Technical Report for Functional Safety

Report No.: SZFS241200010801

Mar. 19th, 2025

Client / Applicant:	Anker Innovations Limited Unit 56, 8th Floor, Tower 2, Admiralty Centre, 18 Harcourt Road, Hong Kong
Manufacturer:	Same as applicant
Project Title:	Rechargeable Li-ion Battery System (Product name: Anker SOLIX Balcony Energy Storage System)
Model Name.:	A17C53Z1-1, A17C53Z1-2, A17C53Z1-3, A17C53Z1-4, A17C53Z1-5, A17C53Z1-20-1, A17C53Z1-20-2, A17C53Z1-20-3, A17C53Z1-20-4, A17C53Z1-20-5, (Main battery unit: A17C53Z1, A17C53Z1-20 Expansion Battery: A17C53Z1-85)
Tested Standards:	UL 60730-1:2016 Annex H
Conclusion	In this report, safety protection function of Battery Management System was assessed to achieved class B according to UL 60730-1:2016 Annex H, detail of safety function items sees Table 1 Safety functions definition.

This evaluation report confirms the achievement of the requirements of functional safety based on the following proofs:

- Proof of systematic safety integrity for defined phases of the life cycle
- Proof of the techniques and measures according to UL 60730-1:2016 Annex H
- Proofs that process and methods are established at the manufacturer guaranteeing that unexceptionable processes.

This evaluation report confirms the achievement of the requirements of functional safety based on the following proofs:

In terms of risk analysis, design, production, validation, change management and quality management comply with the safety-related standard.

Independent organization for functional safety assessment	Assessor	Approver
SGS-CSTC Standards Technical Services Co., Ltd. Shenzhen Branch	Shawn Chen	Jerry Zheng

CONTENTS

List of Figures:

List of Tables:

1. Summary of assessment

This technical report summarizes the safety performance evaluation results towards the software safety functions in Battery Management system, provides by **Anker Innovations Limited**

No deviations were found during the assessment acc. to UL 60730-1:2016 Annex H for safety related software functions in BMS system in terms of systematic capacity.

The validation of functional safety is based on a basic examination regarding quality management system and the functional safety management as part of the software performance level. All project development engineers have completed relevant trainings in functional safety, and most of them previously participated in product development projects involving functional safety.

In this report, the below safety functions for Battery Management System have been assessed:

Identification	Safety Critical Function Items
SF01	Protection for over-voltage of charging
SF02	Protection for under-voltage of discharging.
SF03	Protection for over-current of charging.
SF04	Protection for over-current of discharging.
SF05	Protection for over/under-temperature of charging.
SF06	Protection for over/under-temperature of discharging.

Table 1: Safety functions definition

Supplementary Information:
[1] UL 60730-1:2016 Annex H as a guide
[2] The more detail information please refers to the following report.
[3] This assessment is based on the requirement stated in UL 60730-1:2016 towards software Class B.

2. Assessment Period

Beginning of project: 2024-12-24

End of project: 2025-03-17

3. References

No.	Document Description
[D01]	01 惠州市蓝微电子-ISO9001质量体系证书2023
[D02]	02 17C53Z1-85 BMS Safety Requirement Specification_v1.0 60730
[D03]	03 BMS HW Design Description-17C53Z1-85
[D04]	04 BMS SW Design Specification-17C53Z1-85
[D05]	05 A17C5 BMS2-K01-V0.2-20241112 schematics
[D06]	06 A17C5 BMS2-K01-V0.2 CDF

No.	Document Description
[D07]	07 A17C5 BMS2-K01-V0.2 Layout
[D08]	08 A17C5 BMS-器件降额表
[D09]	09 软件编程规范
[D10]	10 BMS软件代码审查报告
[D11]	11 17CX-BMS功能测试报告
[D12]	12 Fault Insertion Test report
[D13]	13 A17C5系统框图
[D14]	14 A17C5项目变更履历
[D15]	15 Component FMEDA Report (A17C5)_Rev.A

Table 2: References and documents

4. Revision Logs

Version	Changes Description
V1.0	Initial Version

Table 3: Revision logs

5. Symbols and abbreviated terms

No.	Abbreviation	Description
1.	HW	Hardware
2.	SW	Software
3.	SF	Safety Function
4.	CHG (MOS)	Charge MOS
5.	DCHG (MOS)	Discharge MOS
6.	MCU	Microcontroller Unit
7.	ADC	Analog to Digital Converter
8.	WDT	Watch Dog Timer

Table 4: Glossary and Terms

6. Design and Development Tools

No.	Type of Tool	Vendor	Tool Name	Revision
1	Version Control	Git	Git	V 2.42.0
2	Development Tool	Keil	Keil-MDK	V 5.35
3	Compiler	Keil	Armcc	V 5.06
4	Linker	Keil	ArmLink	V 5.06
5	Assembler	Keil	Armasm	V 5.06
6	Simulation	Segger	JLINK	V7.90
7	Schematic & PCB design	Altium	Altium Designer	V 19.1.8

Table 5: Design tools

7. HSI Design and Critical Component

Pin No.	Pin Name	Direction	Function	Mark(s)
1	PE3	I/O	Pre-DSG	/
2	PC14	I/O	OSC32IN	/
3	PC15	I/O	OSC32OUT	/
4	NRST	I/O	Reset pin	/
5	PA3	I/O	B+_ADC	/
6	PB14	I/O	AFE_ ALERT	/

Table 6: MCU I/O assignment table

Object / part No.	Manufacturer/ trademark	Type / model	Technical data	Standard	Mark(s) of conformity
Cell	EVE Power Co., Ltd.	LF105LA	3,2 Vdc, 105 Ah	IEC 62619:2022, EN IEC 62619:2022	TUV SUD (CB report No. 085-282460157-000, Cert. No. SG PSB-BT-05045)
PCB	Hubei LongTeng Electronic Technology Co Ltd	ZLHML005	V-0, 130°C	UL 94, UL 796	UL (E467745)
AFE (U6)	TI	BQ7694202	Vbat: 4,7-55V, Operating temperature: -40 to 85°C	--	--
MCU (U9)	GigaDevice Semiconductor Inc.	GD32F303VET6	Operating voltage: 2,6 to 3,6 V, Operating temperature: -40 to +85 °C	--	--
MOS (Q7, Q8, Q45, Q46, Q47, Q48, Q49, Q50, Q52, Q53)	PINGWEI	PW018N08TS	VDS: 85V, ID: 240A, 150 ºC	--	--
NTC (NTC5, NTC6, NTC7, NTC8, NTC9, NTC10)	MURATA MFG CO LTD	NCU18XH103F6SRB	Tmoa: 150 ºC, 10kohm at 25 ºC	UL1434	UL (E137188)

