TEST REPORT
IEC 60730-1 Annex H & IEC60335-1 Annex R
(Requirements related to functional safety)

Report Number.....:	**CKOQ-ESH-P23040976**
Date of issue.....:	**8/22/2023**
Total number of pages.....:	**27**
Name of Testing Laboratory preparing the Report.....:	**BUREAU VERITAS LCIE CHINA COMPANY LIMITED**
Applicant's name .....:	**SHANGHAI MINDMOTION MICROELECTRONICS CO.,LTD**
Address .....:	**1-3/F,No.54,Lane 565,Shengxia Road,(Shanghai)Pilot Free Trade Zone,P.R.China**
Test specification:	
Standard .....:	**IEC 60730-1 Edition6.0 2022-09 Annex H & IEC 60335-1 Edition6.0 2020-09 Annex R**
Non-standard test method.....:	**N/A**
TRF template used .....:	**IECEE OD-2020-F1:2022, Ed.1.5**

Test item description..... :	See page 4 Product Description
Trademark(s)..... :	
Manufacturer..... :	SHANGHAI MINDMOTION MICROELECTRONICS CO.,LTD
Model/Type reference..... :	See page 4 Product Description
Ratings..... :	CLASS B

CONCLUSION

Samples of the component covered by this Report have been found to comply with the requirements covering the category and the component is found to comply with IEC 60730-1 Annex H & IEC60335-1 Annex R.

Tested by (name, function, signature).....:	Hancheng Su project Engineer	Lukas Su
Approved by (name, function, signature)...:	Jian Qiu Technical Manager	Jacky Qiu

List of Attachments:

TABLE H.2 – MEASURES TO ADDRESS FAULT/ERRORS (Software Class B)

TABLE H.2 – MEASURES TO ADDRESS FAULT/ERRORS (SOFTWARE CLASS C)

TABLE: MANUFACTURER'S DOCUMENTATION REFERENCED IN THIS TRF (INFORMATIVE)

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

EU Group Differences including the following National Differences:
Austria, Belgium, Bulgaria, Cyprus, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany,Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland,Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

US and Canada

BS EN 60730-1:2016+A2:2022 Annex H

EN 60335-1-2012/A2 Annex R

☐ **The product fulfils the requirements of _____ (insert standard number and Year of publication, and delete the text in parenthesis, leave it blank or delete the whole sentence, if not applicable)**

Use of uncertainty of measurement for decisions on conformity (decision rule) :

☒ No decision rule is specified by the IEC standard, when comparing the measurement result with the applicable limit according to the specification in that standard. The decisions on conformity are made without applying the measurement uncertainty ("simple acceptance" decision rule, previously known as "accuracy method").

☐ Other: … (to be specified, for example when required by the standard or client, or if national accreditation requirements apply)

Information on uncertainty of measurement:
The uncertainties of measurement are calculated by the laboratory based on application of criteria given by OD-5014 for test equipment and application of test methods, decision sheets and operational procedures of IECEE.
IEC Guide 115 provides guidance on the application of measurement uncertainty principles and applying the decision rule when reporting test results within IECEE scheme, noting that the reporting of the measurement uncertainty for measurements is not necessary unless required by the test standard or customer.

Calculations leading to the reported values are on file with the NCB and testing laboratory that conducted the testing.

Test item particulars.....:	Not applicable to embedded software
Classification of installation and use .....:	N/A
Supply Connection .....:	N/A
.....:	
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 ..... :	BUREAU VERITAS LCIE CHINA COMPANY LIMITED
Date of receipt of test item..... :	7/6/2023
Date (s) of performance of tests ..... :	8/22/2023

General remarks:

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

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

☒ **This Test Report Form contains requirements according to IEC 60730-1, Standard dated 2022-09.**

Manufacturer's Declaration per sub-clause 4.2.5 of IECEE 02:

The application for obtaining a CB Test Certificate includes more than one factory location and a declaration from the Manufacturer stating that the sample(s) submitted for evaluation is (are) representative of the products from each factory has been provided.....:	☐ **Yes** ☒ **Not applicable**

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

Name and address of factory (ies).....:	SHANGHAI MINDMOTION MICROELECTRONICS CO.,LTD 1-3/F,No.54,Lane 565,Shengxia Road,(Shanghai)Pilot Free Trade Zone,P.R.China

General product information and other remarks:

Product Description
The subject product is an open-source software library called IEC60730_B_STL intended to be used within a 32-bit Mindmotion microcontroller and embedded in the end product application software.

