Test Report issued under the responsibility of:

intertek
Total Quality. Assured.

TEST REPORT

UL 1998
Software in Programmable Components
CSA C22.2#0.8
Safety Functions Incorporating Electronic Technology

Report Number. ..... :	251000057SHA-001
Date of issue ..... :	2026-04-17
Total number of pages ..... :	46 pages
Name of Testing Laboratory preparing the Report ..... :	Intertek Testing Services (Shanghai FTZ) Co., Ltd. Building No. 86, 1198 Qinzhou Road (North), Shanghai 200233, China
Applicant's name ..... :	Refer to 250200098SHA-001
Address ..... :	Refer to 250200098SHA-001
Test specification:	
Standard ..... :	UL 1998:2013 Ed.3+R:16Nov2022 CSA C22.2#0.8:2019 Ed.4
Test procedure ..... :	--
Non-standard test method ..... :	N/A
Test Report Form No. ..... :	TTRF_UL 1998 & CSA C22.2 No. 0.8_A
Test Report Form(s) Originator .... :	INTERTEK
Master TRF ..... :	2024-03

Copyright © 2018 IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE System). All rights reserved.

This publication may be reproduced in whole or in part for non-commercial purposes as long as the IECEE is acknowledged as copyright owner and source of the material. IECEE takes no responsibility for and will not assume liability for damages resulting from the reader's interpretation of the reproduced material due to its placement and context.

This report is not valid as a CB Test Report unless signed by an approved CB Testing Laboratory and appended to a CB Test Certificate issued by an NCB in accordance with IECEE 02.

General disclaimer:

The test results presented in this report relate only to the object tested.
This report shall not be reproduced, except in full, without the written approval of the Issuing CB Testing Laboratory. The authenticity of this Test Report and its contents can be verified by contacting the NCB, responsible for this Test Report.

This report is for the exclusive use of Intertek's Client and is provided pursuant to the agreement between Intertek and its Client. Intertek's responsibility and liability are limited to the terms and conditions of the agreement. Intertek assumes no liability to any party, other than to the Client in accordance with the agreement, for any loss, expense or damage occasioned by the use of this report. Only the Client is authorized to permit copying or distribution of this report and then only in its entirety. Any use of the Intertek name or one of its marks for the sale or advertisement of the tested material, product or service must first be approved in writing by Intertek. The observations and test results in this report are relevant only to the sample tested. This report by itself does not imply that the material, product, or service is or has ever been under an Intertek certification program.

Test Item description	Software embedded in microcontroller of AC EV Charger
Trade Mark	--
Manufacturer.....	Same as applicant
Model/Type reference	Plug in： AC0120AN0600300, Type 1 AC0120AN0601300, Nacs Nema Plug in： AC0096AN0600300, Type 1 AC0096AN0601300, Nacs
Ratings	For model AC0120AN0600300 and AC0120AN0601300: INPUT 208/240VAC (L+L+PE), 60Hz, 50A@50°C OUTPUT 208/240VAC. 50A@50°C. For model AC0096AN0600300 and AC0096AN0601300: INPUT 208/240VAC (L+L+PE), 60Hz, 40A@50°C OUTPUT 208/240VAC.40A@50°C.
Software module(s) and associated version(s).....	Software information: GD32E513ZET6 microcontroller as control core. And the embedded software ID K728_MJ_M_BC_V1.0.1_20260316(M4)., version: V1.0.1 was released on 20260316, size 779KB, checksum 0x033CD730. Hardware information: A0

Responsible Testing Laboratory (as applicable), testing procedure and testing location(s):

☒	**Testing Laboratory:**	Intertek Testing Services (Shanghai FTZ) Co., Ltd.	
Testing location/ address ..... :		Building No. 86, 1198 Qinzhou Road (North), Shanghai 200233, China	
Tested by (name, function, signature) ..... :		Snape Chen (Engineer)	Snape chen
Approved by (name, function, signature) .. :		Helen Cai (Reviewer)	Helen Cai
☐	**Testing procedure: CTF Stage 1:**		
Testing location/ address ..... :		N/A	
Tested by (name, function, signature) ..... :		N/A	
Approved by (name, function, signature) .. :		N/A	
☐	**Testing procedure: CTF Stage 2:**		
Testing location/ address ..... :		N/A	
Tested by (name + signature)..... :		N/A	
Witnessed by (name, function, signature) . :		N/A	
Approved by (name, function, signature) .. :		N/A	
☐	**Testing procedure: CTF Stage 3:**		
☐	**Testing procedure: CTF Stage 4:**		

Testing location/ address ..... :	N/A	
Tested by (name, function, signature) ..... :	N/A	
Witnessed by (name, function, signature) . :	N/A	
Approved by (name, function, signature) .. :	N/A	
Supervised by (name, function, signature) :	N/A	

List of Attachments (including a total number of pages in each attachment):

None

Summary of testing/evaluation:

Determination of the test conclusion is based on IEC Guide 115 in consideration of measurement uncertainty.

From the result of our inspection and tests on the submitted samples, we conclude that they comply with the requirements of the standards.

Tests performed (name of test and test clause):	**Testing location:**
Full	Intertek Testing Services (Shanghai FTZ) Co., Ltd. Building No.86, 1198 Qinzhou Road (North), Shanghai 200233, China

Summary of compliance with National Differences (List of countries addressed):

None

Copy of marking plate(representative):

The artwork below may be only a draft. The use of certification marks on a product must be authorized by the respective NCBs that own these marks.

Refer to 250200098SHA-001

TEST ITEM PARTICULARS:	
Manufacturer's specified operating ambient..... :	-30°C~50°C;
POSSIBLE TEST CASE VERDICTS:	
- test case does not apply to the test object..... :	N/A
- test object does meet the requirement ..... :	P (Pass)
- test object does not meet the requirement ..... :	F (Fail)
TESTING:	
Date of receipt of test item..... :	2025-10-10
Date (s) of performance of tests..... :	2025-10-10 to 2026-04-10
GENERAL REMARKS:	

"(See Enclosure #)" refers to additional information appended to the report.
"(See appended table)" refers to a table appended to the report.

This Test Report is only applicable to controls using software. This TRF is to be used in conjunction with the end product Test Report.

Throughout this report a ☒ comma / ☐ point is used as the decimal separator.

When differences exist; they shall be identified in the General product information section.

Name and address of factory (ies) ..... :	Refer to 250200098SHA-001

GENERAL PRODUCT INFORMATION:

Product Description –

The product covered by this report is a Level 2 AC Electric Vehicle Charging Station, with CCID20, GM/I and BI of personnel protection system, fixed in place for field wiring or fastened in place with input plug, intended for indoor and outdoor use. For the input installation, fastened models shall use with NEMA plug (for rated 40A Max), fixed models use with hardwired (for rated 50A Max).

The product is intended to operate at altitudes up to 3000m.

Model Differences –

All models are designed in the same electrical structure, software and critical components, except for the enclosure colour and rated current which may includes cord set, output cable and the following: Model AC0120AN0600300 and AC0096AN0600300 are with Type 1 connector; Model AC0120AN0601300 and AC0096AN0601300 are with NACS connector.