Table 7: Critical components

8. Assessment Item Information

Inspection item description ……: See First Page
HW Version of battery Module……: Version 3.0
SW Version of battery Module…… V0.3.2.0
HW Version of System Controller Module ……: Version 3.0
SW Version of System Controller Module ……: V0.3.2.0

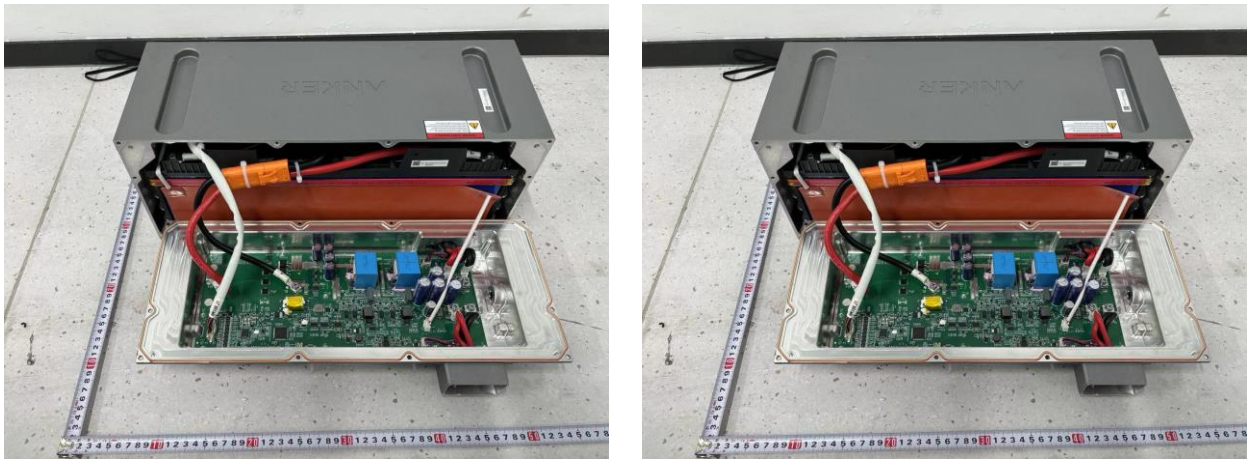
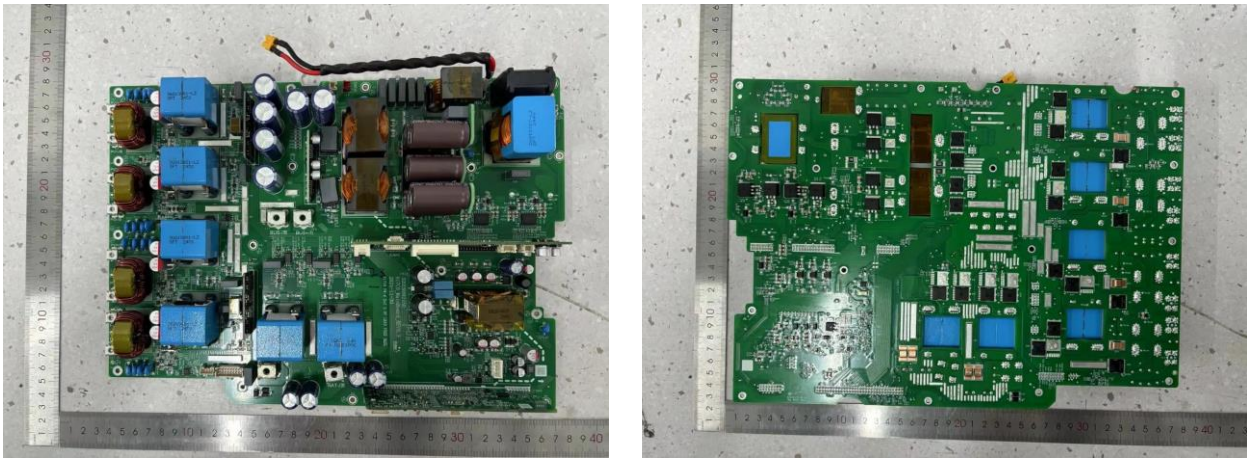


Figure 1 View of Product

Power board：



BMS board:

