failures, the actuators **shall** be allocated to the groups in such a way that does not introduce dangerous situations in reduced operation mode.

3.1.3 Safety-critical System Components

Category:	Comment	ID:	590198

A safety-critical system component is a component that may cause hazardous conditions in case of a failure or malfunction. The following components of the HY-TTC 500 are defined as being safety-critical if any of the ECU's functions is used in a safety-critical application:

- Main CPU (including internal RAM and Flash)
- Safety Companion
- Power supply and internal supply voltages
- Internal temperature monitoring

Category:	Comment	ID:	590200

The following components can be defined as being safety-critical dependent on the application and dangerous failures within these functional blocks can be detected by the HY-TTC 500 I/O driver's diagnostic modules. For details about the internal failure diagnostics, please refer to section *Guideline on Hardware Metrics Determination.*
In the following list, the functions and pin ranges represent the whole HY-TTC 500 family whereas the single variants are subsets of the given functions below. Therefore for the provided functions and the respective pins of the respective variant please see HY-TTC 500 System Manual [TTC500-SysM].

- 5V sensor supplies 0-1 (*IO_SENSOR_SUPPLY_0*, *IO_SENSOR_SUPPLY_1*)
- Analog 3 mode inputs (*IO_ADC_00* ... *IO_ADC_07*) when used in current and voltage measurement modes
- Analog 2 mode inputs (*IO_ADC_08* ... *IO_ADC_23*) when being utilized redundantly
- Digital timer inputs 0-5 (*IO_PWD_00* ... *IO_PWD_05*) when being utilized in single channel mode
- High side PWM outputs (*IO_PWM_00* ... *IO_PWM_35*) when used in PWM output mode
- Digital high side outputs (*IO_DO_00* ... *IO_DO_07*) in combination with digital low side outputs
- Digital low side outputs (*IO_DO_08* ... *IO_DO_15*) in combination with digital high side outputs

Category:	Requirement	Label:	IO_Dependency	ID:	590194
Related To:	320083		Related To':		

If, for a given application, the value read from an analog or digital input is used for determining the set value of a safety-critical output, then this input **shall** also be defined as safety-critical.

Category:	Requirement	Label:	IOs_Nonsafe	ID:	590289
Related To:	320085,673057,648273		Related To':		

The following components do not provide the necessary diagnostic measures and therefore **shall not** be used as safety-critical components, unless the system integrator's application can provide the required diagnostic measures. For details about the custom failure diagnostics, please refer to section *Guideline on Hardware Metrics Determination.*
In the following list, the functions and pin ranges represent the whole HY-TTC 500 family whereas the single variants are subsets of the given functions below. Therefore for the provided functions and the respective pins of the respective variant please see HY-TTC 500 System Manual [TTC500-SysM].

- Variable sensor supply (*IO_SENSOR_SUPPLY_2*)
- Analog 3 mode inputs (*IO_ADC_00* ... *IO_ADC_07*) when used as resistive input or digital input
- Analog 2 mode inputs (*IO_ADC_08* ... *IO_ADC_23*) when being utilized in single channel configuration or as digital input
- Digital timer inputs 0-5 (*IO_PWD_00* ... *IO_PWD_05*) when being utilized in single channel configuration, as analog input or digital input
- Digital timer inputs 6-11 (*IO_PWD_06 ... IO_PWD_11*) when being utilized in combination with a timer input 0-5 or as analog input
- High side PWM outputs (*IO_PWM_00* ... *IO_PWM_35*) when used in digital output mode, as digital input or timer input
- Digital high side outputs (*IO_DO_00* ... *IO_DO_07*) when used without digital low side outputs as secondary shut-off paths, and when used as analog input or digital input
- Digital low side outputs (*IO_DO_08* ... *IO_DO_15*) when used without digital high side outputs as secondary shut-off paths, and when used as analog input or digital input

- Outputs for Proportional Valve Groups (PVG), low power analog voltage loads (VOUT) and digital high side loads (*IO_PVG_00* ... *IO_PVG_07*, *VOUT_00* ... *VOUT_07*, *IO_DO_52* ... *IO_DO_59*)
- LIN interface
- RS232 interface
- CAN interfaces (*IO_CAN_CHANNEL_0* ... *IO_CAN_CHANNEL_6*)
- External EEPROM
- External RAM
- External FRAM
- External Flash
- Real Time Clock
- Ethernet interface
- BroadR-Reach interface
- Debug Interfaces (LEDs, UART as standard IO, watchdog state)

Category:	Comment	ID:	587487

The secondary input function of dedicated outputs cannot be put on a level with the dedicated inputs, regarding their dangerous failure probability, due to the additional failure potential of the output circuit. Therefore, the system integrator is advised to either utilize the dedicated inputs or provide additional means of diagnostics when requiring inputs for safety-critical systems.

Category:	Requirement	Label:	System_FMEA	ID:	590287
Related To:	320077		Related To':		

The system integrator **shall** perform an FMEA for the system components and derive a list of safety-critical I/Os for the system.

3.1.4 Failure Reaction in Case of Errors

Category:	Comment	ID:	723213

The HY-TTC 500 platform distinguishes between different errors with regards to the momentary failure reaction. Depending on the type of error, the I/O-driver's diagnostic modules will initiate specific actions. The following section describes those types of errors and the according HY-TTC 500 platform's behavior. A detailed failure classification into the different error types can be found in the I/O driver API within the TTC 500 System Manual [TTC500-SysM], Part II: Software Development.

3.1.4.1 Fatal Errors

Category:	Comment	ID:	723224

An error is classified as being fatal, if a safe program execution is not possible anymore, regardless of the actual application. The following errors are characterized as being fatal:

- errors that are fatal in their consequence, so that an anti-glitch strategy is not feasible (e.g. RAM or register errors, safe state activation by the Safety Companion)
- temporary errors that persist over the anti-glitch time

For fatal errors, the HY-TTC 500 platform's failure reaction is to enter the safe state immediately. If the according notification callback is configured, the application software will be notified by the I/O-driver diagnostics.

3.1.4.2 Non-fatal Error

Category:	Comment	ID:	723236

An error is classified as being non-fatal, if its occurrence does not prevent the safe program execution, per se. That may be because the error is clearly related to a contained subsystem of the ECU (e.g. an analog input stage) or the error is located outside of the ECU (e.g. an open circuit of a safety-critical actuator).

Non-fatal errors do not directly lead to the safe state. Instead, the I/O-driver diagnostics will execute the application-specific error callback, if it has been correctly passed during the driver initialization.

3.1.4.3 Temporary Errors

Category:	Comment	ID:	723232

An error is classified as being temporary, if it only persists over a time less than or equal to the specified glitch filter time. Also, only those errors that feature dynamic characteristics may fall into the category of temporary errors, e.g. a signal range violation of an analog input signal or an invalid readback voltage of a digital power stage.

In case a temporary error persists over the defined glitch filter time, it may either turn into a fatal error or a non-fatal error, according to its consequence.

3.1.5 Failure Reaction Time

Category:	Comment	ID:	609583

The driver's task begin and task end functions will service the windowed-watchdog.

Category:	Comment	ID:	587495

Several diagnostics performed by the HY-TTC 500 platform are executed periodically. With every call to *IO_Driver_TaskEnd()* the diagnostic task function is executed, performing the I/O driver's diagnostic measures, while the call to *IO_Driver_TaskBegin()* will service the external window watchdog.
The diagnostic state machine distributes the execution of all diagnostics among 6 consecutive cycles. An individual diagnostic measure is therefore performed every 6 application cycles.

Category:	Comment	ID:	722729

If feasible, a failing diagnostic check will be de-glitched for a certain amount of time (i.e. the so-called glitch filter time that can be configured by the system integrator) in order to prevent sporadic external interferences from directly leading to the system's safe state.

When selecting the application software's glitch filter time, the system integrator should account for all those failures that may occur only temporary. For example, a low battery voltage situation caused by cold-start cranking may lead to an invalid sensor supply voltage. However, only violations that do last longer than the specified glitch filter time will signal a persistent error. For details, refer to section *Failure Reaction in Case of Errors.*

Category:	Requirement	Label:	Nonstop_Operation	ID:	587497
Related To:	630889		Related To':		

Because some diagnostics—performed by the HY-TTC 500—are only executed at system start-up, the application software **shall** not keep the ECU in a nonstop operation.

Category:	Comment	ID:	1194468

Details about the HY-TTC 500 platform's power functions can be found in chapter "*Power Supply*".

Category:	Requirement	Label:	Driving_Cycle	ID:	587499
Related To:	320113		Related To':		

A typical driving cycle (i.e. the time between power-up and power-down of the ECU) **shall** not exceed 24 hours.

Category:	Comment	ID:	586825

The term 'typical driving cycle' describes the time interval between power-up and power-down, a vehicle *is designed for*. That means, driving cycles of more than 24 hours shall only happen on rare occasions and are to be exercised with the utmost caution, as the safety related tests performed upon start-up are no longer executed with the specified proof test interval.

Due to the fact, that a number of diagnostics is only performed during system start-up, the typical driving cycle is considered to be equal to the proof test interval.

Category:	Requirement	Label:	Failure_Reaction_Time	ID:	813086
Related To:			Related To':		

The system integrator **shall** consider the HY-TTC 500 platform's effective failure reaction time for each safety function.

Category:	Comment	ID:	813084

For calculating the worst case failure reaction time, the system integrator has to combine the core diagnostic's failure reaction time (being independent from the used I/Os) and the additional I/O related failure reaction time (taking into account the I/O specific diagnostic time delay). That way, the overall failure reaction time can be determined accurately, for each individual safety function.

3.1.5.1 Core Failure Reaction Time

Category:	Comment	ID:	813067

The effective reaction time of the core's diagnostics is based on the following parameters that can be adjusted during the I/O driver initialization call:

- Command period, i.e. the so-called cycle time (*t_cycle*): 1 … 50 ms
- Glitch filter time (*t_glitch*): 1 … 180 ms

In addition, the external watchdog window time (*t_wd*) is defined to be 64 ms.

The configured glitch filter time correlates with the selected cycle time. Each specific failure diagnostic will be executed every sixth application cycle. Under worst case conditions, the applied glitch filter time will therefore increase to the next higher integer multiple of *6 * t_cycle*.
*t_glitch_effective = round_to_multiple(t_glitch, 6*t_cycle)*

Subsequently, the calculation of the core's effective worst case failure reaction time is as follows:
*wc_frt_core = max(((6+1) * t_cycle) + t_glitch_effective, t_wd)*

As a result, the core's calculated worst case failure reaction time can lie between 64 ms and 650 ms according to the safety parameters chosen by the application software.

3.1.5.2 I/O Failure Reaction Time

Category:	Comment	ID:	813423

Specific properties of the input and output stages (and their related signals) might contribute to the overall worst case failure reaction time for a given safety function, as well.

For the overall worst case failure reaction time, the system integrator typically has to add up the worst case failure reaction times of the core and the worst case failure reaction time for the input and output stages (i.e. the single input or output stage type that has the greatest influence).

The following section will outline the detailed impact of every I/O type.

3.1.5.2.1 PWM High Side Outputs

Category:	Comment	ID:	813082

Due to the PWM signal's nature, the configured PWM frequency is directly related to the worst case failure reaction time. The effective increase of the core's failure reaction time is twice the PWM output period plus an additional application cycle.

*wc_frt_io = 2 * pwm_period + t_cycle*

Category:	Comment	ID:	813449
In case the PWM high side current measurement is considered safety-relevant, the effective increase of the core's failure reaction time is 20 ms plus an additional application cycle. *wc_frt_io = 20 ms + t_cycle*			

3.1.5.2.2 Digital High Side Outputs

Category:	Comment	ID:	813461
The digital high side output increases the core's failure reaction time by 20 ms. *wc_frt_io = 20 ms*			

3.1.5.2.3 Timer Inputs

Category:	Comment	ID:	813466
Due to the timer signal's nature, the configured timer frequency is directly related to the worst case failure reaction time. The effective increase of the core's failure reaction time is equal to the inverse of the specified lower frequency threshold. *wc_frt_io = timer_period*			

3.1.5.2.4 Analog Inputs

Category:	Comment	ID:	813469
The analog inputs provide instant diagnostics that do not further increase the core's failure reaction time. Therefore, they do feature a failure reaction time of 0 ms. *wc_frt_io = 0 ms*			

3.1.5.2.5 External Shut-off Inputs

Category:	Comment	ID:	969439
The worst case reaction time for shutting off the corresponding safety switch groups via the external shut-off inputs is only dependent on the particular application cycle time. These analog shut-off inputs are			

sampled every 6th application cycle and the shut-off groups will be deactivated within the next application cycle or within 5 ms - whichever occurs first.

wc_frt_extshutoff = (6 * t_cycle) + min(t_cycle; 5 ms)

Note: This formula assumes an ideal switch without bouncing and simultaneous switching times for both terminals. Depending on the chosen switch, further timing delays have to be considered.

3.1.5.3 Calculation Examples

Category:	Comment	ID:	719711

The following examples will outline the procedure for calculating the worst case failure reaction time for given sets of inputs and outputs together with assumed cycle time (*t_cycle*) and glitch filter time (*t_glitch*).

Category:	Comment	ID:	813591

Example 1:

An application software specifies the cycle time (*t_cycle*) to be 10 ms and the glitch filter time (*t_glitch*) to be 100 ms. A given safety function makes use of the following safety-related inputs and outputs:

- 3 PWM high side outputs configured with an output frequency of 250 Hz
- 2 digital high side outputs
- 2 timer inputs being used with a frequency of 2 kHz, each
- 2 timer inputs being used with a frequency of 100 Hz, each

The resulting worst case failure reaction time of the core can be calculated as follows:
t_glitch_effective = round_to_multiple(100 ms, 6*10 ms) = 120 ms

Note: *round_to_multiple* means to find a positive integer number n that fulfills n*6*t_cycle >= t_glitch. In this example n must be 2 which results in 2*6*10ms = 120ms.

wc_frt_core = max(((6+1) * 10 ms) + 120 ms, 64 ms) = **190 ms**

The additional failure reaction time caused by the PWM high side outputs is:
wc_frt_io_pwm = 2 * 4 ms + 10 ms = 18 ms

The additional failure reaction time caused by the digital high side outputs is:
wc_frt_io_dout = 20 ms

The additional failure reaction time caused by the 2 timer inputs with a frequency of 2 kHz is:
wc_frt_io_timer2kHz = 0.5 ms

The additional failure reaction time caused by the 2 timer inputs with a frequency of 100 Hz is:
wc_frt_io_timer100Hz = 10 ms

For the overall worst case calculation, the I/O type with the greatest influence, i.e. the digital high side outputs, will be used:
wc_frt_io = *wc_frt_io_dout* = ***20 ms***

The overall failure reaction time for this exemplary configuration of the HY-TTC 500 platform is therefore:
wc_frt = *wc_frt_core* + *wc_frt_io* = *190 ms* + *20 ms* = ***210 ms***

That means, the assumed diagnostic coverage for the I/O driver's core diagnostics is only valid for safety functions with a process safety time of 210 ms or higher. For those safety functions that require a shorter failure reaction time, the system integrator needs to either adapt the above-mentioned parameters or provide separate diagnostic measures within the application software.

Category:	Comment	ID:	813743

Example 2:

An application software specifies the cycle time (*t_cycle*) to be 1 ms and the glitch filter time (*t_glitch*) to be 180 ms. A given safety function makes use of the following safety-related inputs and outputs:

- 2 PWM high side outputs configured with an output frequency of 500 Hz and safety-relevant current measurement
- 2 timer inputs being used with a frequency of 10 Hz, each
- 4 analog inputs

The resulting worst case failure reaction time of the core can be calculated as follows:
t_glitch_effective = *round_to_multiple(180 ms, 6*1 ms)* = *180 ms*

Note: *round_to_multiple* means to find a positive integer number n that fulfills *n*6*t_cycle* >= *t_glitch*. In this example n must be 30 which results in *30*6*10ms* = *180ms*.

wc_frt_core = *max(((6+1) * 1 ms) + 180 ms, 64 ms)* = ***187 ms***

The additional failure reaction time caused by the PWM high side outputs is:
*wc_frt_io_pwm = 2 * 2 ms + 1 ms = 5 ms*

The additional failure reaction time caused by the PWM high side current measurement is:
wc_frt_io_current = 20 ms + 1 ms = 21 ms

The additional failure reaction time caused by the 2 timer inputs with a frequency of 10 Hz is:
wc_frt_io_timer = 100 ms

The 4 analog inputs do not contribute to the overall failure rate, at all.
wc_frt_io_analog = 0 ms

For the overall worst case calculation, the I/O type with the greatest influence, i.e. the timer inputs, will be used:
wc_frt_io = *wc_frt_io_timer* = ***100 ms***

The overall failure reaction time for this exemplary configuration of the HY-TTC 500 platform is therefore:
wc_frt *= wc_frt_core + wc_frt_io = 187 ms + 100 ms =* ***287 ms***

That means, the assumed diagnostic coverage for the I/O driver's core diagnostics is only valid for safety functions with a process safety time of 287 ms or higher. For those safety functions that require a shorter failure reaction time, the system integrator needs to either adapt the above-mentioned parameters or provide separate diagnostic measures within the application software.

3.1.6 Probabilistic Failure Rate

Category:	Comment	ID:	586827

With respect to IEC 61508 [IEC 61508], the HY-TTC 500 platform is designed as a 1oo1D architecture and fulfills the requirements for Safety Integrity Level (SIL) 2.
With respect to ISO 13849 [ISO 13849], the HY-TTC 500 platform is designed as a Category 2 system and fulfills the requirements for Performance Level (PL) d.
With respect to ISO 25119 [ISO 25119], the HY-TTC 500 platform is designed as a Category 2 system and fulfills the requirements for Agriculture Performance Level (AgPL) d and Software Requirement Level SRL 2.

Category:	Comment	ID:	3407546

All stated probabilistic values are valid starting from **product version 01.08** (for probabilistic values of the previous product version 01.05 see Safety Manual V1.8.1).

3.1.6.1 Mission Profiles

Category:	Comment	ID:	591167

The hardware failure rate estimation has been performed based on two different assumed environmental conditions, in order to allow the system integrator to choose the mission profile that fits best to the overall system's mission profile.
The both mission profiles differ in their typical usage characteristics:

- The first mission profile (*MP_Conventional*) is targeted towards conventional off-highway vehicles, typically being operated continuously throughout the whole day with a relatively low number of operational cycles:
    - Number of working cycles per day: 5
    - Average temperature variation seen by the ECU's components each working cycle: 35 °C
    - Average temperature variation seen by the ECU's components each non-operational day: 10 °C

- The second mission profile (*MP_Stop-Go*) considers the common usage characteristics of stop-&-go applications, with a high number of very short working tasks throughout the typical working day:
    - Number of working cycles per day: 100
    - Average temperature variation seen by the ECU's components each working cycle: 5 °C
    - Average temperature variation seen by the ECU's components each non-operational day: 10 °C

Both mission profiles are based on the worst-case assumption of 24 h of operational time per day and an average operational utilization of 300 days per year. In addition, the following ambient temperature distribution has been assumed:

Ambient Temperature	Distribution
-40 °C	0.5 %
23 °C	35 %
60 °C	48 %
80 °C	15 %
120 °C	1.5 %

Table 2

3.1.6.2 Probabilistic Values for IEC 61508

Category:	Comment	ID:	3400585

The probabilistic values calculated according to the requirements of IEC 61508 [IEC 61508] based on the mission profile *MP_Conventional* are:

Values	HY-TTC 508	HY-TTC 510	HY-TTC 520	HY-TTC 540	HY-TTC 580	HY-TTC 590/590E
PFH	141 FIT	171 FIT	181 FIT	232 FIT	274 FIT	274 FIT
SFF	98.50 %	98.32 %	98.25 %	97.91 %	97.65 %	97.65 %

Table 3

Category:	Comment	ID:	3400587

The probabilistic values calculated according to the requirements of IEC 61508 [IEC 61508] based on the mission profile *MP_Stop-Go* are:

Values	HY-TTC 508	HY-TTC 510	HY-TTC 520	HY-TTC 540	HY-TTC 580	HY-TTC 590/590E
PFH	135 FIT	166 FIT	176 FIT	227 FIT	269 FIT	269 FIT
SFF	98.55 %	98.35 %	98.27 %	97.92 %	97.65 %	97.65 %

Table 4

3.1.6.3 Probabilistic Values for ISO 13849

Category:	Comment	ID:	3400593

The probabilistic values calculated according to the requirements of ISO 13849 [ISO 13849] based on the mission profile *MP_Conventional* are:

Values	HY-TTC 508	HY-TTC 510	HY-TTC 520	HY-TTC 540	HY-TTC 580	HY-TTC 590/590E
λ_{DU}	118 FIT	149 FIT	159 FIT	210 FIT	251 FIT	251 FIT
λ_{DD}	1548 FIT	1759 FIT	1819 FIT	2122 FIT	2395 FIT	2400 FIT
$MTTF_d$	68.55 years	60.01 years	57.87 years	49.09 years	43.21 years	43.12 years
DC_{AVG}	92.98 %	92.46 %	92.22 %	91.26 %	90.65 %	90.66 %

Table 5

Category: Comment ID: 3400595

The probabilistic values calculated according to the requirements of ISO 13849 [ISO 13849] based on the mission profile *MP_Stop-Go* are:

Values	HY-TTC 508	HY-TTC 510	HY-TTC 520	HY-TTC 540	HY-TTC 580	HY-TTC 590/590E
λ_{DU}	113 FIT	143 FIT	153 FIT	204 FIT	246 FIT	246 FIT
λ_{DD}	1530 FIT	1741 FIT	1802 FIT	2105 FIT	2381 FIT	2386 FIT
$MTTF_d$	69.50 years	60.70 years	58.50 years	49.50 years	43.45 years	43.37 years
DC_{AVG}	93.15 %	92.57 %	92.31 %	91.28 %	90.63 %	90.65 %

Table 6

3.1.6.4 Probabilistic Values for ISO 25119

Category: Comment ID: 4217708

The probabilistic values calculated according to the requirements of ISO 25119 [ISO 25119] based on the mission profile *MP_Conventional* are:

Values	HY-TTC 508	HY-TTC 510	HY-TTC 520	HY-TTC 540	HY-TTC 580	HY-TTC 590/590E
$MTTF_o$	68.55 years	60.01 years	57.87 years	49.09 years	43.21 years	43.12 years
DC	92.98 %	92.46%	92.22 %	91.26 %	90.65 %	90.66 %

Table 7

Category: Comment ID: 4217740

The probabilistic values calculated according to the requirements of ISO 25119 [ISO 25119] based on the mission profile *MP_Stop-Go* are:

Values	HY-TTC 508	HY-TTC 510	HY-TTC 520	HY-TTC 540	HY-TTC 580	HY-TTC 590/590E
$MTTF_o$	69.50 years	60.70 years	58.50 years	49.50 years	43.45 years	43.37 years
DC	93.15 %	92.57 %	92.31 %	91.28 %	90.63 %	90.65 %

Table 8

Category:	Requirement	Label:	Quantitative_Metrics	ID:	591185
Related To:			Related To':		
The system integrator **shall** rely on the HY-TTC 500 platform's probabilistic values only if the overall system characteristics are arguably comparable to one of the provided mission profiles (*MP_Conventional* or *MP_Stop-Go*).					

