Technical Report for Functional Safety

Report No.: SHFS220400014271

August. 04th, 2022

Client / Applicant:	GoodWe Technologies Co., Ltd. No.90 Zijin Rd., New District, Suzhou, China.
Manufacturer:	Same as applicant.
Project Title:	PV inverter
Module No.:	GW5000-MS-US30 /GW6000-MS-US30 /GW7600-MS-US30 / GW9600-MS-US30 /GW11K4-MS-US30 /GEP5.0-1-US30 / GEP6.0-1-US30 /GEP7.6-1-US30 /GEP9.6-1-US30 /GEP11.4-1-US30
Tested Standards:	UL 1998, Third Edition, Dated December 18, 2013.
Conclusion	In this report, safety protection function of PV inverter was assessed to achieved class 1 according to UL 1998, 3rd edition, Date December 18, 2013, 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 1998, 3rd edition, Date December 18, 2013.

-Proofs that process and methods are established at the manufacturer guaranteeing that unexceptionable processes.

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 (Shanghai) Co., Ltd.	Bob Jin	Jerry Zheng

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

CONTENTS

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

Summary of assessment

This technical report summarizes the safety performance evaluation results towards the software safety functions in PV inverter [Model No.: **GW5000-MS-US30 /GW6000-MS-US30 /GW7600-MS-US30 /GW9600-MS-US30 /GW11K4-MS-US30 /GEP5.0-1-US30 / GEP6.0-1-US30 /GEP7.6-1-US30 /GEP9.6-1-US30 /GEP11.4-1-US30**], provides by GoodWe Technologies Co., Ltd. (consecutively in the report referred as GoodWe). The five models beginning with GW (xx) and GEP (xx) have the same function and design, and the difference is only in the description of the model.

No deviations were found during the assessment acc. To UL 1998, 3rd edition, Date December 18, 2013, for safety related software functions in PV inverter 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 Model No.: **GW5000-MS-US30 /GW6000-MS-US30 /GW7600-MS-US30 /GW9600-MS-US30 /GW11K4-MS-US30 /GEP5.0-1-US30 /GEP6.0-1-US30 /GEP7.6-1-US30 /GEP9.6-1-US30 /GEP11.4-1-US30** PV inverter have been assessed:

Identification	Safety Critical Function Items
SF01	Safety protection function against Electric Arc.
SF02	Safety protection function for low insulation value.
SF03	Over temperature protection of environment.
SF04	Leakage current protection of Grid.

Table 1: Safety functions definition

Supplementary Information:

[1] UL 1998, 3rd edition, Date December 18, 2013, 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 1998, 3rd edition, Date December 18, 2013, towards software Class 1.

1. Assessment Period

Beginning of project: 2022-04-25
End of project: 2022-08-04

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国·上海·松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

2. References

No.	Document Description
[D1]	Quality Management Certificate of ISO9001.
[D2]	Development plan of software.
[D3]	SW Design Spec. for UL1998_20220801.
[D4]	Software compilation and development tools.
[D5]	GoodWe C language programming specification_ V2.0.
[D6]	Software version management tool.
[D7]	Software source codes.
[D8]	Software architecture design specification and software design.
[D9]	Software static code test review report.
[D10]	Electronic schematic diagram of TH290-10350-00(190-10153-00)
[D11]	Electronic schematic diagram of TH290-10351-00(190-10153-00)
[D12]	Electronic schematic diagram of TH290-20167-00(190-20024-00)
[D13]	Electronic schematic diagram of TH290-30031-00(190-30029-00)
[D14]	Electronic schematic diagram of TH290-40123-00(190-40096-00)
[D15]	Electronic schematic diagram of TH290-40183-00(190-40096-00)
[D16]	Electronic schematic diagram of TH290-70340-00(190-70181-00)
[D17]	Electronic schematic diagram of TH290-70376-00(190-70181-00)
[D18]	Electronic schematic diagram of TH290-90047-01(190-90036-00)
[D19]	Electronic schematic diagram of TH290-90048-00(190-90050-00)
[D20]	Risk analysis methods and results.
[D21]	MS G3 FMEDA UL1998_v20210729.
[D22]	Modbus communication protocol of main and auxiliary DSP.
[D23]	MS-US safety instructions for arc striking function.
[D24]	MS G3(North America) ISO temperature failure IMI Single failure analysis report.
[D25]	MS-US AFCI single fault analysis 220519.

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

[D26]	MS_G3 microelectronic fault test report.
[D27]	Safety function test plan and test report.
[D28]	MS G3 safety critical component BOM list.
[D29]	MS G3 safety critical component derating design.
[D30]	MS G3 parameters specification.
[D31]	Firmware changed record.
[D32]	MS-US AFCI firmware changed record.
[D33]	CDF-20220628 add substitute materials.

Table 2: References and documents

3. Revision Logs

Version	Changes Description
V1.0	Initial Version

Table 3: Revision logs

4. Symbols and abbreviated terms

Abbreviation	Description
Power Board	功率板
Com-Board	通信板
Output Board (STL)	输出板(塞特勒)
Output Board	输出板
LED Board	灯板
Core Board	核心板
Base Board	基板
WDT	Watch Dog Timer
SPWM	Sine Pulse Width Modulator
ADC	Analog to Digital Converter
MPPT	Maximum Power Point Tracking
PLL	Phase Locked Loop
ROCOF	Rate of Change of Frequency

SF	Safety Function
MCU	Microcontroller Unit
OC	Over Current

Table 4: Abbr. and Terms

5. Design and Development Tools

No.	Type of Tool	Vendor	Tool Name	Revision
1	Version Control	NA	Git	2.35.1
2	Development Tool	ST	MDK-Arm	V5.26.2.0
3	Compiler	ST	ST-Link	V2
4	Simulation	Power simtech	PSIM	V9.0
5	Schematic & PCB design	Altium	Altium Designer	16.1.0

Table 5: Design tools

6. HW Design Description

MCU Name	Input /Output	HW Description	SW Description	Marks
PB7	Output	50mA_TEST_CPU	Current output test	GFCI detection
PB1	Input	S_VGFCI	GFCI Current test	GFCI detection
PB5	Output	ISO_RLY1_CPU2	ISO relay control pin	ISO detection
PA4	Input	S_ISO_AD	ISO voltage sample	ISO detection
PB4	Output	AFCI_IO3_CPU2	Arcing detection	ARC detection
PB3	Input	AFCI_IO4_CPU2	Arcing fault reception	ARC detection
ADCINC6	Input	C14/GPIO60	Radiator temperature sampling	Temperature detection.
PA5	Input	Pwr rating select1	Power identification I/O	Power detection
PA6	Input	Pwr rating select2	Power identification I/O	Power detection
PA7	Input	Pwr rating select3	Power identification I/O	Power detection
PF2-NRST	Input	Main DSP reset slaver DSP signal	Slaver ARM reset signal	DSP related
PA0	Output	M_DSP monitor fail	Relay 0 drive signal	DSP related

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

PA15	Output	AFCI slaver to master	To Master DSP fault signal	DSP related
GPIO115	In/Out	AFCI_OUT_IO_1	Com with DSP	ARC Detect
GPIO97	Output	AFCI_OUT_IO_2	Arc alarm signal	ARC Detect
Note: More definition details refer to Software Detailed Design Description [D3].				

Table 6: HW design description

7. Assessment Item Information

Item description	:	Same describe as first page.
Model reference	:	Same describe as first page.
GW5000-MS-US30 / GEP5.0-1-US30	:	Power: 5.0kw
GW6000-MS-US30 / GEP6.0-1-US30	:	Power: 6.0kw
GW7600-MS-US30 / GEP7.6-1-US30	:	Power: 7.6kw
GW9600-MS-US30 / GEP9.6-1-US30	:	Power: 9.6kw
GW11K4-MS-US30 / GEP11.4-1-US30	:	Power: 11.4kw

HW Module Name	HW Version	SW Ver	Config Description
Power Board (11.4KW):	00(410-01013-00) 00(410-01014-00) 02(410-02019-02)	00	9.6kw / 11.4kw
Power Board (7.6KW):	00(410-01013-00) 00(410-01014-00) 02(410-02019-02)	00	5kw /6kw /7.6kw
Com-Board (11.4KW):	N/A	00	9.6kw / 11.4kw
Com-Board (7.6KW):	N/A	00	5kw /6kw /7.6kw
Output Board (STL):	N/A	00	All Models, Choose 1 of the 2 boards.
Output Board (HF):	N/A	00	
LED Board:	N/A	00	All Models
WIFI/LAN Core Board:	01 (410-02054-01)	01	Optional
WIFI/4G Core Board:	01 (410-02054-01)	01	Optional
WIFI/BT Core Board:	01 (410-02054-01)	01	Optional
Base Board:	N/A	01	Optional
USB Adapter Board:	01	N/A	Optional