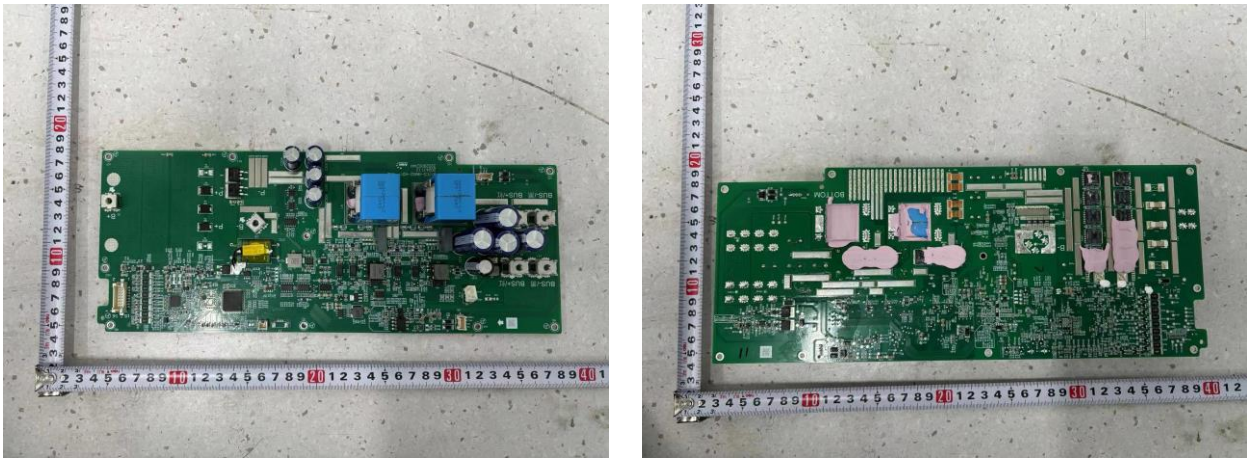


Figure 2 View of Both Sides BMS PCBA

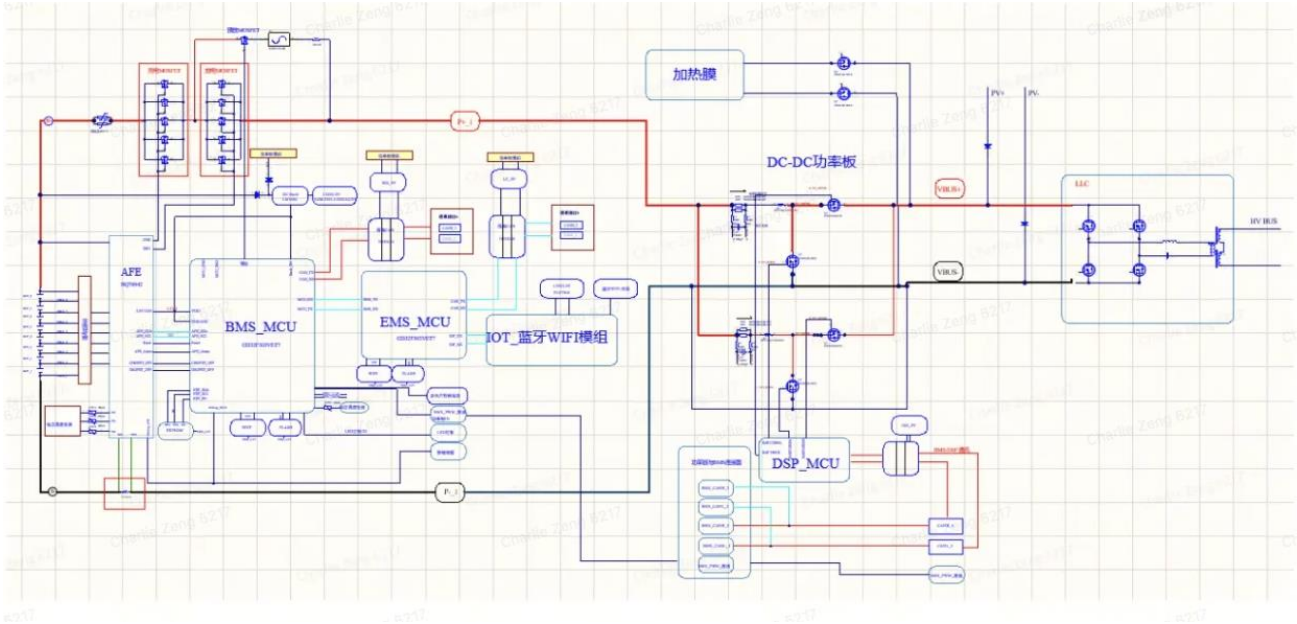


Figure 3 BMS Safety Function System Architecture

9. SW Safety Requirement Specification

9.1. Safety Function Definition

The below protection functions of BMS shall be defined as safety function, refers to **Table 1** safety function definition.

The details requirements for above safety functions specified as following tables:

Ident.	
SRS01	Safety function: Protection for over-voltage of charging
	1. Function Safety Circuit Structure Category: Single channel with periodic self-test.
	2. Safety state description 2.1.1 Over voltage fault detection and enter the safety state: Level 1: When pack voltage exceeds 18.8V or any cell voltage exceeds 3.64V, the system shall turn off the CHG DC-DC and stop charging. Level 2: When any cell voltage exceeds 3.65V, the system shall turn off the CHG DC-DC and CHG MOS and stop charging.
	3. Fault tolerance time interval Over voltage Level 1: FTTI: 3 seconds. Over voltage Level 2: FTTI: 3 seconds.
SR02	Safety function: Protection for under-voltage of discharging.
	1. Function Safety Circuit Structure Category: Single channel with periodic self-test and monitoring
	2. Safety state description 2.1 Under voltage fault detection and enter the safety state: Level 1: When pack voltage drops below 13V or any cell voltage drops below 2.8, the system shall turn off the DSG DC-DC and stop discharging. Level 2: any cell voltage drops below 1.91V, the system shall turn off the DSG DC-DC and DSG MOS and stop discharging.
	3. Fault tolerance time interval Level 1: FTTI: 3 seconds. Level 2: FTTI: 3 seconds.
SRS03	Safety function: Protection for over-current of charging.
	1. Function Safety Circuit Structure Category: Single channel with periodic self-test.
	2. Safety state description 2.1 Charging over-current fault detection and enter the safety state: Level 1: When the current exceeds 80.5 A and duration 3s, the system shall turn off the CHG DC-DC and stop charging. Level 2: When the current exceeds 82.6 A duration 3s or over 100A duration 300ms,

	the system shall turn off the CHG DC-DC and CHG MOS and stop charging.
	3. Fault tolerance time interval FTTI: 3 seconds.
SRS04	Safety function: Protection for over-current of discharging.
	1. Function Safety Circuit Structure Category: Single channel with periodic self-test.
	2. Safety state description 2.1 Discharging over-current fault detection and enter the safety state: Level 1: When the current exceeds 77A, and duration 5s, the system shall turn off the DSG DC-DC and stop discharging. Level 2: When the current exceeds 120A, and duration 300ms, the system shall turn off the DSG DC-DC and DSG MOS and stop discharging.
	3. Fault tolerance time interval Level 1: FTTI: 5 seconds. Level 2: FTTI: 5 seconds.
SRS05	Safety function: Protection for over/under-temperature of charging.
	1. Function Safety Circuit Structure Category: Single channel with periodic self-test.
	2. Safety state description 2.1 Over temperature fault detection and enter the safety state: Level 1: When the temperature exceeds 63℃, and the over temp period exceeds 2s, the system shall turn off the CHG DC-DC and stop charging. Level 2: When the temperature exceeds 64℃, and the over temp period exceeds 10s, the system shall turn off the CHG DC-DC and CHG MOS and stop charging. 2.2 Under temperature fault detection and enter the safety state: Level 1: When the temperature under 1℃, and the over temp period exceeds 2s, the system shall turn off the CHG DC-DC and stop charging. Level 2: When the temperature under 1℃, and the over temp period exceeds 10s, the system shall turn off the CHG DC-DC and CHG MOS and stop charging.
	3. Fault tolerance time interval FTTI: 10 seconds.
SRS06	Safety function: Protection for over/under-temperature of discharging.
	1. Function Safety Circuit Structure Category: Single channel with periodic self-test.
	2. Safety state description 2.1 Over temperature fault detection and enter the safety state: Level 1: When the temperature exceeds 63℃, and the over temp period exceeds 2s, the system shall turn off the DSG DC-DC and stop discharging. Level 2: When the temperature exceeds 64℃, and the over temp period exceeds 10s, the system shall turn off the DSG DC-DC and DSG MOS and stop discharging. 2.2 Under temperature fault detection and enter the safety state: Level 1: When the temperature under -19℃, and the over temp period exceeds 2s, the

	system shall turn off the DSG DC-DC and stop discharging. Level 2: When the temperature under -29℃, and the over temp period exceeds 10s, the system shall turn off the DSG DC-DC and DSG MOS and stop discharging.
	3. Fault tolerance time interval FTTI: 10 seconds.