Category:	Requirement	Label:	System_Metrics	ID:	591187
Related To:			Related To':		
The actual probabilistic values for the whole system (PFH, SFF, MTTFd and DCavg, respectively), including the HY-TTC 500, sensors, actuators and cabling have to be determined by the system integrator. The system integrator **shall** verify that the probabilistic values of the overall system are within the limits specified in IEC 61508 [IEC 61508], ISO 25119 [ISO 25119] and ISO 13849 [ISO 13849], respectively, for the system's required safety performance.					

4 Safety Measures of the HY-TTC 500 Platform

Category:	Comment	ID:	591243
The following section outlines the diagnostics that are implemented by the HY-TTC 500 platform for the individual functional blocks. It also describes how these functions have to be configured by the system integrator for safe operation of the HY-TTC 500 platform.			

Category:	Comment	ID:	1544257
Please consider, that requirements given for a pins alternative functions are also valid for HY-TTC 500 variants which just provide the alternative function functions (e.g. HY-TTC 540 - Pin 101 just provides 'Digital Input' / 'Timer Input' instead of the main function 'HS PWM Output' - nevertheless, the requirements stated in the 'PWM High Side Stages' section for alternative functions have to be considered as well).			

4.1 Power Supply

Category:	Comment	ID:	591645
The HY-TTC 500 platform features two physically separated power supply connections. One power supply connection is exclusively provided for the ECU's logic unit, while the other connection supplies the power stages. In addition, the ECU is equipped with two additional inputs for a power control function: In permanently supplied systems, the terminal 15 input (K15) may be connected with the ignition key lock, the wake up input (Wake-Up) may be connected to a secondary power up source (e.g. the vehicle's door contact). The ECU's activation is triggered, in case one of these inputs is turned on. After deactivating these signals, the ECU may continue to operate before autonomously powering down upon the application's shutdown request. Details about the terminal 15 and wake up inputs can be found in the TTC 500 System Manual [TTC500-SysM]. In case the software-controlled shutdown function via terminal 15 is not utilized (i.e., terminal 15 is tied to battery voltage and the HY-TTC 500 platform's power supply is directly activated and deactivated by the operator), the system integrator is advised to provide the system operator with means to disconnect the ECU's logic unit from battery voltage. In order to allow reliable deactivation—even in case of an external load being shorted to battery voltage—the power switch (e.g. ignition key, circuit breaker …) is required to also disconnect the ECU's logic unit from the power stage supply rail.			

Category:	Requirement	Label:	Operator_Shutdown	ID:	591647
Related To:	284257		Related To':		
The operator **shall** be provided with means to disable the ECU's supply either by utilizing the HY-TTC 500 platform's power control function or by directly disconnecting the ECU's logic supply from battery voltage.					

Category:	Requirement	Label:	Supply_Separation	ID:	591649
Related To:	284257		Related To':		
If the HY-TTC 500 platform's power control function is not utilized and both power supply rails are tied together, the system integrator **shall** assure that the power switch—disconnecting the ECU's logic supply—does also separate the logic supply from the power stage supply.					

Category:	Comment	ID:	591651

The following figure shows an **invalid** wiring example when using a power switch without terminal 15 utilization. In case of external short circuits on the actuator lines, the internal logic core (BAT+ CPU) might still be supplied via reverse conducting power stages, even if the power switch is activated.

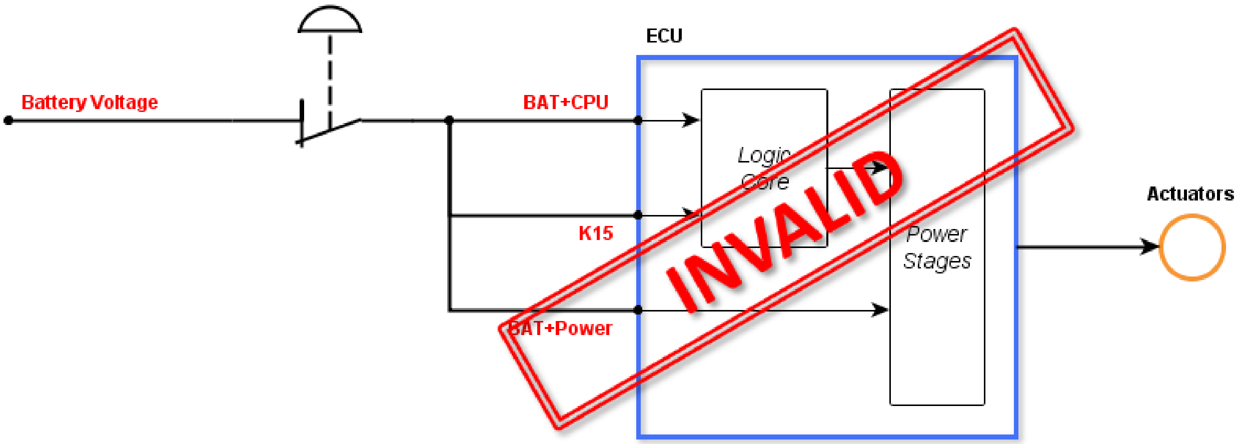

Figure 1

Category:	Comment	ID:	915449

The following figure shows another **invalid** wiring example when using a power switch to concurrently disconnect terminal 15 and the supply for the internal power stages (BAT+ Power). In case of external short circuits in the actuator lines, the terminal 15 input might still be supplied via reverse conducting power stages, even if the power switch is activated.

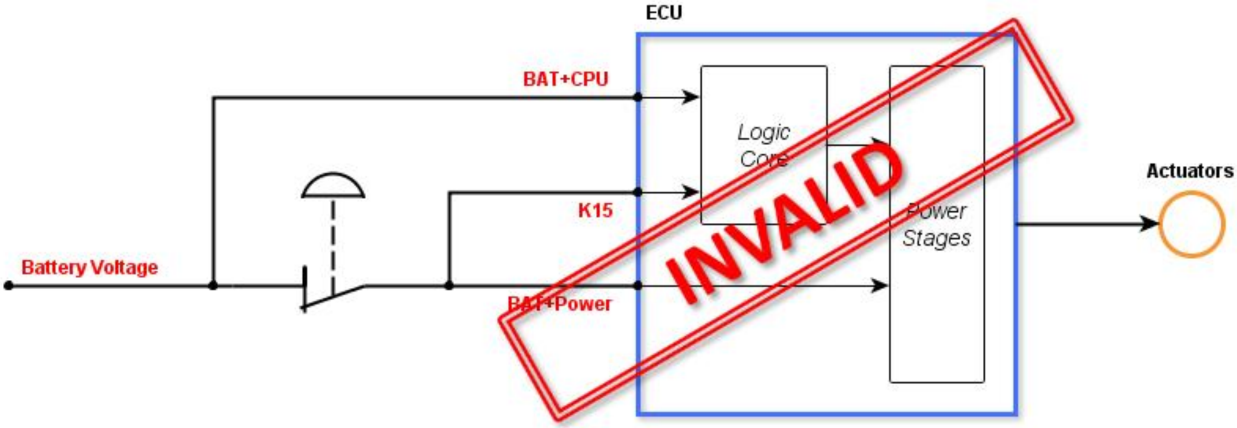

Figure 2

Category:	Comment	ID:	591653

The following figure shows a valid wiring example when using a power switch that independently disconnects the supply for the internal logic core (BAT+ CPU) and also decouples both power supply rails from each other. In case of external short circuits on the actuator lines, the power switch can still de-energize the ECU's logic core and therefore shut down the overall ECU. With this configuration however, a software-controlled after-run is not possible.

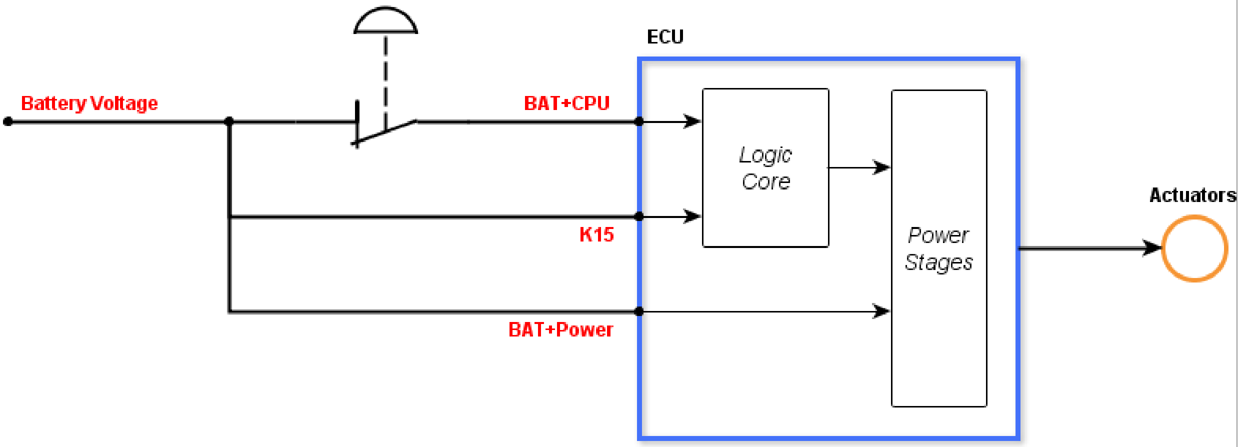

Figure 3

Category:	Comment	ID:	591655

The following figure shows another valid wiring example when using an power switch, only disconnecting the terminal 15 pin (K15). In case of external short circuits on the actuator lines, the ECU's logic core is still functional and might store the occurrence of a shut-off condition to the failure memory before disabling the after-run mode and finally powering down completely.

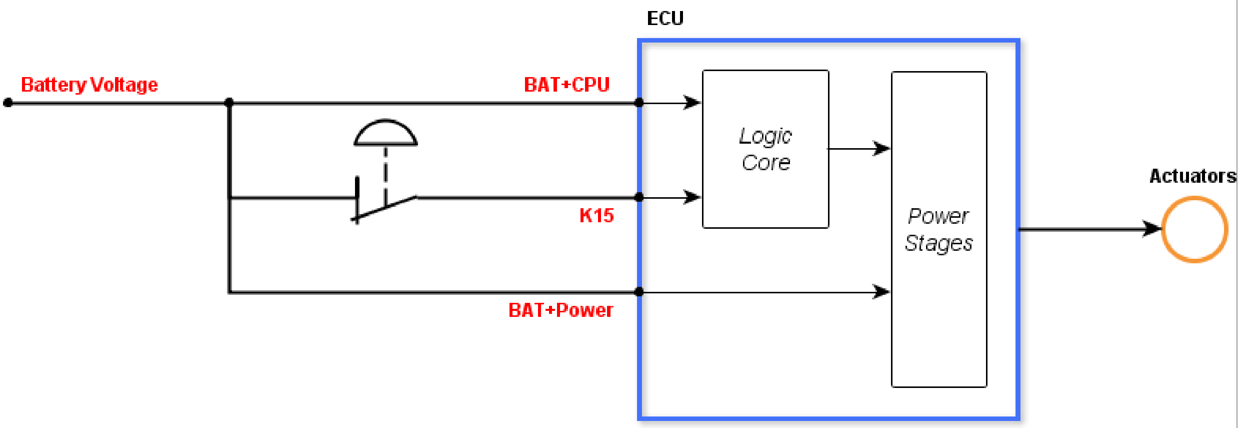

Figure 4

Category:	Requirement	Label:	Power_Override_K15	ID:	717653
Related To:	632325		Related To':		

The application software **shall** not request a power-down of the ECU (by calling *IO_POWER_Set()*) while the voltage level of terminal 15 (K15) is still high.

Category:	Comment	ID:	717655

A power down request while terminal 15 (K15) is high will lead to a reset of the device, i.e., the device will immediately power on again. This procedure will also clear the count of safety-related resets which is typically only performed for safety-critical errors; the number of allowed resets is configured via the safety parameters of the general driver initialization function.

A shutdown is only to be performed if the voltage level of K15 is low. Notice that the HY-TTC 500 may not power down if K15 is high and the device is already in the safe state. This might be the case, if, e.g., the device has already performed the specified maximum number of allowed resets.

4.2 Input Stages

Category:	Comment	ID:	592155

The following section describes the requirements for utilization of input stages in safety-critical environments. Whenever a requirement demands the redundant usage of specific inputs, this redundancy does only correspond to the HY-TTC 500 input stage. The sensor, however, may feature a single channel architecture, as long as it is connected to both used inputs, in parallel.
Still, the system integrator is responsible for calculating the overall dangerous failure rate of the complete channel involved in the execution of a safety function.
The redundancy of input stages may also be established by combining different types of input stages—as long as both of the utilized input types support the desired mode of operation.

4.2.1 Timer Inputs

Category:	Comment	ID:	592163

The digital timer inputs 0-5 (*IO_PWD_00* ... *IO_PWD_05*) provide the necessary diagnostic measures and are usable for safety-critical applications, when adhering to the requirements in the following section.
The digital timer inputs 6-11 (*IO_PWD_06* ... *IO_PWD_11*) do not provide the same set of diagnostic measures and are therefore not usable for safety-critical applications without further restrictions. For details about their suitability, please refer to section *Guideline on Hardware Metrics Determination*.

Category:	Requirement	Label:	Timer_Get	ID:	592203
Related To:		Related To':			

For each safety-critical timer input stage, the application **shall** periodically trigger the measurement of pulse high-time, pulse low-time, period width, frequency or number of edges for pulsed sensor signals via the appropriate driver functions:

- *IO_PWD_ComplexGet()*
- *IO_PWD_IncGet()*
- *IO_PWD_CountGet()*
- *IO_PWD_UniversalGet()*
- *IO_PWD_GetCurrent()*

Note 1: If a universal timer channel is co-configured for incremental mode together with any other combination of modes both the primary and secondary channel are redundantly configured. Thus, for safety-critical configuration, the application software needs to periodically trigger the measurement for **both** channels of complex or edge count modes.
Note 2: If a complex timer channel is configured as safety-critical current timer input (parameter *pupd = IO_PWD_PD_90*) the current measurement function *IO_PWD_GetCurrent()* needs to be called alongside one of the four remaining timer step functions.

Category:	Requirement	Label:	Timer_Guideline	ID:	592213
Related To:		Related To':			

The sensors used for safety-critical digital inputs **shall** be chosen in accordance with section *Sensor Selection Guideline*.

Category:	Requirement	Label:		ID:	920133
Related To:		Related To':			

The probabilistic values for the timer input stages **shall** be chosen in accordance with section *Guideline on Hardware Metrics Determination*.

Category:	Requirement	Label:	Timer_Limits	ID:	592205
Related To:	290425	Related To':			

When using sensors that generate pulses in their idle state, the acceptable upper and lower limits for the measured timer value (i.e. pulse high-time, pulse low-time, period width, frequency or number of edges) **shall** be specified by the system integrator.

Category:	Comment	ID:	592209

The I/O driver does not provide measures for comparing the measured values of redundant inputs. Thus, the application is required to implement these techniques.

Category:	Requirement	Label:	Timer_Consistency	ID:	592211
Related To:	290427,627258	Related To':			

When using timer inputs redundantly, the application **shall** provide the consistency checks for the measured values of the redundant inputs.

4.2.2 Analog Inputs

Category:	Comment	ID:	591421
The analog inputs (*IO_ADC_00* ... *IO_ADC_23*) provide the necessary diagnostic measures and are usable for safety-critical applications, when adhering to the requirements in the following section.			

4.2.2.1 General

Category:	Comment	ID:	592219
The HY-TTC 500 platform provides the following types of analog inputs that can be used for safety-critical applications: • 3 mode analog inputs (for voltage and current measurement), configurable by software • 2 mode analog inputs (for voltage and current measurement), configurable by software Note: The HY-TTC 500 platform does not provide diagnostic measures for the 3 mode analog inputs' resistive measurement setting. If a specific diagnostic coverage is required for usage within safety-critical applications, the system integrator has to provide means to detect failures within these input stages.			

Category:	Requirement	Label:	Analog_Guideline	ID:	592225
Related To:			Related To':		
The sensors used for safety-critical analog inputs **shall** be chosen in accordance with section *Sensor Selection Guideline*.					

Category:	Requirement	Label:	Analog_Metrics	ID:	920136
Related To:			Related To':		
The probabilistic values for the analog input stages **shall** be chosen in accordance with section *Guideline on Hardware Metrics Determination*.					

Category:	Comment	ID:	924662
The I/O driver does not provide measures for comparing the measured values of redundant inputs. Thus, the application is required to implement these techniques.			

Category:	Requirement	Label:	Analog_Consistency	ID:	924664
Related To:	627270		Related To':		
When using analog inputs redundantly, the application **shall** provide the consistency checks for the measured values of the redundant inputs.					

4.2.2.2 Analog 3 Mode Inputs

Category:	Comment	ID:	592223

The analog 3 mode inputs (*IO_ADC_00* ... *IO_ADC_07*) can be configured by software for the following modes that may be used for safety-critical applications:

- Voltage measurement (0…5 V)
- Current measurement (0…24 mA)

The HY-TTC 500 platform does not provide diagnostic measures for the following 3 mode setting.

- Resistance measurement (0…100 kOhm)

If a specific diagnostic coverage is required for usage within safety-critical applications, the system integrator has to provide means to detect failures within these input stages.

Category:	Comment	ID:	592233

The analog 3 mode inputs do provide the necessary measures for allowing single inputs to be used as safety-critical, when configured for voltage or current measurement. Thus, safety-critical analog sensors may be connected to analog 3 mode inputs in a single channel architecture, for those measurement modes.

Category:	Requirement	Label:	Analog3_Get	ID:	592221
Related To:			Related To':		

For each safety-critical analog 3 mode input stage, the application **shall** periodically perform the ADC measurement, by calling the appropriate driver function *IO_ADC_Get().*

4.2.2.3 Analog 2 Mode Inputs

Category:	Comment	ID:	592229

The analog 2 mode inputs (*IO_ADC_08* ... *IO_ADC_23*) can be configured by software for the following modes:

- Voltage measurement (0…5 V or 0…10 V) for analog inputs IO_ADC_08 - IO_ADC_15
- Voltage measurement (0…5 V or 0…32 V) for analog inputs IO_ADC_16 - IO_ADC_23
- Current measurement (0…24 mA)

Category:	Comment	ID:	592237

The analog 2 mode inputs provide the necessary diagnostic measures and are usable for safety-critical applications, when adhering to the requirements in the following section.

Category:	Requirement	Label:	Analog2_Get	ID:	895039
Related To:		Related To':			

For each safety-critical analog 2 mode input stage, the application **shall** periodically perform the ADC measurement, by calling the appropriate driver function *IO_ADC_Get().*

4.3 Power Stages

Category:	Comment	ID:	591657

The HY-TTC 500 platform is capable of controlling safety-critical actuators with either PWM high side outputs or a combination of digital high side and low side stages. The following section will outline the considerations that have to be taken into account during system integration.