Table 7: HW & SW Version and Config description

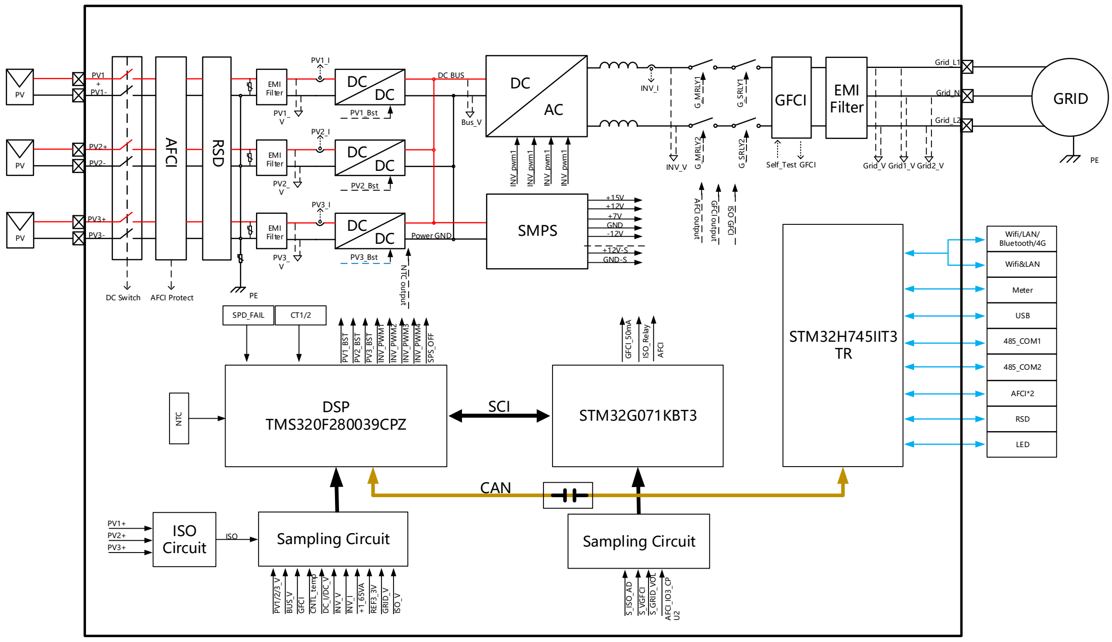


Figure 1 PV Inverter System Architecture

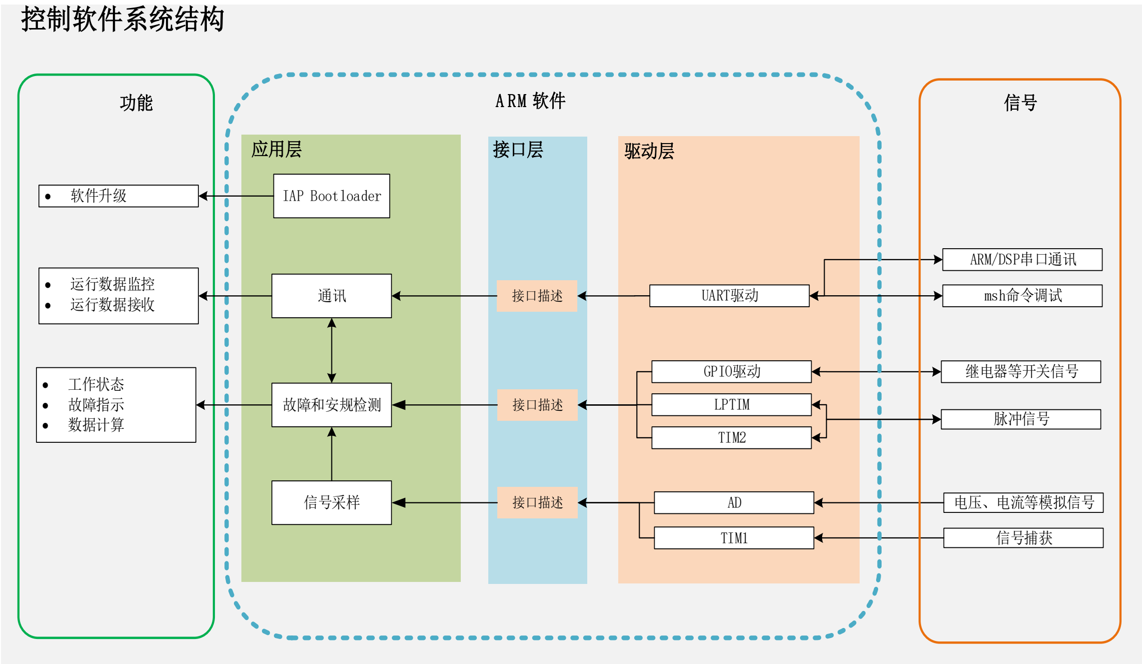


Figure 2 SW Architecture

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国·上海·松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

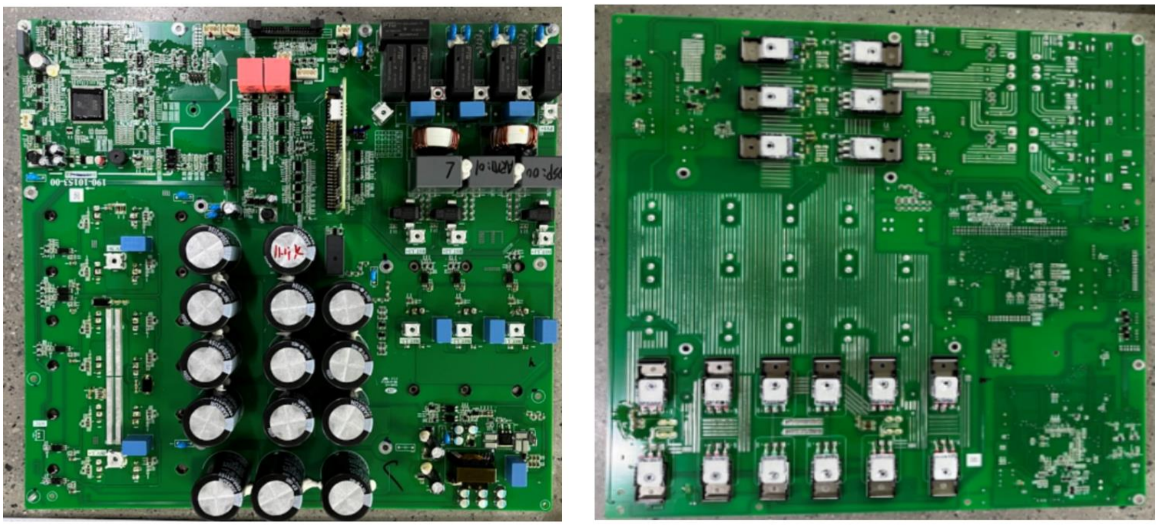


Figure 3 Photo view of Power Board (11.4kw)

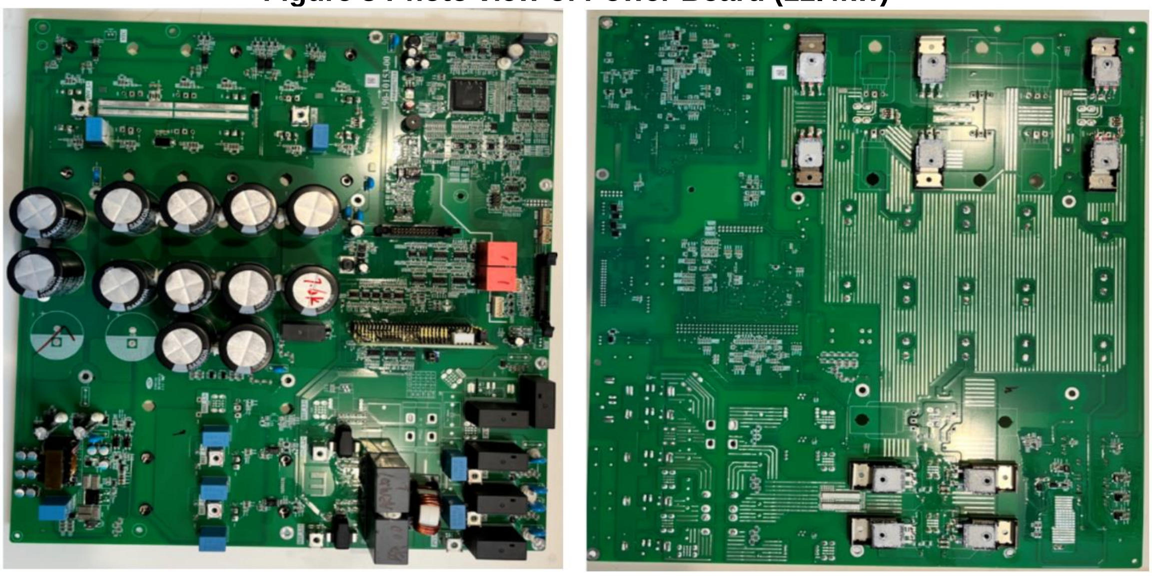


Figure 4 Photo view of Power Board (7.6kw)

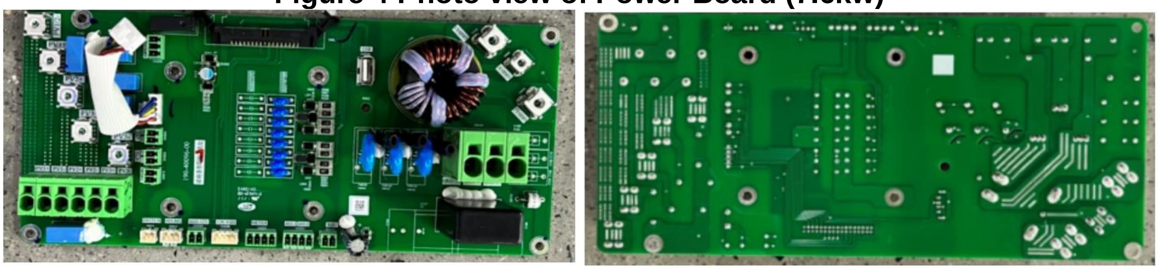


Figure 5 Photo view of Com-Board (11.4kw)