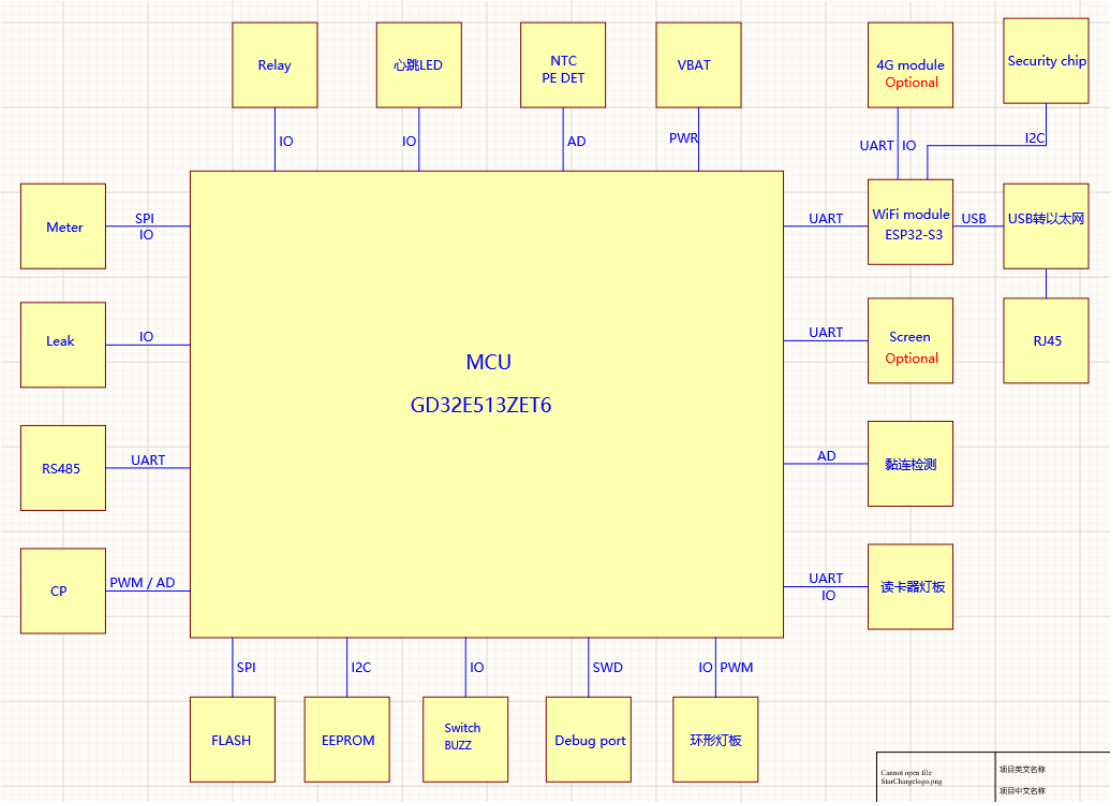
Additional application considerations – (Considerations used to test a component) –

1. This report must be read with report 250200098SHA-001 together.

DESCRIPTION OF SAFETY FUNCTION(S)

Its safety protection function as shown below:

Protection for Over-Temperature, Leakage Current, Grounding Detection, Contactor Stuck-at to Charging Stations.



ITEM	TIME	Remark
Over-Temperature	1s	
Leakage Current	20ms	
Grounding Detection	3s	
Contactor Stuck-at	8s	

Additional information
The following is typical of the information to be summarized on this page: • A description of each safety function of the software; including any declared response times, parameters, Class, etc. • Summary of interactions between the hardware circuitry and the software. • A description of any interfaces between safety and non-safety related software functions. • Software module(s) and associated version(s) • Method of identification of software module(s) and associated versions(s) at the production location

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict

3	**Risk Analysis**		
3.1	A risk analysis shall be conducted to determine:		
	a) The set of risks, and		P
	b) That the software addresses the identified risks.		P
3.2	The risk analysis based on the safety requirements for the programmable component.		P
3.3	An analysis conducted to identify the critical, non-critical, and supervisory sections of the software.		P
3.4	An analysis conducted to identify states or transitions that are capable of resulting in a risk.		P
3.5	The risk analysis following an easily readable approach		P
3.6	Each identified risk shall:		
	a) Have documented evidence to demonstrate the risk has an effective design measure; and		P
	b) Have documentation showing assurance evidence (e.g. executed test cases, simulation results, or qualification data) to support coverage through risk mitigation and/or other relevant control measures.		P
4	**Process Definition**		
4.1	All software process activities described		P
4.2	The software process activities identified with distinct entry points, exit points, and criteria for transitioning among activities.		P
4.3	The software process shall include a risk analysis		P
	The risk analysis shall be traceable		P
4.4	Criteria for transitioning among activities shall include consideration of the safety-related requirements for the programmable component.		P
4.5	Work products identified and associated with software process activities.		P

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
4.6	All software process activities supporting the communication of issues that could impact the safety-related functioning of the programmable component.		P
4.7	Safety-related requirements for the programmable component shall be traceable forward and backward throughout the software process activities and shall be documented as evidence supporting compliance with this standard.		P
4.8	The verification, validation, and testing activities in the software process shall address errors at their source.		P
5	**Qualification of Design, Implementation, and Verification Tools**		
5.1	Evidence of tool qualification shall be provided for all tools using at least one of the following forms:		
	a) Documentation attesting to supporting measurement tool calibration and verification and validation activities of software design, implementation, analysis, verification and process support tools		P
	b) Evidence that the tool(s) has/have met formally defined requirements by a third-party tool certification program covering as minimum the requirements of 5.1(a).		N/A
5.2	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):		
	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		N/A
	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.		N/A
6	**Software Design**		
6.1	A fault in the software not initiate an event that results in a risk.		P
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.		P
6.3	Detection of a failure handled in a manner that is in accordance with the product safety requirements.		P

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
6.4	The software shall employ means to identify and respond to states that are capable of resulting in a risk.		P
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.		P
6.6	Means shall be employed for the prevention, detection, and resolution of non-terminating and non-deterministic states and error states		P
6.7	All variables shall be set to initial values before being used by any instruction.		P
	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).		P
6.8	The software shall fulfill the specified requirements for the safety related software.		P
6.9	The software design shall avoid unnecessary complexity and		P
	shall allow verification by static analysis.		P
6.10	Manufacturers shall develop their own company-specific Coding Standards/Guidelines that specify:		
	a) Which software constructs and practices should be avoided in general (and why),		P
	b) Conditions under which certain constructs and tactics not normally recommended may be employed, and		P
	c) Coding practices that are recommended		P
7	**Critical and Supervisory Sections of Software**		
7.1	The software initialized to a documented RA state.		P
7.2	All critical and supervisory sections of the software partitioned from other critical and supervisory sections of the software, as well as from non-critical sections.		N