4.3.1 PWM High Side Stages

Category:	Comment	ID:	592276

The PWM high side stages (*IO_PWM_00* ... *IO_PWM_35*) provide the necessary diagnostic measures and are usable for safety-critical applications, when adhering to the subsequent requirements. Every PWM high side stage also provides a dedicated current measurement function that can also be utilized for safety-critical functions, if required for a given system.

Category:	Comment	ID:	592272

Typically, the PWM high side stages of the HY-TTC 500 platform will be used for controlling valves. For a safe operation of these valves, the safety platform monitors the duty cycle and frequency of the PWM signals, at runtime. In addition, the outputs are checked for short circuits to ground or power supply as well as for open circuits (e.g. cable break).

In order to perform these diagnostics, the PWM signal's nature of having steadily changing voltage levels is used for comparing the desired signal sequence with the actual measurement. As a result, the minimum and maximum duty cycles are limited, so that a test pulse for diagnostic measurements is present under all conditions which can be used for continuously testing the ability to deactivate the power stages.

The duty cycle limits and duty cycle tolerances are defined in the I/O driver. Depending on the initial I/O driver configuration, the HY-TTC 500 will either directly enter the safe state or leave the decision to the application software via the optional error callback (see section *Application Callbacks*).

Category:	Requirement	Label:	PWM_Minimum_Energy	ID:	592111
Related To:		Related To':			

The system integrator **shall** ensure that the PWM stage's lower duty cycle limit (i.e. the minimum possible duty cycle) does not already energize the connected actuator in a way that could lead to a dangerous situation.

Category:	Comment	ID:	919117
The minimum possible duty cycle results from the minimum pulse length (100 µs) that is present even if the application software deactivates a safety-critical high side stage. Depending on the configured PWM frequency, the minimum duty cycle might go up to a value of 10 %, i.e. for a PWM frequency of 1000 Hz.			

Category:	Comment	ID:	592687
If the application tries to initialize a PWM stage with a frequency which is not supported by the HY-TTC 500, the I/O driver will use the next higher available frequency. For the list of available frequencies refer to the HY-TTC 500 System Manual [TTC500-SysM], Part II: Software Description.			

Category:	Comment	ID:	592689
Note that for frequencies which do not result in a period of an integral multiple of 1 ms, the I/O driver only provides averaged values calculated over 2 or 4 PWM periods, as stated in the HY-TTC 500 System Manual [TTC500-SysM], Part II: Software Description.			

Category:	Comment	ID:	843350
Every PWM high side stage features an internal secondary shut-off path, the so-called safety switch. Depending on the device variant, up to three separate safety switches are available, each one allocated to a predefined group of PWM high side stages. Details of the safety switch allocation can be found in the HY-TTC 500 System Manual [TTC500-SysM]. Due to the PWM high side stages' reverse conducting characteristics, a short circuit to battery voltage at any PWM high side output's connector pin—even those not being used for safety-critical applications—might influence the safety integrity of all remaining high side stages sharing the same safety switch, by preventing that single safety switch from de-energizing. To that end, the system integrator is advised to evaluate the criticality of such failures when allocating the HY-TTC 500 platform's connector pins to the system's safety functions.			

Category:	Requirement	Label:	PWMHS_Short_Group	ID:	843420
Related To:			Related To':		
The system integrator **shall** take into account the possibility of an external short circuit to battery voltage at a PWM high side stage's connector pin and consider the impact on those PWM high side stages sharing the same internal safety switch.					

Category:	Comment	ID:	843422
These considerations are also relevant when using the PWM high side stages' secondary functions, i.e. the digital or frequency input capabilities.			

Category:	Comment	ID:	592695
If the application software initializes PWM stages by passing safety parameters, the I/O driver checks the specified PWM frequency and returns an error if the valid range is violated.			

Category:	Requirement	Label:	PWMHS_Set	ID:	592699
Related To:			Related To':		
For each safety-critical PWM output, the application **shall** periodically call the PWM high side stage's appropriate task function *IO_PWM_SetDuty()* to trigger the feedback measurements.					

Category:	Requirement	Label:	PWMHS_Current_Get	ID:	592701
Related To:			Related To':		
If the current measurement of a safety-critical PWM output is also considered safety-critical, the application software **shall** periodically call the PWM high side stage's appropriate task function *IO_PWM_GetCur()* or *IO_PWM_GetCurQueue()* to trigger the current measurements.					

Category:	Requirement	Label:	PWMHS_Resolve	ID:	1195152
Related To:			Related To':		
When using the PWM ouput's resolve function to distinguish between open loads and battery short circuits, i.e. *IO_PWM_ResolveOpenLoadShortCircuit()*, the system integrator **shall** consider the impact on all remaining PWM output pins (*IO_PWM_00* ... *IO_PWM_35*).					

Category:	Comment	ID:	1195168
Details about the PWM output's resolve function can be found in the HY-TTC 500 System Manual [TTC500-SysM], Part II: Software Description.			

Category:	Requirement	Label:	PWMHS_Metrics	ID:	920124
Related To:			Related To':		
The probabilistic values for the PWM high side stages **shall** be chosen in accordance with section *Guideline on Hardware Metrics Determination*.					

4.3.1.1 Alternative Pin Functions

Category:	Requirement	Label:	PWMHS_Alternative_Group	ID:	843776
Related To:			Related To':		
When utilizing the secondary function inputs of PWM high side stages, sharing a safety switch with safety-related PWM high side stages, the system integrator **shall** employ input devices (i.e. sensors and switches) whose failure modes do not violate the overall system's safety functions.					

Category:	Comment	ID:	844022
That would be, e.g. the avoidance of sensors with push pull stages or switches to battery voltage, excluding the possibility of dangerously influencing the remaining PWM high side stages.			

4.3.2 Digital High Side Stages

Category:	Comment	ID:	592286

The digital high side stages (*IO_DO_00* ... *IO_DO_07*) provide the necessary diagnostic measures and are usable for safety-critical applications, when adhering to the subsequent requirements.

Category:	Comment	ID:	717651

Typically, the digital high side outputs of the HY-TTC 500 platform will be used for controlling valves. For a safe operation of these valves, the safety platform monitors the output level of the digital output signals, at runtime. In addition, the outputs are checked for short circuits to ground or power supply as well as for open circuits (e.g. cable break).

Depending on the initial I/O driver configuration, the HY-TTC 500 will either directly enter the safe state or leave the decision to the application software via the optional error callback (see section *Application Callbacks*).

Category:	Requirement	Label:	DigitalHS_ShutOff	ID:	592274
Related To:			Related To':		

When operating digital high side outputs in a safety-critical manner, the system integrator **shall** utilize low side stages as secondary shut-off paths or provide other means that allow to redundantly disable the connected actuators.

Category:	Requirement	Label:	DigitalHS_Init	ID:	592331
Related To:	648174		Related To':		

When utilizing the low side stages as secondary shut-off paths, the application software **shall** specify the shut-off path configuration used for each safety-critical digital output when calling the digital output driver initialization function *IO_DO_Init()*.

Category:	Requirement	Label:	DigitalHS_Voltage	ID:	592655
Related To:			Related To':		

For each safety-critical digital high side output, the application **shall** periodically call the digital high side stage's appropriate task function *IO_DO_Set()* to trigger the feedback measurements.

Category:	Comment	ID:	591251

The measurement values required for diagnostics will be checked internally by the diagnostic module of the I/O driver. The system integrator has to take care of correctly setting up the safety-critical outputs during initialization and periodically calling the output's step functions (e.g. *IO_DO_Set()*) with a cycle time that is appropriate for the diagnostic purpose of the overall system.

Category:	Requirement	Label:	DigitalHS_Period	ID:	814657
Related To:			Related To':		

When operating digital high side outputs in a safety-critical manner and changing the output's state with periods shorter than the HY-TTC 500 platform's overall worst case failure reaction time, the application software **shall** periodically evaluate the return value of the task function *IO_DO_Set()* in order to check for dangerous failures.

Category:	Comment	ID:	814594

In case of such frequent state changes by the application software via *IO_DO_Set()*, the HY-TTC 500 platform's glitch filter strategy might cover potential failures of the corresponding digital output (e.g. an external short circuit to battery voltage). These error conditions will however be passed to the application via the *IO_DO_Set()* return value, even if a certain failure is currently being de-glitched.

Therefore, the system integrator is advised to frequently check the task function's return value for error conditions that may prove to be dangerous according to the overall system concept.

Category:	Comment	ID:	814943

Periodically changing a digital high side output's state even faster (i.e. with a period shorter than 20 ms) will completely prevent the HY-TTC 500 diagnostics from reading correct feedback values, anymore. This will result in a persistent error condition that executes the application software's error callback function.

Category:	Comment	ID:	814673

For operating high side outputs with periodically changing states and a period shorter than the HY-TTC 500 platform's overall worst case failure reaction time, the system integrator should utilize the dedicated PWM high side outputs. These outputs provide superior diagnostic measures for detecting failures within dynamically changing output signals.

Category:	Requirement	Label:	DigitalHS_Metrics	ID:	920129
Related To:			Related To':		

The probabilistic values for the digital high side stages **shall** be chosen in accordance with section *Guideline on Hardware Metrics Determination*.

4.3.3 Digital Low Side Stages

Category:	Comment	ID:	895058

The digital low side stages (*IO_DO_08* ... *IO_DO_15*) provide the necessary diagnostic measures and are usable for safety-critical applications, when adhering to the subsequent requirements.

Category:	Comment	ID:	895062
The digital low side stages are primarily intended to be utilized in combination with safety-critically used digital high side stages. Together they provide two independent shut-off paths that allow disabling the connected actuators even in case of possible failures.			

Category:	Requirement	Label:	DigitalLS_ShutOff	ID:	895065
Related To:			Related To':		
When operating digital low side outputs in a safety-critical manner, the system integrator **shall** utilize high side stages as secondary shut-off paths or provide other means that allow to redundantly disable the connected actuators.					

Category:	Requirement	Label:	DigitalLS_ShutOffReq	ID:	895067
Related To:			Related To':		
When utilizing the high side stages as secondary shut-off paths, the system integrator **shall** adhere to the above-mentioned requirements in section *Digital High Side Stages*.					

Category:	Requirement	Label:	DigitalLS_Metrics	ID:	920131
Related To:			Related To':		
The probabilistic values for the digital low side stages **shall** be chosen in accordance with section *Guideline on Hardware Metrics Determination*.					

4.3.4 Memory Protection Unit

Category:	Requirement	Label:	MPU_Protection	ID:	718454
Related To:	438806		Related To':		
If demanded by the system's design, the application software **shall** use the Memory Protection Unit (MPU) to protect critical memory areas from unpermitted access.					

Category:	Comment	ID:	4106003
The following section is only applicable if the system integrator uses the memory protection unit			

Category:	Comment	ID:	4105505
If the MPU is used, the I/O Driver source code needs to execute in privileged CPU mode.			

Category:	Comment	ID:	718479
If the MPU is not used at all, the entire CPU internal memories need to be considered as "safe" areas.			

Category:	Comment	ID:	718472

If the MPU is used, the I/O Driver code needs read and write permissions for the following RAM memory sections:

- CSM_VAR_ZERO_INIT_UNSPECIFIED, CSM_VAR_NO_INIT_UNSPECIFIED
- IO_DRIVER_DATA_NORMAL
- IO_DRIVER_COMMON
- Shared Memory area (0x0803FEE0 to 0x0803FFFF)

Category:	Comment	ID:	4106230

If the MPU is used, the I/O Driver code needs read and executable permissions for the following internal flash memory section:

- CSM_CODE
- IO_DRIVER_CODE
- Exception vectors and the Bootloader memory area (0x0 to 0x0001FFFF)

Category:	Comment	ID:	4106267

If the MPU is used, the I/O Driver code needs at least read permissions for the following internal flash memory sections:

- CSM_CONST
- IO_DRIVER_CONST

Category:	Comment	ID:	4106271

The I/O Driver code executes in the main application thread and in exceptions. Requirements for the MPU access permissions have to be fulfilled in both cases:

- In the main thread, the application enables and disables the User MPU regions using the IO_MPU API functions as needed to comply with the I/O Driver requirements and with the safety requirements specific to the application. E.g. when a User MPU region is configured to deny access to one of the I/O Driver memory sections, this region must be disabled from the API before any I/O Driver function can be called.
- The behavior in exceptions depends on the selected MPU protection policy as configured in the IO_MPU API. Depending on the setting, the I/O Driver automatically disables selected User MPU regions in order to ensure the necessary access permissions.

Category:	Comment	ID:	4106341

The system needs at least read access permissions to the VIM (Vector Interrupt Manager) peripheral memory area (0xFFFFFE00 to 0xFFFFFEFF), if the MPU is used.

5 Application Interface

Category:	Comment	ID:	608636
The following section describes the interface between the application and the HY-TTC 500 platform. It also lists those diagnostic measures that have to be performed by the application software in order to guarantee safe operation of the HY-TTC 500 ECU under foreseeable conditions.			

Category:	Comment	ID:	609543
The interface between the application and the HY-TTC 500 platform is defined by the C-driver API. For a detailed description please refer to the HY-TTC 500 I/O Driver User Manual [TTC500-IOUM]. In case the application software is not written in C (but e.g. generated with Matlab/Simulink), the system integrator has to ensure that the generated object or C-code is correct by performing appropriate tests for fulfilling the respective safety performance.			

Category:	Requirement	Label:	Register_Mofication	ID:	1195043
Related To:			Related To':		
The HY-TTC 500 I/O driver C library provides API functions to control and configure the CPU and its peripherals. In order to avoid malfunction caused by the interference between driver software and application software, the system integrator **shall** not modify any CPU registers.					

Category:	Comment	ID:	609551
If the system integrator is required to access certain CPU registers, a detailed analysis has to be performed to clarify the impact on functionality and safety capability of the driver software.			

Category:	Requirement	Label:	BSP_Modification	ID:	609553
Related To:			Related To':		
The HY-TTC 500 board support package - bsp library delivered as part of the safety platform - **shall** be used by the system integrator without any modifications.					

Category:	Comment	ID:	609555
The bsp includes the start-up code for the Main CPU that needs to be linked to the application and the linker command files (containing addresses and size of RAM, Flash and stack area). The start-up code will call the applications main function.			

Category:	Comment	ID:	609549
For ultimately entering the safe state (i.e. in case the application software detects a fatal error, e.g. a redundancy mismatch), the HY-TTC 500 I/O driver library provides the function *DIAG_EnterSafestate()* that allows an application driven safe state. Whenever a requirement demands the application software to enter the safe state, this function has to be utilized for the corresponding state transition.			

5.1 Initialization

Category:	Requirement	Label:	Driver_Init	ID:	609559
Related To:	460039		Related To':		
The application software **shall** call the general initialization function *IO_Driver_Init()* before calling any other driver function.					

Category:	Requirement	Label:	IO_Init	ID:	609561
Related To:	626915		Related To':		
At start-up, the application software **shall** initialize the I/Os by calling the initialization functions of the used I/O drivers prior to using the so-called I/O driver '*step functions*' (i.e. the periodically called driver functions).					

Category:	Requirement	Label:	IO_Config	ID:	609563
Related To:	626913		Related To':		
The application software **shall** provide the appropriate safety parameters for all safety-critical I/Os when calling their I/O driver initialization function.					

Category:	Requirement	Label:	IO_Glitchfilter	ID:	609565
Related To:	625511		Related To':		
The application software **shall** specify the glitch-filter time that should be applied to the inputs and outputs of the device when calling the general driver initialization function *IO_Driver_Init()*.					

Category:	Requirement	Label:	IO_Cycle	ID:	609567
Related To:	625511		Related To':		
The application software **shall** specify the cycle time that will be maintained by the application when calling the general driver initialization function *IO_Driver_Init()*.					

Category:	Requirement	Label:	Init_Cycle_Window	ID:	717009
Related To:	625511		Related To':		
The application software **shall** specify the window for the application cycle time that should be tolerated when calling the general driver initialization function *IO_Driver_Init()*.					

Category:	Requirement	Label:	ECU_Resets	ID:	609569
Related To:	625511		Related To':		
The application software **shall** specify the maximum number of ECU resets that will be performed in case of safety-critical errors, when calling the general driver initialization function *IO_Driver_Init()*.					

Category:	Requirement	Label:	Init_Failure	ID:	609571
Related To:	626917		Related To':		
If an error occurs during I/O initialization (i.e. at least one of the initialization functions does return a value other than *IO_E_OK*), the application software **shall** activate the safe state.					

Category:	Requirement	Label:	DiagState_Application	ID:	608561
Related To:	626925		Related To':		
The application software **shall** start its control algorithms (i.e. evaluation of analog/digital inputs, control of PWM and digital outputs), only after the Main CPU has entered the diagnostic state *DIAG_STATE_MAIN*.					

5.2 Generic

Category:	Requirement	Label:	Flash_Execution	ID:	718497
Related To:	282118		Related To':		
The system integrator **shall** ensure to execute safety-critical applications only from the internal flash of the Main CPU.					

Category:	Requirement	Label:	IO-Driver_CPU_RAM	ID:	608567
Related To:			Related To':		
The system integrator **shall** ensure to link all safety-critical data, including the I/O driver data, to the internal RAM of the Main CPU.					

Category:	Comment	ID:	719664
Only the Main CPUs internal Flash and RAM memories provide with the Single Error Correction Double Error Detection (SECDED) mechanism the necessary means for safety-critical applications. The external Flash and RAM memories do not provide the necessary means for safety-critical applications.			

Category:	Comment	ID:	723745
The Main CPU of the HY-TTC 500 platform features a Floating Point Unit (FPU), which is capable to generate exceptions in case of: • division by zero • overflow • underflow • input denormal • invalid operation			

Category:	Requirement	Label:	FPU_Exception	ID:	717649
Related To:	567739		Related To':		

The application software **shall** configure the FPU exception handler which, if demanded by the system's characteristics, **shall** activate the safe state in case of an exception.

Category:	Requirement	Label:	Zero_Division	ID:	919526
Related To:	918156		Related To':		

The application software **shall** configure the behavior for integer divisions by zero. By default no exception is generated and the result of an integer division by zero is always zero.

Category:	Requirement	Label:	Interrupt_Time	ID:	718511
Related To:			Related To':		

The application periodic interrupt handler function **shall** not introduce any significant delay, i.e. the periodic interrupt handler function must only contain basic statements. An acceptable upper limit for the execution of the callback function is *200 us*. This assures that the device's operation is not influenced by the implementation of the callback function.

Category:	Requirement	Label:	IO_Interrupt	ID:	718456
Related To:			Related To':		

The application software **shall** not perform any I/O handling in the periodic interrupt handler function.

Category:	Requirement	Label:	Task_Interrupt	ID:	609581
Related To:			Related To':		

The application software **shall** not call the driver's task begin *IO_Driver_TaskBegin()* and task end functions *IO_Driver_TaskEnd()* from inside a periodic interrupt handler. Library functions being called from an interrupt handler might cause unexpected problems and the HY-TTC 500 platform may be unable to detect systematic software failures (e.g. infinite loops) in case an interrupt is used to service the window-watchdog.

5.3 Runtime

Category:	Requirement	Label:	Main_Return	ID:	717643
Related To:	712341		Related To':		

The application's main function **shall** never return.

Category:	Requirement	Label:	Driver_Cycle	ID:	609577
Related To:	295131		Related To':		

The software cycle **shall** be executed periodically with a cycle time that does not exceed/underrun the parameters (i.e. *io_driver_safety_conf.command_period* +/-

*(io_driver_safety_conf.command_period*io_driver_safety_conf.*window_size)) that have been passed to the general initialization function *IO_Driver_Init()*.

Category:	Requirement	Label:	RTC_Modification	ID:	609579
Related To:	314453		Related To':		

As the I/O driver depends on accurate timing, the application software **shall** not modify the RTC registers.

Category:	Requirement	Label:	Driver_TaskBegin	ID:	609573
Related To:	295119		Related To':		

The driver's task begin function *IO_Driver_TaskBegin()* **shall** be called by the application at the beginning of each software cycle.

Category:	Requirement	Label:	Driver_TaskEnd	ID:	609575
Related To:	295127		Related To':		

The driver's task end function *IO_Driver_TaskEnd()* **shall** be called by the application at the end of each software cycle.

Category:	Requirement	Label:	Driver_Step	ID:	717021
Related To:	625419		Related To':		

The I/O step functions (set and get functions) **shall** be called periodically for all configured inputs and outputs in each software cycle.

5.4 Failure Diagnostics

Category:	Comment	ID:	592663

Those consistency checks for safety-critical system components that will be implemented by the application software have to be executed with a periodicity that correlates with the overall system's process safety time. The worst case failure reaction time has to be calculated with respect to the overall application parameters, similar to the algorithm in section *Failure Reaction Time*.