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

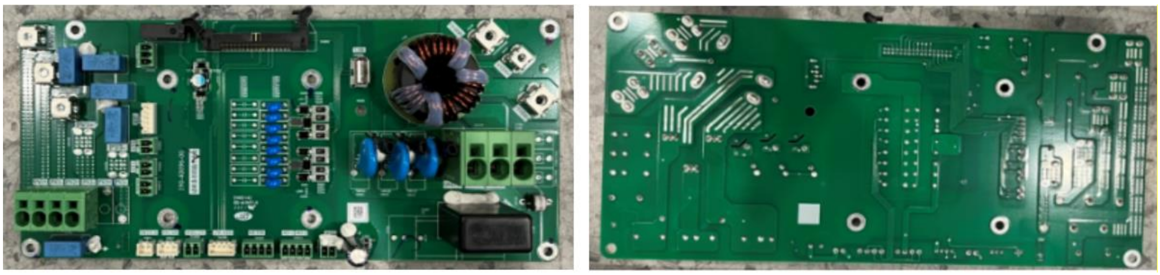


Figure 6 Photo view of Com-Board (7.6kw)

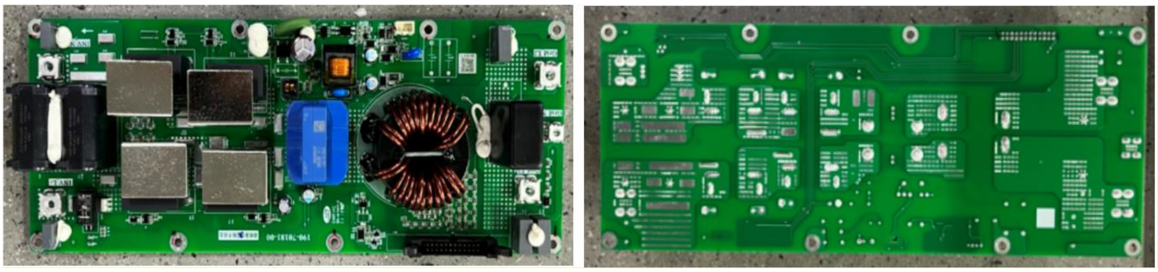


Figure 7 Photo view of Output Board (STL)

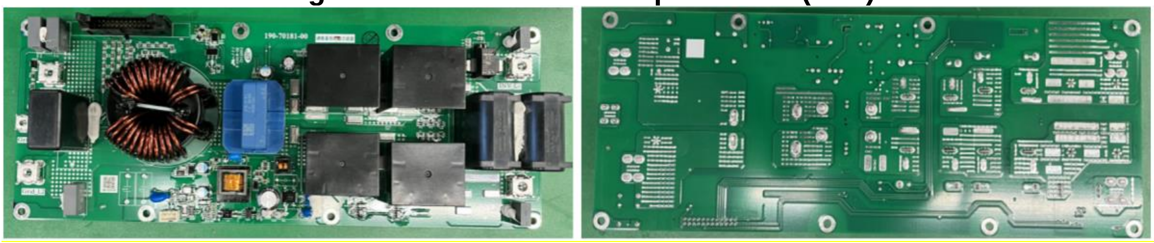


Figure 8 Photo view of Output Board (HF)

Figure 9 Photo view of LED Board

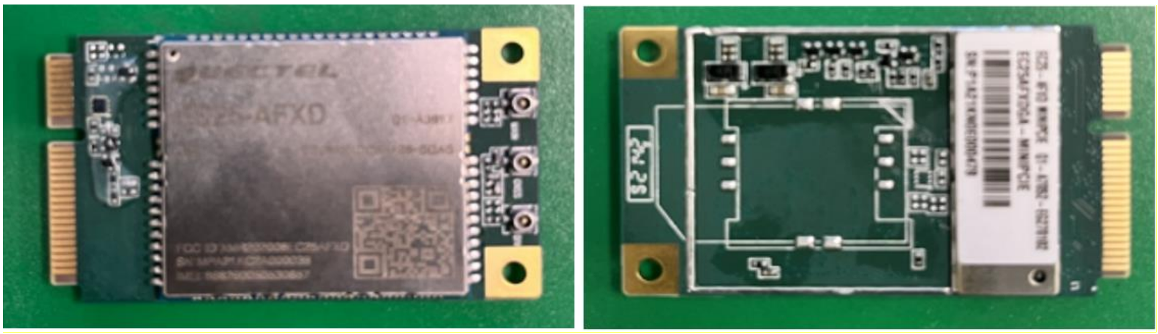


Figure 10 Photo view of WIFI-4G- Core Board

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

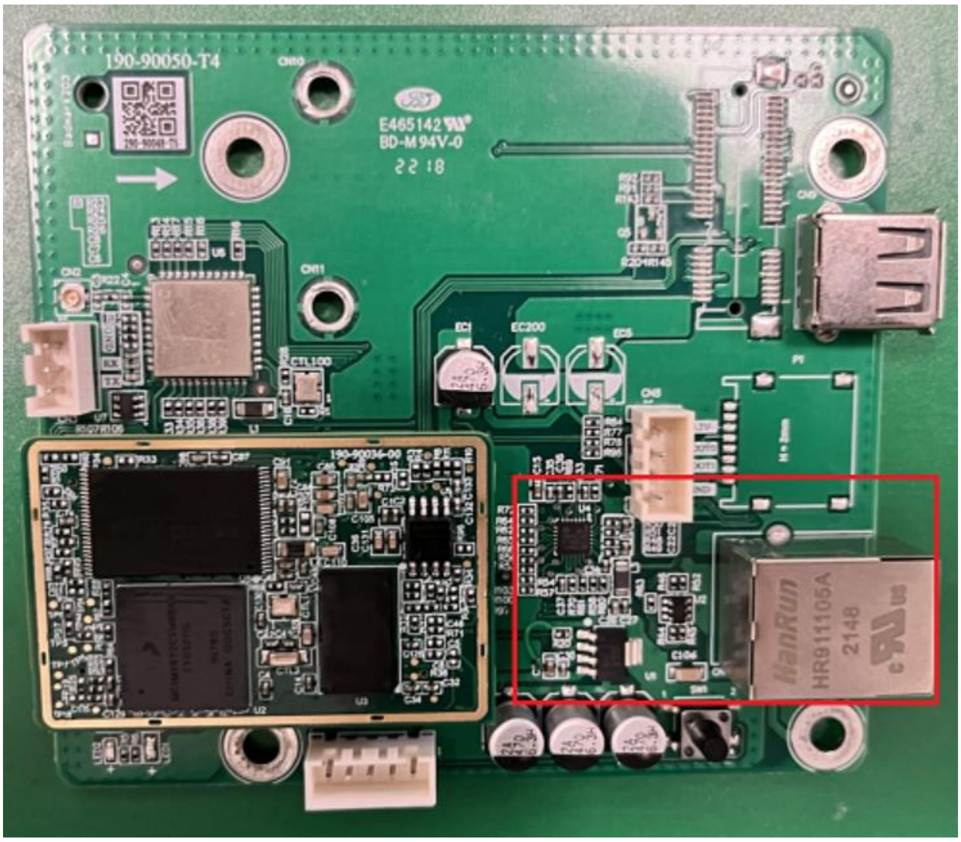


Figure 11 Photo view of WIFI-LAN- Core Board

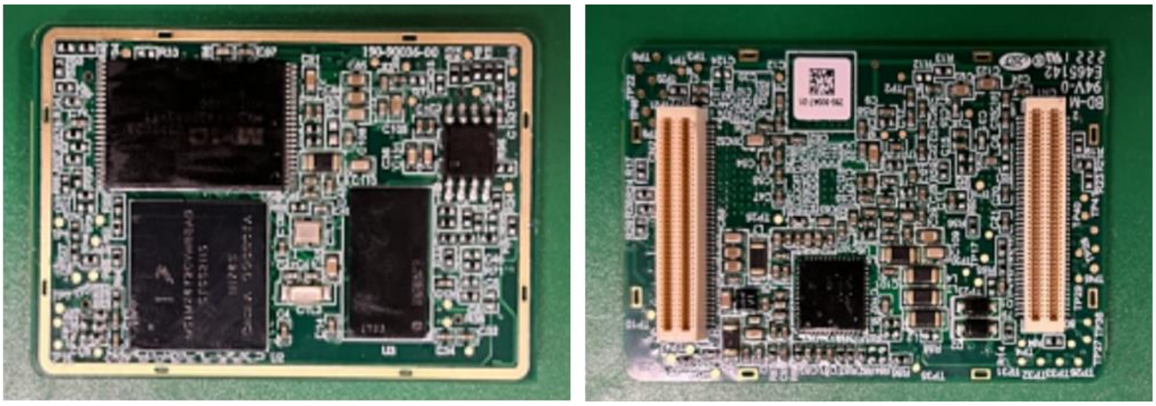


Figure 12 Photo view of WIFI-BT- Core Board

SGS-CSTC Standards Technical Services (Shanghai) Co.,Ltd. Testing Center E&E Safety Laboratory
NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