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
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.		N/A
7.4	Means employed to avoid, or detect and recover from, memory usage and addressing conflicts.		P
7.5	The supervisory section shall maintain control of the execution of the software		P
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.		P
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		P
	otherwise specified in the product safety requirements.		N/A
7.8	Provisions to control the accessibility of instructions and data dedicated to critical and supervisory section functions.		P
7.9	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.		P
7.10	Supervisory and critical sections of software shall be resident in non-volatile memory.		P
	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.		N/A
7.11	Means employed to preserve the integrity of data used by critical and supervisory sections of software.		P
7.12	Fixed or one-time changing data used for critical and supervisory sections of software shall reside in non-volatile memory.		P

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
	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.		N/A
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.		P
	Appendix A contains examples of acceptable measures for microelectronic hardware.		P
8.2	Physical failures of the following microelectronic hardware shall be considered:		
	a) CPU registers, instruction decoding and execution, program counter, addressing and data paths;		P
	b) Interrupt handling and execution;		P
	c) Clock;		P
	d) Non-volatile and volatile memory and memory addressing;		P
	e) Internal data path and data addressing;		N/A
	f) External communication and data, addressing, and timing;		P
	g) Input/output devices such as analog I/O, D/A and A/D converters, and analog multiplexers;		P
	h) Monitoring devices and comparitors; and		P
	i) Application-Specific Integrated Circuits (ASICs), Gate Array Logics (GALs), Programmable Logic Arrays (PLAs), and Programmable Gate Arrays (PGAs) hardware.		N/A
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.		P

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
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.		N/A
	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		N/A
	b) Feature(s) affected by the error have not been used by the manufacturer in the development of safety-related software.		N/A
	c) Appropriate software related documentation shall be updated to avoid risks related to changes of either the software or the programmable component.		N/A
9	**Product Interface**		
9.1	For power interruptions of any duration, the software shall maintain a documented RA state.		P
9.2	When initialization is allocated as a software function, the software shall initialize the product to a documented RA state.		P
9.3	Upon any situation in which the software terminates, the product shall maintain a documented RA state.		P
9.4	A procedure or instruction intended to halt the programmable component shall maintain an RA state of the product.		P
10	**User Interfaces**		
10.1	The requirements in this section only apply to software that accepts user input, unless		N/A
	Otherwise specified in the product safety requirements.		N/A
10.2	The time limits and other parameters of the software shall not be changeable by a user		N/A

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
10.3	The time limits and other parameters of the software 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.		N/A
10.4	The software shall require two or more user responses to initiate an operation that is capable of resulting in a risk.		N/A
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.		N/A
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.		N/A
10.7	Incorrect input shall not adversely affect execution of critical sections of software.		N/A
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.		N/A
10.9	User cancellation of the current operation shall require a single input by the user.		N/A
10.10	Cancellation of processing shall leave the software in an RA state.		N/A
11	**Software Analysis and Testing**		
11.1	**Software analysis**		
11.1.1	Software design and code analysis 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.		P
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;		P

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
	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;		P
	c) That fail-safe and fail-operational procedures bring the product to an RA state. See 6.3, 6.4, and 7.6;		P
	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;		P
	e) The integrity of the partitions between supervisory, critical, and non-critical sections of software. See 7.2;		P
	f) That partition violations caused by such occurrences as data handling errors, control errors, timing errors, and misuse of resources do not occur; and		P
	g) Consistency in the data and control flows across interfaces.		P
11.2	**Software testing**		
11.2.1	Software testing shall include development and post-release testing.		P
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.		P
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.		P
11.2.4	Tests shall be conducted to demonstrate:		
	a) Correctness and completeness with respect to the safety requirements for the programmable component;		P
	b) Coverage of each decision and function that is capable of involving a risk;		P
	c) That fail-safe and fail-operational procedures bring the product to an RA state. See 6.3, 6.4, and 7.6;		P

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
	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;		P
	e) The integrity of the partitions between supervisory, critical, and non-critical sections of software. See 7.2;		P
	f) That partition violations caused by such occurrences as data handling errors, control errors, timing errors, and misuse of resources do not occur; and		P
	g) Consistency in the data and control flows across interfaces.		P
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.		P
11.3	**Failure mode and stress testing**		
11.3.1	Failure mode tests and stress tests shall be conducted.		P
11.3.2	Failure mode and stress testing shall include consideration of the following:		
	a) Operator errors		P
	b) Microelectronic hardware component faults;		P
	c) Errors in data received from external sensors or other software processes;		P
	d) Failures associated with the entry into, and execution of, critical and supervisory sections of software;		P
	e) Failures, errors, and other abnormal conditions associated with decisions and functions that are capable of providing risk reduction, including negative condition branches; and		P
	f) Other processes and procedures that are capable of adversely affecting the intended operation of the software.		P
11.3.3	Test cases shall include the following:		
	a) Out-of-range;		P
	b) Boundary condition; and		P

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
	c) Type mismatched values for parameters at which decisions are made.		P
11.3.4	Failure mode tests shall address all foreseeable faults identified in Risk Analysis, Section 3.		P
12	**Documentation**		
12.1	**User documentation**		
12.1.1	User documentation (e.g, manual, guide, or other documents) shall be prepared,		N/A
	Except for embedded software that has no direct user interaction		P
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.		N/A
12.2	**Software plan**		
12.2.1	A software plan shall be documented, which describes the software development activities.		P
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.		P
12.2.3	The software plan shall ensure that design methodologies support readability, understandability, testability and maintainability of the software.		P
12.3	**Risk analysis approach and results**		
12.3.1	The risk analysis approach and results (see Section 3)documented.		P
12.3.2	The risk analysis shall illustrate how events, or logical combinations of events, are capable of leading to an identified hazard.		P
12.3.3	The risk analysis shall list all identified risks associated with the product.		P
12.4	**Configuration management plan**		

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
12.4.1	A configuration management plan documented.		P
12.4.2	The configuration management plan shall describe:		
	a) How changes to the software and hardware are managed;		P
	b) The initiation, transmittal, review, disposition, implementation and tracking of discrepancy reports and change requests; and		P
	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.		P
12.5	**Programmable system architecture**		
12.5.1	The programmable system architecture shall be documented.		P
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.		P
12.5.3	The programmable system architecture shall describe the software-to-software interfaces and the hardware-to-software interfaces.		P
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.		P
12.6	**Programmable component and software requirements specification**		
12.6.1	A programmable component and software requirements specification documented.		P
12.6.2	The programmable component and software requirements specification shall describe functional, performance, and interface requirements of the programmable system and the software.		P

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
12.6.3	The specification shall include a description of all modes of operation, identification of failure behavior, and required responses.		P
12.6.4	The programmable system and software requirements specification shall be traceable to the risk analysis results documented in 12.3.		P
12.7	**Software design documentation**		
12.7.1	Software design documentation shall be prepared.12.3.		P
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.		P
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.		P
12.7.4	The software design documentation shall describe details of how the design of the software meets the system and software requirements specification.		P
12.8	**Analysis and test documentation**		
12.8.1	All analysis and test methods and results shall be documented.		P
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).		P
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.		P
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).		P
12.8.5	Test cases shall be documented and traceable to the software implementation.		P
12.8.6	Test results shall be documented and traceable to the test case(s) that produced them.		
13	**Off-the-Shelf (OTS) Software**		