The effective reaction time is based on the following parameters:

- The maximum cycle time (*t_cycle*) that is defined during the I/O driver initialization call
- The interval between the execution of the consistency check (*n_rounds_check*) in software cycles
- The external watchdog window time (*t_wd*) that is defined to be 64 ms.

The calculation of the effective worst case failure reaction time is as follows:
*wc_frt = max(t_cycle * (n_rounds_check + 1), t_wd)*

Compliance with the system's failure reaction time has been assumed during the HY-TTC 500 platform's FMEDA. Consequently, the effective diagnostic coverage for the relevant system components is only valid, if the application software's consistency checks are executed with an adequate frequency.

Category:	Comment	ID:	717254

The following example outlines the procedure for calculating the worst case failure reaction time for a user application that utilizes redundant timer inputs with an assumed cycle time (*t_cycle*) of 10 ms and a consistency check for the redundant inputs that is executed every fourth application cycle (*n_rounds_check*).

The resulting worst case failure reaction time is:
*wc_frt = max(10 ms * (4 + 1), 64 ms) = 64 ms*

That means, the assumed diagnostic coverage for the timer input's safety mechanism (*redundancy*) is only valid for safety functions with a process safety time of 64 ms or higher. For those safety functions that require a shorter failure reaction time, the system integrator needs to either adapt the above-mentioned parameters or provide separate diagnostic measures within the application software.

Category:	Comment	ID:	719152

The Main CPUs internal Flash, configuration flash and RAM memories are protected by Single Error Correction Double Error Detection (SECDED).

- Single bit errors are automatically corrected
- Double bit errors are detected

However, the system may require the application to check for stricter limits and limit the number of correctable single bit errors.

Category:	Requirement	Label:	Monitor_Memory	ID:	719577
Related To:			Related To':		

If demanded by the system's characteristics, the application software **shall** monitor the count of corrected single bit errors of the Main CPUs internal memories according to the required limits and activate the safe state in case the limits are violated.

Category:	Comment	ID:	586829

The I/O driver interfaces to monitor the correctable error count for each memory type are:

- Flash: DIAG_GetFlashErrors()
- Configuration Flash: DIAG_GetCfgFlashErrors()
- RAM: DIAG_GetRamB0Errors() and DIAG_GetRamB1Errors()

Category:	Requirement	Label:	Modify_SECDED	ID:	586801
Related To:			Related To':		

The system integrator **shall** not disable or modify any configuration item of the mechanisms related to the SECDED of the Main CPU.

Category:	Comment	ID:	586791

The ECC values of the flash locations which will be intentionally read by the Main CPU need to be programmed into the flash memory. They will be generated and programmed while flashing the application with the TTC-Downloader.

Category:	Requirement	Label:	Stack_Check	ID:	718462
Related To:			Related To':		

The safety measures of the HY-TTC 500 platform do not check for stack overflows. The system integrator **shall** apply appropriate measures to check the stack, by means of e.g.:

- Periodic check for a preset pattern at the end of the stack
- Usage of the Memory Protection Unit (MPU) to prevent write access with a barrier at the end of the stack

Category:	Requirement	Label:	Systematic_Errors	ID:	717262
Related To:	320031,695693,695695		Related To':		

The safety measures of the HY-TTC 500 platform cannot detect systematic application errors (e.g. wrong calculation algorithms or bit-modification in RAM variables). The system integrator **shall** apply appropriate measures to the application development process for handling such errors, by means of e.g.:

- Systematic development process according to the requirements of the respective performance level
- Plausibility checks for allowing the detection of bit-modifications in critical memory areas
- Usage of the Memory Protection Unit (MPU) to prevent bit-modifications in critical memory areas

Category:	Requirement	Label:	IO_Deglitching	ID:	717264
Related To:	320033		Related To':		

The application **shall** adequately debounce glitches originating from EMI or other disturbances for all safety-critical I/Os. The HY-TTC 500 platform will only filter glitches for the platform's internal diagnostic measures to prevent inadvertent activation of the safe state, but will not filter the sensor values for the application.

Category:	Requirement	Label:	Data_Protection	ID:	717266
Related To:	631193,686246		Related To':		

The application **shall** provide the appropriate protection for safety-critical data that is stored to the ECU's non-volatile memory (e.g. CRC protection or redundant data storage).

Category:	Requirement	Label:	Config_Data_Protection	ID:	717494
Related To:	697105		Related To':		

The application **shall** provide the appropriate protection for safety-critical configuration data that is located in the ECU's "application configuration data" memory region (e.g. CRC protection or redundant data storage).

Category:	Comment	ID:	717256
The HY-TTC 500 platform automatically performs board temperature monitoring during runtime with regards to the limits specified in the HY-TTC 500 System Manual [TTC500-SysM] and activates the safe state in case of range violations. This range check is not configurable, however, it can be extended by an additional check within the application software.			

Category:	Requirement	Label:	Temperature_Monitoring	ID:	717268
Related To:			Related To':		
If the system's characteristics demand more stringent temperature limits than those defined in the HY-TTC 500 System Manual [TTC500-SysM], the application software **shall** implement a temperature check according to the required limits and activate the safe state in case of range violations.					

Category:	Comment	ID:	717334
The HY-TTC 500 platform performs battery voltage monitoring with regards to the limits specified in the HY-TTC 500 System Manual [TTC500-SysM]. However, the system may require the application to check for stricter limits.			

Category:	Requirement	Label:	Battery_Monitoring	ID:	717346
Related To:	648254		Related To':		
If demanded by the system's characteristics, the application software **shall** monitor the battery supply according to the required limits and activate the safe state in case the limits are violated.					

5.5 Safe State

5.5.1 Application Callbacks

Category:	Comment	ID:	723615
The HY-TTC 500 I/O driver provides 2 application callbacks, which can be configured when calling the general driver initialization function *IO_Driver_Init()*. The callbacks are executed depending on the error type before the safe state is entered: • Error callback - executed for *non-fatal* errors • Notification callback - executed for *fatal* errors			

Category:	Comment	ID:	723687
Within the error callback function, the application software can decide which action shall be taken (e.g. disable a PWM shut-off group).			

Category:	Comment	ID:	723689

Within the notification callback function, the application software could notify other controllers (e.g. in a CAN network), that a fatal error occurred and, if configured, a reset of the ECU will take place.

Category:	Requirement	Label:	Error_Callback_Action	ID:	723747
Related To:			Related To':		

If demanded by the system's design, the application software **shall** define an error callback function, returning an action for each failure of the safety-critical I/O's being part of a safety function.

Category:	Requirement	Label:	Error_Callback_LS	ID:	969456
Related To:			Related To':		

An error callback for a high side digital output or a PWM high side stage **shall** be treated with the same severity as an error on the corresponding low side safety switch.

Category:	Requirement	Label:	Error_Callback_Timing	ID:	590305
Related To:	626937		Related To':		

The application software's error callback function **shall** not introduce any significant delay when deciding the action to take, i.e. the error callback function must only contain basic statements for deciding which action to take. An acceptable upper limit for the execution of the callback function is *1 ms*. This assures that the device's failure reaction time is not increased by the implementation of the callback function.

Category:	Comment	ID:	590311

The notification callback has no such limitation as the safe state is activated before this callback is called. It is still recommended to keep the notification callback function short because most interrupts (depending on the error) are disabled during its execution.

Category:	Requirement	Label:	IO_Callback	ID:	609585
Related To:			Related To':		

The application software **shall** not perform any I/O handling in the error callback or notification callback function with exception of the following functions:

- *IO_RTC_GetDateAndTimeStatus*
- *IO_RTC_GetDateAndTime*
- *IO_EEPROM_GetStatus*
- *IO_EEPROM_Read*
- *IO_EEPROM_Write*

Category:	Requirement	Label:	Error_Diagnostics	ID:	609587
Related To:	626893		Related To':		

Upon activation of the safe state, the application software **shall** save the error code that has caused the safe state in a non-volatile failure memory, e.g. the EEPROM.

Category:	Requirement	Label:	Startup_Failure_Memory	ID:	717487
Related To:	626899		Related To':		

Upon start-up, the application software **shall** check the failure memory's last entries and instruct the Main CPU to enter the safe state, if the last entries show fatal errors that might prevent a safe system operation, e.g. a failing Main CPU, watchdog or voltage monitor.

Category:	Requirement	Label:	Startup_Safety_Switch	ID:	808049
Related To:	706225		Related To':		

If the application software's error callback is executed due to a failing safety switch startup test (i.e. error code *DIAG_E_SSW_TEST*), the application software **shall** define an action to be taken according to the overall system design.

Category:	Comment	ID:	808085

In case of a failing safety switch startup test that cannot be traced back to an isolated failure of an associated PWM high side stage, the complete safety switch group might be impaired. The system integrator is therefore advised to immediately disable the affected safety switch and all connected PWM high side stages.

A defective safety switch—acting as secondary shut-off path of a safety-related PWM high side stage—is considered dangerous and does therefore not allow further operation of the affected PWM high side stages.

Category:	Requirement	Label:	Runtime_Safety_Switch	ID:	808047
Related To:	541719		Related To':		

If the application software's error callback is executed due to a failing safety switch test during runtime (i.e. error code *DIAG_E_SSW_PERIODIC*), the application software **shall** define an action to be taken according to the overall system design.

Category:	Comment	ID:	808549

In case of a failing safety switch runtime test, the ECU might sustain permanent damage due to internal over-heating. The system integrator is therefore advised to immediately disable the affected safety switch and all connected PWM high side stages.

5.6 C-driver Examples

Category:	Comment	ID:	592665
The correct integration of the HY-TTC 500 I/O drivers into the application software is crucial for maintaining an overall program flow that ensures safe operation of all inputs and outputs. In order to assist the application software programmer in adhering to the intended application structure, the source code of an exemplary safety application can be found in the HY-TTC 500 System Manual [TTC500-SysM].			

6 Development Environment

6.1 Compiler & Linker

Category:	Requirement	Label:		ID:	3407524
Related To:			Related To':		
The following Compiler and Linker **shall** be used for the application interface: *ARM C/C++ Code Generation Tools* Version: *V5.1.6 or newer (see below)* Vendor: *Texas Instruments*					

Category:	Comment	ID:	3407534
Be aware, that TTControl has only validated Compiler version V5.1.6 specifically by running test applications compiled with this version. For this reason if a Compiler version newer than V5.1.6 is necessary it is the solely responsibility of the system integrator to consider the following requirements.			

Category:	Comment	ID:	5732724
TTControl has analysed the known bugs of the TMS470 Code Generation Tools V5.1.6 for the development of the I/O driver, however it is strongly recommended, that the system integrator performs an analysis checking the known existing bugs for the used compiler, since some which did not have an impact for the I/O driver implementation might have an impact on the implementation of the application.			

Category:	Requirement	Label:		ID:	3407526
Related To:			Related To':		
If a newer Compiler version than V5.1.6 is used, it **shall** be a version with long-term support (LTS) by Texas Instruments.					

Category:	Requirement	Label:		ID:	3407528
Related To:			Related To':		
If a newer Compiler version than V5.1.6. is used, the API/ABI compatibility **shall** be verified.					

Category:	Requirement	Label:		ID:	3407530
Related To:			Related To':		
If a newer Compiler version than V5.1.6 is used, the system integrator **shall** perform additional, potentially required validation steps.					

Category:	Requirement	Label:	Compiler_Options	ID:	717023
Related To:	710322,710307,710356		Related To':		
The following Compiler and Linker options **shall** be used for the application interface:					

- Compiler options:
  ```
  -mv7R4
  --abi=eabi
  --auto_inline=0
  --endian=big
  --float_support=VFPv3D16
  --small_enum
  --fp_mode=strict
  --opt_for_speed=3
  --code_state=32
  --no_inlining
  --gen_func_subsections
  --check_misra=none
  --issue_remarks
  --display_error_number
  --aliased_variables
  --no_stm
  --unaligned_access=off
  ```

- Linker options:
  ```
  --reread_libs
  --rom_model
  --warn_sections
  --be32
  --mapfile_contents=all
  --issue_remarks
  --display_error_number
  --disable_auto_rts
  --fill_value=0
  --minimize_trampolines
  ```

Category:	Requirement	Label:	RTS_Library	ID:	717032
Related To:	710299		Related To':		

The following runtime support library **shall** be used for linking the application image:
rtsv7R4_T_be_v3D16_eabi.lib

Category:	Requirement	Label:		ID:	4119016
Related To:			Related To':		

The system integrator **shall** allocate a minimum of 512 bytes for the stack of the Abort CPU mode (i.e _StackABORT_END_ <= _StackABORT_ - 512).

Category:	Requirement	Label:		ID:	4119020
Related To:			Related To':		

The system integrator **shall** allocate a minimum of 512 bytes for the stack of the Undefined CPU mode (i.e _StackUND_END_<= _StackUND_- 512).

Category:	Comment	ID:	4119019
The minimum stack size for the Abort and Undefined CPU mode are necessary to ensure correct operation of the respective exception handlers in the Bootloader. Further, processing of the exceptions is done in the I/O Driver BSP, which may require larger stack sizes depending on the application handling of the exception (notification callback).			

Category:	Requirement	Label:		ID:	4119017
Related To:		Related To':			
The system integrator **shall** set the sections *CSM_CODE, CSM_CONST,IO_DRIVER_CODE* and *IO_DRIVER_CONST* inside the internal Flash.					

Category:	Requirement	Label:		ID:	4119021
Related To:		Related To':			
The system integrator **shall** set the sections *CSM_VAR_ZERO_INIT_UNSPECIFIED* and *CSM_VAR_NO_INIT_UNSPECIFIED* inside the internal RAM.					

Category:	Requirement	Label:		ID:	4119015
Related To:		Related To':			
The system integrator **shall** set the section *IO_DRIVER_DATA_NORMAL* into the internal RAM.					

Category:	Requirement	Label:		ID:	4119018
Related To:		Related To':			
The system integrator **shall** reserve the address range starting at 0x0803FEE0 with the size of 288 bytes for the Shared Memory.					

Category:	Requirement	Label:		ID:	4119014
Related To:		Related To':			
The system integrator **shall** set the section IO_DRIVER_DATA_COMMON starting at the address 0x0803FAE0 and reserve 1 KB for it.					

Category:	Requirement	Label:		ID:	5707591
Related To:		Related To':			
The system integrator **shall** ensure that the size of the *bool* data type is 1 Byte.					

6.2 Application Download

Category:	Requirement	Label:	Application_Flashing	ID:	1200803
Related To:			Related To':		
The system integrator **shall** transfer the application software to the HY-TTC 500 platform's internal flash memory by means of TTControl's TTC-Downloader or by integrating TTControl's TTC-Downloader-DLL.					

Category:	Comment	ID:	592667
The system-specific application software may be loaded by the system integrator into the Main CPU's internal flash with a programming tool that communicates with the ECU's bootloader and allows to download application via CAN, Ethernet or BroadR-Reach, i.e. TTControl's TTC-Downloader. For detailed instructions regarding the download process please refer to the corresponding TTC-Downloader Release Notes Document [TTCD-RN]. Alternatively, the application download to the internal flash memory can be performed by utilizing the dedicated TTC-Downloader-DLL that allows the system integrator to implement their own programming tool, using the specific TTC-Downloader-DLL API.			

7 Information for Use

Category:	Comment	ID:	592445

The following section will outline the location of information that is important for safe use of the HY-TTC 500 platform according to ISO 13489-1, section 11 [ISO 13849].

Category:	Comment	ID:	592451

- The HY-TTC 500 is compliant to ISO 13849-1:2015 and ISO 13849-2:2012 [ISO 13849] PL d and fulfills the requirements of a category 2 system. It is also compliant to IEC 61508 [IEC 61508] SIL 2 and ISO 25119 AgPL d/SRL 2.
- The proof test interval and the process safety time are specified in section *Failure Reaction Time*.
- Since the HY-TTC 500 is not designed for maintenance, there are no specific maintenance requirements. Disposal notes can be found in the HY-TTC 500 System Manual [TTC500-SysM].
- The platform's safety concept can be found in section *Safety Concept Overview*.
- The interfaces are described in the HY-TTC 500 System Manual [TTC500-SysM], section *Connector and Pins*.
- The device's general operating limits are listed in the HY-TTC 500 System Manual [TTC500-SysM], section *Features of HY-TTC 500*. The I/O-specific limits can be found in the corresponding subsection (i.e. section *Maximum ratings*) of each I/O chapter.
- Examples of applications for use are referenced in sections *C-driver Examples.* General requirements for safe operation based on the HY-TTC 500 platform are stated throughout this document in the according subsections. Specific considerations on utilization of sensors according to the requirements of category 2 can be found in section *Sensor Selection Guideline*.
- Information for trouble-shooting can be found in the HY-TTC 500 System Manual [TTC500-SysM], part III.
- The assumed safety function of the HY-TTC 500 platform is specified in section *Safety Function*. After I/O driver initialization in a safety-critical manner, the safety function of the HY-TTC 500 platform cannot be disabled.
- The detailed quantitative analysis results according to IEC 61508 [IEC 61508] SIL 2, ISO 25119 [ISO 25119] AgPl d/SRL 2 and ISO 13849 [ISO 13849] PL d together with the assumed environmental conditions can be found in section *Probabilistic Failure Rate*.

8 Guideline on Hardware Metrics Determination

Category:	Comment	ID:	894081

The HY-TTC 500 platform provides measures against random hardware failures that allow the realization of safety functions with Safety Integrity Levels up to SIL 2, Performance Levels up to PL d and Agriculture Performance Level AgPL d. Typically, these safety mechanisms are scaleable according to the actual demands of the system integrator's applications. The following section will provide a guideline on how to utilize these diverse safety mechanisms, together with their presumed diagnostic coverage based on the content of IEC 61508, ISO 13849 and ISO 25119.

Category:	Comment	ID:	3404454

All stated metrics are valid starting from **product version 01.08** (for metrics of the previous product version 01.05 see Safety Manual V1.8.1).

8.1 MTTFd Values of Functional Blocks

Category:	Comment	ID:	919710

Based on the specific failure modes of the HY-TTC 500 platform's hardware parts, a detailed FMEDA has been conducted. The following section lists the obtained MTTFd values for every functional block according to the two exemplary mission profiles (see section *Mission Profiles*). These values are also available as a dedicated library for usage within the SISTEMA software utility.

The listed MTTFd values are directly related to the main connector's pins, regardless of their configured functions. That means, the dangerous failure rate does not change, if—for example—a dedicated output pin is configured to be used as an analog input, or a dedicated analog input is configured to be used as a digital input.

8.1.1 Hardware Metrics HY-TTC 508

Category:	Comment	ID:	3276670

The following table covers all those functional blocks for which the HY-TTC 508 ECU offers diagnostic measures to detect dangerous hardware failures.
The corresponding diagnostic coverage for each component highly depends on the implemented diagnostic measures and needs to be estimated by the system integrator. A guideline on this selection can be found in section *Failure Diagnostics*.

Functional Block		**Mission Profile** *Conventional*		**Mission Profile** *Stop & Go*	
	SW-define	**MTTF$_d$ per I/O**	**λd per I/O**	**MTTF$_d$ per I/O**	**λd per I/O**
Core HY-TTC 508		206 years	555 FIT	199 years	573 FIT

5V Sensor Supply	IO_SENSOR_SUPPLY_0	2379 years	48 FIT	2237 years	51 FIT
Analog Input 3 Mode	IO_ADC_00-IO_ADC_07	5747 years	20 FIT	6394 years	18 FIT
Analog Input 2 Mode 10V	IO_ADC_08-IO_ADC_15	5793 years	20 FIT	6430 years	18 FIT
Analog Input 2 Mode 32V	IO_ADC_16-IO_ADC_23	5626 years	20 FIT	6224 years	18 FIT
Timer Input 0-5	IO_PWD_00-IO_PWD_05	6837 years	17 FIT	7217 years	16 FIT
High Side PWM Output	IO_PWM_00-IO_PWM_05, IO_PWM_14-IO_PWM_17	5255 years	22 FIT	5195 years	22 FIT
High Side PWM Current Measurement		8433 years	14 FIT	8454 years	14 FIT
High Side Digital Output	IO_DO_00-IO_DO_07	7005 years	16 FIT	6660 years	17 FIT
Low Side Digital Output	IO_DO_08-IO_DO_15	4663 years	24 FIT	4247 years	27 FIT
Transient Core Failures		42 years	2705 FIT	42 years	2705 FIT

Table 9

Note 1: The item *Core* contains the HY-TTC 500 platform's integral logic components (e.g. internal power supply or Main CPU) and is vital to the ECU's general function. Therefore, its failure rate has to be added to every individual safety function, regardless of the utilized set of functional blocks.
Note 2: The item *Transient Core Failures* includes the Main CPU's soft errors. These failures are typically only applicable to metrics calculations based on IEC 61508.