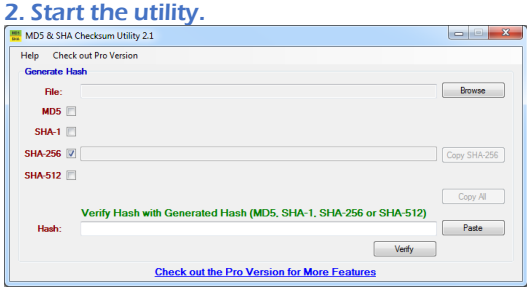
STL	**Common STL stack source files**	
	File	**Descrption**
Start-up test	IEC60730_B_startup.c	Start-up STL flow control & start-up test
	IEC60730_B_cpustartIAR.s	Cpu start-up self test
	IEC60730_B_cpustartKEIL.s	Cpu start-up self test
Run time test	IEC60730_B_runtimetest.c	Run time self tests structure

	IEC60730_B_flashtest.c	Partial Flash CRC run time self test
	IEC60730_B_transpRam.c	Partial RAM run time self test structure
	IEC60730_B_clocktest.c	Clock run time self test
	IEC60730_B_aux.c	It includes call interfaces for error handling functions, watchdog detection and initialization, CSS interrupt handling, SysTick time base handling, and runtime RAM detection.
Headers	IEC60730_B_clock.h	Clock test header
	IEC60730_B_cpu.h	CPU test header
	IEC60730_B_crc32.h	Flash memory test header
	IEC60730_B_init.h	Support interface header
	IEC60730_B_lib.h	Overall STL includes control
	IEC60730_B_param.h	Support param header
	IEC60730_B_Ram.h	RAM test header
	IEC60730_B_startup.h	Initial process STL header
	IEC60730_B_var.h	Support var header

STL	Header	File
Source	Keil	IEC60730B_M0_COM_KEIL_v1_0.lib
		IEC60730B_M0_COM_KEIL_v1_0_debug.lib
	IAR	IEC60730B_M0_COM_IAR_v1_0.a
		IEC60730B_M0_COM_IAR_v1_0_debug.a

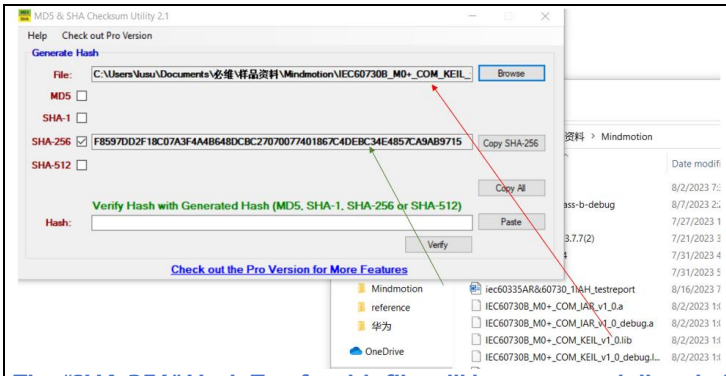
File Name	SHA-256 Hash-Tag:
IEC60730B_M0_COM_KEIL_v1_0.lib	F8597DD2F18C07A3F4A4B648DCBC27070077401867C4DEBC34E4857CA9AB9715
IEC60730B_M0_COM_KEIL_v1_0_debug.lib	DC4BFF10B34184E1AC30EF7889FA4DE00CBC419A4D9484D9C795BEC0B79F2FC7
IEC60730B_M0_COM_IAR_v1_0.a	307F1EED803AA489F370544373A4A7F98C4312B0A0C2BE91DE9FA2F9EE212631
IEC60730B_M0_COM_IAR_v1_0_debug.a	6E7D51375ED8A17C2AC677EF1E07F5DD3A43DDB77EA06E818BAD887902B60B13

1. Download from internet a utility like "MDS_and_SHA_Checksum_Utility.exe" via the following link: https://download.cnet.com/MD5-SHA-Checksum-Utility/3000-2092_4-10911445.html. (Another example is the link https://www.nirsoft.net/utils/hash_my_files.html. Click to "Download HashMyFiles".)
2. Start the utility.