Table 8: Safety function definition

9.2. Safe State

Safety state please refer to the definition of each safety function in the part of “protection working mode definition”.

9.3. Safety Response Time

Safety response time please refer to the definition of each safety function in the part of “protection working mode definition”.

10. Assessment based on UL 60730-1:2016 Annex H

The colour legend applicated for software assessment as below.

Colour	Meaning
Green	Requirements fulfilled
Yellow	Measures are acceptable, improvement recommended
Red	Requirement not assessed in this report
White	Requirement not applicable

Table 9: Colour of requirement

H.6	Classification, additions	
H.6.18	Class of control function (A, B, C).....	Class B
H.7	Information in addition to Table 1 provided:	
	66 - Software sequence documentation; clause: H.11.12.2.9; method: X.....	Requirements fulfilled. The functional safety software specifies the operation sequence, and the functional requirements fully consider the relevant hardware architecture and component functions. See Chapter 9.1 of this document.

	67 - Program documentation; clause: H.11.12.2.9, H.11.12.2.12; method: X	Requirements fulfilled. Each time the software runs, it initializes the safety related operable components to make them enter the safe state, and then starts self-inspection and operation, see document **Error! Reference source not found.** and **Error! Reference source not found.**.
	68 - Software fault analysis; clause: H.11.12, H.27.1.1.4; method: X.....	Requirements fulfilled. The software fault analysis considers the influence of control devices and test devices, See document [D04]
	69 - Software class(es) and structure; clause: H.11.12.2, H.11.12.3, H.27.1.2.2.1, H.27.1.2.3.1; method: D ...	Requirements fulfilled. The software has taken enough measures to detect faults and avoid the architectural design of fault measures, refer to document [D02] and [D04].
	70 - Analytical measures and fault/error control techniques employed; clause: H.11.12.1.2, H.11.12.2.2, H.11.12.2.4; method: X	Requirements fulfilled. Analytical measures are FMEA and Static Code analysis are employed, See document [D10](code inspection report) and [D15].
	71 - Software fault/error detection time(s) for controls with software Classes B or C; clause: H.2.17.10, H.11.12.2.6; method: X.....	Requirements fulfilled. Software fault/error detection time(s) for controls are defined in [D02] [D04] [D12] and chapter 9.1 of this document.
	72 - Control response(s) in case of detected fault/error; clause: H.11.12.2.7; method: X.....	Requirements fulfilled. For controls with functions and detection of a fault/error results in the response declared in document [D02] [D04] [D12] and chapter 9.1 of this document.
	93 – Maximum number of reset actions within a time period; clause H.11.12.4.3.6, H.11.12.4.3.4; method: D	Requirements fulfilled. The reset function is limited to a certain time interval, see document [D02] [D04] [D12].
	94 – Number of remote reset actions; clause H.17.1.4.3; method: X.....	Requirement not applicable Not used in the project.

	m – Controls with software classes B or C had information provided for safety-related segments of the software. Information on the non-safety related segments was sufficient to establish that they did not influence safety-related segments	Requirements fulfilled. Safety-related segments of the software and non-safety related segments are designed in different modules and allocated to different storage spaces, refer to document [D02] [D04] [D12]
	n – Software sequence was documented and, together with the operating sequence, included a description of the control system philosophy, the control flow, data flow and the timings.....	Requirements fulfilled. This information is described in the software architecture design and SW Design Specification document. See document [D02] and [D04] (Software architecture design document).
	o - Safety-related data and safety-related segments of the software sequence, the malfunction of which could result in non-compliance with the requirements of Clauses 17, 25, 26 and 27, are identified.....	Requirements fulfilled. Identify the safety related data in the software sequence and this part of the function of the safety related section, and do the function safety, data protection and memory detection, refer to document [D02] (Safety Function Conception).
	– Included the operating sequence	Requirements not applicable. No operation is required to use the product.
	– Software fault analysis was related to the hardware fault analysis in Clause H.27	Requirements fulfilled. The software fault analysis refers to document [D04].
	q - Programming documentation was supplied in a programming design language declared by the manufacturer.....	Requirements fulfilled. The actual programming language is consistent with the manufacturer's declaration, and C language is used, see document [D10] (Software coding specification).
	r – Different software classes applied to different control functions	Requirements fulfilled. The functional safety requirements and levels of the project are derived from the concept of hazard analysis and functional safety. According to the traceability relationship, each functional safety has its own safety level, all are class B. For more details, refer to the document [D04].

	s - Measures declared are chosen by manufacturer from the requirements of Clauses H.11.12.1.2 to H.11.12.2.4 inclusive.....	Requirements fulfilled. The product meets single channel with functional test. Measures are declared with software class B. See document [D04] for details.
H.11	Constructional requirements	
H.11.12	Controls using software	
	Controls using software were so constructed that the software did not impair control compliance with the requirements of this standard	Requirements fulfilled. It has been confirmed that software did not impair control compliance with the requirements of this standard. The remote-control module operates in configuration and debugging mode, and the module code is partitioned and isolated, refer to [D04].
H.11.12.1	Requirements for the architecture	
H.11.12.1.1	Control functions with software class B or C use measures to control and avoid software-related faults/errors in safety-related data and safety-related segments of the software, as detailed in H.11.12.1.2 to H.11.12.3 inclusive	Requirements fulfilled. The software uses watchdog, timing monitoring, time slot monitoring and other measures. See document [D02] and [D04](Software architecture design document) for more information.
H.11.12.1.2	Control functions with software class C have one of the following structures:	
	– single channel with periodic self-Inspect and monitoring (H.2.16.7)	Requirement not applicable Software is class B.
	– dual channel (homogenous) with comparison (H.2.16.3)	Requirement not applicable Software is class B.
	– dual channel (diverse) with comparison (H.2.16.2)	Requirement not applicable Software is class B.
	Control functions with software class B have one of the following structures:	
	– single channel with functional test (H.2.16.5)	Requirement not applicable All safety functions comply with H.2.16.6.