Category:	Comment	ID:	3276672

The following table covers all those functional blocks for which the HY-TTC 508 ECU does not provide any diagnostic measures. However, the system integrator may implement measures against dangerous failures on system level. To that end, every block's overall failure rate is assumed to be evenly distributed between safe and dangerous failures according to the general approach in ISO 13849, i.e. MTTFd = 2 * MTTF.
The diagnostic measures and the determination of their diagnostic coverage is in the responsibility of the system integrator. Therefore, no detailed guideline can be given here.

Functional Block		**Mission Profile *Conventional***		**Mission Profile *Stop & Go***	
	SW-define	**MTTF$_d$ per I/O**	**λd per I/O**	**MTTF$_d$ per I/O**	**λd per I/O**
Ext. Flash		2361 years	48 FIT	2025 years	56 FIT
Ext. RAM		3163 years	36 FIT	2416 years	47 FIT
Ext. EEPROM		7698 years	15 FIT	7427 years	15 FIT
High Side Digital / PVG / VOUT Output	IO_PVG_00-IO_PVG_05	3219 years	35 FIT	3372 years	34 FIT
Timer Input 6-11	IO_PWD_06-IO_PWD_11	15100 years	8 FIT	15574 years	7 FIT
Timer Input 12-19*	IO_PWD_12-IO_PWD_19	5255 years	22 FIT	5195 years	22 FIT
BroadR-Reach Interface		1062 years	108 FIT	1081 years	106 FIT
CAN Interface 0-2	IO_CAN_CHANNEL_0- IO_CAN_CHANNEL_2	8394 years	14 FIT	9481 years	12 FIT
CAN Termination		49849 years	2 FIT	56794 years	2 FIT
Real Time Clock		1512 years	75 FIT	1602 years	71 FIT

Table 10

* ... for the respective coverage capabilities see section *PWM High Side Stages*

8.1.2 Hardware Metrics HY-TTC 510

Category:	Comment	ID:	1534877

The following table covers all those functional blocks for which the HY-TTC 510 ECU offers diagnostic measures to detect dangerous hardware failures.

The corresponding diagnostic coverage for each component highly depends on the implemented diagnostic measures and needs to be estimated by the system integrator. A guideline on this selection can be found in section *Failure Diagnostics*.

Functional Block		**Mission Profile** ***Conventional***		**Mission Profile** ***Stop & Go***	
	SW-define	**MTTF_d per I/O**	**λd per I/O**	**MTTF_d per I/O**	**λd per I/O**
Core HY-TTC 510		214 years	533 FIT	209 years	547 FIT
5V Sensor Supply	IO_SENSOR_SUPPLY_0-IO_SENSOR_SUPPLY_1	2379 years	48 FIT	2237 years	51 FIT
Analog Input 3 Mode	IO_ADC_00-IO_ADC_07	5747 years	20 FIT	6394 years	18 FIT
Analog Input 2 Mode 10V	IO_ADC_08-IO_ADC_15	5793 years	20 FIT	6430 years	18 FIT
Analog Input 2 Mode 32V	IO_ADC_16-IO_ADC_23	5626 years	20 FIT	6224 years	18 FIT
Timer Input 0-5	IO_PWD_00-IO_PWD_05	6837 years	17 FIT	7217 years	16 FIT
High Side PWM Output	IO_PWM_00-IO_PWM_07, IO_PWM_14-IO_PWM_21	5255 years	22 FIT	5195 years	22 FIT
High Side PWM Current Measurement		8433 years	14 FIT	8454 years	14 FIT
High Side Digital Output	IO_DO_00-IO_DO_07	7005 years	16 FIT	6660 years	17 FIT
Low Side Digital Output	IO_DO_08-IO_DO_15	4663 years	24 FIT	4247 years	27 FIT
Transient Core Failures		42 years	2705 FIT	42 years	2705 FIT

Table 11

Note 1: The item *Core* contains the HY-TTC 500 platform's integral logic components (e.g. internal power supply or Main CPU) and is vital to the ECU's general function. Therefore, its failure rate has to be added to every individual safety function, regardless of the utilized set of functional blocks.

Note 2: The item *Transient Core Failures* includes the Main CPU's soft errors. These failures are typically only applicable to metrics calculations based on IEC 61508.

Category:	Comment	ID:	1534879

The following table covers all those functional blocks for which the HY-TTC 510 ECU does not provide any diagnostic measures. However, the system integrator may implement measures against dangerous failures on system level. To that end, every block's overall failure rate is assumed to be evenly distributed between safe and dangerous failures a ccording to the general approach in ISO 13849, i.e. MTTFd = 2 * MTTF.

The diagnostic measures and the determination of their diagnostic coverage is in the responsibility of the system integrator. Therefore, no detailed guideline can be given here.

Functional Block	**Mission Profile**	**Mission Profile**

		Conventional		***Stop & Go***	
	SW-define	**MTTF_d per I/O**	**λd per I/O**	**MTTF_d per I/O**	**λd per I/O**
Ext. RAM		3163 years	36 FIT	2416 years	47 FIT
Ext. EEPROM		7698 years	15 FIT	7427 years	15 FIT
Variable Sensor Supply	IO_SENSOR_SUPPLY_2	1587 years	72 FIT	1554 years	73 FIT
High Side Digital / PVG / VOUT Output	IO_PVG_00-IO_PVG_07	3219 years	35 FIT	3372 years	34 FIT
Timer Input 6-11	IO_PWD_06-IO_PWD_11	15100 years	8 FIT	15574 years	7 FIT
Timer Input 12-19*	IO_PWD_12-IO_PWD_19	5255 years	22 FIT	5195 years	22 FIT
LIN Interface	IO_LIN	3074 years	37 FIT	3174 years	36 FIT
CAN Interface 0-2	IO_CAN_CHANNEL_0-IO_CAN_CHANNEL_2	8394 years	14 FIT	9481 years	12 FIT
CAN Termination		49849 years	2 FIT	56794 years	2 FIT

Table 12

* ... for the respective coverage capabilities see section *PWM High Side Stages*

8.1.3 Hardware Metrics HY-TTC 520

Category:	Comment	ID:	1534873

The following table covers all those functional blocks for which the HY-TTC 520 ECU offers diagnostic measures to detect dangerous hardware failures.
The corresponding diagnostic coverage for each component highly depends on the implemented diagnostic measures and needs to be estimated by the system integrator. A guideline on this selection can be found in section *Failure Diagnostics*.

Functional Block		**Mission Profile *Conventional***		**Mission Profile *Stop & Go***	
	SW-define	**MTTF_d per I/O**	**λd per I/O**	**MTTF_d per I/O**	**λd per I/O**
Core HY-TTC 520		214 years	533 FIT	209 years	547 FIT
5V Sensor Supply	IO_SENSOR_SUPPLY_0-IO_SENSOR_SUPPLY_1	2379 years	48 FIT	2237 years	51 FIT
Analog Input 3 Mode	IO_ADC_00-IO_ADC_07	5747 years	20 FIT	6394 years	18 FIT
Analog Input 2 Mode 10V	IO_ADC_08-IO_ADC_15	5793 years	20 FIT	6430 years	18 FIT
Analog Input 2 Mode 32V	IO_ADC_16-IO_ADC_23	5626 years	20 FIT	6224 years	18 FIT
Timer Input 0-5	IO_PWD_00-IO_PWD_05	6837 years	17 FIT	7217 years	16 FIT
High Side PWM Output	IO_PWM_00-IO_PWM_09, IO_PWM_14-IO_PWM_21	5255 years	22 FIT	5195 years	22 FIT
High Side PWM Current Measurement		8433 years	14 FIT	8454 years	14 FIT
High Side Digital Output	IO_DO_00-IO_DO_07	7005 years	16 FIT	6660 years	17 FIT
Low Side Digital Output	IO_DO_08-IO_DO_15	4663 years	24 FIT	4247 years	27 FIT
Transient Core Failures		42 years	2705 FIT	42 years	2705 FIT

Table 13

Note 1: The item *Core* contains the HY-TTC 500 platform's integral logic components (e.g. internal power supply or Main CPU) and is vital to the ECU's general function. Therefore, its failure rate has to be added to every individual safety function, regardless of the utilized set of functional blocks.
Note 2: The item *Transient Core Failures* includes the Main CPU's soft errors. These failures are typically only applicable to metrics calculations based on IEC 61508.

Category:	Comment	ID:	1534875

The following table covers all those functional blocks for which the HY-TTC 520 ECU does not provide any diagnostic measures. However, the system integrator may implement measures against dangerous failures on system level. To that end, every block's overall failure rate is assumed to be evenly distributed between safe and dangerous failures according to the general approach in ISO 13849, i.e. MTTFd = 2 * MTTF.
The diagnostic measures and the determination of their diagnostic coverage is in the responsibility of the system integrator. Therefore, no detailed guideline can be given here.

Functional Block		Mission Profile *Conventional*		Mission Profile *Stop & Go*	
	SW-define	**MTTF$_d$ per I/O**	**λd per I/O**	**MTTF$_d$ per I/O**	**λd per I/O**
Ext. RAM		3163 years	36 FIT	2416 years	47 FIT
Ext. EEPROM		7698 years	15 FIT	7427 years	15 FIT
Variable Sensor Supply	IO_SENSOR_SUPPLY_2	1587 years	72 FIT	1554 years	73 FIT
Timer Input 6-11	IO_PWD_06-IO_PWD_11	15100 years	8 FIT	15574 years	7 FIT
Timer Input 12-19*	IO_PWD_12-IO_PWD_19	5255 years	22 FIT	5195 years	22 FIT
CAN Interface 0-2	IO_CAN_CHANNEL_0-IO_CAN_CHANNEL_2	8394 years	14 FIT	9481 years	12 FIT
CAN Interface 3	IO_CAN_CHANNEL_3	2594 years	44 FIT	2512 years	45 FIT
CAN Termination		49849 years	2 FIT	56794 years	2 FIT

Table 14

* ... for the respective coverage capabilities see section *PWM High Side Stages*

8.1.4 Hardware Metrics HY-TTC 540

Category:	Comment	ID:	1534869

The following table covers all those functional blocks for which the HY-TTC 540 platform offers diagnostic measures to detect dangerous hardware failures.
The corresponding diagnostic coverage for each component highly depends on the implemented diagnostic measures and needs to be estimated by the system integrator. A guideline on this selection can be found in section *Failure Diagnostics*.

Functional Block		Mission Profile *Conventional*		Mission Profile *Stop & Go*	
	SW-define	**MTTF$_d$ per I/O**	**λd per I/O**	**MTTF$_d$ per I/O**	**λd per I/O**
Core HY-TTC 540		214 years	533 FIT	209 years	547 FIT

5V Sensor Supply	IO_SENSOR_SUPPLY_0-IO_SENSOR_SUPPLY_1	2379 years	48 FIT	2237 years	51 FIT
Analog Input 3 Mode	IO_ADC_00-IO_ADC_07	5747 years	20 FIT	6394 years	18 FIT
Analog Input 2 Mode 10V	IO_ADC_08-IO_ADC_15	5793 years	20 FIT	6430 years	18 FIT
Analog Input 2 Mode 32V	IO_ADC_16-IO_ADC_23	5626 years	20 FIT	6224 years	18 FIT
Timer Input 0-5	IO_PWD_00-IO_PWD_05	6837 years	17 FIT	7217 years	16 FIT
High Side PWM Output	IO_PWM_00-IO_PWM_27	5255 years	22 FIT	5195 years	22 FIT
High Side PWM Current Measurement		8433 years	14 FIT	8454 years	14 FIT
High Side Digital Output	IO_DO_00-IO_DO_07	7005 years	16 FIT	6660 years	17 FIT
Low Side Digital Output	IO_DO_08-IO_DO_15	4663 years	24 FIT	4247 years	27 FIT
Transient Core Failures		42 years	2705 FIT	42 years	2705 FIT

Table 15

Note 1: The item *Core* contains the HY-TTC 500 platform's integral logic components (e.g. internal power supply or Main CPU) and is vital to the ECU's general function. Therefore, its failure rate has to be added to every individual safety function, regardless of the utilized set of functional blocks.
Note 2: The item *Transient Core Failures* includes the Main CPU's soft errors. These failures are typically only applicable to metrics calculations based on IEC 61508.

Category:	Comment	ID:	1534871

The following table covers all those functional blocks for which the HY-TTC 540 platform does not provide any diagnostic measures. However, the system integrator may implement measures against dangerous failures on system level. To that end, every block's overall failure rate is assumed to be evenly distributed between safe and dangerous failures according to the general approach in ISO 13849, i.e. MTTFd = 2 * MTTF.
The diagnostic measures and the determination of their diagnostic coverage is in the responsibility of the system integrator. Therefore, no detailed guideline can be given here.

Functional Block		**Mission Profile *Conventional***		**Mission Profile *Stop & Go***	
	SW-define	**MTTF$_d$ per I/O**	**λd per I/O**	**MTTF$_d$ per I/O**	**λd per I/O**
Ext. RAM		3163 years	36 FIT	2416 years	47 FIT
Ext. EEPROM		7698 years	15 FIT	7427 years	15 FIT
Variable Sensor Supply	IO_SENSOR_SUPPLY_2	1587 years	72 FIT	1554 years	73 FIT
Timer Input 6-11	IO_PWD_06-IO_PWD_11	15100 years	8 FIT	15574 years	7 FIT
Timer Input 12-19*	IO_PWD_12-IO_PWD_19	5255 years	22 FIT	5195 years	22 FIT
Analog Input **	IO_ADC_52-IO_ADC_59	3219 years	35 FIT	3372 years	34 FIT
CAN Interface 0-2	IO_CAN_CHANNEL_0-IO_CAN_CHANNEL_2	8394 years	14 FIT	9481 years	12 FIT
CAN Interface 3	IO_CAN_CHANNEL_3	2594 years	44 FIT	2512 years	45 FIT
CAN Termination		49849 years	2 FIT	56794 years	2 FIT

Table 16

* ... for the respective coverage capabilities see section *PWM High Side Stages*
** ... for the respective coverage capabilities see section *High Side Digital/PVG/VOUT Output*

8.1.5 Hardware Metrics HY-TTC 580

Category:	Comment	ID:	1534713

The following table covers all those functional blocks for which the HY-TTC 580 platform offers diagnostic measures to detect dangerous hardware failures.
The corresponding diagnostic coverage for each component highly depends on the implemented diagnostic measures and needs to be estimated by the system integrator. A guideline on this selection can be found in section *Failure Diagnostics*.

Functional Block		**Mission Profile** *Conventional*		**Mission Profile** *Stop & Go*	
	SW-define	**MTTF$_d$ per I/O**	**λd per I/O**	**MTTF$_d$ per I/O**	**λd per I/O**
Core HY-TTC 580		201 years	567 FIT	195 years	584 FIT
5V Sensor Supply	IO_SENSOR_SUPPLY_0-IO_SENSOR_SUPPLY_1	2379 years	48 FIT	2237 years	51 FIT
Analog Input 3 Mode	IO_ADC_00-IO_ADC_07	5747 years	20 FIT	6394 years	18 FIT
Analog Input 2 Mode 10V	IO_ADC_08-IO_ADC_15	5793 years	20 FIT	6430 years	18 FIT
Analog Input 2 Mode 32V	IO_ADC_16-IO_ADC_23	5626 years	20 FIT	6224 years	18 FIT
Timer Input 0-5	IO_PWD_00-IO_PWD_05	6837 years	17 FIT	7217 years	16 FIT
High Side PWM Output	IO_PWM_00-IO_PWM_35	5255 years	22 FIT	5195 years	22 FIT
High Side PWM Current Measurement		8433 years	14 FIT	8454 years	14 FIT
High Side Digital Output	IO_DO_00-IO_DO_07	7005 years	16 FIT	6660 years	17 FIT
Low Side Digital Output	IO_DO_08-IO_DO_15	4663 years	24 FIT	4247 years	27 FIT
Transient Core Failures		42 years	2705 FIT	42 years	2705 FIT

Table 17

Note 1: The item *Core* contains the HY-TTC 500 platform's integral logic components (e.g. internal power supply or Main CPU) and is vital to the ECU's general function. Therefore, its failure rate has to be added to every individual safety function, regardless of the utilized set of functional blocks.
Note 2: The item *Transient Core Failures* includes the Main CPU's soft errors. These failures are typically only applicable to metrics calculations based on IEC 61508.

Category:	Comment	ID:	1534715

The following table covers all those functional blocks for which the HY-TTC 580 platform does not provide any diagnostic measures. However, the system integrator may implement measures against dangerous failures on system level. To that end, every block's overall failure rate is assumed to be evenly distributed between safe and dangerous failures according to the general approach in ISO 13849, i.e. MTTFd = 2 * MTTF.
The diagnostic measures and the determination of their diagnostic coverage is in the responsibility of the system integrator. Therefore, no detailed guideline can be given here.

Functional Block	**Mission Profile** *Conventional*	**Mission Profile** *Stop & Go*

	SW-define	**MTTF_d per I/O**	**λd per I/O**	**MTTF_d per I/O**	**λd per I/O**
Ext. Flash		2361 years	48 FIT	2025 years	56 FIT
Ext. RAM		3163 years	36 FIT	2416 years	47 FIT
Ext. EEPROM		7698 years	15 FIT	7427 years	15 FIT
Variable Sensor Supply	IO_SENSOR_SUPPLY_2	1587 years	72 FIT	1554 years	73 FIT
High Side Digital / PVG / VOUT Output	IO_PVG_00-IO_PVG_07	3219 years	35 FIT	3372 years	34 FIT
Timer Input 6-11	IO_PWD_06-IO_PWD_11	15100 years	8 FIT	15574 years	7 FIT
LIN Interface	IO_LIN	3074 years	37 FIT	3372 years	34 FIT
RS232 Interface	IO_UART	2270 years	50 FIT	2496 years	46 FIT
CAN Interface 0-2	IO_CAN_CHANNEL_0-IO_CAN_CHANNEL_2	8394 years	14 FIT	9481 years	12 FIT
CAN Interface 3-6	IO_CAN_CHANNEL_3-IO_CAN_CHANNEL_6	2594 years	44 FIT	2512 years	45 FIT
CAN Termination		49849 years	2 FIT	56794 years	2 FIT
Real Time Clock		1512 years	75 FIT	1602 years	71 FIT

Table 18

8.1.6 Hardware Metrics HY-TTC 590/HY-TTC 590E

Category:	Comment	ID:	3276664

The following table covers all those functional blocks for which the HY-TTC 590/590E platform offers diagnostic measures to detect dangerous hardware failures.

The corresponding diagnostic coverage for each component highly depends on the implemented diagnostic measures and needs to be estimated by the system integrator. A guideline on this selection can be found in section *Failure Diagnostics*.

Functional Block		**Mission Profile *Conventional***		**Mission Profile *Stop & Go***	
	SW-define	**MTTF_d per I/O**	**λd per I/O**	**MTTF_d per I/O**	**λd per I/O**
Core HY-TTC 590/590E		199 years	573 FIT	194 years	589 FIT
5V Sensor Supply	IO_SENSOR_SUPPLY_0-IO_SENSOR_SUPPLY_1	2379 years	48 FIT	2237 years	51 FIT
Analog Input 3 Mode	IO_ADC_00-IO_ADC_07	5747 years	20 FIT	6394 years	18 FIT
Analog Input 2 Mode 10V	IO_ADC_08-IO_ADC_15	5793 years	20 FIT	6430 years	18 FIT
Analog Input 2 Mode 32V	IO_ADC_16-IO_ADC_23	5626 years	20 FIT	6224 years	18 FIT
Timer Input 0-5	IO_PWD_00-IO_PWD_05	6837 years	17 FIT	7217 years	16 FIT
High Side PWM Output	IO_PWM_00-IO_PWM_35	5255 years	22 FIT	5195 years	22 FIT
High Side PWM Current Measurement		8433 years	14 FIT	8454 years	14 FIT
High Side Digital Output	IO_DO_00-IO_DO_07	7005 years	16 FIT	6660 years	17 FIT
Low Side Digital Output	IO_DO_08-IO_DO_15	4663 years	24 FIT	4247 years	27 FIT
Transient Core Failures		42 years	2705 FIT	42 years	2705 FIT

Table 19

Note 1: The item *Core* contains the HY-TTC 500 platform's integral logic components (e.g. internal power supply or Main CPU) and is vital to the ECU's general function. Therefore, its failure rate has to be added to every individual safety function, regardless of the utilized set of functional blocks.
Note 2: The item *Transient Core Failures* includes the Main CPU's soft errors. These failures are typically only applicable to metrics calculations based on IEC 61508.

Category:	Comment	ID:	3276666

The following table covers all those functional blocks for which the HY-TTC 590/590E platform does not provide any diagnostic measures. However, the system integrator may implement measures against dangerous failures on system level. To that end, every block's overall failure rate is assumed to be evenly distributed between safe and dangerous failures according to the general approach in ISO 13849, i.e. MTTFd = 2 * MTTF.
The diagnostic measures and the determination of their diagnostic coverage is in the responsibility of the system integrator. Therefore, no detailed guideline can be given here.