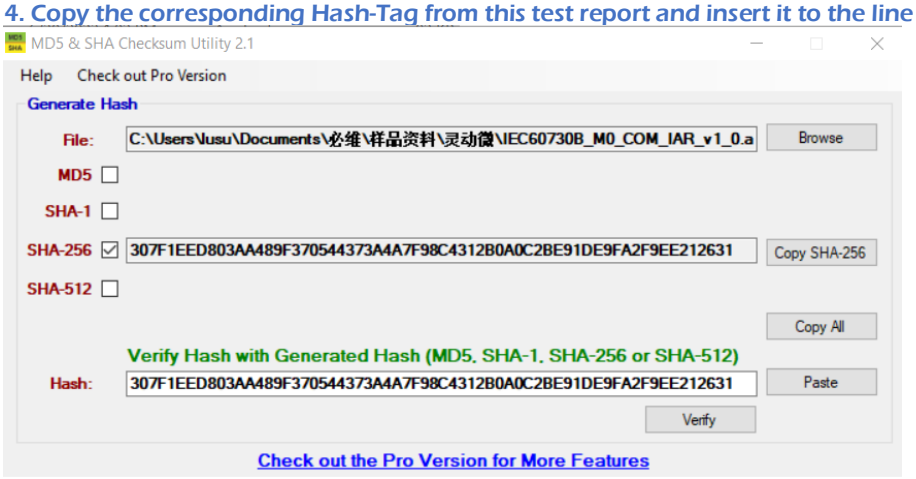
Delete the hooks for "MDS", "SHA-1" and SHA-512

3. In the windows file explorer mark the downloaded object code file and move it the line "File" (see red arrow).

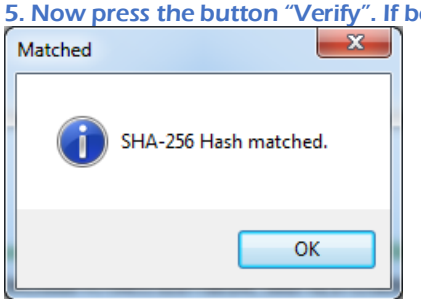


The "SHA-256" Hash-Tag for this file will be generated directly (see green arrow).

4. Copy the corresponding Hash-Tag from this test report and insert it to the line "Hash" (see red arrow).



5. Now press the button "Verify". If both Hash-Tags are identically the window below will pop up.



The STL is called upon power-on initialization and/or periodically within the application to achieve the periodic self-test safety requirements in Annex H.11.12 of IEC/UL/CSA 60730-1, Software Class B:

- CPU core test
- RAM functional check
- Flash CRC integrity check
- System clock monitoring
- Stack boundary test

The functions investigated in this report include self-tests of the following microelectronic hardware components:

- CPU Registers
- CPU Program Counter
- Clock
- Variable Memory (RAM)
- Invariable Memory (FLASH memory)

Model Differences –

The files referenced under this test report support the following cores in reference to the devices as shown by the table below:

CPU CORE	MCU FAMILY NAME
Cortex-M0	MM32A0140、MM32A0160、MM32F0010、MM32F0020、MM32F003、MM32F0040、MM32F0130、MM32F0140、MM32F0160、MM32F0270、MM32F031xx_q、MM32F031xx_s、MM32F031xx_n、MM32G0001、MM32G0140、MM32G0160、MM32L0xx_n、MM32SPIN0230、MM32SPIN023C、MM32SPIN0280、MM32SPIN030C、MM32SPIN030CN、MM32SPIN040C、MM32SPIN040CN、MM32SPIN05、MM32SPIN06、MM32SPIN07PF、MM32SPIN080C、MM32SPIN080CN、MM32SPIN160C、MM32SPIN222C、MM32SPIN223C、MM32SPIN2x、MM32SPIN320B、MM32SPIN360C、MM32SPIN37PSD、MM32SPIN380C、MM32SPIN422C、MM32SPIN560C、MM32SPIN580C、MM32W0130、MM32W0xx

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

In case of fail detection, FailSafePOR() routine is called (defined in IEC60730_B_aux.c file).
By default, there is no specific handling inside the procedure except for debug support and an empty loop waiting for a watchdog reset (the reset can be prevented in debug mode). It is fully upon user responsibility to build up a handler inside this routine and perform all the necessary steps to bring the application in a safe state, while taking.

DESCRIPTION OF SAFETY FUNCTION(S)

(Similar to Protective Electronic Circuit, per IEC 60335-1)

Reference Documents	Name
Application Guide	Mindmotion Software Design Guidance to Compliance with IEC Standards.pdf
Test report	Mindmotion self monitoring fault injection test software test report.pdf