	– single channel with periodic self-test (H.2.16.6)	Requirements fulfilled. All safety functions are single channel with periodic self-test and monitoring, more detail information see document [D02][D04][D12].
	– dual channel without comparison (H.2.16.1)	Requirement not applicable All safety functions comply with H.2.16.6.
H.11.12.1.3	Other structure permitted with equivalent level of safety to those in H.11.12.1.2.....	Requirement not applicable All safety functions comply with H.2.16.6.
H.11.12.2	Measures to control faults/errors	
H.11.12.2.1	Redundant memory with comparison provided on two areas of the same component: data stored in different formats	Requirements fulfilled. All memory data are designed to be redundant and heterogeneous. Check document [D02] and [D04]for more information.
H.11.12.2.2	Software class C using dual channel structures with comparison: additional fault/error detection means	Requirement not applicable Software is class B.
H.11.12.2.3	Software class B or C: means for recognition and control of errors in transmission to external safety-related data paths: Means took into account errors of data, addressing, transmission timing and sequence of protocol	Requirements fulfilled. It is taking into Errors of data, addressing, transmission timing and sequence of protocol and E2E measures, more information see document [D04] and Table 11 below in this document.
H.11.12.2.4	Software class B or C: within the control, measures are taken to address the fault/errors in safety-related segments and data indicated in Table H.1 and identified in Table 1 requirement 68.	Requirements fulfilled. The relevant assessment is shown in Table 11 below in this document.
H.11.12.2.5	Measures others than those specified in H.11.12.2.4 utilized to satisfy the requirements listed in Table H.1	Requirements fulfilled. All measures are applied according to Table H.1 of UL 60730-1 Annex H.
H.11.12.2.6	Software fault/error detection:	
	– occur not later than declared time(s), Table 1, requirement 71	Requirements fulfilled. Software fault/error detection time(s) for controls are defined in **Error! Reference source not found.** and chapter 9.1 of this file.

	– acceptability of declared time(s): evaluated during fault analysis of the control	Requirements fulfilled. The response time of all functional safety faults is far less than the fault tolerance time, see chapter 9.1 of this file or document [D12].
H.11.12.2.7	For controls with functions, classified as Class B or C, detection of fault/error:	
	– results in the response declared in Table 1, requirement 72	Requirements fulfilled. The response time of all functional safety faults is far less than the fault tolerance time, see chapter 9.1 of this file or document [D12].
	– for Class C: independent means capable of performing this response provided	Requirements not applicable. Software is class B.
H.11.12.2.8	Class C, dual channel structure, loss of dual channel capability: deemed to be an error	Requirement not applicable Software is class B.
H.11.12.2.9	Software referenced:	
	– to relevant parts of the operating sequence	Requirements not applicable. The software runs devices without user operation.
	– to the associated hardware functions	Requirements fulfilled. Hardware watchdog chip helps realize timing monitoring, see document [D12] for more information.
H.11.12.2.10	Labels used for memory locations are unique	Requirements fulfilled. Labels used for storage locations are constants or uniquely expressed by variable names, see document [D10] (code inspection report).
H.11.12.2.11	Software protected from user alteration of safety-related segments and data	Requirements fulfilled. Users cannot modify the code segment, and the parameter configuration will not change the security architecture. They can only configure within a limited data range. And there are complete integrity inspection and monitoring modules to ensure data security. It refers to document [D04] for more.

H.11.12.2.12	Software and safety-related hardware under its control is initialized to and terminates at a declared state, Table 1, requirement 66.....	Requirements fulfilled. The start and end of the software will return to the safe state, that is, the charging and discharging relay is disconnected, see document [D02](Safety Function Conception) and [D10] (code inspection report).
H.11.12.3	Measures to avoid errors	
H.11.12.3.1	For controls with software class B or C the measures shown in Figure H.1 to avoid systematic faults are applied	Requirements fulfilled. The fault avoidance measures in figure h.1 have been implemented and tested and verified. See relevant table h.1 evaluation items, see document [D02] [D04] for more information.
	Other methods utilized that incorporate disciplined and structured processes including design and Inspect phases	Requirements fulfilled. The design follows the design specifications and structured software, and has been completely tested, see document [D04].
H.11.12.3.2	Specification	
H.11.12.3.2.1	Software safety requirements	
H.11.12.3.2.1.1	The specification of the software safety requirements includes:	
	• A description of each safety related function to be implemented, including its response time(s): - functions related to the application including their related software classes - functions related to the detection, annunciation and management of software or hardware faults	Requirements fulfilled. All safety related functions, including detection functions, are gradually decomposed from architecture design to modules, and finally to unit design by technical traceability number and integrity inspection. See related document [D02].
	• A description of interfaces between software and hardware	Requirements fulfilled. Interfaces between software and hardware is descripted, see related document [D03] for more information.
	• A description of interfaces between any safety and non-safety related functions	Requirements fulfilled. interfaces between any safety and non-safety related functions described, see related document [D03] for more information.

H.11.12.3.2.2	Software architecture	
H.11.12.3.2.2.1	The description of software architecture includes the following aspects:	
	• Techniques and measures to control software faults/errors (refer to H.11.12.2)	Requirements fulfilled. The technologies and measures for controlling software faults / errors are fully applied, including the detection and software structure application, as well as the verification of program code during power on, [D04] (Software architecture design document).
	• Interactions between hardware and software	Requirements fulfilled. The interaction between software and hardware is fully defined in relevant documents. See document [D03] for complete information.
	• Partitioning into modules and their allocation to the specified safety functions	Requirements fulfilled. All modules of architecture design are numbered and have a traceability relationship with functional safety, which comes from the software design specification, see document [D04] for more information.
	• Hierarchy and call structure of the modules (control flow)	Requirements fulfilled. The module architecture is divided into three layers: application layer, logic layer and driver layer. Each module has a flow chart to clearly show the relationship between modules. See document [D04] for more information.
	• Interrupt handling	Requirements fulfilled. Considering the mutual monitoring between interrupt nesting and interrupt itself, the function of monitoring program timing is designed by using interrupt. See document [D04] for complete information.
	• Data flow and restrictions on data access	Requirements fulfilled. The data flow has a special control flow chart, and the program is designed in strict accordance with the flow chart. Access is restricted by authentication code, access quantity and other measures. Refer to document[D04].