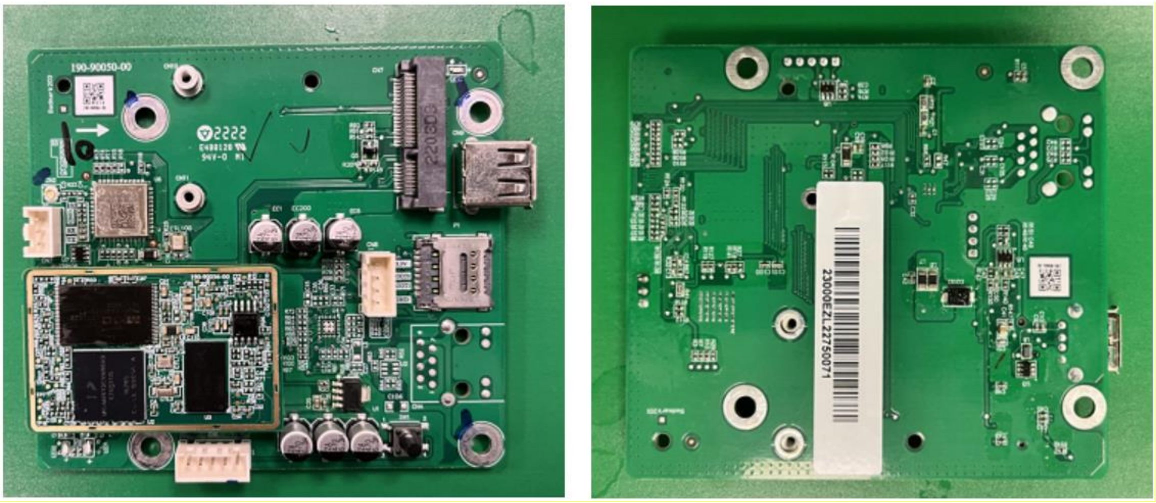


Figure 13 Photo view of Base Board

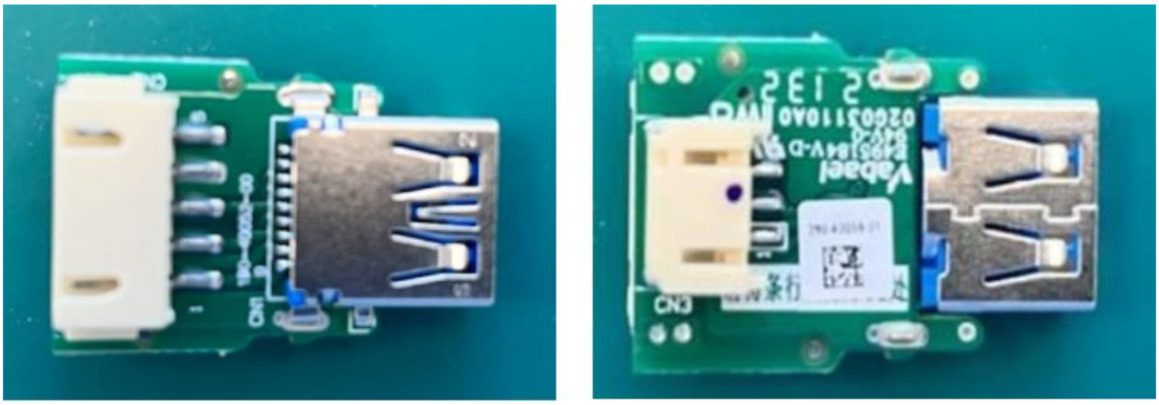


Figure 14 Photo view of USB Adapter Board

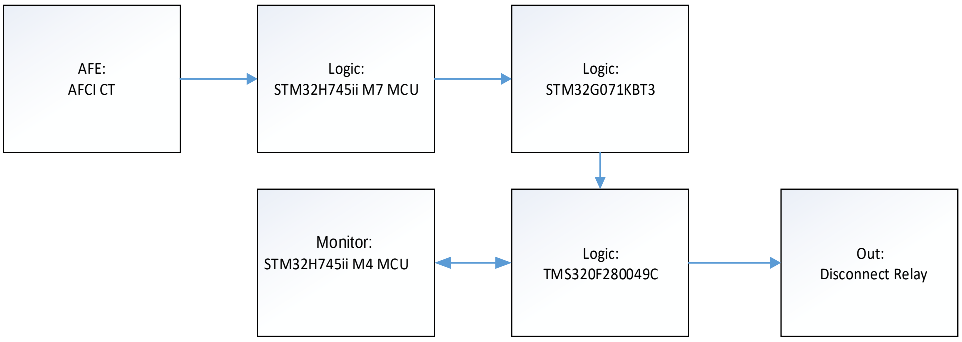
8. SW Safety Requirement Specification

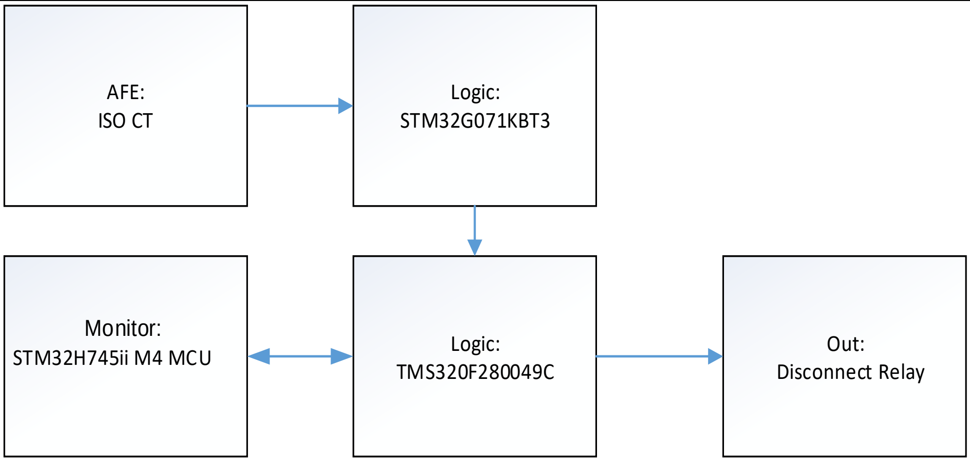
8.1. Safety Function Definition

The below protection functions of AC Wallbox Charging Station shall be defined as safety function, refer to **Table 1: Safety functions definition**.

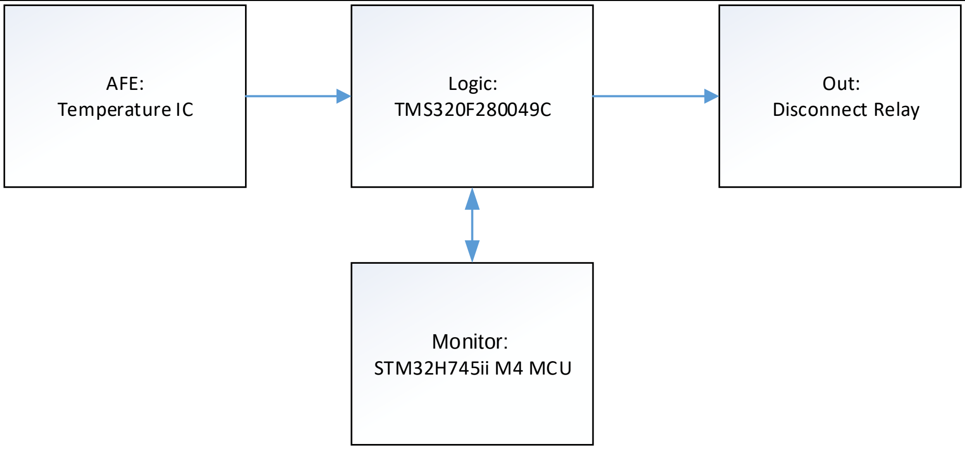
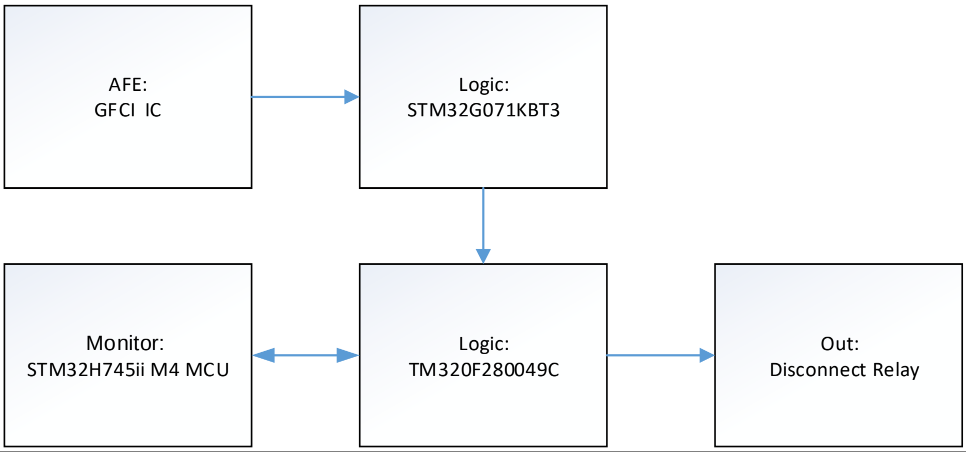
The details requirements for above safety functions specified as following tables:

Ident.	
SRS01	Safety function: Safety protection function against Electric Arc.
	1. Function Safety Circuit Structure

	Single channel with periodic self-test and monitoring. 
	2. Safety state description 2.1 Fault Detection The arcpulling module inputs the sampled signal into the AI algorithm model and obtains the arc-pulling probability of a sampling period. If the probability is greater than different thresholds, such as: Probility > 0.8, the arc-pulling count value +5; Probility > 0.9, the arc-pulling count value +10; Respectively, and the arc-pulling When the count value exceeds 20, the arc alarm signal will be output. The shortest three sampling period is about 50ms, and the longest 2s can send the arc alarm signal 2.2 Fault Recovery Wait 5 minutes to clear the fault information, start self-checking. 2.3 Enter the safety state Cut off the Gird Relay and Warning by CAN Bus to upper Level.
	3. Fault tolerance time interval Time：2.5s
SRS02	Safety function: Safety protection function for low insulation value
	1. Function Safety Circuit Structure Single channel with periodic self-test and monitoring.

	
	2. Safety state description 2.1 Fault Detection Checking when the inverter self-checks ,The Value of ISO less than 100KΩ and duration 20ms. 2.2 Fault Recovery Wait 5s to clear the fault information, start self-checking. 2.3 Enter the safety state Cut off the Gird Relay and Warning by CAN Bus to upper Level.
	3. Fault tolerance time interval Time:1s
SRS03	Safety function: Over temperature protection of environment
	1.Function Safety Circuit Structure Single channel with periodic self-test and monitoring.