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

IEC 60335-1(Annex R)			
Clause	Requirement + Test	Result - Remark	Verdict
R	**ANNEX R (NORMATIVE) SOFTWARE EVALUATION**		
	Programmable electronic circuits requiring software incorporating measures to control the fault/error conditions specified in Table R.1 or R.2 validated in accordance with the requirements of this annex	Self-test routines for software of class R.1	P
R.1	Programmable electronic circuits using software		-
	Programmable electronic circuits requiring software incorporating measures to control the fault/error conditions specified in Table R.1 or R.2 constructed so that the software does not impair compliance with the requirements of this standard	The measures for controlling fault/error conditions specified in Tables R.1 or R.2 were used.	P
R.2	Requirements for the architecture		-
R.2.1	General		-
R.2.1.1	Programmable electronic circuits requiring software incorporating measures to control the fault/error conditions specified in Table R.1 or R.2 use measures to control and avoid software-related faults/errors in safety-related data and safety-related segments of the software		P
R.2.1.2	Programmable electronic circuits requiring software incorporating measures to control the fault/error conditions specified in Table R.2 have one of the following structures:		-
	- single channel with periodic self-test and monitoring		N/A
	- dual channel (homogenous) with comparison		N/A
	- dual channel (diverse) with comparison		N/A
	Programmable electronic circuits requiring software incorporating measures to control the fault/error conditions specified in Table R.1 have one of the following structures:		-
	- single channel with functional test		N/A
	- single channel with periodic self-test		N/A
	- dual channel without comparison		N/A
R.2.2	Measures to control faults/errors		-
R.2.2.1	When redundant memory with comparison is provided on two areas of the same component, the data in one area is stored in a different format from that in the other area		N/A

R.2.2.2	Programmable electronic circuits with functions requiring software incorporating measures to control the fault/error conditions specified in Table R.2 and that use dual channel structures with comparison, have additional fault/error detection means for any fault/errors not detected by the comparison		N/A
R.2.2.3	For programmable electronic circuits with functions requiring software incorporating measures to control the fault/error conditions specified in Table R.1 or R.2, means are provided for the recognition and control of errors in transmissions to external safety-related data paths		N/A
R.2.2.4	For programmable electronic circuits with functions requiring software incorporating measures to control the fault/error conditions specified in Table R.1 or R.2, the programmable electronic circuits incorporate measures to address the fault/errors in safety-related segments and data indicated in Table R.1 and R.2 as appropriate		P
R.2.2.5	For programmable electronic circuits with functions requiring software incorporating measures to control the fault/error conditions specified in Table R.1 or R.2, detection of a fault/error occurs before compliance with clause 19 is impaired	Self-test routines only; compliance to clause 19 has to be insured by the user of the self-test routines	N/A
	For appliances intended for remote communication through public networks, where normative Annex U is applicable as determined by 22.62, detection of a fault/error occurs before compliance with normative Annex U is impaired		N/A
R.2.2.6	The software is referenced to relevant parts of the operating sequence and the associated hardware functions		P
R.2.2.7	Labels used for memory locations are unique		P
R.2.2.8	The software is protected from user alteration of safety-related segments and data		P
R.2.2.9	Software and safety-related hardware under its control is initialized and terminates before compliance with clause 19 is impaired	Self-test routines only; compliance to clause 19 has to be insured by the user of the self-test routines	N/A
	For appliances intended for remote communication through public networks where normative Annex U is applicable as determined by 22.62, the software and safety-related hardware under its control is initialized and terminates before compliance with normative Annex U is impaired		N/A
R.3	Measures to avoid errors		-
R.3.1	General		-

	For programmable electronic circuits with functions requiring software incorporating measures to control the fault/error conditions specified in Table R.1 or R.2, the following measures to avoid systematic faults in the software are applied		-
	Software that incorporates measures used to control the fault/error conditions specified in Table R.2 is inherently acceptable for software required to control the fault/error conditions specified in Table R.1	Class R.1 only	N/A
R.3.2	Specification		
R.3.2.1	Software safety requirements:	Software version:1.0	P
	The specification of the software safety requirements includes the descriptions listed		P
R.3.2.2	Software architecture		-
R.3.2.2.1	The specification of the software architecture includes the aspects listed - techniques and measures to control software faults/errors (refer to R.2.2); - interactions between hardware and software; - partitioning into modules and their allocation to the specified safety functions; - hierarchy and call structure of the modules (control flow); - interrupt handling; - data flow and restrictions on data access; - architecture and storage of data; - time-based dependencies of sequences and data	Document ref. No: Mindmotion Software Design Guidance to Compliance with IEC Standards	P
R.3.2.2.2	The architecture specification is validated against the specification of the software safety requirements by static analysis		P
R.3.2.3	Module design and coding		-
R.3.2.3.1	Based on the architecture design, software is suitably refined into modules		P
	Software module design and coding is implemented in a way that is traceable to the software architecture and requirements		N/A
	The module design specifies:		-
	- function(s)		P
	- interfaces to other modules		P
	- data		P
R.3.2.3.2	Software code is structured		P
R.3.2.3.3	Coded software is validated against the module specification by static analysis		P