	• Architecture and storage of data	Requirements fulfilled. There is a data storage module in the architecture design. The data storage makes the technical design of heterogeneous dual storage in different data storage areas and has data verification. Complete information see document [D02][D04].
	• Time based dependencies of sequences and data	Requirements fulfilled. Sequence and data time monitoring has been designed in the architecture, and the interrupt program feeds the external watchdog regularly, see document [D04]
H.11.12.3.2.2.2	The architecture specification is verified against the specification of the software safety requirements by static analysis	Requirements fulfilled. Complete information see document [D04]for detail.
H.11.12.3.2.3	Module design and coding	
H.11.12.3.2.3.1	Software is suitably refined into modules. Software module design and coding are implemented in a way that is traceable to the software architecture and requirements. The module design specified:	Requirements fulfilled. The software has architecture design and module design and has identification number and traceability, see document [D04].
	– function(s)	Requirements fulfilled. In the architecture design document, modules are decomposed layer by layer from the top module to the unit module, see document [D04].
	– interfaces to other modules	Requirements fulfilled. Each module description includes interface description and consistency check between interfaces, see document [D04].
	– data	Requirements fulfilled. The architecture design includes data flow control and data type description, see [D04] for information.

H.11.12.3.2.3.2	Software code is structured	Requirements fulfilled. The software is gradually decomposed into modules according to the architecture design, and the coding rules are written according to MISRA-C and the additional rules formulated by the company, see document [D09].
H.11.12.3.2.3.3	Coded software is verified against the module specification, and the module specification is verified against the architecture specification by static analysis	Requirements fulfilled. There are static analysis documents to verify the module code design, see document [D10].
H.11.12.3.2.4	Design and coding standards	/
	Program design and coding standards is used during software design and maintenance	Requirements fulfilled. See document [D10] (code inspection report) for more.
	Coding standards	
	– specified programming practice	Requirements fulfilled. There are verification documents, see document [D10] (code inspection report).
	– proscribed unsafe language features	Requirements fulfilled. It proscribed unsafe language features, mainly based on MISRA C 2004, see document [D09] (Software coding specification) for more information.
	– specify procedures for source code documentation	Requirements fulfilled. Source code development follows the rule, more information refer to unit code list and Programing file.
	– specify data naming conventions	Requirements fulfilled. The coding specification has a data naming convention, and the design follows the coding specification, see document [D09][D10].
H.11.12.3.3	Testing	
H.11.12.3.3.1	Module design (software system design, software module design and coding)	

H.11.12.3.3.1.1	A test concept with suitable test cases is defined based on the module design specification.	Requirements fulfilled. There are test concept documents to describe the test purpose, test standards, test specifications, etc. See document [D11][D12].
H.11.12.3.3.1.2	Each software module is tested as specified within the test concept	Requirements fulfilled. See document[D11][D12] for detail.
H.11.12.3.3.1.3	test cases, test data and test results are documented	Requirements fulfilled. See document [D11][D12] for more.
H.11.12.3.3.1.4	Code verification of a software module by static means includes such techniques as software inspections, walk-throughs, static analysis and formal proof	Requirements fulfilled. See document [D10][D11][D12] for more information.
	Code verification of a software module by dynamic means includes functional testing, white-box Inspecting and statistical testing	Requirements fulfilled. See document [D10][D11][D12] for more information.
H.11.12.3.3.2	Software integration testing	
H.11.12.3.3.2.1	A test concept with suitable test cases is defined based on the architecture design specification	Requirements fulfilled. There are test concept documents to describe the test purpose, test standards, test specifications, see document [D10][D11][D12].
H.11.12.3.3.2.2	The software is tested as specified within the test concept	Requirements fulfilled. Tests that have been applied within test concept, see document [D10][D11][D12] for more information.
H.11.12.3.3.2.3	Test cases, test data and test results are documented	Requirements fulfilled. See document [D10][D11][D12] for more.
H.11.12.3.3.3	Software validation	
H.11.12.3.3.3.1	A validation concept with suitable Inspect cases is defined based on the software safety requirements specification	Requirements fulfilled. Software test confirmation has been reflected in the test report, see document [D10][D11][D12].

H.11.12.3.3.3.2	The software is validated with reference to the requirements of the software safety requirements specification as specified within the validation concept	Requirements fulfilled. The software is validated with reference to the requirements of the software safety requirements specification.
	The software is exercised by simulation or stimulation of:	
	• input signals present during normal operation	Requirements fulfilled. The software has been exercised by simulation refer to [D11].
	• anticipated occurrences	Requirements fulfilled. See document [D11]. for more information.
	• undesired conditions requiring system action	Requirements fulfilled. See document [D11]. for more information.
H.11.12.3.3.3.4	Test cases, test data and test results are documented	Requirements fulfilled. See document [D11]. for more information.
H.11.12.3.4	Other Items	
H.11.12.3.4.1	Equipment used for software design, verification and maintenance was qualified appropriately and demonstrated to be suitable for purpose in manifold applications	Requirements fulfilled. The equipment has calibration records and has been verified to meet the requirements of testing, refer to document [D11].
H.11.12.3.4.2	Management of software versions: All versions are uniquely identified for traceability	Requirements fulfilled. There are special software version management specifications and management software version, see document [D10] (code inspection report).
H.11.12.3.4.3	Software modification	
H.11.12.3.4.3.1	Software modifications are based on a modification request which details the following:	/
	• the hazards which may be affected	Requirements fulfilled. There is a special hazard analysis, see document [D02].