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

	
	2. Safety state description 2.1 Fault Detection The Value of Temperature > 85℃ and duration 2s. 2.2 Fault Recovery The Value of Temperature < 80℃ and duration 5s. 2.3 Enter the safety state Cut off the Gird Relay and Warning by CAN Bus to upper Level.
	3. Fault tolerance time interval Time:5s
SRS04	Safety function: Leakage current protection of Grid.
	1. Function Safety Circuit Structure Single channel with periodic self-test and monitoring. 

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国 · 上海 · 松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

	2. Safety state description 2.1 Fault Detection Sequential value of leakage current is more than 30mA and duration 120ms. Sequential value of leakage current is more than 60mA duration 80ms Sequential value of leakage current is more than 150mA duration 10ms. Slowly varying value of leakage current is more than 300mA duration 120ms. 2.2 Fault Recovery Wait 5s to clear the fault information, start self-checking 2.3 Enter the safety state Cut off the Gird Relay and Warning by CAN Bus to upper Level.
	3. Fault tolerance time interval 30mA leakage current: 300ms 60mA leakage current: 150ms 150mA leakage current: 40ms 300mA leakage current: 300ms

Table 8: Safety function definition

8.2. Safe State

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

8.3. Safety Response Time

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

9. Assessment based on UL 1998, 3rd edition, Date December 18, 2013

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

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

3	Risk Analysis	
3.1	A risk analysis shall be conducted to determine:	Requirements fulfilled. Please see document [D20] (Risk analysis methods and results) for more information.
	a) The set of risks; and	Requirements fulfilled. Please see document [D20] (Risk analysis methods and results) for more information.
	b) That the software addresses the identified risks.	Requirements fulfilled. The software conforms to class B design and meets the identified risk requirements, see document [D24] & [D25].
3.2	The risk analysis shall be based on the safety requirements for the programmable component.	Requirements fulfilled. The risk analysis is based on the safety requirements, document refers to [D20].
3.3	An analysis shall be conducted to identify the critical, non-critical, and supervisory sections of the software.	Requirements fulfilled. An analysis is conducted refers to [D20].
3.4	An analysis shall be conducted to identify states or transitions that are capable of resulting in a risk.	Requirements fulfilled. document refers to [D20].
4	Process Definition	
4.1	All software process activities shall be described (see Section 12, Documentation).	Requirements fulfilled. All software process activities are described, refer to document [D2] (Development plan of software).

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

4.2	The software process activities shall be identified with distinct entry points, exit points, and criteria for transitioning among activities.	Requirements fulfilled. All software process activities are clearly identified and described in corresponding documents, refer to document [D2] and [D3].
4.3	The software process shall include a risk analysis in accordance with the requirements of Section 3, Risk Analysis. The risk analysis shall be traceable to the Programmable Component and Software Requirements Specification (see 12.6).	Requirements fulfilled. The software process includes a risk analysis in accordance with the requirements. Please refers to documents[D2] and [D3].
4.4	Criteria for transitioning among activities shall include consideration of the safety-related requirements for the programmable component.	Requirements fulfilled. Please refers to documents [D3].
4.5	Work products (e.g., meeting minutes, analysis and test results, formal documentation, etc.) shall be identified and associated with software process activities.	Requirements fulfilled. Work products is identified and associated with software process activities. Please refers to document [D3].
4.6	All software process activities shall support the communication of issues that could impact the safety-related functioning of the programmable component.	Requirements fulfilled. All software process activities support the communication of issues that refer to Software change management process [D3].
4.7	Safety-related requirements for the programmable component shall be traceable throughout the software process activities and documented evidence supporting compliance with this standard.	Requirements fulfilled. There are safety-related requirement IDs to help trace. Please see document [D3] and [D26] and [D27].

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

4.8	The verification, validation, and testing activities in the software process shall address errors at their source.	Requirements fulfilled. All activities are address errors at their source, see document [D3].
5	Qualification of Design, Implementation, and Verification Tools	
5.1	Evidence of tool qualification shall be provided for all tools used in the design, implementation, and verification of software in the programmable component using at least one of the following forms:	Requirements fulfilled. All development tools are qualification, see document [D3] & [D4].
	a) Documentation attesting to tool calibration, verification, and validation activities in accordance with 11.1.1, 11.2.1, 11.2.4, 12.1, 12.2, 12.4, 12.8 and Sections 14, and 15 of this standards.	Requirements fulfilled. Related information refers to document [D3].
	b) Evidence that the tool(s) has met formally defined requirements by a third-party tool certification program.	Requirements fulfilled. Related information refers to document [D3] & [D4].
5.2	When available from the tool vendor or other sources (e.g., the user community), the manufacturer shall provide a list of known bugs for the precise revision/version of the tool that the manufacturer intends to use to develop software. For each identified error in the known bug report for the tool, the following evidence shall be provided when implementing 5.1(a).	Requirements fulfilled. See document [D4] for software development tools.

	a) The feature that leads to an error has been fixed, tested, and approved for distribution by the tool vendor in a new release that has been incorporated into the manufacturer's version of the tool, or	Requirements fulfilled. See document [D2] & [D4] for more formation.
	b) The feature that leads to an error has not been used by the manufacturer in the development of safety-related software and does not lead to a risk.	Requirements fulfilled. Please see Description of software and hardware development tools [D2].
6	Software Design	
6.1	A fault in the software shall not initiate an event that results in a risk.	Requirements fulfilled. The software specially monitors the timing and functions and will enter a safe state if a fault is found, see document [D7].
6.2	The software shall maintain an RA state upon detection of a condition that is capable of resulting in a risk as identified in Section 3, Risk Analysis.	Requirements fulfilled. The software shall maintain an RA state, please see Related document [D2].
6.3	Detection of a failure in the software during the intended operation of the product shall be handled in a manner that is in accordance with the product safety requirements.	Requirements fulfilled. See document [D23] and [D25].
6.4	The software shall employ means to identify and respond to states that are capable of resulting in a risk. Examples of such means include initialization, fail-safe and fault-tolerant concepts, run-time checks, and built-in tests.	Requirements fulfilled. These safety functions are described in document [D3](SW Design Spec. for UL1998_20220801).

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

6.5	In allocating resources to tasks, consideration shall be given to the scheduling frequency of the task, the criticality of the task, and the resources utilized by the task, as well as the impact that each of these factors has on the ability to address the identified risks.	Requirements fulfilled. These key resources have been considered. See document [D3](SW Design Spec. for UL1998_20220801).
6.6	Means shall be employed for the prevention, detection, and resolution of non-terminating and non-deterministic states and error states such as division by zero, under/overvoltage condition of internal/external power supplies to the programmable components, and under/overflow that are capable of affecting the intended operation of the software.	Requirements fulfilled. These measures are considered in document [D3] (SW Design Spec. for UL1998_20220801) and [D5] (GoodWe C language programming specification_ V2.0).
6.7	All variables shall be set to initial values before being used by any instruction. If a design, implementation, or verification tool is responsible for ensuring that variables are set to initial values, the tool's qualification shall include verification of this (see Section 5).	Requirements fulfilled. There is no tool to initialize variables, but the initialization is carried out by the program after power on, see document [D3] for more information.
7	Critical and Supervisory Sections of Software	
7.1	The software shall be initialized to a documented RA state.	Requirements fulfilled. RA state is described in Software Introduction and security functions and is initialized at start of program run, refer to document [D3].

7.2	All critical and supervisory sections of the software shall be partitioned from other critical and supervisory sections of the software, as well as from non-critical sections.	Requirements fulfilled. All critical and supervisory sections of the software had partitioned. See document [D8] (Software architecture design specification and software design) for detailed description.
7.3	When it is not possible to partition the critical and supervisory sections from the non-critical sections of the software as in 7.2, all of the software shall be considered critical or supervisory.	Requirements fulfilled. It has been explained above.
7.4	Means shall be employed to avoid, or detect and recover from, memory usage and addressing conflicts.	Requirements fulfilled. Measures are employed to avoid, or detect and recover from, memory usage and addressing conflicts, see document [D3].
7.5	The supervisory section shall maintain control of the execution of the software during the operation of the programmable component.	Requirements fulfilled. The supervisory section is always valid during the function operation cycle. It refers to document [D8](Software architecture design specification and software design).

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

7.6	Software shall initiate a fail-safe or a fail-operational procedure in the event that a failure in a critical or supervisory section is detected.	Requirements fulfilled. Software will initiate a fail-safe or a fail-operational procedure in the event that a failure in a critical or supervisory section is detected, see document [D8] (Software shall initiate a fail-safe or a fail-operational procedure in the event that a failure in a critical or supervisory section is detected.).
7.7	When the initiation of a safety-related function is capable of resulting in a risk, a minimum of two instruction sequences shall be employed to verify the initiation of the safety-related function, unless otherwise specified in the product safety requirements.	Requirements fulfilled. There must be more than 2 command sequences to start. More details refer to document [D8].
7.8	There shall be provisions to control the accessibility of instructions and data dedicated to critical and supervisory section functions.	Requirements fulfilled. Refer to document [D8] for more information.
7.9	There shall be provisions to protect instructions and data for critical and supervisory sections of software from being affected by any function except critical and supervisory section functions.	Requirements fulfilled. The codes of key and supervisory parts are stored separately from other codes and have independent functions and are not affected by functions, see document [D7].