	The module specification is validated against the architecture specification by static analysis	Reviews and source code walk through	P
R.3.3	Software validation		-
	The software is validated with reference to the requirements of the software safety requirements specification		P
	Compliance is checked by simulation of:		P
	- input signals present during normal operation		P
	- anticipated occurrences		P
	- undesired conditions requiring system action		P
R.3.4	Management items		-
R.3.4.1	Management of software versions		N/A
	A software version management system at the module level is put in place		N/A
R.3.4.2	Software modification		
R.3.4.2.1	Software modifications are based on a modification request which details the following:		P
	- the hazards which may be affected		N/A
	- the proposed change		P
	- the reasons for change		P
R.3.4.2.2	An analysis is carried out to determine the impact of the proposed modification on functional safety		P
R.3.4.2.3	A detailed specification for the modification is generated including the necessary activities for verification and validation, such as a definition of suitable test cases		P
R.3.4.2.4	The modification is carried out as planned		-
R.3.4.2.5	The assessment of the modification is carried out based on the specified verification and validation activities, which may include:		N/A
	- a reverification of changed software modules		N/A
	- a reverification of affected software modules		N/A
	- a revalidation of the complete system		N/A
R.3.4.2.6	All details of modification activities are documented		N/A

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

IEC 60730-1 (Software)			
9.12.4	**REMOTELY ACTUATED CONTROL FUNCTIONS**		-
9.12.4.2.1	Data Exchange – Remotely actuated control functions can be connected to separate, independent devices, which may themselves contain control functions or provide other information. Any data exchange between these devices does not compromise the integrity of class B control function or class C control function.		N/A
9.12.4.2.2	Type of data - Message types for data exchange in a control function or functions are allocated to class A control function, class B control function or class C control function. Regarding the safety or protective relevance or influence, message types or data exchange are allocated only to class B control function or class C control functions, see Table 8.		N/A
9.12.4.2.3	Communication of safety related data – See H.9.12.4.2.3		N/A
9.12.4.2.4	For the operation of remotely actuated control function, the duration or limits of operation shall be set before switching on, unless an automatic switching off is realized at the end of a cycle or the system is designed for permanent operation. (operation for longer than 24 h without interruption or new cycle).	Structure depends on the end use application.	N/A
9.12.4.3	Priority of remotely actuated control functions over control functions does not lead to a hazardous condition.		N/A
9.12.4.4.1	Remote reset action is manually initiated		N/A
	When a reset function is initiated by a hand-held device, at least two manual actions are required to activate a reset.		N/A
9.12.4.4.2	Reset functions are capable of resetting the system as intended		N/A
9.12.4.4.3	Unintended resets from safe state do not occur.		N/A
9.12.4.4.4	Any fault of the reset function does not cause the control or controlled function to result in a hazardous condition. In such a case, the reset function complies with the Class B requirements, see H.13.2.2.		N/A
9.12.4.4.5	For reset functions initiated by manual action not in visible sight of the appliance, the following additional requirements apply:		N/A
	– the actual status and relevant information of the process under control is visible to the user before, during and after the reset action;		N/A

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

	– the maximum number of reset actions within a time period is declared. Following this, any further reset is denied unless the appliance is physically checked .....:		N/A
9.12.4.4.6	For integrated controls and incorporated controls, the reset function is evaluated in the final application.	Remote control does not involve.	N/A
	If the reset is activated by manual switching of a device, this function is specified by the manufacturer and is suitable in the final application.....:	Remote control does not involve.	N/A
9.12.4.4.7	Independently mounted controls performing remote reset functions is tested for a minimum 1000 reset actions.	Remote control does not involve.	N/A
	For integrated and incorporated devices, unless otherwise specified, the minimum reset cycles shall be declared by the manufacturer.....:	Remote control does not involve.	N/A
	After the test, the reset device shall be capable to reset the system as intended. Unintended resets shall not occur.	Remote control does not involve.	N/A

H.5	**INFORMATION**		
	Information in addition to Table 1 provided:		
	H.3 – Software sequence documentation; clause, H.9.12.2.9, method X	Open source code Verified	P
	H.4 - Programme documentation; clause H.9.12.2.9, H.9.12.2.11, method X .....:	Open source code Verified	P
	H.5 - Software fault analysis; clause H.9.12, 13.1.3, method X .....:	Refer to appended table for list of microelectronic component addressed by the IEC60730_B_STL along with related failure/error Verified by inspection	P
	H.6 - Software class(es) and structure; clause: H.9.12.2, H.9.12.3, H.13.2.2.1, H.13.2.3.1, method: D	Class B Structure depends on the end use application	P
	H.7 - Analytical measures and fault/error control techniques employed; clause: H.9.12.1.2, H.9.12.2.2, H.9.12.2.4; method X .....:	Refer to appended table for list of microelectronic component addressed by the IEC60730_B_STL along with related failure/error	P