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
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:		
	a) The name and version/revision identifier of the OTS software;		N/A
	b) The name of the OTS software provider;		N/A
	c) A description of the purpose for which the software is being used;		N/A
	d) A clear description of the function provided by the software;		N/A
	e) An interface specification showing all control and data flows in and out of the OTS software; and		N/A
	f) References to the OTS software documentation for each callable routine that interfaces with the manufacturer's software.		N/A
13.2	At least one of the following forms of evidence shall be provided for OTS software:		
	a) Documentation attesting to verification and testing activities of the OTS software to the extent that risks involving the OTS software are addressed.		N/A
	b) Evidence that the OTS software has met formally defined requirements by an independent OTS software certification program.		N/A
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.		N/A
	For each identified error in the known bug report for the OTS software the following evidence shall be provided when implementing 13.2(a):		
	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		N/A
	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.		N/A

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
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.		N/A
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.	First version	N/A
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.		N/A
14.3	All changes are to be evaluated in accordance with this standard.		N/A
14.4	Documentation shall be reviewed to determine that it correctly reflects safety-related design and changes that have been made in the software.		N/A
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 including related documentation to facilitate traceability.		P
15	**Identification**		
15.1	Software shall be traceable to a unique identifier stored in non-volatile memory.		P
15.2	The unique identifier shall reflect changes that have been made to critical and supervisory sections of the software.		P
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.		P

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
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.		P

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict

4.2	**Compliance**		
4.2.1	The applicable safety requirements of this standard are met and verification of the safety functions of the declared control class is demonstrated		P
4.2.2	All defined safety output conditions have been verified against the defined safe state		P
5	**Functional safety requirements**		P
5.1	**Control functions**		
5.1.1*	Clause 5 applies to equipment with control class B and C		P
5.1.2*	Control class is defined	Class B	P
5.1.3*	Safety control functions using hardware-only designs shall comply, as a minimum, to the requirements in the Clauses specified in Table 2 when applicable.	The safety functions implemented bythe cooperation of the hardware and software.	N/A
5.2	**Equipment description and architecture**		
5.2.1*	An architectural description of the hardware and software components shall be prepared and include a brief description of the components and interfaces.		P
	Details about safety-related devices, user interfaces, software-hardware interfaces, and displays		P
5.2.2 *	A schematic diagram shall be provided.		P
5.2.3*	An operational description of the product, including all operational modes, shall be provided.		P
	This shall include a list of all error messages showing corrective actions to be performed by a user or operator.		P
5.2.4 *	Description of the mechanism used to indicate fault status. Operator actions as response shall be documented.		P
5.2.5	For class C, the microcontroller (MCU) configuration shall be:		
	(a) single channel with periodic self-test and monitoring;	Class B	N/A
	(b) dual channel (diverse) with comparison; or	Class B	N/A
	(c) dual channel (homogeneous) with comparison.	Class B	N/A
5.2.6	For class B, the MCU configuration shall be one of the following:		

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
	(a) single channel with functional test;	Functional test is conducted during the initialization stage.	P
	(b) single channel with periodic self-test; or	Periodic self-test is conducted during operation.	P
	c) dual channel (without comparison).	-	N/A
5.2.7	Where a EUT has multiple assemblies, the architectural description describes the safety role of each assembly.		N/A
	For single-channel configuration the role of the main assembly is defined.		
	The role of secondary assemblies shall be described, including the data interchange with the main assembly		
5.2.8	Where failure of OTS could have adverse effects with respect to safety, the following requirements shall apply:		
	(a) OTS name, release ID, the manufacturer's name, and the list of known problems that could affect safety are described.	No OTS software	N/A
	(b) A description of the role of the OTS.		N/A
	(c) Evidence that the OTS supports EUT safety:		N/A
	- (i) OTS software has been developed under a formal quality assurance program that includes design and code reviews, validation testing and operation and interface requirements, or		N/A
	- (ii) OTS software covered by an independent OTS software certification program.		N/A
5.2.9	Where OTS contains both hardware and software, it meets the requirements of Clause 5.2.8, Items (a), (b) and (c)(ii).	No OTS software	N/A
5.3	**System hazard analysis**		
5.3.1	**Identifying hazards**		
5.3.1.1 *	The identified hazard(s) covered by the design are defined by a short statement.		P
5.3.1.2 *	External event(s) that can trigger a hazard are identified.		P
	Operational modes are defined.		P
5.3.2 *	**Hazard analysis (HA)**		
5.3.2.1	Potential failure events that can trigger hazard are identified and show the interrelationships in a fault tree.		P

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
5.3.2.2	The FMEA analysis covers safety-related failure modes for all major hardware and software components. Covers table A.2		P
5.3.2.3	Results are in a hazard analysis report		P
5.3.2.4	Demonstrated that risks have been reduced to a level as low as reasonably practicable		P
5.4	**Safety requirements and design**		
5.4.1*	The safety requirements of the EUT describes the required corrective action for all noted potential failure events		P
	Safety design includes both hardware and software components		P
5.4.2*	For class C controllers, detection and response to a fault is provided by an independent method.	Class B	N/A
5.4.3*	Operation of the non-safety function(s) does not adversely affect safety functions.		P
5.4.4*	For hardware-only control systems, the safety functions are documented.		N/A
5.4.5 *	The safety design covers the handling of the failure modes identified in Clause 5.3.2.2.		P
5.4.6	The internal operational steps required to place the safety control function into a safe state are documented. All relevant input/output devices are referenced.		P
5.4.7 *	The main assembly operates safely where a secondary assembly fails or where there is a communication error		P
	For data transmission errors, the design includes techniques to mitigate the effects of any failure modes that include, at a minimum, the following conditions:		
	(a) corruption of the message data;	-	P
	(b) loss of a message;	-	P
	(c) the unplanned repetition of a message;	-	P
	(d) extra data	-	P
	(e) out-of-sequence messages; and	-	P
	(f) time delays that could impact safety.	-	P
	The design technique is documented.	-	P
5.4.8	Transmission reliability is equivalent to the requirements from item 6 in Table B.1.		P
5.4.9	Remote control devices		
5.4.9.1*	The following safety requirements apply for a system containing a remote control device:		

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
	(a) A remote command shall not result in an unsafe condition.		N/A
	(b) System reset action from a remote device requires also manual on-site intervention unless allowed for in the product standard.		N/A
5.4.9.2 *	A system reset requested from a remote device shall meet the following conditions:		
	(a) The request requires two manual actions		N/A
	(b) The maximum number of system resets shall be 5 within 15 minutes or as stated in product standard		N/A
5.4.9.3	A remote device with an external connection port not affect the safety integrity of the EUT.		N/A
5.4.9.4 *	System reset action from a remote-control device has access to relevant operational status information before, during and after the reset action.		N/A
5.4.9.5	An “emergency stop” function from a remote- control device places the EUT in its defined safe position within 2 seconds or as required by the FTT in the product standard.		N/A
5.4.9.6	A means exists to verify the integrity of the “emergency stop” function, and checking interval is less than the stated FTT.		N/A
5.4.10	**Remote control –Wireless devices**		
5.4.10.1	For a wireless remote device, the following requirements related to authentication and termination applies:		
	(a) device is enabled using a defined form of authentication by the main assembly		N/A
	Evidence exist to show that no operational data is transmitted before authentication		N/A
	(b) If the authentication fails, this shall not affect the safety.		N/A
	(c) Only remote devices declared as authenticated can communicate with the main assembly.		N/A