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

7.10	Supervisory and critical sections of software shall be resident in non-volatile memory. If supervisory and critical sections of software are transferred to volatile memory during operation, risks associated with the transfer and execution of software from volatile memory shall be considered in Section 3, Risk Analysis.	Requirements fulfilled. Supervisory and critical sections of software shall be resident in non-volatile memory. It not transferred to volatile memory during operation.
7.11	Means shall be employed to preserve the integrity of data used by critical and supervisory sections of software.	Requirements fulfilled. The data is stored in a fixed code and checked with a checksum boundary, see document [D3].
7.12	Fixed or one-time changing data used for critical and supervisory sections of software shall reside in non-volatile memory. If fixed or one-time changing data used for critical and supervisory sections of software are transferred to volatile memory during operation, risks associated with the transfer and access of this data from volatile memory shall be considered in Section 3, Risk Analysis.	Requirements fulfilled. Fixed or one-time changing data used for critical and supervisory sections of software all time reside in non-volatile memory. There is no data transfer process. See document [D3] for detail information.
8	Measures To Address Microelectronic Hardware Failure Modes	
8.1	Means shall be employed to address all microelectronic hardware failure modes identified by Section 3, Risk Analysis. Appendix A contains examples of acceptable measures for microelectronic hardware.	Requirements fulfilled. Software Introduction and security functions [D3] described means be employed.
8.2	Physical failures of the following microelectronic hardware shall be considered:	/

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

	a) CPU registers, instruction decoding and execution, program counter, addressing and data paths;	Requirements fulfilled. This is described in Table 11 below.
	b) Interrupt handling and execution;	Requirements fulfilled. This is described in Table 11 below.
	c) Clock;	Requirements fulfilled. This is described in Table 11 below.
	d) Non-volatile and volatile memory and memory addressing;	Requirements fulfilled. This is described in Table 11 below.
	e) Internal data path and data addressing;	Requirements fulfilled. This is described in Table 11 below.
	f) External communication and data, addressing, and timing;	Requirements fulfilled. This is described in Table 11 below.
	g) Input/output devices such as analog I/O, D/A and A/D converters, and analog multiplexers;	Requirements fulfilled. Meet the fault coverage through power on self-test and periodic cycle detection.
	h) Monitoring devices and comparitors; and	Requirements fulfilled. The project adopts a monitoring device and another programmable module for monitoring, see document [D3].
	i) Application-Specific Integrated Circuits (ASICs), Gate Array Logics (GALs), Programmable Logic Arrays (PLAs), and Programmable Gate Arrays (PGAs) hardware.	Requirements not applicable. Not used in the project.

8.3	Analysis of possible combinations of microelectronic hardware failures, software faults, and other events that are capable of resulting in a risk shall be conducted. This includes, for example, microelectronic hardware failures that cause software faults that are capable of resulting in a risk.	Requirements fulfilled. Analysis of possible combinations of microelectronic hardware failures, software faults, and other events that are capable of resulting in a risk shall be conducted in “SW Design Spec. for Inverter [D2]”.
8.4	When available from the programmable component vendor or other sources (e.g. the user community), the manufacturer shall provide erratum for the precise revision/version of the programmable component that the manufacturer intends to use. For each identified error in the erratum, the following evidence shall be provided:	/
	a) The error has been fixed, tested, and approved for distribution by the programmable component vendor in a new release that has been incorporated into the manufacturer’s version of the programmable component, or	Requirements not applicable. Not using OTS components in the market.
	b) Feature(s) affected by the error have not been used by the manufacturer in the development of safety-related software.	Requirements not applicable. Not using OTS components in the market.
9	Product Interface	
9.1	For power interruptions of any duration, the software shall maintain a documented RA state.	Requirements fulfilled. When the power supply fails, the software will maintain RA status, see document [D3] for detail information.

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

9.2	When initialization is allocated as a software function, the software shall initialize the product to a documented RA state.	Requirements fulfilled. RA state will be performed before software initialization, refer to document [D3].
9.3	Upon any situation in which the software terminates, the product shall maintain a documented RA state.	Requirements fulfilled. Please see document [D3].
9.4	A procedure or instruction intended to halt the programmable component shall maintain an RA state of the product.	Requirements fulfilled. A procedure or instruction intended to halt the programmable component shall maintain an RA state of the product.
10	User Interfaces	
10.1	The requirements in this section only apply to software that accepts user input, unless otherwise specified in the product safety requirements.	Requirements not applicable. Not used this function.
10.2	The time limits and other parameters of the software shall not be changeable by a user such that the intended execution of critical and supervisory sections of software is adversely affected.	Requirements fulfilled. No one except the manufacturer's professional will be able to modify the software.
10.3	The time limits and other parameters of the software that are intended to be configured by qualified service personnel shall be prevented from being changed to the extent that the intended operation of the critical or supervisory sections of software is adversely affected.	Requirements fulfilled. All configured data are judged accordingly, such as integrity, effective range, verification, etc, see document [D30].

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

10.4	The software shall require two or more user responses to initiate an operation that is capable of resulting in a risk.	Requirements fulfilled. When the software is started with complete functions, the information of battery pack, power grid and load side will be judged first, see document [D3] for more information.
10.5	Input commands which are capable of resulting in a risk when executed, shall not be initiated without operator intervention when those commands are received from an external source.	Requirements fulfilled. In case of command input with possible risk, the operator shall input the command at the same time and enter the corresponding mode before starting, see document [D3].
10.6	For a system as described in 10.5, no operation that is capable of resulting in a risk shall be initiated by a single user input.	Requirements fulfilled. It is described in 10.5 above.
10.7	Incorrect input shall not adversely affect execution of critical sections of software.	Requirements fulfilled. When the software executes the input information, it will first make various judgments on the input data, including verification, range detection, information integrity, etc.
10.8	If required to do so by the product safety requirements and when determined by the Risk Analysis, the software shall provide for user cancellation of the current operation and return the programmable component to an RA state.	Requirements fulfilled. Only in the debugging mode, and enter the RA state first, can it be executed, see document [D8] for more information.
10.9	User cancellation of the current operation shall require a single input by the user.	Requirements fulfilled. Please see document [D3].

10.10	Cancellation of processing shall leave the software in an RA state.	Requirements fulfilled. Cancellation of processing will leave the software in an RA state, see document [D3].
11	Software Analysis and Testing	
11.1	Software analysis	/
11.1.1	Software design and code analysis shall be conducted to evaluate that the critical and supervisory sections of software only perform those functions which they are intended to perform and do not result in a risk.	Requirements fulfilled. Software design and code analysis are conducted to evaluate by [D24] & [D25].
11.1.2	The software design and code analysis shall be conducted to demonstrate:	/
	a) Correctness and completeness with respect to the safety requirements for the programmable component;	Requirements fulfilled. Correctness and completeness with respect to the safety requirements for the programmable component by [D24] & [D25].
	b) Coverage of each branching condition and function evaluation that addresses and remediates risks associated with abnormal operations, or involves a risk associated with its normal operation;	Requirements fulfilled. The code is white box tested, and the branches and statements are completely covered.
	c) That fail-safe and fail-operational procedures bring the product to an RA state. See 6.3, 6.4, and 7.6;	Requirements fulfilled. That fail-safe and fail-operational procedures bring the product to an RA state. Refer to [D3].

	d) That the scheduling requirements are met and safety-related functions meet the timing constraints specified by the safety requirements for the programmable component. See 6.5;	Requirements fulfilled. The allocation of safety related components inherits parameters according to the technical requirements of safety related functions, and can trace the upper technical requirements, see document [D8].
	e) The integrity of the partitions between supervisory, critical, and non-critical sections of software. See 7.2;	Requirements fulfilled. The integrity of the partitions between supervisory, critical, and non-critical sections of software is describe in document [D8].
	f) That partition violations caused by such occurrences as data handling errors, control errors, timing errors, and misuse of resources do not occur; and	Requirements fulfilled. All partition codes and data have boundary detection and memory data monitoring, see document [D3].
	g) Consistency in the data and control flows across interfaces.	Requirements fulfilled. Consistency in the data and control flows across interfaces, refer to document [D3] (SW Design Spec. for UL1998_20220801).
11.2	Software testing	/
11.2.1	Software testing shall include development and post-release testing.	Requirements fulfilled. All testing activities are planned, including development testing, such as unit testing, module testing, and software and hardware integration testing after software release, see [D2].

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

11.2.2	Tests of the software shall be conducted and test results documented to evaluate that the software only performs those functions for which it is intended and does not result in a risk.	Requirements fulfilled. Conduct software testing and record the test results. The evaluation shows that if the software only performs its expected functions, it will not cause risks, see document [D26] & [D27].
11.2.3	Test cases shall be developed based on the risk analysis, the documented descriptions of the software operation and safety features (see 12.7.2), and the software analysis. See 11.1.	Requirements fulfilled. All test cases have complete descriptions of each test step, expected results and test records, see document [D26] & [D27].
11.2.4	Tests shall be conducted to demonstrate:	/
	a) Correctness and completeness with respect to the safety requirements for the programmable component;	Requirements fulfilled. All safety related components have been fully tested, documented and safety assessed, see document [D24] & [D25] & [D26].
	b) Coverage of each decision and function that is capable of involving a risk;	Requirements fulfilled. The test adopts fault injection, function use and possible error input, etc., which are all tested and verified, see [D20].
	c) That fail-safe and fail-operational procedures bring the product to an RA state. See 6.3, 6.4, and 7.6;	Requirements fulfilled. All safety related dangerous faults will enter RA status, see document [D3].

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

	d) That the scheduling requirements are met and safety-related functions meet the timing constraints specified by the safety requirements for the programmable component. See 6.5;	Requirements fulfilled. The scheduling cycle of each functional module is verified and meets the requirements described in the architecture design, see document [D3] and [D8].
	e) The integrity of the partitions between supervisory, critical, and non-critical sections of software. See 7.2;	Requirements fulfilled. Document [D27] describes the relevant information.
	f) That partition violations caused by such occurrences as data handling errors, control errors, timing errors, and misuse of resources do not occur; and	Requirements fulfilled. This function is described in Table 11 and verified by simulation test. No dangerous event will occur, but it will enter the expected safety state after it occurs.
	g) Consistency in the data and control flows across interfaces.	Requirements fulfilled. The consistency of data flow and control flow has also been verified by static test and dynamic test, see [D27].
11.2.5	The outputs that the software generates to control product hardware shall be tested to determine their effects on the product hardware, based on the expected output.	Requirements fulfilled. Verify the output of all software through hardware, including data storage and all States of the output of each relay, see document [D27].
11.3	Failure mode and stress testing	/
11.3.1	In addition to testing under normal usage, failure mode tests and stress tests shall be conducted.	Requirements fulfilled. Test under failure mode, such as over and under voltage test of input voltage, see document [D27].