	• the proposed change	Requirements fulfilled. The purpose of design change is described in document [D14].
	• the reasons for change	Requirements fulfilled. The reasons of design change are described in document [D14].
H.11.12.3.4.3.2	An analysis is carried out to determine the impact of the proposed modification on functional safety.	Requirements fulfilled. Impact analysis and risk assessment on the modified part. It refers to [D14].
H.11.12.3.4.3.3	A detailed specification for the modification is generated including the necessary activities for verification and validation, such as a definition of suitable Inspect cases	Requirements fulfilled. There are special modified detailed specifications, see document [D14].
H.11.12.3.4.3.4	The modification is carried out as planned	Requirements fulfilled. All modifications are carried out in accordance with the process specification, refer to [D14].
H.11.12.3.4.3.5	The assessment of the modification is carried out based on the specified verification and validation activities.	Requirements fulfilled. Confirmation and evaluation are carried out in strict accordance with the process, see document [D14].
H.11.12.3.4.3.6	All details of modification activities are documented	Requirements fulfilled. See description above.
H.11.12.3.5	For class C control functions: One of the combinations (a–p) of analytical measures given in the columns of table H.9 is used during hardware development	Requirements not appliable. Software is class B.
H.11.12.4	Remotely actuated control functions	

H.11.12.4.1.1	Data Exchange – General – Remotely actuated control functions are connected to separate, independent devices, which may themselves contain control functions or provide other information and any data exchange between these devices does not compromise the integrity of class B control function or class C control function.	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.1.2	Type of data - Message types for data exchange in a control function or functions are allocated to class A control function, class B control function or class C control function. The safety or protective relevance or influence, message types or data exchange are allocated only to class B control function or class C control functions, see Table H.10.	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.1.3.1	Communication of Safety Related Data – Transmission – Safety relevant data is transmitted authentically concerning:	/
	– data corruption	Requirement not applicable. No remotely actuated control functions.
	– address corruption	Requirement not applicable. No remotely actuated control functions.
	– wrong timing or sequence	Requirement not applicable. No remotely actuated control functions.
	Data variation or corrupted data did not lead to an unsafe state	Requirement not applicable. No remotely actuated control functions.
	Before transmitted data was used it was ensured that data corruption, address corruption and wrong timing or sequence are addressed using the measures as given in Annex H.	Requirement not applicable. No remotely actuated control functions.
	The following failure modes are addressed.....	/
	– permanent “auto-sending” or repetition,	Requirement not applicable. No remotely actuated control functions.

	– interruption of data transfer	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.1.3.2	Access to data exchange - All types of access to class B control function or class C control function related data exchange systems is clearly restricted	Requirement not applicable. No remotely actuated control functions.
	Adequate hardware/software measures are taken to prevent unauthorized access to the control functions (class B and C; operating data, configuration parameters and/or software modules)	Requirement not applicable. No remotely actuated control functions.
	Access to data exchange of class B control function or class C control function related operating data through public networks, has appropriate cryptographical techniques implemented.	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.1.3.3	For class B and class C software revisions the requirements of H.11.12.3 and hardware configuration management are applied, and the control maintains its protective functions	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.1.4	Remotely actuated control function operation have the duration or limits set before switching on except when automatic switching off is realized at the end of a cycle or the system is designed for permanent operation.	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.2	Priority of remotely actuated control functions over control functions does not lead to a hazardous condition.	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.3.1	Remote reset action is manually initiated.	Requirement not applicable. No remotely actuated control functions.
	Reset functionality initiated by a hand-held device required at least two manual actions to activate	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.3.2	Reset functions are capable of resetting the system as intended	Requirement not applicable. No remotely actuated control functions.

H.11.12.4.3.3	Unintended resets from safe state do not occur.	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.3.4	Any fault of the reset function does not cause the control or controlled function to result in a hazardous condition, and was evaluated for its Class B classification	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.3.5	For reset functions initiated by manual action not in visible sight of the appliance, the following additional requirements apply:	Requirement not applicable. No remotely actuated control functions.
	– the actual status and relevant information of the process under control is visible to the user before, during and after the reset action;	Requirement not applicable. No remotely actuated control functions.
	– the maximum number of reset actions within a time period is declared. Following this, any further reset is denied unless the appliance is physically checked	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.3.6	The reset function is evaluated on the final application.	Requirement not applicable. No remotely actuated control functions.
	Manual switching of a thermostat or device with similar function that activates a reset is declared by the manufacturer and is suitable in the final application	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.4	Software Download and Installation	
	Software updates provided by the manufacturer and transmitted to the control via remote communication were checked prior to its use:	/
	– against corruption through communication ensuring Hamming distance 3 for software class B, or Hamming distance 4 for software class C;	Requirement not applicable. No remotely actuated control functions.

	– that the software version is compatible with the hardware version of the control according to the version management documentation.	Requirement not applicable. No remotely actuated control functions.
	The software which performs the above-mentioned checks had measures to control the fault/error conditions specified in H.11.12.2.	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.4.2	In case of software download via remote communication, the cryptographic techniques in H.11.12.4.5 were provided. In addition to the requirements in H.11.12.4.5, identification procedures were provided for the software packages.	Requirement not applicable. No remotely actuated control functions.
	The cryptographic techniques employed were part of the control, did not rely upon part of the router or similar data transmission device itself, and were performed prior to transmission.	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.4.3	Each update of software had provisions for authorization by the user and a version ID number which were accessible.	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.4.4	The installation of class B software or class C software was permitted during and after which the software installation process the control remained in compliance with the requirements of this standard.	Requirement not applicable. No remotely actuated control functions.
H.11.12.4.5	Cryptographical techniques	
	In cases where class B control function or class C control function related operating data, configuration parameters and/or software modules were transmitted over a public network, and/or where software updates were provided by the manufacturer via remote communication, cryptographic techniques were employed.	Requirements not applicable. No use a public network.
H.27.1.2	Protection against internal faults to ensure functional safety	

H.27.1.2.1	Design and construction requirements	
H.27.1.2.1.1	Fault avoidance and fault tolerance	
	Controls incorporating control functions of class B or C are designed according to H.27.1.2 taking into account the failure modes of Cl. H.11.12 for software	Requirements fulfilled. Controls with control functions are designed according to H.27.1.2 considering the failure modes of IC. H.11.12 for software, see document [D04].
	Systematic errors are avoided	Requirements fulfilled. Systematic errors are avoided refer to document [D04].
	Random faults are dealt with by a proper system configuration	Requirements fulfilled. A special watchdog monitoring module is designed to monitor the random faults of the software, please see document [D04] for more information.
	Functional analysis of the application resulted in a structured design with:	/
	– Control flow	Requirements fulfilled. Control flow is described in document [D02][D04].
	– Data flow	Requirements fulfilled. Data flow is described in document [D02][D04].
	– Time related functions required by the application	Requirements fulfilled. In the design of software modules, there are descriptions of module time requirements, including cycle and other parameters, refer to document [D02][D04].
	For custom-chips special attention was made to minimize systematic errors	Requirements not applicable. No custom-chips.
	System configuration was failsafe or:	/