Functional Block		**Mission Profile *Conventional***		**Mission Profile *Stop & Go***	
	SW-define	**MTTF_d per I/O**	**λd per I/O**	**MTTF_d per I/O**	**λd per I/O**
Ext. Flash		2361 years	48 FIT	2025 years	56 FIT
Ext. RAM		3163 years	36 FIT	2416 years	47 FIT
Ext. FRAM		7698 years	15 FIT	7427 years	15 FIT
Variable Sensor Supply	IO_SENSOR_SUPPLY_2	1587 years	72 FIT	1554 years	73 FIT
High Side Digital / PVG / VOUT Output	IO_PVG_00-IO_PVG_07	3219 years	35 FIT	3372 years	34 FIT
Timer Input 6-11	IO_PWD_06-IO_PWD_11	15100 years	8 FIT	15574 years	7 FIT
LIN Interface	IO_LIN	3074 years	37 FIT	3174 years	36 FIT
RS232 Interface	IO_UART	2270 years	50 FIT	2496 years	46 FIT
CAN Interface 0-2	IO_CAN_CHANNEL_0-IO_CAN_CHANNEL_2	8394 years	14 FIT	9481 years	12 FIT
CAN Interface 3-6	IO_CAN_CHANNEL_3-IO_CAN_CHANNEL_6	2594 years	44 FIT	2512 years	45 FIT
CAN Termination		49849 years	2 FIT	56794 years	2 FIT
Real Time Clock		1512 years	75 FIT	1602 years	71 FIT

Table 20

8.2 Failure Diagnostics

Category:	Comment	ID:	920153

In order to detect dangerous hardware failures within the HY-TTC 500 platform, certain diagnostic measures are in place. Some of these measures will be permanently enabled regardless of the application software, while others depend on the system integrator's implementation on system level. The following section will give a guideline on choosing an appropriate set of measures according to the desired value of diagnostic coverage for each individual functional block.

In general, these measures are intended to detect hardware failures inside the HY-TTC 500 platform. Depending on the used components (i.e. switches, sensors or actuators), the measures might, however, also contribute to the detection of external failures.

The selection of appropriate diagnostic measures requires the system integrator to regard the input elements' individual characteristics (i.e. possible signal ranges, failure modes, architectural parameters). Therefore, the following list of diagnostic measures is only considered a general guideline without claiming complete validity. It is the responsibility of the system integrator to perform a hazard and risk analysis for the overall system, to select suitable measures against dangerous failures of individual components and to identify the actual diagnostic coverage that can be claimed for a specific diagnostic measure.

Note: If the overall system architecture permits the usage of functional structures without diagnostic coverage (e.g. for a system with a category B architecture according to ISO 13849) the implementation of these failure diagnostics might not be required. It may be sufficient to rely on the function blocks' MTTFd values, as outlined in section *MTTFd Values of Functional Blocks*. Either way, TTControl suggests to implement an appropriate set of failure diagnostics, regardless of the system's architectural demands, in order to achieve the best possible safety performance.

8.2.1 Combined Safety Mechanisms

Category:	Comment	ID:	958838

When combining safety mechanisms that supplement each other in terms of their diagnostic capabilities, the overall diagnostic coverage is assumed to be higher than the value of every single mechanisms. The above-listed table makes use of that principle and therefore suggests, to some extent, slightly higher DC values for combined safety mechanisms.

8.2.2 Core

Category:	Comment	ID:	894365

If the application software passes a safety configuration to the general driver initialization function, the core's diagnostic functions are implicitly executed during runtime and cannot be disabled by the application software. Therefore, the diagnostic coverage to be used for the core is an average value based on several diagnostic measures. Detected failures within the HY-TTC 500 platform's core will directly lead to the safe state and trigger the according notification callback.

Also, if the system requires any kind of diagnostic coverage for one or more input or output stages (i.e. a category 2 subsystem), the general driver initialization function *IO_Driver_Init()* has to be called with a safety configuration. Only then, the HY-TTC 500 platform can be considered to reliably transfer the system to a safe state in case of detected failures.

Measures	Variant	DC	Remarks	References
Various measures	HY-TTC 508	91.10 % (Mission Profile *Conventional*)	Requires safety-critical initialization	-

		92.19 % (Mission Profile *Stop & Go*)	via application software	
	HY-TTC 510/520/540	90.88 % (Mission Profile *Conventional*) 91.98 % (Mission Profile *Stop & Go*)	Requires safety-critical initialization via application software	-
	HY-TTC 580	91.27 % (Mission Profile *Conventional*) 92.32 % (Mission Profile *Stop & Go*)	Requires safety-critical initialization via application software	-
	HY-TTC 590/590E	91.34 % (Mission Profile *Conventional*) 92.38 % (Mission Profile *Stop & Go*)	Requires safety-critical initialization via application software	-

Table 21

8.2.3 5 V Sensor Supplies

Category:	Comment	ID:	920236

The 5 V sensor supplies' correct functioning is implicitly checked by the HY-TTC 500 platform's I/O driver, if at least one safety-critical analog input is allocated to the corresponding sensor supply. To that end, the analog feedback signal is permanently checked for its voltage level and the I/O driver triggers an error callback in case of deviations.
If there is no safety-critical analog input assigned to a specific 5 V sensor supply, but the overall system design requires diagnostic measures for the supply output, the application software can still read and evaluate the measured voltage level by calling the appropriate task function *IO_ADC_Get()* with the corresponding sensor supply parameter.

Due to the sensor supply's nature of providing a steady, defined output voltage, the analog feedback measurement is considered a reliable safety mechanism with a high diagnostic coverage. Consequently, the assumed diagnostic coverage for the 5 V sensor suppy is **99%**.

Functional Mode	I/O-Driver	Appl.	Measures	DC	References
Sensor Supply	-	-	-	0 %	-
	-	✓	Supply Voltage monitoring	99 %	IEC 61508-7 A.13.1 - *Monitoring* ISO 13849-1 Table E.1 - *Direct Monitoring* ISO 26262-5 Table D.7 *Voltage / current control (input)* ISO 25119-2 Table C.7 *Voltage source control*
	✓	-	Supply Voltage monitoring	99 %	IEC 61508-7 A.13.1 - *Monitoring* ISO 13849-1 Table E.1 - *Direct Monitoring* ISO 26262-5 Table D.7 *Voltage / current control (input)* ISO 25119-2 Table C.7 *Voltage source control*

Table 22

8.2.4 Analog 3 Mode Inputs

Category:	Comment	ID:	920909

The analog 3 mode inputs can be utilized in fundamentally different applications, ranging from reading simple binary switches to current sensing elements, ratiometric output voltages or resistive sensor types. While the voltage and current measurement modes allow claiming a high diagnostic coverage even in single channel configuration, the resistance measurement might require additional measures to achieve certain DC levels.

Functional Mode	I/O-Driver	Appl.	Measures	No. of Pins	DC*	References
Voltage Input / Current Input	-	-	-	1	0 %	-
	-	✓	Signal range check	1	60 %	ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	✓	-	Signal range check	1	60 %	ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	-	✓	Redundancy	2**	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
	-	✓	Signal range check & redundancy	2**	99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
	✓	-	Internal comparison of redundant measurement paths	1	99 %***	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 -

						Plausibility check ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
	✓	✓	Signal range check & internal comparison of redundant measurement paths	1	99 %***	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
	✓	✓	Signal range check, internal comparison of redundant measurement paths & sensor redundancy	2**	99-99.9 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
Resistive Input	-	-	-	1	0 %	-
	-	✓	Signal range check	1	60 %	ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	-	✓	Redundancy	2	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
	-	✓	Signal range check & redundancy	2	99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
Digital Input	-	-	-	1	0 %	-

	-	✓	Redundancy	2**	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*

Table 23

* HW block, interface and electrical part of the external device
** Secondary pin can be from a different pin type
*** The external device's DC value might be lower (e.g. 60 %), unless specified by the manufacturer otherwise

Note 1: The MTTFd values (as specified in the dedicated table in section *MTTFd Values of Functional Blocks*) are equally valid for all above-mentioned functional modes.
Note 2: For those functional modes that require two input channels, the MTTFd value does only reflect the failure rate of a single channel.

Voltage Input / Current Input:
When using the voltage & current measurement modes, the analog 3 mode inputs' internal structure provides the HY-TTC 500 platform with the ability to internally diagnose hardware faults with a high diagnostic coverage. The I/O driver's diagnostic modules will trigger an error callback in case of a detected failure.

Resistive Input:
Due to restrictions in the resistance measurement mode, the reference channel cannot be used to directly monitor the correct function of the analog input stage. Therefore, no implicitly executed safety mechanisms can be claimed by the system integrator for defining the input stages' diagnostic coverage values. Consequently, additional measures have to be implemented in the application software, if the overall safety function requires diagnostic coverage for the analog input stages.

Digital Input:
In the digital input configuration, certain failure modes of the analog input stages might not be detectable by the HY-TTC 500 I/O driver's diagnostic modules. Hence, a redundant usage of independent input stages is recommended for safety functions that require a certain diagnostic coverage.

Regardless of the measurement mode, the connected input elements (e.g. switches or sensors) might require the implementation of certain safety mechanisms, as well, to assure failure detection within those elements. Such mechanisms have to be selected according to the possible failure modes and the targeted failure rates.

8.2.4.1 Redundancy

Category:	Comment	ID:	920872

The redundant usage of two analog inputs allows for continuous cross monitoring of the corresponding input signal. Plausibility checks within the application software permit the system integrator to detect a single fault in one of the input paths and transfer the overall system to a safe state. When defining the time interval of such checks, the system integrator needs to consider the overall system's failure reaction time. For details on calculating the worst case failure reaction times of such consistency checks, see section *Failure Diagnostics*.

Redundancy can also be claimed when combining two different input types (e.g. an analog input 3 mode with an analog input 2 mode for current measurement, or an analog 2 mode with a timer input for measuring digital signals), as long as the inputs' specifications both match the desired input signal).

This safety mechanism's diagnostic coverage is considered to lie between a value of **90-99 %**, depending on the characteristics of the input elements (e.g. their possible failure modes) and the plausibility check's strictness.

8.2.4.2 Signal Range Check

Category:	Comment	ID:	544467

In order to check for short circuits to ground or battery voltage as well as open loads of dedicated inputs, a signal range check (SRC) can be utilized. That means a predefined margin on the upper and lower end of the measurable range is excluded from the sensor's valid output values. If for the signal range check a range of 5…95 % is configured to be valid for a sensor, all values below 5 % or above 95 % are considered erroneous by the I/O driver.

In case the application software passes a safety configuration (i.e. defined signal ranges together with a redundant input channel) to the voltage/current input's initialization function, the measured values will be checked internally by the I/O driver for their upper and lower limits periodically during runtime and the I/O driver's diagnostic modules will trigger an error callback upon detection of a signal range violation. In case of single-channel configuration of 3 mode analog inputs or utilization as resistive inputs, the application software has to implement such a diagnostic measure. This measure can, of course, only be applied to input stages with sensors that allow to define lower and upper limit values that still lie within the measurable ranges.

Since this safety mechanism is able to detect only basic failure modes both internal and external to the HY-TTC 500 platform, the according diagnostic coverage is considered to be low, i.e. **60 %**.

8.2.4.3 Internal Comparison of Redundant Measurement Paths

Category:	Comment	ID:	959698

The analog 3 mode inputs' internal structure allows to continuously monitor the correct operation of the analog input stages. This procedure relies on an independent reference channel that allows permanent plausibility checks of the measurement channel when in voltage or current measurement modes. Failures will be detected by the I/O driver's diagnostic modules and trigger an according error callback.

This safety measure is considered to provide a high diagnostic coverage (i.e. **99 %**) for the internal input structure. The diagnostic capabilities for failures within the sensor device, however, might vary between different sensor devices and depend on their detailed internal diagnostics and the sensor's architectural category.

8.2.5 Analog 2 Mode Inputs

Category:	Comment	ID:	920350

The analog 2 mode inputs enable ratiometric and absolute voltage measurements, as well as reading current sensors. According to the utilized input elements, different diagnostic measures might be suitable. Similar to the resistance measurement mode of the analog 3 mode inputs, the analog 2 mode inputs do not feature internal reference channels to claim diagnostic coverage values without additional measures.

Functional Mode	I/O-Driver	Appl.	Measures	No. of Pins	DC*	References
Voltage Input / Current Input	-	-	-	1	0 %	-
	-	✓	Signal range check	1	60 %	ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	-	✓	Redundancy	2**	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
	-	✓	Single range check & redundancy	2**	99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
	✓	✓	Signal range check & redundancy	2**	99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
Digital Input	-	-	-	1	0 %	-

	-	✓	Redundancy	2**	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*

Table 24

* HW block, interface & electrical part of the external device
** Secondary pin can be from a different pin type

Note 1: The MTTFd values (as specified in the dedicated table in section *MTTFd Values of Functional Blocks*) are equally valid for all above-mentioned functional modes
Note 2: For those functional modes that require two input channels, the MTTFd value does only reflect the failure rate of a single channel.
Note 3: For details about the implementation of these safety measures see the according chapters in section *Analog Input 3 Modes*.

Voltage Input / Current Input:
Due to the analog 2 mode inputs' internal structure, internal diagnostics cannot realiably detect dangerous failures on their own. Even though a basic signal range check will be performed by the HY-TTC 500 I/O driver's diagnostic modules for redundantly configured analog inputs, additional measures might be required to achieve the overall safety function's diagnostic coverage for the analog input stages.

Digital Input:
In the digital input configuration, certain failure modes of the analog input stages might not be detectable by the HY-TTC 500 I/O driver's diagnostic modules. Hence, a redundant usage of independent input stages is recommended for safety functions that require a certain diagnostic coverage.

8.2.6 Timer Inputs (IO_PWD_00 ... IO_PWD_05)

Category:	Comment	ID:	591419

The HY-TTC 500 platform's timer inputs 00-05 (*IO_PWD_00 ... IO_PWD_05*) allow to directly measure the signals of dedicated frequency sensors with different output characteristics (e.g. PNP-type, NPN-type, current loop). Depending on the actual measurement mode, the execution of diverse safety measures might be feasible.

Functional Mode	I/O-Driver	Appl.	Measures	No. of Pins	DC*	References
Timer Input	-	-	-	1	0 %	-
	✓	-	Frequency range check	1	90-99 %	IEC 61508-7 - *Test pattern* ISO 13849-1 Table E.1 - *Cyclic test stimulus* ISO 26262-5 Table D.5 *Test pattern* ISO 25119-2

	-	✓	Frequency range check	1	90-99 %	IEC 61508-7 - *Test pattern* ISO 13849-1 Table E.1 - *Cyclic test stimulus* ISO 26262-5 Table D.5 *Test pattern*
	-	✓	Redundancy	2**	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* SO 25119-2 Table C.6 *Comparator*
Encoder Input	-	-	-	2	0 %	-
	✓	-	Signal range check	2	0-99 %***	ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
Analog Input	-	-	-	1	-	-
	-	✓	Signal range check	1	60 %	ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	-	✓	Redundancy	2**	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* SO 25119-2 Table C.6 *Comparator*
	-	✓	Signal range check & redundancy	2**	99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Input comparison / voting* SO 25119-2 Table C.6 *Comparator*
Digital Input	-	-	-	1	0 %	-
	-	✓	Redundancy	2**	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting*

	SO 25119-2 Table C.6 *Comparator*

Table 25

* HW input, interface and electrical part of the external device
** Secondary pin can be from a different pin type
*** Diagnostic coverage is highly dependent on the overall system architecture and the actual failure modes of the encoder element

Timer Input:
For the timer input mode, the I/O driver's diagnostic modules allow to internally check the input signal for a predefined frequency and pulse width range. Apart from that, the application software can implement appropriate measures on their own, as well.

Encoder Input:
The I/O driver's diagnostic modules allow defining a lower and upper threshold for the encoder's count value.

Analog Input:
Similarly, the analog input measurement is not equipped with automatically enabled safety mechanisms. Therefore, no safety mechanisms can be claimed by the system integrator and additional measures have to be enabled, if the overall safety function requires diagnostic coverage for the analog input function.

Digital Input:
In the digital input configuration, certain failure modes of the timer input stages might not be detectable by the HY-TTC 500 I/O driver's diagnostic modules. Hence, a redundant usage of independent input stages is recommended for safety functions that require a certain diagnostic coverage.

Regardless of the measurement mode, the connected input elements (e.g. switches or sensors) might require the implementation of certain safety mechanisms, as well, to assure failure detection within those elements. Such mechanisms have to be selected according to the possible failure modes and the targeted failure rates.

8.2.6.1 Redundancy

Category:	Comment	ID:	923491

The redundant usage of two timer inputs allows for continuous cross monitoring of the corresponding input signal. Plausibility checks within the application software permit the system integrator to detect a single fault in one of the input paths and transfer the overall system to a safe state. When defining the time interval of such checks, the system integrator needs to consider the overall system's failure reaction time. For details on calculating the worst case failure reaction times of such consistency checks, see section *Failure Diagnostics*.

Redundancy can also be claimed when combining two different input types (e.g. a timer input's analog measurement with an analog input 2 mode, or a timer input's digital measurement with an analog input 3 mode for measuring static digital values), as long as the inputs' specifications both match the desired input signal.

This safety mechanism's diagnostic coverage is considered to lie between a value of **90-99 %**, depending on the characteristics of the input elements (e.g. their possible failure modes) and the plausibility check's strictness.

8.2.6.2 Frequency Range Check

Category:	Comment	ID:	923493

In order to check for short circuits to ground or battery voltage as well as open loads of dedicated inputs, a frequency range check can be utilized. That means that predefined upper and lower limits for the measurement signals (in terms of frequency and pulse width) are defined. If for the signal range check a frequency range of 1 kHz…10 kHz is configured to be valid for a sensor, all values below 1 kHz or above 10 kHz are considered erroneous by the I/O driver.

For the timer input mode, the application software may pass a safety configuration (i.e. defined signal ranges) to the input's initialization function. The measured values will then be checked internally by the I/O drivers for their upper and lower limits periodically during runtime. This measure can, of course, only be applied to input stages with sensors that continuously generate output pulses even in their idle state. The internal signal range check can, however, not be used for the analog input mode of the timer inputs. It is, therefore, in the responsibility of the application software to implement such a range check for the analog input mode.

Since this safety mechanism is able to detect numerous failure modes both internal and external to the HY-TTC 500 platform, the according diagnostic coverage for the timer input mode is considered to be medium to high, i.e. **90-99 %**, depending on the range of invalid measurement values.

8.2.6.3 Signal Range Check

Category:	Comment	ID:	959614

In order to check for short circuits to ground or battery voltage as well as open loads of dedicated inputs, a signal range check (SRC) can be utilized. That means a predefined margin on the upper and lower end of the measurable range is excluded from the sensor's valid output values. If for the signal range check a range of 5…95 % is considered to be valid for a sensor, all values below 5 % or above 95 % can be considered erroneous.

The application software might check the measured values for their upper and lower limits periodically during runtime and is able to initiate the safe state upon detection of a signal range violation. This measure can, of course, only be applied to input stages with sensors that allow to define lower and upper limit values that still lie within the measurable ranges.

Since this safety mechanism is able to detect only basic failure modes both internal and external to the HY-TTC 500 platform, the according diagnostic coverage is considered to be low, i.e. **60 %**.

8.2.7 Timer Inputs (IO_PWD_06 ... IO_PWD_11)

Category:	Comment	ID:	959339

The HY-TTC 500 platform's timer inputs 06-11 (*IO_PWD_06 ... IO_PWD_11*) allow to directly measure the signals of dedicated frequency sensors with different output characteristics (e.g. PNP-type, NPN-type, current loop). However, due to their internal structure, these timer inputs **must not** be utilized safety-critically on their own in measurement modes timer input, encoder input or digital input.

Depending on the actual measurement mode, the execution of diverse safety measures might be feasible.

Functional Mode	I/O-Driver	Appl.	Measures	No. of Pins	DC*	References
Timer Input**	-	✓	Redundancy	2	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
Analog Input	-	-	-	1	0 %	-
	-	✓	Signal range check	1	60 %	ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	-	✓	Redundancy	2	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
	-	✓	Redundancy & signal range check	2	99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
Digital Input***	-	✓	Redundancy	2	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check*

						ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*

Table 26

* HW input, interface and electrical part of the external device
** Only usable in combination with a timer input from group *IO_PWD_00 ... IO_PWD_05*.
*** Only usable in combination with a digital input from groups *IO_ADC_00 ... IO_ADC_23, IO_PWD_00 ... IO_PWD_05, IO_DO_00 ... IO_DO_15 or IO_PVG_00 ... IO_PVG_07*.

Note: For details about the implementation of these safety measures see the according chapters in the above section *Timer Inputs (IO_PWD_00 ... IO_PWD_05*).

Timer Input:
Due to their internal structure, the timer inputs 6-11 (*IO_PWD_06 ... IO_PWD_11*) in measurement mode *timer input* **must not** be utilized safety-critically on their own or in combination with another timer input from this group. They may be used, however, as secondary channels in a redundant architecture in combination with timer inputs 0-5 (*IO_PWD_00 ... IO_PWD_05*).