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

	H.8 - Software fault/error detection time(s) for controls with software classes B or C; clause H.3.17.10, H.9.12.2.6; method X .....:	Overall RAM and FLASH run time test duration depends on repetition frequency of the steps, their sizes and size of memory area under test. It depends on the end use application.	P
	H.9 - Control response(s) in case of detected fault/error; clause . H.9.12.2.7, method X.....:	In case of fail detection, FailSafePOR() routine is called (defined in defined in IEC60730_B_aux.c file). Program stays in endless loop waiting for watchdog reset alternatively user can build up a handler inside this routine.	P
	a – For controls with software classes B or C, information is provided for safety-related segments of the software. Information on the non-safety related segments is sufficient to establish that they do not influence safety-related segments.....:	IEC60730_B_STL library is class B software	N/A
	b - Software sequence is documented and, together with the operating sequence of table requirement 46, include a description of the control system philosophy, the control flow, data flow and the timings. .....:	Mindmotion Software Design Guidance to Compliance with IEC Standards.pdf	P
	c - Safety-related data and safety-related segments of the software sequence, the malfunction of which could result in non-compliance with the requirements of Clauses 13, 19, 24 and H.25, are identified .....:	IEC60730_B_STL are designed to embed mechanisms to mitigate microelectronic failure/error in the end use application	P
	– Included the operating sequence.....:	IEC60730_B_STL has its own control flow mechanism	P
	– Software fault analysis is related to the hardware fault analysis in Clause H.13.2.	IEC60730_B_STL are linked to specific Mindmotion family members, as mentioned in product description	P
	e - Programming documentation is supplied in a programming design language declared by the manufacturer.....	Written in assembly and C language Startup and runtime CPU and RAM tests written in Assembler for Keil compilers	P
	f - Different software classes applied to different control functions .....:		N/A
	g - Measures declared are chosen by manufacturer from the requirements of Clauses H.9.12.1.2 to H.9.12.2.4 inclusive. .....:	See appended table	P

H.9	**CONSTRUCTIONAL REQUIREMENTS**	
H.9.12	Controls using software	

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

	Controls using software are constructed that the software did not impair control compliance with the requirements of this document.		P
H.9.12.1	Requirements for the architecture		
H.9.12.1.1	Control functions with software class B or C use measures to control and avoid software-related faults/errors in safety-related data and safety-related segments of the software, as detailed in H.9.12.1.2 to H.9.12.3 inclusive .....:	Software Class B; verified by inspection based on manufacturer provided document, Mindmotion Software Design Guidance to Compliance with IEC Standards	N/A
H.9.12.1.2	Control functions with software class C have one of the following structures:		N/A
	- single channel with periodic self-test and monitoring (H.3.16.7);		N/A
	- dual channel (homogenous) with comparison (H.3.16.3);		N/A
	- dual channel (diverse) with comparison (H.3.16.2).		N/A
H.9.12.1.2.2	Control functions with software class B have one of the following structures:		
	- single channel with functional test (H.3.16.5);	It depends on the end use application	P
	- single channel with periodic self-test (H.3.16.6);	It depends on the end use application	P
	- dual channel without comparison (H.3.16.1).	It depends on the end use application	P
H.9.12.1.3	Other structures are permitted if they can be shown to provide an equivalent level of safety to those in H.9.12.1.2. .....:		N/A
H.9.12.2	Measures to control faults/errors		
H.9.12.2.1	Redundant memory with comparison provided on two areas of the same component: data stored in different formats	Used for safety critical (“Class B”) Variables only	P
H.9.12.2.2	Software class C using dual channel structures with comparison have additional fault/error detection means for any fault/errors not detected by the comparison.	Not Applicable	N/A
H.9.12.2.3	Software class B or C: means for recognition and control of errors in transmission to external safety-related data paths: Means take into account errors of data, addressing, transmission timing and sequence of protocol	Not Applicable	N/A
H.9.12.2.4	Software class B or C: within the control, measures are taken to address fault/errors in safety-related segments and data indicated in Table H.2 and declared in Table H.1, requirement H.5	Software Class B; verified by inspection based on manufacturer provided document, Mindmotion Software Design Guidance to Compliance with IEC Standards	P