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
5.4.10.2	When battery has 72 hours remaining, an audible and/or visual alarm is initiated and continues for the duration. The 72 hour time may be superseded by the Part 2 standard.		N/A
5.4.10.3	Where a command from the wireless remote device can result in a safety critical output of the system, then the following requirements apply:		
	(a) The main assembly or control unit can set operation to either a 'wireless' or 'local' mode.		N/A
	(b) When the feature is set to "local" mode, the wireless remote device cannot operate		N/A
	(c) All remote command features are available in the "local" mode.		N/A
5.4.10.4	Where a command from the wireless remote device can result in a safety related output of the system, then the following requirements apply:		
	(a) A minimum of 2 states of battery condition exists; normal state when battery is fully operational, and "low battery" when battery needs to be changed or recharged.		N/A
	(b) The "low battery" indication is provided to the main unit at an interval of 1 minute or as declared by the Part 2 standard.		N/A
	(c) Remote is disabled at end of "low battery" period		N/A
5.4.10.5	Corrupted data shall not lead to an unsafe state.		N/A
	Faults caused by transmission errors shall be detected.		N/A
	Corrupted messages shall result in a retry with a maximum of three retries, after which the system shall indicate an error and go to a safe state.		N/A
5.4.11	**Management of unintended or unauthorized access**		
	Devices with communication ports shall have considerations for management of unintended or unauthorized access, e.g., cybersecurity, considering accepted industry good practice, and cybersecurity standards and legislation.		N/A
	Remote modification of protective functions, firmware/software, configuration, etc. shall be triggered by or accepted by an operator action at the device.		N/A
5.5	**Protection against faults to ensure functional safety**		

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
5.5.1.2 *	Control reaches a safe state less than FTT time or as specified by the manufacturer or by the productstandard.		P
5.5.1.3 *	Detection and response to a fault shall be in a shorter time frame than the fault tolerating time.		P
5.5.1.4 *	Using an analysis of the circuit to select circuit components.		P
	If the control ceases to function as a result of a test, it shall remain in a safe state or as defined by the relevant Part 2 standard		P
5.5.1.5 *	Class C - a relay used for a safety output has measures to handle contact welding.	Class B	N/A
5.5.1.6	For wireless remote-control devices, the following minimum requirements apply:		
	(a) Authentication integrity is being maintained in all operating modes.		N/A
	(b) “Emergency stop” function works in all operating modes.		N/A
	(c) Integrity of the local mode.		N/A
5.5.2*	During and at the end of each test required in Clause 5, the EUT shall comply with either Item (a) or (b), and there shall be no loss of safety functions:		
	(a) the control continues to operate normally and meets requirements of the product standard; or		P
	(b) the controller proceeds to a safety shut-down or a lock-out with safety outputs in defined safe state. After a safety shut-down the control may resume operation.		P
	After a lockout, the system becomes operational - only with operator intervention.		P
5.5.3 *	**Class B controls internal fault**		
5.5.3.1	For a class B control, a fault in an electronic component or that fault, together with another fault arising from the first fault, shall result in:		
	(a) the system proceeds to a safety shutdown condition and remains in this condition until the fault is removed;	-	P
	(b) the system proceeding to lock-out, provided that after the subsequent system reset from lock-out, under the same fault conditions would again proceed to lock-out;		P
	(c) the system remains operational in accordance with the safety-related		P

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
	specifications in the product standard; or		
	(d) the system continuing to operate, the fault being detected and identified during the next start- up, resulting in Item (a) or (b).	-	P
5.5.3.2	The system remains in a safe state if a fault occurs during a safety shutdown or lockout. Detection and response to a fault is in a shorter time frame than the safety time frame specified by the manufacturer or as per the product standard.	.	P
5.5.3.3	For a safety class B control, a second independent fault is not required.	Class B	P
5.5.3.4	Fault during lockout or safety shutdown: A first fault in an electronic component or that fault, together with another fault arising from the first induced while the controller is staying in the safety-shutdown or lockout position, shall result in:		
	(a) the control remains in safety shutdown or lockout condition		P
	(b) the control becomes inoperative with all safety-related output terminals remaining de- energized; or		P
	(c) the control resumes operation resulting in Item (a) or (b) under the condition that the safety-related output terminals are energized not longer than the stated fault reaction time.		P
	If the cause of the original safety shutdown or lockout condition no longer exists and the control again becomes operational, the system shall be operational in accordance with safety-related specifications in the product standard.		P
5.5.4 *	**Class C controls internal faults**		
5.5.4.1	A class C control function is in a safe state under first and second fault conditions.	Class B	N/A
5.5.4.2	First fault, for a safety class C control, a first fault in an electronic component or that fault, together with another fault arising from the first fault, shall result in		
	(a) the system proceeds to a safety shutdown condition and remains in this condition until the fault is removed;	Class B	N/A
	(b) the system proceeding to lock-out, provided that after the subsequent system reset from lock-out, under the same fault conditions		N/A

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
	would again proceed to lock-out;		
	(c) the system remains operational in accordance with the safety-related specifications in the product standard; or		N/A
	(d) the system continuing to operate, the fault being detected and identified during the next start- up, resulting in Item (a) or (b).		N/A
5.5.4.3	Second fault, when the control remains operational (5.5.4.2(c)) the application of the second independent fault considered together with the first fault results in one of the conditions specified in Clause 5.5.4.2. Occurrence of the second independent fault follows a start-up sequence after the first fault, or as stated by the manufacturer.		N/A
5.5.4.4	**Faults during define safe state**		
5.5.4.4.2	When the control is in the lock-out or safety shut-down condition as a result of an internal fault, a second assessment shall be applied – as in clause 5.5.4.6		N/A
5.5.4.5	First fault during defined safe state (these apply when control is in a lock- out or safety shutdown without an internal fault (5.5.4.4.1)		N/A
5.5.4.5.1	A first fault in an electronic component or that fault, together with another fault arising from the first, induced with the controller safety-shutdown or lockout position, results in:		N/A
	(a) the controller remaining in safety-shutdown or lockout;		N/A
	(b) the controller becoming inoperative with all safety-related output terminals remaining de- energized; or		N/A
	(c) the controller resuming operation, resulting in Item (a) or (b),		N/A
	The safety-related output terminals are energized no longer than the fault reaction time		N/A
5.5.4.5.2	If the cause of the original safety shutdown condition no longer exists and the controller again becomes operational, the system shall be operational in accordance with the product standard, and clause 5.5.4.6 applies		N/A
5.5.4.5.3	Controller does not become operational after a lockout if the original cause no		N/A