Analog Input:
Similarly, the analog input measurement is not equipped with automatically enabled safety mechanisms. Therefore, no safety mechanisms can be claimed by the system integrator and additional measures have to be enabled, if the overall safety function requires diagnostic coverage for the analog input function.

Digital Input:
Due to their internal structure, the timer inputs 6-11 (*IO_PWD_06 ... IO_PWD_11*) in measurement mode *digital input* **must not** be utilized safety-critically on their own or in combination with another timer input from this group. They may be used, however, as secondary channels in a redundant architecture in combination with dedicated analog inputs, timer inputs 0-5, dedicated digital outputs or PVG outputs (*IO_ADC_00 ... IO_ADC_23, IO_PWD_00 ... IO_PWD_05, IO_DO_00 ... IO_DO_15 or IO_PVG_00 ... IO_PVG_07*).

8.2.8 PWM High Side Stages

Category:	Comment	ID:	921278

The PWM high side stages allow operation of both resistive and inductive loads in a safety-critical manner. Due to the PWM control, they feature a continuous monitoring mechanism in the granularity of the PWM frequency. With internal safety switches being able to override a faulty power stage output, an independent secondary shut-off path is present to transfer the system to a safe state, in case of dangerous failures.

Functional Mode	I/O-Driver	Appl.	Measures	No. of Pins	DC*	References
HS PWM Output	-	-	-	1	0 %	-
	✓	-	Periodic PWM feedback & status	1	98.53 % (MP_C)	IEC 61508-7 A.2.2 - *Dynamic principles*

			monitoring & shut-off path test		98.44 % (MP_S)	ISO 13849-1 Table E.1 - *Cross monitoring of output signals and intermediate results* ISO 26262-5 Table D.5 *Monitored outputs* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	✓	✓	Periodic PWM feedback & status monitoring & shut-off path test	1 or 2**	98.53 % (MP_C) 98.44 % (MP_S)	IEC 61508-7 A.2.2 - *Dynamic principles* ISO 13849-1 Table E.1 - *Cross monitoring of output signals and intermediate results* ISO 26262-5 Table D.5 *Monitored outputs* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	-	✓	Periodic PWM feedback & status monitoring & shut-off path test	1 or 2**	98.53 % (MP_C) 98.44 % (MP_S)	IEC 61508-7 A.2.2 - *Dynamic principles* ISO 13849-1 Table E.1 - *Cross monitoring of output signals and intermediate results* ISO 26262-5 Table D.5 *Monitored outputs* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	-	✓	Monitoring of static failure modes (open load, short circuit) & shut-off path test	1 or 2**	60 % or higher, depending on safety function	IEC 61508-2 A.1 - *Final elements / Stuck-at*
HS PWM Current Measurement* **	-	-	-	-****	0 %	-
	✓	-	Current measurement signal range check	-****	65.05 % (MP_C) 64.68 % (MP_S)	ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	-	✓	Current measurement plausibility check	-****	90-99 %	IEC 61508-2 Table A.14 - *Monitoring* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	✓	✓	Current measurement signal range check & plausibility check	-****	90-99 %	IEC 61508-2 Table A.14 - *Monitoring* ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*

HS Digital Output	-	-	-	1	0 %	-
	-	✓	Status monitoring & shut-off path test	1 or 2**	90 %	IEC 61508-7 A.1.1 - *Failure detection by online monitoring* ISO 13849-1 Table E.1 - *Redundant shut-off path with monitoring of one of the actuators* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
Digital Input*****	-	✓	Redundancy	2	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 Input comparison / voting ISO 25119-2 Table C.6 *F Comparator*

Table 27

* HW block, interface and electrical part of the external device (MP_C = Mission Profile *Conventional* / MP_S = Mission Profile *Stop & Go*)
** Secondary shut-off path can be, e.g. internal safety switch, an independent output stage or a hydraulic shut-off valve.
*** The metrics of the *HS PWM Current Measurement* mode need to be added to the metrics of the *HS PWM Output* mode in case the current measurement is considered safety-critical in the overall system.
**** The *HS PWM Current Measurement* mode does not require an additional connector pin as it will base its measurement on the according HS PWM output pin.
***** Only usable in combination with a digital input from groups *IO_ADC_00 ... IO_ADC_23, IO_PWD_00 ... IO_PWD_05, IO_DO_00 ... IO_DO_15 or IO_PVG_00 ... IO_PVG_07*.

HS PWM Output:
The I/O driver's diagnostic module continuously compares the desired output duty cycle and frequency with the feedback measurements, thus allowing to reliably detect failures within the PWM output stages. This measure is active for every PWM high side output that is initialized as safety-critical and will trigger an error callback in case of dangerous failures.
Due to their superior diagnostic capabilities, the system integrator is advised to use the PWM output mode rather than the digital output mode for safety-critical applications, even if the corresponding actuators are only operated statically. This can be achieved by implementing a pseude-digital mode, that only changes between minimum and maximum output duty cycles.

HS PWM Current Measurement:
In case the PWM output stages current measurement is also defined as safety-critical, the I/O driver's diagnostic module provides an implicitly executed range check that is able to detect basic failures within the current measurement path of the output stage. When detecting such failures, the I/O driver's diagnostic module will trigger an error callback. If the system integrator requires higher DC values, the implementation of additional measures (e.g. plausibility checks of the measured current values) within the application software is required.

HS Digital Output:
If explicitly configured as digital outputs, the PWM high side stages will be operated statically and will not make use of any PWM signals. The state of such digital outputs will not be automatically monitored by the I/O driver's diagnostic modules. An according plausibility check of the digital feedback value needs to be implemented by the system integrator.

Digital Input:
Due to their internal structure, the PWM ouput stages in measurement mode digital input **must not** be utilized safety-critically on their own or in combination with another input from this group. They may be used, however, as secondary channels in a redundant architecture in combination with dedicated analog inputs, timer inputs 0-5, dedicated digital outputs or PVG outputs (*IO_ADC_00 ... IO_ADC_23, IO_PWD_00 ... IO_PWD_05, IO_DO_00 ... IO_DO_15 or IO_PVG_00 ... IO_PVG_07*).

8.2.8.1 Plausibility Check

Category:	Comment	ID:	923888

The integrity of the measured PWM output current can be checked by performing dedicated plausibility checks with independent measurement signals. That could be, for example, the direct comparison to an independent current sensor or the evaluation of the controlled actuators' physical state (with position or speed sensors). Another practical plausibility check for the safety-critical current measurement would be to check the actual current measurement value against an expected current, based on the PWM output's duty cycle and the actuator's resistive characteristics.

Depending on the plausibility check's strictness, diagnostic coverage values between **90 %** and **99 %** are considered feasible.

8.2.8.2 Status Monitoring

Category:	Comment	ID:	923591

The digital state of the PWM high side outputs can be read via the static feedback signals. That way, the application software is able to verify the correct function of the digital high side outputs and activate the safe state in case of dangerous failures. The additional internal safety switches constitute a secondary shut-off path that can de-energize the actuators independently from the PWM power stages.

This safety mechanism allows to detect a substantial amount of possible hardware failures and is therefore considered to yield a DC value of **90 %**.

8.2.8.3 Shut-off Path Test

Category:	Comment	ID:	1194918

In order to check the proper operation of the secondary shut-off path, its ability to transfer the system into a safe state needs to be tested in certain intervals, e.g. at the beginning of each driving cycle or during pre-defined maintenance activities. That way, the system can be considered to offer a valid category 2 architecture, according to ISO 13849.

8.2.8.4 Redundancy

Category:	Comment	ID:	921253

The redundant usage of independent digital inputs allows for continuous cross monitoring of the corresponding input signal. Plausibility checks within the application software permit the system integrator to detect a single fault in one of the input paths and transfer the overall system to a safe state. When defining the time interval of such checks, the system integrator needs to consider the overall system's failure reaction time. For details on calculating the worst case failure reaction times of such consistency checks, see section *Failure Diagnostics*.

Redundancy can also be claimed when combining two different input types (e.g. a PWM stage's digital input measurement with an timer input, or a PWM stage's digital input measurement with the digital sampling of an analog input 3 mode), as long as the inputs' specifications both match the desired input signal.

This safety mechanism's diagnostic coverage is considered to lie between a value of **90-99 %**, depending on the characteristics of the input elements (e.g. their possible failure modes) and the plausibility check's strictness.

8.2.9 Digital High Side Stages

Category:	Comment	ID:	894367

The digital high side stages allow operation of both resistive and inductive loads in a safety-critical manner. They feature internal feedback mechanisms that allow continuous monitoring of the effective output voltage. In case of dangerous failures, the assigned low side outputs act as secondary shut-off paths that provide the ability for transfering the system into a safe state.

Functional Mode	I/O-Driver	Appl.	Measures	No. of Pins	DC*	References
HS Digital Output	-	-	-	1	0 %	IEC 61508-7 A.1.1 - *Failure detection by online monitoring* ISO 13849-1 Table E.1 - *Redundant shut-off path with monitoring of one of the actuators*

						ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	✓	-	Voltage monitoring & shut-off path test	2**	90 %	IEC 61508-7 A.1.1 - *Failure detection by online monitoring* ISO 13849-1 Table E.1 - *Redundant shut-off path with monitoring of one of the actuators* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	-	✓	Voltage monitoring & shut-off path test	1 or 2***	90 %	IEC 61508-7 A.1.1 - *Failure detection by online monitoring* ISO 13849-1 Table E.1 - *Redundant shut-off path with monitoring of one of the actuators* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
Analog Input	-	-	-	1	0 %	-
	-	✓	Signal range check	1	60 %	ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	-	✓	Redundancy	2	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
	-	✓	Redundancy & signal range check	2	99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
Digital Input	-	-	-	1	0 %	-

	-	✓	Redundancy	2	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*

Table 28

* HW block, interface and electrical part of the external device
** Secondary shut-off path, i.e. a dedicated digital low side output, needs to be configured during pin initialization.
*** Secondary shut-off path can be, e.g. an independent output stage or a hydraulic shut-off valve.

HS Digital Output:
The I/O driver's diagnostic module continuously compares the desired output status with the feedback measurements, thus allowing to detect failures within the digital high side output stages. This measure is active for every pair of digital high side output and digital low side output that is initialized as safety-critical and will trigger an error callback in case of dangerous failures.
If the digital high side output is not configured safety-critical—and thus, is not used in combination with a digital low side output—no safety measures are executed by the I/O driver's diagnostic modules.

Analog Input:
The digital high side stages' analog input measurement is not equipped with automatically enabled safety mechanisms. Therefore, no safety mechanisms can be claimed by the system integrator and additional measures have to be enabled, if the overall safety function requires diagnostic coverage for the analog input function.

Digital Input:
In the digital input configuration, certain failure modes of the digital high side stages (including an unintentional activation of power stages) might not be detectable by the HY-TTC 500 I/O driver's diagnostic modules. Hence, a redundant usage of independent input stages is recommended for safety functions that require a certain diagnostic coverage.

8.2.9.1 Voltage Monitoring

Category:	Comment	ID:	924316

The current state of the digital high side outputs can be read via the static voltage feedback signals. That way, the application software is able to verify the correct function of the digital high side outputs and activate the safe state in case of dangerous failures. If the independent digital low side outputs are not used as secondary shut-off paths, the system integrator is responsible to provide other means that allow bringing the overall system to a safe state, e.g. by a separate emergency valve that disrupts the hydraulic oil flow and stops any dangerous movements.

This safety mechanism allows to detect a substantial amount of possible hardware failures and—with a proper secondary shut-off path in place—is therefore considered to yield a DC value of **90 %**.

8.2.9.2 Shut-off Path Test

Category:	Comment	ID:	964457

In order to check the proper operation of the secondary shut-off path, its ability to transfer the system into a safe state needs to be tested in certain intervals, e.g. at the beginning of each driving cycle or during pre-defined maintenance activities. That way, the system can be considered to offer a valid category 2 architecture, according to ISO 13849.

8.2.9.3 Redundancy

Category:	Comment	ID:	894468

The redundant usage of independent inputs allows for continuous cross monitoring of the corresponding input signal. Plausibility checks within the application software permit the system integrator to detect a single fault in one of the input paths and transfer the overall system to a safe state. When defining the time interval of such checks, the system integrator needs to consider the overall system's failure reaction time. For details on calculating the worst case failure reaction times of such consistency checks, see section *Failure Diagnostics*.

Redundancy can also be claimed when combining two different input types (e.g. a digital output stage's analog input measurement with an analog input 3 mode, or a digital output stage's digital input measurement with a timer input), as long as the inputs' specifications both match the desired input signal.

This safety mechanism's diagnostic coverage is considered to lie between a value of **90-99 %**, depending on the characteristics of the input elements (e.g. their possible failure modes) and the plausibility check's strictness.

8.2.9.4 Signal Range Check

Category:	Comment	ID:	923589

In order to check for short circuits to ground or battery voltage as well as open loads of dedicated inputs, a signal range check (SRC) can be utilized. That means a predefined margin on the upper and lower end of the measurable range is excluded from the sensor's valid output values. If for the signal range check a range of 5…95 % is considered to be valid for a sensor, all values below 5 % or above 95 % should be considered erroneous by the application software.

Unlike the analog 2 mode and 3 mode inputs, the digital high side outputs do not offer an internal signal range check that is executed by the I/O driver's diagnostic modules. It is, therefore, in the responsibility of the application software to implement such a range check.

Since this safety mechanism is able to detect only basic failure modes both internal and external to the HY-TTC 500 platform, the according diagnostic coverage is considered to be low, i.e. **60 %**.

8.2.10 Digital Low Side Stages

Category:	Comment	ID:	894369

The digital low side stages allow operation of both resistive and inductive loads in a safety-critical manner. They feature internal feedback mechanisms that allow continuous monitoring of the effective output voltage. In case of dangerous failures, the assigned low side outputs act as secondary shut-off paths that provide the ability for transfering the system into a safe state.

Functional Mode	**I/O-Driver**	**Appl.**	**Measures**	**No. of Pins**	**DC***	**References**
LS Digital Output	-	-	-	1	0 %	-
	✓	-	Voltage monitoring & shut-off path test	2**	90 %	IEC 61508-7 A.1.1 - *Failure detection by online monitoring* ISO 13849-1 Table E.1 - *Redundant shut-off path with monitoring of one of the actuators* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	-	✓	Voltage monitoring & shut-off path test	1 or 2***	90 %	IEC 61508-7 A.1.1 - *Failure detection by online monitoring* ISO 13849-1 Table E.1 - *Redundant shut-off path with monitoring of one of the actuators* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
Analog Input	-	-	-	1	0 %	-
	-	✓	Signal range check	1	60 %	ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
	-	✓	Redundancy	2	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / vonting* ISO 25119-2 Table C.6 *Comparator*
	-	✓	Redundancy & signal range check	2	99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check*

						ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Input comparison / vonting* ISO 25119-2 Table C.6 *Comparator*
Digital Input	-	-	-	1	0 %	-
	-	✓	Redundancy	2	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / vonting* ISO 25119-2 Table C.6 *Comparator*

Table 29

* HW block, interface and electrical part of the external device
** Secondary shut-off path, i.e. a dedicated digital low side output, needs to be configured during pin initialization.
*** Secondary shut-off path can be, e.g. an independent output stage or a hydraulic shut-off valve.

LS Digital Output:
The I/O driver's diagnostic module continuously compares the desired output status with the feedback measurements, thus allowing to detect failures within the digital low side output stages. This measure is active for every pair of digital high side output and digital low side output that is initialized as safety-critical and will trigger an error callback in case of dangerous failures.
If the digital low side output is not configured safety-critical—and thus, is not used in combination with a digital high side output—no safety measures are executed by the I/O driver's diagnostic modules.

Analog Input:
The digital low side stages' analog input measurement is not equipped with automatically enabled safety mechanisms. Therefore, no safety mechanisms can be claimed by the system integrator and additional measures have to be enabled, if the overall safety function requires diagnostic coverage for the analog input function.

Digital Input:
In the digital input configuration, certain failure modes of the digital low side stages (including an unintentional activation of power stages) might not be detectable by the HY-TTC 500 I/O driver's diagnostic modules. Hence, a redundant usage of independent input stages is recommended for safety functions that require a certain diagnostic coverage.

8.2.10.1 Voltage Monitoring

Category:	Comment	ID:	924656

The current state of the digital low side outputs can be read via the static voltage feedback signals. That way, the application software is able to verify the correct function of the digital low side outputs and activate the safe state in case of dangerous failures. If the independent digital high side outputs are not used as secondary shut-off paths, the system integrator is responsible to provide other means that allow bringing the overall system to a safe state, e.g. by a separate emergency valve that disrupts the hydraulic oil flow and stops any dangerous movements.

This safety mechanism allows to detect a substantial amount of possible hardware failures and—with a proper secondary shut-off path in place—is therefore considered to yield a DC value of **90 %**.

8.2.10.2 Shut-off Path Test

Category:	Comment	ID:	964475

In order to check the proper operation of the secondary shut-off path, its ability to transfer the system into a safe state needs to be tested in certain intervals, e.g. at the beginning of each driving cycle or during pre-defined maintenance activities. That way, the system can be considered to offer a valid category 2 architecture, according to ISO 13849.

8.2.10.3 Redundancy

Category:	Comment	ID:	924660

The redundant usage of independent inputs allows for continuous cross monitoring of the corresponding input signal. Plausibility checks within the application software permit the system integrator to detect a single fault in one of the input paths and transfer the overall system to a safe state. When defining the time interval of such checks, the system integrator needs to consider the overall system's failure reaction time. For details on calculating the worst case failure reaction times of such consistency checks, see section *Failure Diagnostics*.

Redundancy can also be claimed when combining two different input types (e.g. a digital output stage's analog input measurement with an analog input 3 mode, or a digital output stage's digital input measurement with a timer input), as long as the inputs' specifications both match the desired input signal.

This safety mechanism's diagnostic coverage is considered to lie between a value of **90-99 %**, depending on the characteristics of the input elements (e.g. their possible failure modes) and the plausibility check's strictness.

8.2.10.4 Signal Range Check

Category:	Comment	ID:	924652

In order to check for short circuits to ground or battery voltage as well as open loads of dedicated inputs, a signal range check (SRC) can be utilized. That means a predefined margin on the upper and lower end of the measurable range is excluded from the sensor's valid output values. If for the signal range check a range of 5…95 % is considered to be valid for a sensor, all values below 5 % or above 95 % should be considered erroneous by the application software.

Unlike the analog 2 mode and 3 mode inputs, the digital low side outputs do not offer an internal signal range check that is executed by the I/O driver's diagnostic modules. It is, therefore, in the responsibility of the application software to implement such a range check.

Since this safety mechanism is able to detect only basic failure modes both internal and external to the HY-TTC 500 platform, the according diagnostic coverage is considered to be low, i.e. **60 %**.

8.2.11 High Side Digital / PVG / VOUT Output

Category:	Comment	ID:	924869

The high side digital output stages with PVG and VOUT mode do not directly allow safety-critical operation of any loads. They do feature internal feedback mechanisms that allow continuous monitoring of the effective output voltage but none of these measures are automatically executed by the I/O driver's diagnostic modules. Also, they do not provide an integral shut-off path that would allow to independently de-energize an erroneous output stage.
Thus, if the system integrator intends to use those functional blocks in a safety-critical application, dedicated measures to detect dangerous failures need to be implemented within the application software.

Functional Mode	I/O-Driver	Appl.	Measures	No. of Pins	DC*	References
HS Digital Output	-	-	-	1	0 %	-
	-	✓	Status monitoring & shut-off path test	1 or 2**	90 %	IEC 61508-7 A.1.1 - *Failure detection by online monitoring* ISO 13849-1 Table E.1 - *Redundant shut-off path with monitoring of one of the actuators* ISO 26262-5 Table D.5 *Failure detection by on-line monitoring* ISO 25119-2 Table C.6 *Failure detection by online monitoring*
Analog Input	-	-	-	1	0 %	-
	-	✓	Signal range check	1	60 %	ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
	-	✓	Redundancy	2	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
	-	✓	Redundancy & signal range check	2	99 %	IEC 61508-7 - *Input comparison / voting*

						ISO 13849-1 Table E.1 - *Plausibility check* ISO 13849-1 Table E.1 - *Monitoring some characteristics* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*
Digital Input	-	-	-	1	0 %	-
	-	✓	Redundancy	2	90-99 %	IEC 61508-7 - *Input comparison / voting* ISO 13849-1 Table E.1 - *Plausibility check* ISO 26262-5 Table D.5 *Input comparison / voting* ISO 25119-2 Table C.6 *Comparator*

Table 30

* HW block, interface and electrical part of the external device
** Secondary shut-off path can be, e.g. an independent output stage or a hydraulic shut-off valve.

HS Digital Output:
The state of the digital high side outputs will not be automatically monitored by the I/O driver's diagnostic modules. An according plausibility check of the output stage's feedback value needs to be implemented by the system integrator, if required by the overall system architecture.