11.3.2	Failure mode and stress testing shall include consideration of the following:	/
	a) Operator errors that are capable of adversely affecting the intended operation or the control of the programmable component;	Requirements fulfilled. Document [D27] relevant factors are considered.
	b) Microelectronic hardware component faults;	Requirements fulfilled. Table 11 of this report has been provided with failure test to prove microelectronic failure, see document [D26] (MS_G3 microelectronic fault test report).
	c) Errors in data received from external sensors or other software processes;	Requirements fulfilled. Communication error cases have been included in the test report, see document [D27].
	d) Failures associated with the entry into, and execution of, critical and supervisory sections of software;	Requirements fulfilled. Please see document [D27] for more information.
	e) Failures, errors, and other abnormal conditions associated with decisions and functions that are capable of providing risk reduction, including negative condition branches; and	Requirements fulfilled. Please see document [D27] for more information.
	f) Other processes and procedures that are capable of adversely affecting the intended operation of the software.	Requirements fulfilled. Please see document[D27] for more information.
11.3.3	Test cases shall include the following, as determined in accordance with 11.1.2(b):	/

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

	a) Out-of-range;	Requirements fulfilled. Range test of effective signals, including boundary test and equivalent test, see document [D27].
	b) Boundary condition; and	Requirements fulfilled. Please see document [D27].
	c) Type mismatched values for parameters at which decisions are made.	Requirements fulfilled. Please see document [D27].
11.3.4	Failure mode tests shall address all foreseeable faults identified in Risk Analysis, Section 3.	Requirements fulfilled. Please see document [D27].
12	Documentation	
12.1	User documentation	/
12.1.1	Except for embedded software that has no direct user interaction, user documentation (e.g, manual, guide, or other documents) shall be prepared.	Requirements fulfilled. There are product technical specifications and user instructions.
12.1.2	The user documentation shall describe the required data and control inputs, input sequences, options, program limitations and other activities or items necessary for intended execution of the software.	Requirements fulfilled. The user documentation refers to [D3] for more information.
12.1.3	All error messages shall be identified and corrective actions described in the user documentation.	Requirements fulfilled. The user documentation refers to [D23] for more information.
12.2	Software plan	/

12.2.1	A software plan shall be documented, which describes the software development activities.	Requirements fulfilled. Related documents [D3] for detail information.
12.2.2	The software plan shall include a description of the software design methodology, development rationale, any metrics to be collected, applicable standards and the engineering methods/techniques employed, and an itemized list of all documents produced throughout the software process.	Requirements fulfilled. All information and activities are considered in document [D3].
12.3	Risk analysis approach and results	/
12.3.1	The risk analysis approach and results (see Section 3) shall be documented.	Requirements fulfilled. Related document [D20] (Risk analysis methods and results).
12.3.2	The risk analysis shall illustrate how events, or logical combinations of events, are capable of leading to an identified hazard.	Requirements fulfilled. Related document [D20] (Risk analysis methods and results).
12.3.3	The risk analysis shall list all identified risks associated with the product.	Requirements fulfilled. Related document [D20] (Risk analysis methods and results).
12.4	Configuration management plan	/
12.4.1	A configuration management plan, which applies to off-the-shelf software, software tools, and the manufacturer-provided software, shall be documented.	Requirements fulfilled. Please see related document [D30] (MS G3 parameters specification).
12.4.2	The configuration management plan shall describe:	/

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国 • 上海 • 松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

	a) How changes to the software and hardware are managed;	Requirements fulfilled. There are change management processes, change applications and change records, see document [D31] & [D32].
	b) The initiation, transmittal, review, disposition, implementation and tracking of discrepancy reports and change requests; and	Requirements fulfilled. Please see related document [D31] & [D32].
	c) The methods and activities employed to formally control receipt, storage and backup, handling, and release of software and all documentation identified in this section.	Requirements fulfilled. Please see related document [D31] & [D32].
12.5	Programmable system architecture	
12.5.1	The programmable system architecture shall be documented.	Requirements fulfilled. The programmable system architecture is documented, see document [D8] (Software architecture design specification and software design).
12.5.2	The programmable system architecture shall describe the programmable component, including interfaces to users, sensors, actuators, displays, microelectronic hardware architecture, top-level software architecture, the mapping of the software to the hardware, and block diagrams of the programmable system showing a high-level view of the product architecture.	Requirements fulfilled. Please see related document [D8] (Software architecture design specification and software design).

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

12.5.3	The programmable system architecture shall describe the software-to-software interfaces and the hardware-to-software interfaces.	Requirements fulfilled. Please see related document [D8] (Software architecture design specification and software design).
12.5.4	The configuration(s) of the programmable component(s) that the software is intended to be operated with shall be identified. See 2.39.	Requirements fulfilled. See document [D3] for detail information.
12.6	Programmable component and software requirements specification	/
12.6.1	A programmable component and software requirements specification shall be documented.	Requirements fulfilled. Refer to document [D3] (SW Design Spec. for UL1998_20220801).
12.6.2	The programmable component and software requirements specification shall describe functional, performance, and interface requirements of the programmable system and the software.	Requirements fulfilled. Please see related document [D3] (SW Design Spec. for UL1998_20220801).
12.6.3	The specification shall include a description of all modes of operation, identification of failure behavior, and required responses.	Requirements fulfilled. Please see related document [D3] (SW Design Spec. for UL1998_20220801).
12.6.4	The programmable system and software requirements specification shall be traceable to the risk analysis results documented in 12.3.	Requirements fulfilled. Please see related document [D3] (SW Design Spec. for UL1998_20220801).
12.7	Software design documentation	/

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

12.7.1	Software design documentation shall be prepared.	Requirements fulfilled. Software design documentation is prepared, contain file [D3].
12.7.2	The software design documentation shall include a description of the operation and safety features of the software, with respect to the intended function.	Requirements fulfilled. All information and function are described, please see related document [D3] (SW Design Spec. for UL1998_20220801).
12.7.3	The software design documentation shall include the inputs and outputs, functions, data descriptions and relationships, control and data flow, fault handling, and algorithms.	Requirements fulfilled. Please see related documents [D3] (SW Design Spec. for UL1998_20220801).
12.7.4	The software design documentation shall describe details of how the design of the software meets the system and software requirements specification.	Requirements fulfilled. Please see document [D3] (SW Design Spec. for UL1998_20220801).
12.8	Analysis and test documentation	/
12.8.1	All analysis and test methods and results shall be documented.	Requirements fulfilled. Please see related documents [D20] & [D26] & [D27].
12.8.2	A test plan shall be documented which covers all software that is used in the programmable component, including off-the-shelf and third-party supplied software (See Off-The-Shelf Software, Section 13).	Requirements fulfilled. Please see related documents [D26] & [D27].

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

12.8.3	The test plan shall include or reference the documented test procedures which are used to verify the correct implementation of the software in the programmable component.	Requirements fulfilled. Have a complete safety test plan, see related documents [D27] (Safety function test plan and test report).
12.8.4	Test procedures shall include a description of the test parameters, test criteria, test configuration, and any special provisions or assumptions regarding the set-up, execution, and interpretation of the test cases (See 11.2.3, 11.2.4, and 11.3.2).	Requirements fulfilled. Please see related document [D27] (Safety function test plan and test report).
12.8.5	Test cases shall be documented and traceable to the software implementation.	Requirements fulfilled. Please see related document [D27] (Safety function test plan and test report).
12.8.6	Test results shall be documented and traceable to the test case(s) that produced them.	Requirements fulfilled. Please see related document [D27] (Safety function test plan and test report).
13	Off-the-Shelf (OTS) Software	/
13.1	For all OTS software that interfaces with the manufacturer-supplied software, the following information shall be provided in the software plan, see 12.2:	Requirements not appliable. Not used.
	a) The name and version/revision identifier of the OTS software;	Requirements not appliable. Not used.
	b) The name of the OTS software provider;	Requirements not appliable. Not used.
	c) A description of the purpose for which the software is being used;	Requirements not appliable. Not used.

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

	d) A clear description of the function provided by the software;	Requirements not appliable. Not used.
	e) An interface specification showing all control and data flows in and out of the OTS software; and	Requirements not appliable. Not used.
	f) References to the OTS software documentation for each callable routine that interfaces with the manufacturer's software.	Requirements not appliable. Not used.
13.2	At least one of the following forms of evidence shall be provided for OTS software:	Requirements not appliable. Not used.
	a) Documentation attesting to verification and testing activities of the OTS software to the extent that risks involving the OTS software are addressed.	Requirements not appliable. Not used.
	b) Evidence that the OTS software has met formally defined requirements by an independent OTS software certification program.	Requirements not appliable. Not used.
13.3	When available from the OTS software developer or other sources (e.g., the user community), the manufacturer shall provide a list of known bugs for the precise revision/version of the OTS software that the manufacturer intends to use in the embedded software. For each identified error in the known bug report for the OTS software the following evidence shall be provided when implementing 13.2(a):	Requirements not appliable. Not used.