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

H.9.12.2.5	Measures others than those specified in H.9.12.2.4 are permitted if they can be shown to satisfy the requirements listed in Table H.2.	Not Applicable	N/A
H.9.12.2.6	Software fault/error detection:		
	- occur not later than the time declared in Table H.1, requirement H.8.	Overall RAM and FLASH run time test duration depends on repetition frequency of the steps, their sizes and size of memory area under test. It depends on the end use application.	P
	- acceptability of the declared time(s) is evaluated during the fault analysis of the control.	It depends on the end use application	P
H.9.12.2.7	For controls with functions, classified as Class B or C, detection of fault/error:		
	- shall result in the response declared in Table H.1, requirement H.9.	In case of fail detection, fault routine is called (defined in defined in IEC60730_B_aux.c file). Program stays in endless loop waiting for watchdog reset alternatively user can build up a handler inside this routine	P
	- for Class C control functions: independent means capable of performing this response are provided	Not Applicable	N/A
H.9.12.2.8	Class C, dual channel structure, loss of dual channel capability: deemed to be an error	Not Applicable	N/A
H.9.12.2.9	Software is referenced:		
	– to relevant parts of the operating sequence	Mindmotion Software Design Guidance to Compliance with IEC Standards	P
	– to the associated hardware functions	Mindmotion Software Design Guidance to Compliance with IEC Standards	P
H.9.12.2.10	Software is protected from user alteration of safety-related segments and data	Open code	N/A
H.9.12.2.11	Software and safety-related hardware under its control are initialized to and terminate at a declared state, Table H.1, requirement H.4.	Refer to Table H.1 requirement H.3	p
H.9.12.3	Measures to avoid errors		
H.9.12.3.1	For controls with software class B or C the measures shown in Figure H.1 to avoid systematic faults shall be applied.	Verified by inspection based on manufacturer documents 'Mindmotion Software Design Guidance to Compliance with IEC Standards'. See appended table.	P

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

	Other software lifecycle models are permitted if they incorporate disciplined and structured processes including design and test phases.	Not Applicable	N/A
H.9.12.3.2	Specification		p
H.9.12.3.2.1	Software safety requirements		P
H.9.12.3.2.1.1	The specification of the software safety requirements include:		P
	• A description of each safety related function to be implemented, including its response time(s): - functions related to the application including their related software classes - functions related to the detection, annunciation and management of software or hardware faults	Verified by inspection	P
	• ... A description of interfaces between software and hardware	Mindmotion Software Design Guidance to Compliance with IEC Standards	P
	• ... A description of interfaces between any safety and non-safety related functions	Not Applicable	N/A
H.9.12.3.2.2	Software architecture		P
H.9.12.3.2.2.1	The description of software architecture includes the following aspects:		P
	• Techniques and measures to control software faults/errors (refer to H.9.12.2)	Mindmotion Software Design Guidance to Compliance with IEC Standards	P
	• Interactions between hardware and software	Mindmotion Software Design Guidance to Compliance with IEC Standards	P
	• Partitioning into modules and their allocation to the specified safety functions	Mindmotion Software Design Guidance to Compliance with IEC Standards	P
	• Hierarchy and call structure of the modules (control flow)	Mindmotion Software Design Guidance to Compliance with IEC Standards	P
	• Interrupt handling	May be indirectly addressed via timing and flow control Shall be reviewed in the end use application	N/A
	• Data flow and restrictions on data access	Mindmotion Software Design Guidance to Compliance with IEC Standards	P
	• Architecture and storage of data	Mindmotion Software Design Guidance to Compliance with IEC Standards	P

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

	• Time based dependencies of sequences and data	Indirectly addressed via timing and flow control	N/A
H.9.12.3.2.2.2	The architecture specification is verified against the specification of the software safety requirements by static analysis	Verified by inspection	P
H.9.12.3.2.3	Module design and coding		P
H.9.12.3.2.3.1	Software is suitably refined into modules. Software module design and coding are implemented in a way that is traceable to the software architecture and requirements. The module design specified:	Verified by inspection of source code	P
	– function(s)		P
	– interfaces to other modules		P
	– data		P
H.9.12.3.2.3.2	Software code is structured	Verified by inspection of source code	P
H.9.12.3.2.3.3	Coded software is verified against the module specification, and the module specification is verified against the architecture specification by static analysis	Verified by inspection of source code	P
H.9.12.3.2.4	Design and coding standards		-
	Program design and coding standards are used during software design and maintenance	Verified by inspection	P
	Coding standards .....:	Verified by inspection	—
	– specified programming practice	Verified by inspection	P
	– proscribed unsafe language features	Verified by inspection	N/A
	– specify procedures for source code documentation	Verified by inspection	P
	– specify data naming conventions	Verified by inspection	P
H.9.12.3.3	Testing		-
H.9.12.3.3.1	Module design (software system design, software module design and coding)		P
H.9.12.3.3.1.1	A test concept with suitable test cases is defined based on the module design specification.	Verified by inspection of manufacturer provided test report document' Mindmotion self monitoring fault injection test software test report'	P
H.9.12.3.3.1.2	Each software module is tested as specified within the test concept	Verified by inspection of manufacturer provided test report document	P
H.9.12.3.3.1.3	Test cases, test data and test results are documented	Verified by inspection of manufacturer provided test report document	P