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict

	longer exists.		
5.5.4.6	Second fault during defined safe state (these are applied when the control is in a lock-out or safety shutdown without an internal fault (5.5.4.4.1)) This clause also applies when the control is in a lockout or safety shut-down with an internal fault (5.5.4.4.2)		N/A
5.5.4.6.1	Any second fault (together with any other fault arising from that fault) in any one component, induced while the control is staying in the safety shutdown or lockout position, result in one of the conditions in Clause 5.5.4.5 5.1	Class B	N/A
5.5.4.6.2	The timing for introducing the second fault meets the specified fault tolerating time. It is less or equal to 24 hours.	Class B	N/A
5.6	**Software development**		
5.6.1	**Software requirements**		
5.6.1.1	Requirements allocated to software is documented – and includes at a minimum:		
	(a) related to handling I/O device faults		P
	(b) microelectronic failures –Table B.1		P
	(c) special hardware associated with safety		P
	(d) safety functions that impact software		P
	(e) handling fault conditions, and error messages		P
	(f) safety requirements to handle OTS software		N/A
	g) requirements for field upgrades		N/A
5.6.1.2	For Class C – criteria for acceptance in testing exists for each requirement in 5.6.1.1	Class B	N/A
5.6.1.3	Software safety requirements can be traced back to the EUT safety requirements		P
5.6.1.4	Potential software failures that can lead to a hazard are included in requirements		P
5.6.1.5	Requirements for the interface to non-safety functions exist (when applicable).		P
5.6.2	**Software design**		

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
5.6.2.1	Software design includes all software requirements. A software architecture exists		P
5.6.2.2	Class C, - the design meets the software safety requirements.	Class B	N/A
5.6.2.3	Safety shutdown and lockout logic shall be clearly identified in the design and in the code		P
5.6.2.4	Timing restrictions & timing diagram.		P
5.6.2.5	Class C – Design includes high level description of the routines handling micro-electronic failures, with execution intervals	Class B	N/A
5.6.2.6	The software is to implement both safety and non-safety functions, all of the software shall be treated as safety related		N/A
	Unless adequate independence between the two software partitions can be demonstrated.		P
5.6.2.7	Non-safety related software does not impact safety -related software		P
5.6.2.8	Integrity of critical data is preserved.		P
5.6.2.9	A single user input does not initiate an operation resulting in a risk		P
5.6.2.10	User input is not able to alter safety-related software to compromise safety		P
5.6.2.11	User cancellation of an input operation shall not affect operational safety		P
5.6.2.12	User input shall be performed and accepted within a specified time limit		P
	A time-out cancels the operation.		
5.6.2.13	The sequence of operation is controlled.		P
5.6.2.14	After initialization EUT is in safe state		P
5.6.2.15	Software places the EUT in a safe state when detecting a condition capable of resulting in a risk		P
5.6.3	Software review and testing		
5.6.3.1	Reviews held to cover software design and software code. Records documented.		P

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
5.6.3.2	Software design meets the safety requirements and the architecture.		P
	Modules meet documented software design.		P
5.6.3.3	Class C-- Review meeting agenda exists	Class B	N/A
	Class C-- Errors and defects documented.		N/A
5.6.3.4	Class C-- Module testing criteria and results documented	Class B	N/A
5.7	**System integration and validation testing**		
5.7.1 *	EUT system testing follows the validation test plan, including:		
	(a) safety-related system requirements;		P
	(b) 1st and 2nd faults (5.5)		P
	(c) Potential failure events that lead to a safety shutdown or a lockout condition; and		P
	(d) Microelectronic failures (Table B.1)		P
5.7.2 *	The tests cover all potential failure events for either a safety shutdown or a lockout.		P
5.7.3 *	System (hardware and software) validation test plan includes:		
	(a) the testing procedure;		P
	(b) system configuration and software version used		P
	(c) the test cases for all requirements and expected results;		P
	(d) any OTS software; and	No OTS software	N/A
	(e) test results and traceability to test cases		P
5.7.4	Has demonstrated (in test results) that all safety requirements for software work as intended.		P
5.7.5	Stress and boundary testing shall be performed to verify the safety integrity. As a minimum, the following scenarios are addressed:		
	(a) software fault conditions;		P
	(b) errors in data from an input signal; and		P

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
	(c) errors in input data from a user.		P
5.7.6 *	Compliance to the requirements of this Standard shall require the successful completion of validation tests based on the test cases selected by the certification body		P
5.7.7	**Communications errors** Detection of errors – as specified in 5.4.7 - associated with data transmission results in one of the following conditions for the EUT or as specified in the product standard:		
	(a) recovery from the error in order to continue operating;		P
	(b) placing the EUT in a safe state while providing an indication of the error;		P
	(c) disabling the offending remote-control unit, and continuing operation, where this is allowed by the product standard.		N/A
	Response to data errors shall be provided such that the safety of the EUT is maintained, and		P
	error conditions are adequately identified.		P
5.7.8	Testing of remote controls		
5.7.8.1 *	Remote controls shall be tested to verify handling of the following conditions:		
	(a) Operation of a system reset command be in accordance with Clause 5.4.9.2 and 5.4.9.4.		N/A
	(b) Data from a remote device cannot modify any safety critical software or parameters.		N/A
5.7.8.2	For wireless remote-control devices, the following minimum test conditions, or as in product standard, have been verified:		
	(a) Commands from the remote control are ignored by the EUT when in “local” mode		N/A
	Safe shutdown works in all operating modes.		N/A
	(b) All remote commands are ignored if a control was not authenticated		N/A
5.8	**Maintenance and change control**		
5.8.1 *	Equipment changes use engineering change procedures. This includes or references software change procedure.		P
5.8.2	Safety impact of software changes is evaluated. Change records are retained		P
5.8.3	All software and hardware changes shall be tracked and recorded		P

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
5.8.4	Field upgrades (if applicable): –handling of upgrades are covered by the design - it can be demonstrated that any risks to safety are addressed.		N/A
5.8.5	**Managing software changes**		
5.8.5.1	Following software activities are managed during the project development activities:		
	(a) identification of the software items – at least for software code and documentation- are controlled, including a method for identifying version;		P
	(b) managing change requests – including tracking and approval;		P
	(c) status of change activities including an audit trail of all software changes; and		P
	(d) managing software releases		P
5.8.5.2	The audit trail of changes exists and includes as a minimum - the reason for the modification, and - the applicable software release.		P
	It has been demonstrated that the change(s) work correctly and do not adversely impact the safety of the system		P
5.8.5.3	Formal release of software and documentation shall be controlled		P
5.8.5.4	Equipment change handling shall use documented engineering change procedures. Where the safety control includes software, this engineering change procedure shall include or make reference to procedures for handling software changes.		P
5.8.5.5	The software version is unique identifier and marked on the equipment. Identifier shall be stored in non-volatile memory. Using this identifier, it is possible to demonstrate that the equipment safety software is the same as the approved software. Where multiple MCUs exist, the unique identifier shall be marked on each individual MCU that contains safety-related software.		P
5.8.5.6	The software version shall be traceable to the microcontroller used within the product configuration.		P