Analog Input:
The high side digital output stages' analog input measurement is not equipped with automatically enabled safety mechanisms. Therefore, no safety mechanisms can be claimed by the system integrator and additional measures have to be enabled, if the overall safety function requires diagnostic coverage for the analog input function.

Digital Input:
In the digital input configuration, certain failure modes of the digital high side stages (including an unintentional activation of power stages) might not be detectable by the HY-TTC 500 I/O driver's diagnostic modules. Hence, a redundant usage of independent input stages is recommended for safety functions that require a certain diagnostic coverage.

8.2.11.1 Status Monitoring

Category:	Comment	ID:	924867

The current state of the digital high side outputs can be read via the static feedback signals. That way, the application software is able to verify the correct function of the digital high side outputs and activate the safe state in case of dangerous failures. Since the HY-TTC 500 platform does not offer an integral shut-off path that allows to independently disable the connected actuator, the system integrator is responsible to provide other means that allow bringing the overall system to a safe state, e.g. by a separate emergency valve that disrupts the hydraulic oil flow and stops any dangerous movements or by utilizing an independent digital low side output of the HY-TTC 500 platform.

This safety mechanism allows to detect a substantial amount of possible hardware failures and—with a proper secondary shut-off path in place—is therefore considered to yield a DC value of **90 %.**

8.2.11.2 Shut-off Path Test

Category:	Comment	ID:	964502

In order to check the proper operation of the secondary shut-off path, its ability to transfer the system into a safe state needs to be tested in certain intervals, e.g. at the beginning of each driving cycle or during pre-defined maintenance activities. That way, the system can be considered to offer a valid category 2 architecture, according to ISO 13849.

8.2.11.3 Redundancy

Category:	Comment	ID:	925634

The redundant usage of independent inputs allows for continuous cross monitoring of the corresponding input signal. Plausibility checks within the application software permit the system integrator to detect a single fault in one of the input paths and transfer the overall system to a safe state. When defining the time interval of such checks, the system integrator needs to consider the overall system's failure reaction time. For details on calculating the worst case failure reaction times of such consistency checks, see section *Failure Diagnostics*.

Redundancy can also be claimed when combining two different input types (e.g. a digital output stage's analog input measurement with an analog input 3 mode, or a digital output stage's digital input measurement with a timer input), as long as the inputs' specifications both match the desired input signal.

This safety mechanism's diagnostic coverage is considered to lie between a value of **90-99 %**, depending on the characteristics of the input elements (e.g. their possible failure modes) and the plausibility check's strictness.

8.2.11.4 Signal Range Check

Category:	Comment	ID:	925638

In order to check for short circuits to ground or battery voltage as well as open loads of dedicated inputs, a signal range check (SRC) can be utilized. That means a predefined margin on the upper and lower end of the measurable range is excluded from the sensor's valid output values. If for the signal range check a range of 5…95 % is configured to be valid for a sensor, all values below 5 % or above 95 % should be considered erroneous by the application software.

Unlike the analog 2 mode and 3 mode inputs, the digital high side outputs do not offer an internal signal range check that is executed by the I/O driver's diagnostic modules. It is, therefore, in the responsibility of the application software to implement such a range check.

Since this safety mechanism is able to detect only basic failure modes both internal and external to the HY-TTC 500 platform, the according diagnostic coverage is considered to be low, i.e. **60 %**.

9 Guideline on Sensor Selection

Category:	Comment	ID:	592065

The following section shall provide a general overview of commonly used sensors and will discuss their interoperability with the dedicated sensor inputs of the HY-TTC 500 platform. This section is only considered a guideline and does not alter any requirements stated in the herein before mentioned sections.

9.1 Analog Sensors

Category:	Comment	ID:	592087

For being capable of providing analog inputs for safety-critical applications, the HY-TTC 500 platform requires diagnostic measures to be present within the analog input path. Depending on the analog input type, the system integrator may have to comply with specific requirements in order to allow safety-critical utilization, as specified in the before-mentioned section *Analog Inputs*.

The following section will describe typical analog sensor types together with their detailed characteristics.

9.1.1 Usage of Redundant Sensors

Category:	Comment	ID:	592125

Redundantly connected sensors do allow the reliable detection of failures within a single sensor path. However, for those failures that commonly compromise both sensor signals at once, e.g. short circuits between the separate sensor lines, dedicated preconditions are necessary.

9.1.1.1 Diverse Sensor Characteristics

Category:	Comment	ID:	592129

If redundant sensors are used for detection of short circuits between sensor lines, external to the ECU, sensors with diverse characteristics are recommended in order to continuously monitor the signal lines for external short circuits. The following types of diverse sensors are commonly used:

- Two identical potentiometers with opposite characteristics (i.e. when changing the physical input value, one sensor reacts with an increasing sensor value while the other one reacts with a decreasing sensor value). With a short circuit between those two sensors, the ECU will measure a value of 50 % full range for both sensors. This output value is plausible but wrong.
  As a consequence, this kind of diverse sensor operation is only feasible for sensors that result in safe output conditions when emitting a sensor value of 50 %. This could be, for example, a joystick containing two sensors with opposite characteristics. In its idle position, as well as when the sensor lines are shorted, it outputs sensor values of 50 %, each. Basically, a short circuit would not be detected by the application software, but this condition would lead to a safe condition, anyway.

- Two identical potentiometers with different proportional factor at their outputs. That could mean, for example, that the one sensor outputs a value that is double the voltage of the second sensor, for any position. That way, the both sensors can never show the same output values at the same time, enabling the application software to detect short circuits between these sensor lines.

9.1.1.2 Indentical Sensor Characteristics

Category:	Comment	ID:	592133

When identical sensors are used for redundancy, short circuits between both sensor lines cannot be detected, per se. However, two identical sensors will allow best precision regarding measurement accuracy.

Since the HY-TTC 500 platform does provide measures to identify external short circuits between two redundantly used sensors with identical characteristics, the system integrator can rely on the mechanisms to detect these external short circuits during start-up, as described in section *External Short Circuit Check*.

9.1.2 Potentiometric Analog Sensors

Category:	Comment	ID:	592117

Potentiometric analog sensors are commonly used for analog position sensors (e.g. pedals or joysticks), movement sensors or active sensors that resemble the behavior of potentiometers. These sensors produce an analog output voltage that is proportional to the mechanical position as well as to the sensor supply.
Consequently, a linear position sensor being in its center position will show an output signal with a voltage of exactly 50 % of the sensor supply voltage. By using the ratiometric measurement, the sensor supply's error does not influence the measurement value accuracy.

Please note that it is not allowed to supply a sensor by one ECU and measure the sensor's output signal on another ECU. Ground shifts between the two ECUs would considerably degrade the measurement accuracy.

Category:	Comment	ID:	592123

The following figure shows the typical wiring of potentiometric analog sensors.

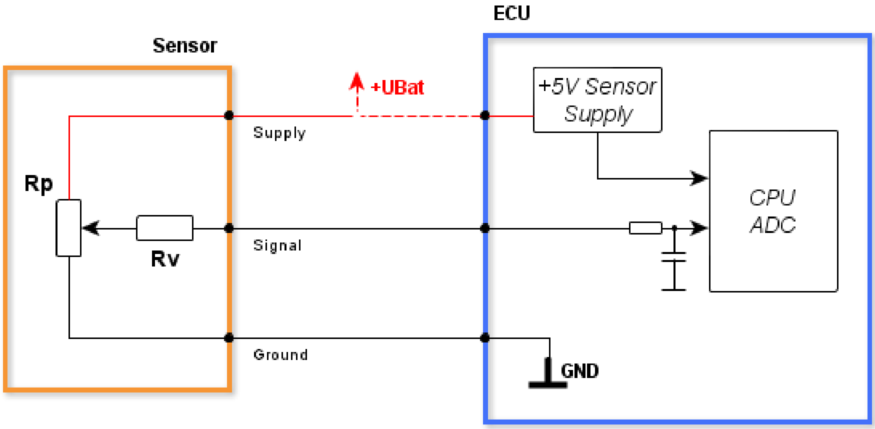

Figure 5

9.1.3 Current Loop Sensors

Category:	Comment	ID:	592119

Current loop sensors are typically 2-wire sensors with one wire being connected to battery supply, while the other wire is connected to an ECU's analog input with current measurement capabilities. The standard current range is given with 4…24mA, where 4 mA corresponds to the minimum physical value while 24 mA is the maximum valid measurement value.

Category:	Comment	ID:	592121

The following figure shows the typical wiring of current loop sensors.

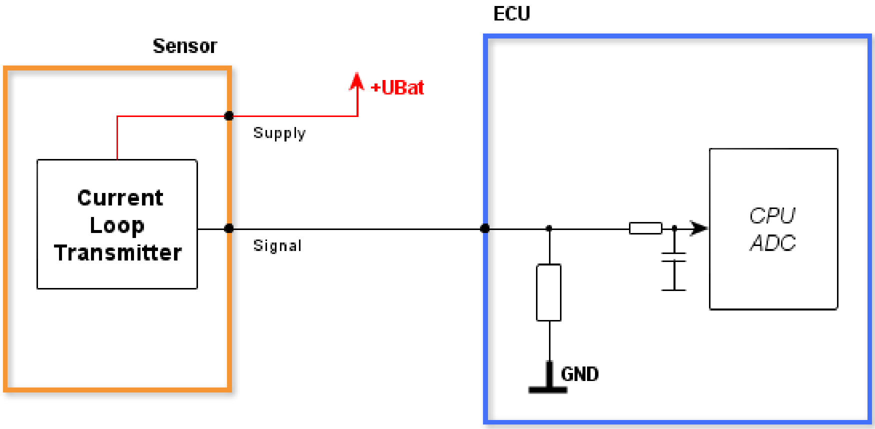

Figure 6

9.2 Digital Sensors

Category:	Comment	ID:	592069

For being capable of providing digital inputs for safety-critical applications, the HY-TTC 500 platform requires diagnostic measures to be present within the digital timer input path. When using general digital sensors, the redundant usage of separate digital timer inputs is a necessary requirement to the system integrator.
The following section will describe typical digital sensor types together with their detailed characteristics.

9.2.1 PWM Position Sensors

Category:	Comment	ID:	592073

Typically, PWM position sensors are analog sensors (pedals, joystick) with potentiometers or contactless active sensors providing PWM signals. The PWM duty cycle is proportional to the measured physical quantity. PWM sensors may be supplied by a 5 V supply as well as being directly connected to battery voltage.

Since these sensors typically do not provide any means to reliably detect failures (e.g. short circuits or open circuits of the sensor lines), a redundant utilization of separate timer inputs is required. The application has to monitor and compare the measurement values and has to enter the safe state, in case of deviations between the independent inputs.

Category:	Comment	ID:	592075

The following figure shows the typical wiring of PWM position sensors.

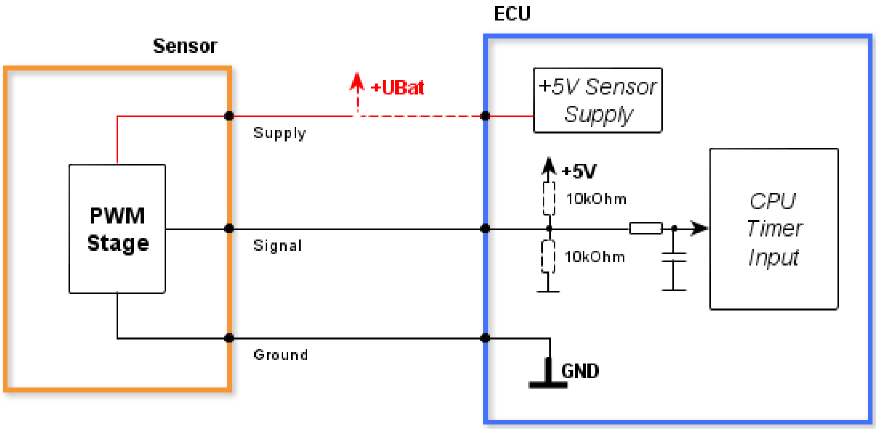

Figure 7

9.2.2 RPM Sensors

Category:	Comment	ID:	592079

RPM sensors are active sensors with mainly magnetically sensitive detectors. The HY-TTC 500 platform is compatible to those RPM sensors that feature 3-wire connection and can be supplied with either 5 V or battery voltage while providing push-pull or open collector output stages.

A rotary sensor wheel (toothed gear wheel) produces a rectangular output signal on the sensor input, with one pulse being emitted for each tooth that passes the sensor wheel.

Without rotation, the output is statically low or high, depending on whether there is a tooth or a gap next to the active sensor region. When using traditional sensors, however, an idle sensor may be confused with a defective sensor connection (i.e. a shorted sensor line or a broken wire).
In order to distinguish between the conditions *no speed* or *defective sensor*, the following measures can be applied:

- An RPM sensor that emits a test pulse (e.g. one pulse every 100 ms) while standing still. If the signal is stuck at any level, the application can expect the sensor or its signal lines to be defective and may activate the safe state.
- The redundant utilization of two separate timer inputs. By comparing the measured values of both sensor inputs, the application can identify sensor failures and change to the safe state.

Category:	Comment	ID:	592081

The following figure shows the typical wiring of RPM sensors.

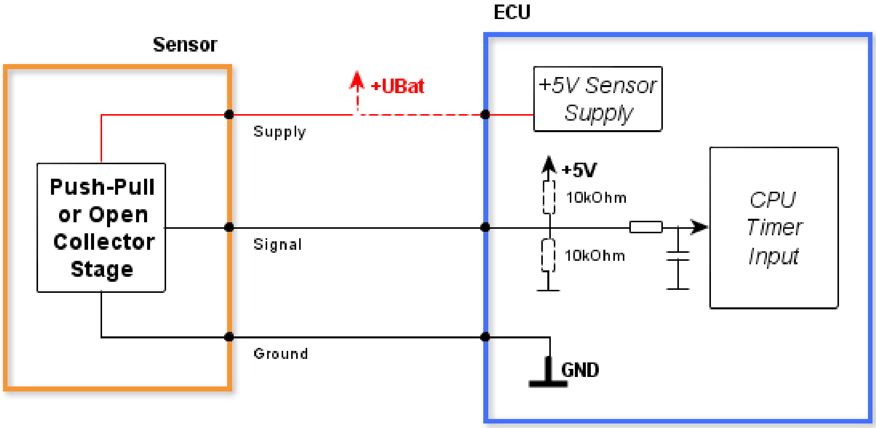

Figure 8

9.2.3 Digital Switches

Category:	Comment	ID:	592099
Digital switches that statically emit logical high or low levels, do not provide any measures for detection of potential failures, typically. Thus, the system integrator has to redundantly utilize two separate inputs when requiring safety-critical inputs. The application software is responsible for comparing the measurements and change to the safe state in case of discrepancies between both input values.			

Category:	Comment	ID:	592101
During operation, redundantly used digital switches may show a certain offset regarding their actual switching threshold. Consequently, there may be a particular time period where the comparison of the sensors' input values appears to be implausible. The system integrator is advised to provide adequate debouncing of those intermediate states within the application software.			

9.3 External Short Circuit Check

Category:	Comment	ID:	592623
For detecting short circuits between two redundantly used sensors, the HY-TTC 500 platform provides independent sensor supply outputs and the ability to separately disable them, one by one. Redundant sensors are to be connected to different sensor supplies. That way, the freedom from short circuits can be checked during start-up by disabling a sensor supply output and verifying that the signals of all supplied sensors drop to a value close to zero. If a corresponding sensor still emits legal sensor values, a short circuit to a redundant (and still supplied) sensor is very likely. These short circuit checks will, however, not be performed by the diagnostic modules provided with the HY-TTC 500 platform. Instead, they need to be implemented within the application software. A possible implementation for such a short circuit check would be a start-up test that sequentially enables the sensor supplies and checks the corresponding set of functional sensors for each sensor supply state.			

10 Glossary

Category:	Comment	ID:	717045

Agriculture Performance Level (AgPL)
Discrete level (one out of a possible five) used for specifying the system's ability to perform a safety function under foreseeable conditions, where agriculture performance level e has the highest level of safety integrity and agriculture performance level a has the lowest. (ISO 25252-1)

Application
The term *application* in the context of this document refers to the software part developed by the system integrator that is executed by the Main CPU on the HY-TTC 500 in addition to the provided HY-TTC 500 software platform.

Fail-safe system
A system is *fail-safe* if there is a safe state in the environment that can be reached in case of a system failure.

Fault
Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.

Fault Tolerance
The ability of a functional unit to continue to perform a required function in the presence of faults or errors.

Failure
The termination of the ability of a functional unit to perform a required function.

Performance Level (PL)
Discrete level (one out of a possible five) used for specifying the system's ability to perform a safety function under foreseeable conditions, where performance level e has the highest level of safety integrity and performance level a has the lowest. (ISO 13849-1)

Periodically
The term '*periodically*' or '*periodical*' within this documents refers for example to a frequently call of a function or a regular check of a state or variable. However, the 'periodically' condition is not related to certain time base, but to software cycles. Whenever something has to be done periodically, the said event shall be triggered at least *once per software cycle*.

Safe State
In the *safe state* zero current is applied to the safety-critical outputs of the ECU, i.e. in case of an error all outputs will be switched off.

Safety-critical / Safety-relevant System
The term *safety-critical* in the context of this document refers to a system whose failure or malfunction may result in death or injury. The HY-TTC 500 has been designed to fulfill ISO 13849 Category 2, Performance Level d and IEC 61508, Safety Integrity Level 2 requirements.

Safety Function
Execution of the control function programmed by the system integrator (e.g. controlling the outputs in accordance to input values) in a fail-safe principle.

Safety Integrity Level (SIL)
Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where SIL 4 has the highest level of safety integrity and SIL 1 has the lowest (IEC 61508-4).

Safety Lifecycle
Necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities are no longer available for use.

Software Cycle
The term '*software cycle*' in the context of this document means one passage of the while(1) loop within the main application. A *software cycle* (one round within the main-loop) includes all regular called functions from the application as well as the important driver functions IO_Driver_TaskBegin and IO_Driver_TaskEnd.

Software Requirement Level (SRL)
Ability of safety-related parts to perform a software safety-related function (3.45) under foreseeable conditions. The SRL is categorized into four groups: SRL = B,1,2 and 3, where B is the lowest and 3 the highest. (ISO 25119-1)

System
The term *system* in the context of this document refers to the final system (e.g. vehicle, machine …) in which the HY-TTC 500 is integrated.

System Integrator
The *system integrator* defines and develops the system and integrates the HY-TTC 500 into the system. The system integrator is responsible for the safe operation of the application.

11 Acronyms

Category:	Comment	ID:	591305

ABI - Application Binary Interface
ADC - Analog-to-Digital Converter
AgPL - Agriculture Performance Level [ISO 25119]
API - Application Programming Interface
CAN - Controller Area Network
CPU - Central Processing Unit
CRC - Cyclic Redundancy Check
DC - Duty Cycle or Direct Current
ECC - Error Correction Code
ECU - Electronic Control Unit
E/E/PES - Electric/Electronic/Programmable Electronic System [IEC 61508]
EEPROM - Electrically Erasable Programmable Read-Only Memory
FMEDA - Failure Modes Effects and Diagnostic Analysis
FPU - Floating Point Unit
HY-TTC 500 - Safety-relevant ECU developed by TTControl
MPU - Memory Protection Unit
MTTFd - Mean time to dangerous failure [ISO 13849]
OTP - One-time programmable: A program-only-once Flash memory
PFH - Probability of failure per hour [IEC 61508]
PL - Performance Level [ISO 13849]
PWM - Pulse width modulation
RAM - Random access memory
RPM - Revolutions per minute
SECDED - Single Error Correction Double Error Detection
SFF - Safe failure fraction [IEC 61508]
SIL - Safety Integrity Level [IEC 61508]
SR - Safety-related
SRC - Signal Range Check
SRL - SOftware Requirement Level [ISO 25119]
SRP/CS - safety–related part of a control system [ISO 13849]
TMS570 - MCU TMS5703137 from Texas Instruments

12 References

Category:	Comment	ID:	591265
[TTC500-SysM] TTTech. System Manual for HY-TTC 500, Document ID D-TTC5F-G-20-002 [TTC500-SM-26262] TTTech. HY-TTC 500 Safety Manual Addon for ISO26262, Manual ID D-TTC5F-M-02-007 [TTC500-IOUM] TTTech. I/O Driver User Manual for HY-TTC 500, Document ID S-TTC5F-G-20-001 [TTCD-RN] TTTech. TTC-Downloader Release Notes Document, Document ID D-TTCSW-DN-20-001 [ISO 13849] ISO. ISO 13849 - Safety of machinery - Safety-related parts of control systems, 2015/2012. [IEC 61508] IEC. IEC 61508 Functional safety of electrical / electronic / programmable electronic safety-related systems, 2010. [ISO 25119] ISO. ISO 25119 – Tractors and machinery for agriculture and forestry — Safety-related parts of control systems, 2019 [CortexR4F-TRM] Cortex-R4 and Cortex-R4F Revision:r1p3 Technical Reference Manual, ARM DDI 0363E (ID013010), ARM, 2009			