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

	a) The feature that leads to an error has been fixed, tested, and approved for distribution by the OTS software developer in a new release that has been incorporated into the manufacturer's version of the software; or	Requirements not appliable. Not used.
	b) The feature that leads to an error has not been used by the manufacturer in the development of safety-related software and does not lead to a risk.	Requirements not appliable. Not used.
13.4	For OTS software that performs supervisory section functions or is used by the supervisory section of software, the requirements contained in 6.5, 11.1.2(d), 11.1.2(e), 11.1.2(f), and Section 7, of this standard apply.	Requirements not appliable. Not used.
14	Software Changes and Document Control	
14.1	Changes to parameter settings and data shall not create a risk or impact a risk that has previously been identified other than to reduce or eliminate it.	Requirements fulfilled. Please see document [D3] & [D31].
14.2	Changes or patches to the software shall not create a risk or impact a risk that has previously been identified other than to reduce or eliminate it.	Requirements fulfilled. Please see document [D3] & [D31].
14.3	To determine compliance, all changes are to be evaluated in accordance with this standard.	Requirements fulfilled. Please see document [D3] & [D31].
14.4	Documentation shall be reviewed to determine that it correctly reflects safety-related changes that have been made in the software.	Requirements fulfilled. Please see document [D24] & [D25].

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

14.5	There shall be procedures to maintain and control software changes to the configuration of the programmable components and critical and supervisory sections of software to facilitate traceability.	Requirements fulfilled. Procedures are developed, please see document [D1] & [D2].
15	Identification	
15.1	Software shall be traceable to a unique identifier stored in non-volatile memory.	Requirements fulfilled. The security requirements, technical requirements and functional modules defined by the software have unique ID identification, see document [D8] & [D26] & [D27].
15.2	The unique identifier shall reflect changes that have been made to critical and supervisory sections of the software.	Requirements fulfilled. Please see related document [D8].
15.3	Each time a change or patch is incorporated in the critical or supervisory sections of software, a new unique identifier shall be assigned.	Requirements fulfilled. A new unique identifier shall be assigned when software design changed, see document [D31] & [D32].
15.4	Documentation shall include sufficient information to identify each item that is investigated with the software. For example, identification of software elements shall include the version number, release number, and date. Microelectronic hardware elements shall include the component vendor, part number and revision level that uniquely identifies the programmable component die.	Requirements fulfilled. The information in the document and the information of components or assemblies are sufficient to help identify and record the technical information required for the development of safety functions, see all document.

Table 10: Checklist of UL 1998, 3rd Edition

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

Component	Fault / Error	SW class 1	SW class 2	Measures description
1. CPU				
1.1 Registers	stuck-at	Rq		Requirements fulfilled. Call the security library function provided by ST chip manufacturer.
	DC fault		Rq	Requirement not applicable. SW is class 1.
1.2 Instruction decoding and execution	wrong decoding and execution		Rq	Requirement not applicable. SW is class 1.
1.3Program counter	stuck-at	Rq		Requirements fulfilled. Call the security library function provided by ST chip manufacturer.
	DC fault		Rq	Requirement not applicable。 SW is class 1.
1.4 Addressing	DC fault		Rq	Requirement not applicable。 SW is class 1.
1.5 Data paths	DC fault		Rq	Requirement not applicable。 SW is class 1.
2 Interrupt handling and execution	no interrupt or too frequent interrupt	Rq		Requirements fulfilled. Call the security library function provided by ST chip manufacturer.
	no interrupt or too frequent interrupt and interrupt related to different sources		Rq	Requirement not applicable. SW is class 1.
3. Clock	wrong frequency (for quartz Synchronized clock: harmonics/ subharmonics only)	Rq		Requirements fulfilled. Call the security library function provided by ST chip manufacturer.
			Rq	Requirement not applicable. SW is class 1.
4. Memory				
4.1 Non-	all single-bit	Rq		Requirements fulfilled.

volatile memory	faults			Call the security library function provided by ST chip manufacturer.
	all single and double bit errors		Rq	Requirement not applicable. SW is class 1.
4.2 Volatile memory	DC fault	Rq		Requirements fulfilled. Call the security library function provided by ST chip manufacturer.
	DC fault and dynamic cross links		Rq	Requirement not applicable. SW is class 1.
4.3 Addressing (relevant to variable and invariable memory)	stuck-at	Rq		Requirements fulfilled. Call the security library function provided by ST chip manufacturer.
	DC fault		Rq	Requirement not applicable. SW is class 1.
5. Internal data path				
5.1 Data	stuck-at	Rq		Requirements fulfilled. Call the security library function provided by ST chip manufacturer.
	DC fault		Rq	Requirement not applicable. SW is class 1.
5.2 Addressing	wrong address	Rq		Requirements fulfilled. Call the security library function provided by ST chip manufacturer.
	wrong and multiple addressing		Rq	Requirement not applicable. SW is class 1.
6. External communication				
6.1 Data	all single-bit and double bit errors	Rq		Requirements fulfilled. Application interrupts occurrence and external communications can be checked by different methods, one of them could be a control using a set of incremental counters where every interrupt or communication event increments a specific counter. The values in the counters are then verified at given time intervals by cross-checking against some other independent time base. Data exchange during communication

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 61915666 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86-21) 61915666 f (86-21) 61915678 e sgs.china@sgs.com

				sessions should be checked, including redundant information into the data packets. Parity, sync signals, CRC check sums, block repetition or protocol numbering can be used for this purpose. Robust application software protocol stacks like TCP/IP give higher level of protection, if necessary. Periodicity and effective occurrence of the communication events together with protocol error signals has to be permanently checked.
	all single-bit, double bit and triple bit errors		Rq	Requirement not applicable. SW is class 1.
6.2 Addressing	wrong address	Rq		Requirements fulfilled. The applied software March test can then be used optionally for testing those parts of RAM not covered by the hardware parity check, or as a supplementary testing method. Reliability of an information stored in the SRAM can be increased by applying additional indirect testing techniques, such as double storage of safety critical information in physically separated areas in form of two inverted patterns (this is based on the fact that corruption caused by radiation or EMI usually attacks a limited physical memory section), or by applying dedicated check sum signature to each part of these data.
	wrong and multiple addressing		Rq	Requirement not applicable. SW is class 1.
6.3 Timing	wrong point in time	Rq	Rq	Requirements fulfilled. Dedicated I/Os can be used for timing measurement of procedures executed both at start-up and during run time. Start-up tests are performed within a single run, their duration depends from the MCU performance and from the size

				of the tested area. Tests during run time are performed block by block, so their duration depends also upon the size of the block under test and upon the frequency of repetition of testing. The user has to find a balance between the performance needed to run the application and that for testing the hardware running it. The main challenge is to achieve a short overall diagnostic test interval while keeping application process safety time within acceptable length. In critical cases run time testing can be limited to areas collecting critical code or data. The partial test interval is derived from SysTick 1 ms interval and it is set to 10 ms by default by parameter SYSTICK_10ms_TB.
	wrong sequence	Rq	Rq	Requirements fulfilled. When shortening it, user should consider that the interval is used to calculate clock cross reference ratio between system clock and LSI during run time too, so its length shall never drop below an interval corresponding to the number of LSI periods applied for the clock cross-measurement (set to eight by default).
7. Input/output periphery				
7.1 Digital I/O	open and short circuit or as specified in the product standard	Rq	Rq	Requirements fulfilled. Class 1 tests must detect any malfunction on digital I/Os, too. It could be covered by plausibility checks together with some other application parts (e.g. change of an analogy signal from temperature sensor should be checked when heating/cooling digital control is switched on/off). Selected port bits can be locked by applying the correct lock sequence to the lock bit in the GPIOx_LCKR to prevent unexpected changes to the port configuration. Reconfiguration is only possible at the next reset sequence in

				this case. In Compliance with IEC, UL and CSA standards AN443526/61 DocID025817 Rev 6 addition, the bit banding feature can be used for atomic manipulation of the SRAM and peripheral registers.
7.2 Analog I/O				
7.2.1 A/D-and D/Aconverter	open and short circuit or as specified in the product standard	Rq	Rq	Requirements fulfilled. Can be tested by applying additional signal source injection on the tested pin • Some devices feature internal pull-down or pull-up resistor activation on the analogy input or free pin with DAC functionality (or a digital GPIO output) can be used for the injection. • Some devices feature Routing interface. It can be used for internal connection between pins to make testing loop-back, additional signal injection or duplicate measurement at some other independent channel.
7.2.2 Analog multiplexer	Wrong addressing	Rq	Rq	Requirements fulfilled. Measured values should be checked for plausibility and verified by measurements performed by other redundant channels, while free channels can be used for reading some reference voltages in conjunction with testing of analogy multiplexers used in the application. The internal reference voltage should also be checked.
8. Monitoring devices and comparators	any output outside the static and dynamic functional specification		Rq	Requirement not applicable. SW is class 1.
9. Components not covered by items	any output outside the static and dynamic functional	Rq	Rq	Requirements fulfilled. DAC output functionality •Free ADC channels can be used to check if the DAC output channel is working correctly

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国 • 上海 • 松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com

	specification			• The Routing interface can be used for connection between the ADC input channel and the DAC output channel Comparator functionality •Comparison between known voltage and DAC output or internal reference voltage can be used for testing comparator output on another comparator input. • Analog signal disconnection can be tested by pull-down or pull-up activation on tested pin and comparing this signal with DAC voltage as reference on another comparator input. Operational amplifier • Functionality can be tested forcing (or measuring) a known analogy signal to the operational amplifier (OPAMP) input pin, and internally measuring the output voltage with the ADC. The input signal to OPAMP can be also measured by ADC (on another channel).

Table 11: Checklist of Measures to address fault/errors

--End of the report--

NO.588 West Jindu Road, Songjiang District, Shanghai, China 201612 t (86–21) 61915666 f (86–21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路 588 号 邮编: 201612 t (86–21) 61915666 f (86–21) 61915678 e sgs.china@sgs.com