	Incorporated components with direct safety-critical functions guarded by safeguards that cause a completely independent safety shut-down in accordance to H.11.12 software class B or C:	/
	- safeguards are built into hardware and,	Requirements fulfilled. See document [D03] for more information.
	- safeguards are supplemented by software	Requirements fulfilled. Safeguards are supplemented by software Refer to [D04].
	Time slot monitoring is sensitive to both an upper and a lower limit of the time interval.	Requirements fulfilled. See document [D04] description.
	Faults resulting in a shift of the upper and/or lower limit are taken into account.	Requirements fulfilled. The influence of hardware parameter changes caused by temperature and other environments is considered. See document [D02].
	In a class C control function when a single fault in a primary safeguard can render the safeguard inoperative, a secondary safeguard is provided	Requirement not applicable. Software is Class B.
	The reaction time of the secondary safeguard is in accordance with Clause H.27.1.2.3.	Requirement not applicable. Software is Class B.
H.27.1.2.1.2	Documentation	
	The documentation was based on H.11.12.3.2	Requirements fulfilled.
	The functional analysis of the control and the safety related programs under its control are documented in a clear hierarchical way in accordance with the safety philosophy and the program requirements.	Requirements fulfilled. Relevant information is described in the security concept and architecture design, see document [D04].
	Documentation provided for assessment included:	

	• A description of the system philosophy, the control flow, data flow and timings.	Requirements fulfilled. Refer to document [D04].
	• A clear description of the safety philosophy of the system with all safeguards and safety functions clearly indicated. Sufficient design information is provided to enable the safety functions or safeguards to be assessed	Requirements fulfilled. A clear description of the safety philosophy of the system with all safeguards and safety functions clearly indicated, see document [D04].
	• Documentation for any software within the system	Requirements fulfilled. See document unit code list and Programing file.
	Programming documentation is supplied in a programming design language declared by the manufacturer.....	Requirements fulfilled. Programming Language: C The code development complies with code rule, see document [D09].
	Safety related data and safety related segments of the operating sequence are identified and classified according to H.11.12.3	Requirements fulfilled. There are relevant timing monitoring and module management in the software architecture design, see [D04].
	There is a clear relationship between the various parts of the documentation	Requirements fulfilled. The documents are generated according to the product concept to design, and the corresponding documents are generated according to the process of traceability and development. See document [D04].
H.27.1.2.2	Class B control function	
H.27.1.2.2.1	Design and construction requirements	
	Control function shall be designed such that under single fault conditions it remains in or proceeds to the defined state.	Requirements fulfilled. All-important single faults related to safety will be detected and identified and enter the safe state, refer to test report [D04].
H.27.1.2.3	Class C control function	
H.27.1.2.3.1	Design and construction requirements	

	Control function shall be designed such that under first and second fault conditions it remains in or proceeds to the defined state.	Requirement not applicable. It a class B software
H.27.1.2.5	Circuit and construction evaluation	
H.27.1.2.5.3	Assessment	
	Only the safety related software (software class B and C) as identified according to H.27.1.2.1.2 were subjected to further assessment	Requirements fulfilled. The following documents are provided: 1. A description of the system philosophy, the control flow, data flow and timings. 2. Description of system safety concept and relevant documents, including all safeguard measures and functions clearly indicated by safety measures. 3. Software architecture design, detailed design, and other test documents.

Table 10: Checklist of UL 60730-1:2016 Annex H

Component	Fault / Error	Measures description
1.1 CPU Registers	Stuck at DC Fault	Requirements fulfilled. For more information, please refer to the documentation for [D02][D04][D12].
1.3 CPU Program counter	Stuck at DC fault	Requirements fulfilled. For more information, please refer to the documentation for [D02][D04][D12].
2 Interrupt handling and execution	No interrupt or too frequent Interrupt No interrupt or too frequent interrupt related to different sources	Requirements fulfilled. For more information, please refer to the documentation for [D02][D04][D12].
3 Clock	Wrong frequency (for quartz synchronized clock: harmonics/ subharmonics only)	Requirements fulfilled. For more information, please refer to the documentation for [D02][D04][D12].
4.1 Memory Invariable memory	All single bit faults 99,6 % coverage of all information errors	Requirements fulfilled. For more information, please refer to the documentation for [D02][D04][D12].

4.2 Memory Variable memory	DC fault & DC fault and dynamic cross links	Requirements fulfilled. Same as above 4.1.
4.3 Memory Addressing (relevant to variable and invariable memory)	Stuck at & DC fault	Requirements fulfilled. For more information, please refer to the documentation for [D02][D04][D12].
5.1 Internal data path Data	Stuck at & DC fault	Requirements fulfilled. For more information, please refer to the documentation for [D02][D04][D12].
5.2 Internal data path Addressing	Wrong address & Wrong address and multiple addressing	Requirements fulfilled. For more information, please refer to the documentation for [D02][D04][D12].
6.0-6.1 External communication Data	Hamming distance 3 & Hamming distance 4	Requirements fulfilled. For more information, please refer to the documentation for [D04].
6.2 External communication Addressing	Wrong address & Wrong and multiple addressing	Requirements fulfilled. For more information, please refer to the documentation for [D04].
6.3 External communication Timing	Wrong point in time & Wrong sequence	Requirements fulfilled. For more information, please refer to the documentation for [D04].
7.1 Input/output periphery Digital I/O	Fault conditions specified in H.27	Requirements fulfilled. For more information, please refer to the documentation for [D02][D04][D12].
7.2.1 Input/output periphery Analog I/O A/D- and D/A-convertor	Fault conditions specified in H.27	Requirements fulfilled. For more information, please refer to the documentation for[D02][D04][D12].
7.2.2 Input/output periphery Analog I/O Analog multiplexer	Wrong addressing	Requirements fulfilled. For more information, please refer to the documentation for[D02][D04][D12].
9. Custom chips e.g., ASIC, GAL, Gate array	Any output outside the static and dynamic functional specification	Requirements not applicable. No custom chips.

Table 11: Checklist of Measures to address fault/errors.

----------End of the report----------