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict

5.9	**Software tools**		
5.9.1	Tool documentation includes:		
	(a) the name of the tool supplier or developer;		P
	(b) tool model, application, or trade name;		P
	(c) the tool version;		P
	(d) purpose of tool is described; and		P
	(e) a list of all errors, faults, or failures of tool performance. Also other known problems as identified by the manufacturer (“bug list”).		P
5.9.2	The manufacturer has identified if any of the tool bugs (Clause 5.9.1(e)) affect the safety software.		P
5.10 *	**Subcontractor management**		
5.10.1	Subcontractor is aware of all clauses that can affect the quality of the work performed		N/A
5.10.2	Manufacturer has verified work performed by sub-contractor		N/A
5.10.3	Documentation exists to cover: - Responsibilities of the subcontractor, and - Methods for checking completed work		N/A
5.10.4	Class C – A document exists that demonstrates the capability of the subcontractor to perform the work as adequate.	Class B	N/A
6 *	**Safety tests for electronic components**		
6.3.2	Power up and power down operation. EUT does not exhibit any unsafe conditions when powered up 25 time from a controllable power supply – from 20 to 110 % of the equipment rated voltage at a rate not exceeding 10V/s.		P
	EUT does not exhibit any unsafe conditions when subjected 25 times to a reduction of the line voltage from 100 to 20 % of equipment rated voltage, – at a rate not exceeding 10 V/s		P
6.3.4.2	Initially operated at rated voltage, the control is subject to a voltage dips as per clause 6.3.3.3 without exhibiting any unsafe condition.		P
6.4.4.5	A fault shall be simulated or applied to one electronic device or other circuit component at a time, in accordance with Table A.1. The control shall comply with the safety requirements given in the product standard and either of the following		

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
	conditions:		
	(a) The control shall continue to operate normally within the declared values.		P
	(b) The output of the control shall assume the declared safety conditions. At the conclusion of all testing, the product shall undergo a dielectric strength test and comply with the spacing requirements of the product standard.		P
7	**Documentation**		
7.1 *	System documentation		
7.1.1	The operational description for the equipment under test includes:		
	(a) description of all modes of operation;		P
	(b) a description of the error display method, with a list of all error messages and their meaning; and		P
	(c) the corrective actions to be performed by a user/operator for each error indication.		P
7.1.2	An architectural description of the equipment exists covering the requirements of Clause 5.2.		P
	Description includes a block diagram identifying the major components in the system, including all devices that are safety related.		P
	Major parts are identified		P
7.1.3	The documentation covering the safety requirements and the safety design for the EUT shall include, at a minimum:		
	(a) all requirements for corrective actions, (design requirements) to handle failure modes identified in the fault tree analysis and the FMEA analysis.		P
	Each requirement has a unique ID		P
	(b) safety requirements cover those from this standard and from the product standard; and		P
	(c) design description covering both the hardware and software.		P
7.1.4	A hazards analysis report exists as per clause 5.3 and documented according to clause 7.1.5.		P
7.1.5	The HA report for the EUT meets the requirements of Clause 5.3 and includes, as		

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict

	a minimum,		
	(a) name of author and report date		P
	(b) the software version		P
	(c) the list of identified safety hazard(s) that are included in the design;		P
	(d) for each hazard - a list of the potential failure events and relationships using a fault tree; and		P
	(e) brief description of the safety measures to handle each of the potential failures		P
7.1.6	Test results, documented in accordance with the requirements in Clause 5, shall include, at a minimum, the following:		
	(a) reference to software version used, the date, and the person running the tests;		P
	(b) details of test data and procedures used; and		P
	(c) details showing if each test passed or failed.		P
7.1.7	Product documentation shall include, at a minimum,		
	(a) PCB layout and drawings of PCB traces;		P
	(b) bill of materials with reference to the MCU and software version;		P
	(c) list of critical components; and		P
	(d) list of the safety-related errors issued and the corrective actions required.		P
7.1.8	Product specifications and installation details meet the requirements of Clause 6.		P
7.1.9	A schematic diagram has been provided.		P
7.1.10	The results of the test to verify the safety design of the EUT shall be documented and include		P
	(a) handling first and second faults;		P
	(b) FMEA; and		P
	(c) test results for remote control devices.		N/A

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict
7.1.11	Secondary assemblies		N/A
7.1.11.1	The interface between any secondary assembly and the main assembly shall be described. This description includes, at a minimum,		
	(a) list of commands and responses initiated,		N/A
	(b) the handling of failures associated with the communications link; and		N/A
	(c) the status of each assembly during safety shutdown and system reset.		N/A
7.1.11.2	Test results for secondary assemblies, including remote devices demonstrate compliance with the applicable requirements in clauses 5.4 and 5.7. The test documentation meets format in clause 7.1.6.		N/A
7.2	**Software documentation**		
7.2.1	Software safety requirements are documented		P
7.2.2	The software design is documented (Clause 5.6.2) and includes the following items:		
	(a) cover safety-related requirements;		P
	(b) software architecture;		P
	(c) Description of function for all safety-related software modules		P
	(d) hardware-software interfaces for the MCU and for all input/output devices;		P
	(e) critical timing requirements with timing diagram as needed;		P
	(f) for class C, documentation each software safety requirement is included in the software design; and	Class B	N/A
	(g) If field upgrades are planned) – description covers field upgrades with reference to need tomaintain safety integrity		N/A
7.2.3	Test plans and results are documented (reference Clauses 5 and 7.1.6) and covers:		
	(a) class C -- module testing (5.6.3.4);	Class B	N/A
	(b) class C -- software integration testing;	Class B	N/A
	(c) system validation test plan with test cases for all safety related requirements (5.7); and		P
	(d) class C -- procedure for handling failed test cases is documented.	Class B	N/A

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict

7.2.4	OTS software documented -- Clause 5.2.8	No OTS software used for this product.	N/A
	Software tools documented – Clause 5.9.		P
7.2.5	Minutes of design and code review meetings are documented (clause 5.6.3) and include list of attendees, date of the meeting, and a list of the findings.		P
	For class C -- review criteria includes documented coding standards	Class B	N/A
7.2.6	The program execution sequence is documented and includes error handling and initialization sequences.		P
7.2.7	The memory map is documented.		P
7.2.8	Design details for handling the data transmission failures listed in Table 12 are documented, and use the Table format.		P
7.3	**Support documentation**		
7.3.1	A project development plan is documented and includes:		P
*	(a) description of the development phases from safety requirements to testing and software release;		P
	(b) class C -- reference to deliverables produced in each development phase; and	Class B	N/A
	(c) * the subcontractor control requirements (Clause 5.10)	No subcontractor.	N/A
7.3.2	Procedures for configuration management are documented and include:		
	(a) procedures for managing software items during development		P
	Procedure includes details for identifying the software code and documentation and their versions.		P
	(b) the methods used to control software changes: (i) changes are documented, reviewed and approved. (ii) class C -- procedures for the formal approval of safety-related software changes;	Class B	P
	(c) methods for managing both procedure and product documentation; and		P
	(d) methods for formal release of software, and methods to test modified software release.		P

CSA C22.2#0.8			
Clause	Requirement + Test	Result - Remark	Verdict

Note: The Clauses specified in Table 2 of CSA C22.2 No. 0.8 are marked with an asterisk (*)

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict

APPENDIX A

TABLE OF MEASURES TO ADDRESS FAULTS / ERRORS (MICROELECTRONIC FAILURES) CSA C22.2 NO. 0.8, TABLE B.1 / UL 1998 TABLE A.2.1.

COVERAGE FOR MICROELECTRONIC HARDWARE FAILURE MODES (SOFTWARE CLASS 1/B)			
Component	Fault/error	Declared measures	Verdict
1. CPU	-	-	-
1.1 Registers	Stuck at	Static Memory Test	P
1.3 Program counter	Stuck at	Register flip check	P
2. Interrupt handling and execution	No interrupt	-	N/A
	Too frequent interrupt	-	N/A
3. Clock	Wrong frequency (for quartz synchronized clock: harmonics/ sub-harmonics only)	Frequency monitoring	P
4. Memory	-	-	-
4.1 Invariable memory	All single bit faults	Multiple checksum	P
4.2 Variable memory	DC fault	Hash value verification is performed through CRC calculation	P
4.3. Addressing (relevant to variable and invariable memory)	Stuck at	-	N/A
5. Internal data path	-	-	-
5.1 Data	Stuck at	-	N/A
5.2 Addressing	Wrong address	-	N/A
6. External communication	-	-	-
6.1 Data	Hamming distance 3	Multiple checksum	P
6.2 Addressing	Wrong address	-	P
6.3 Timing	Wrong point in time	-	P
	Wrong sequence	-	P
7. Input/output periphery	-	-	-
7.1 Digital I/O	Failures due to open and short circuit of the I/O	PLAUSIBILITY CHECK	P
7.2 Analog I/O	-	-	-

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict

7.2.1 A/D and D/A-convertor	Open and short circuit failures Or Failure in D/A conversion	-	P
7.2.2 Analog multiplexer	Wrong addressing	-	P
9. Custom chips e.g. ASIC, GAL, gate array	Any output outside the static and dynamic functional specification	-	N/A

Coverage for microelectronic hardware failure modes (Software Class 2/C)			
Component	Fault/error	Declared measures	Verdict
1. CPU	-	-	-
1.1 Registers	DC fault		N/A
1.2 Instruction decoding and execution	Wrong decoding and execution		N/A
1.3 Program counter	DC fault		N/A
1.4 Addressing	DC fault		N/A
1.5 Data paths instruction decoding	DC fault		N/A
	execution		N/A
2. Interrupt handling and execution	No interrupt		N/A
	Too frequent interrupt related to different sources		N/A
3. Clock	Wrong frequency (for quartz synchronized clock: harmonics/ sub-harmonics only)		N/A
4. Memory	-	-	-
4.1 Invariable memory	99,6 % coverage of all information errors		N/A
4.2 Variable memory	DC fault		N/A
	Dynamic cross links		N/A
4.3 Addressing (relevant to variable and invariable memory)	DC fault		N/A
5. Internal data path	-	-	-
5.1 Data	DC fault		N/A
5.2 Addressing	Wrong address		N/A
	Multiple addressing		N/A
6 External communication	-	-	-

UL 1998			
Clause	Requirement + Test	Result - Remark	Verdict
6.1 Data	Hamming distance 4		N/A
6.2 Addressing	Wrong address		N/A
	Multiple addressing		N/A
6.3 Timing	Wrong point in time		N/A
	Wrong sequence		N/A
7. Input/output periphery	-	-	-
7.1 Digital I/O	Failures due to open and short circuit of the I/O		N/A
7.2 Analog I/O	-	-	-
7.2.1 A/D and D/A-convertor	Open and short circuit failures Or Failure in D/A conversion		N/A
7.2.2 Analog multiplexer	Wrong addressing		N/A
8. Monitoring devices and comparators	Any output outside the static and dynamic functional specification		N/A
9 Custom chips e.g. ASIC, GAL, gate array	Any output outside the static and dynamic functional specification		N/A

APPENDIX B

TABLE: List of critical components

	TABLE: List of critical components				P
Object / part No.	Manufacturer/ trademark	Type / model	Technical data	Standard	Mark(s) of conformity[1]
MCU	GD	GD32E513ZE T6	512KB Flash，128KB SRAM, 180MHz, LQFP144	UL1998 CSA C22.2 No. 0.8	Test with appliance
Supplementary information: 1) Provided evidence ensures the agreed level of compliance. See OD-CB2039. 2) Description line content is optional. Main line description needs to clearly detail the component used for testing 3) Only the programmable component(s) and components directly interfacing with them (such as: oscillators, external memory components, monitoring devices, etc.) are to be shown in the table of this Test Report Form. The end-product Test Report Form would include the Critical Components from this Table as well as all the additional Hardware Critical Components related to the Safety Function(s).					

Photo 1.

Description: Inside view



Photo 2.

Description: PCB1

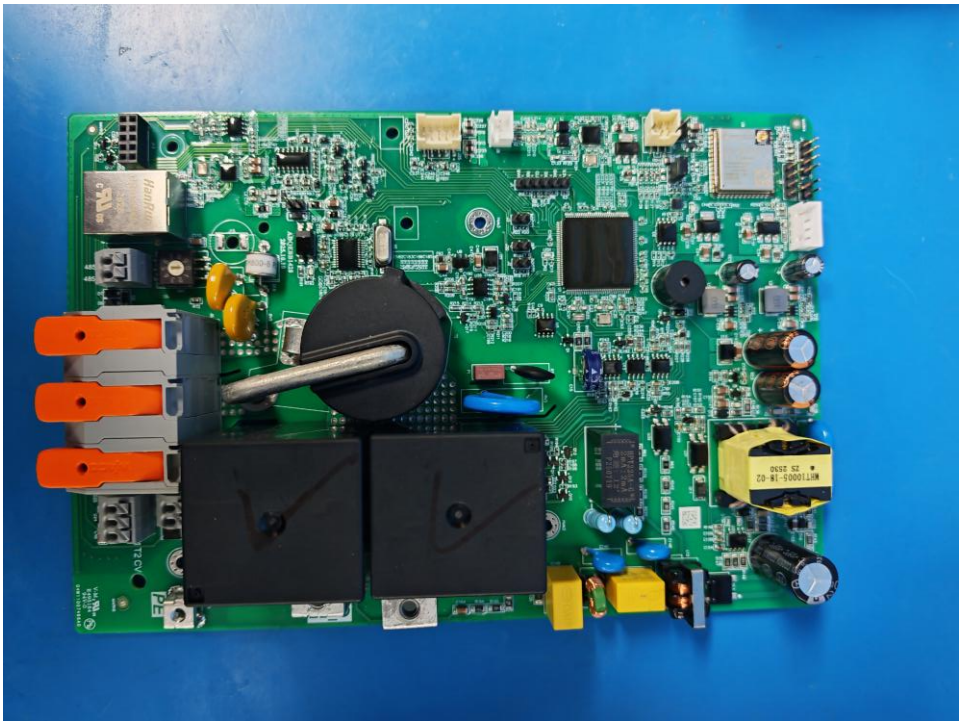


Photo 3.

Description: PCB2