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict
H.9.12.3.3.1.4	Code verification of a software module by static means includes such techniques as software inspections, walk-throughs, static analysis and formal proof	Verified by inspection of manufacturer provided test report document	P
	Code verification of a software module by dynamic means includes functional testing, white-box testing and statistical testing	Verified by inspection of manufacturer provided test report document	P
H.9.12.3.3.2	Software integration testing		
H.9.12.3.3.2.1	A test concept with suitable test cases is defined based on the architecture design specification	Verified by inspection of manufacturer provided test report document	P
H.9.12.3.3.2.2	The software is tested as specified within the test concept	Verified by inspection of manufacturer provided test report document	P
H.9.12.3.3.2.3	Test cases, test data and test results are documented	Verified by inspection of manufacturer provided test report document	P
H.9.12.3.3.3	Software validation		P
H.9.12.3.3.3.1	A validation concept with suitable test cases is defined based on the software safety requirements specification	Verified by inspection of manufacturer provided test report document	P
H.9.12.3.3.3.2	The software is validated with reference to the requirements of the software safety requirements specification as specified within the validation concept		P
	The software is exercised by simulation or stimulation of:		P
	• ..... input signals present during normal operation	Not Applicable	N/A
	• ..... anticipated occurrences	Anticipated failure/error	P
	• ..... undesired conditions requiring system action	Anticipated failure/error	P
H.9.12.3.3.3.3	Test cases, test data and test results are documented		P
H.9.12.3.4	Other Items		P
H.9.12.3.4.1	Equipment used for software design, verification and maintenance is qualified appropriately and demonstrated to be suitable for purpose in manifold applications	Verified by inspection of manufacturer provided test report document	P
H.9.12.3.4.2	Management of software versions: All versions are uniquely identified for traceability	Software version:1.0	P
H.9.12.3.4.3	Software modification		

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

H.9.12.3.4.3.1	Software modifications are based on a modification request which details the following:	Verified by inspection of manufacturer provided test report document	P
	• .....the hazards affected		P
	• .....the proposed change		P
	• .....the reasons for change		P
H.9.12.3.4.3.2	An analysis is carried out to determine the impact of the proposed modification on functional safety.	Verified by inspection	P
H.9.12.3.4.3.3	A detailed specification for the modification is generated including the necessary activities for verification and validation, such as a definition of suitable test cases	Verified by inspection	P
H.9.12.3.4.3.4	The modification is carried out as planned	Verified by inspection	P
H.9.12.3.4.3.5	The assessment of the modification is carried out based on the specified verification and validation activities.	Verified by inspection	P
H.9.12.3.4.3.6	All details of modification activities are documented	Verified by inspection	P
H.9.12.3.5	For class C control functions: one of the combinations (a–p) of analytical measures given in the columns of table H.10 is used during hardware development .....:	Not Applicable	N/A
H.9.12.4	Remotely actuated control functions		N/A
H.9.12.4.2.3.1	Communication of Safety Related Data – Transmission – Safety relevant data is transmitted authentically concerning:		N/A
	– data corruption		N/A
	– address corruption		N/A
	– wrong timing or sequence		N/A
	Data variation or corrupted data do not lead to an unsafe state		N/A
	Before transmitted data is used, it is ensured that data corruption, address corruption and wrong timing or sequence are addressed using the measures as given in Annex H.		N/A
H.9.12.4.2.3.2	Access to data exchange		N/A
	Adequate hardware/software measures are taken to prevent unauthorized access to the control functions (class B and C; operating data, configuration parameters and/or software modules)		N/A

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

	Access to data exchange of class B control function or class C control function related operating data through public networks, has appropriate cryptographic techniques implemented.		N/A
H.9.12.4.2.3.3	For class B and class C software revisions the requirements of H.9.12.3 and hardware configuration management are applied and the control maintains its protective functions		N/A
H.9.12.4.5	Software Download and Installation		N/A
H.9.12.4.5.1	Software updates provided by the manufacturer and transmitted to the control via remote communication are checked prior to its use:		N/A
	– against corruption through communication ensuring Hamming distance 3 for software class B, or Hamming distance 4 for software class C;		N/A
	– that the software version is compatible with the hardware version of the control according to the version management documentation.		N/A
	The software which performs the above mentioned checks contain measures to control the fault/error conditions specified in H.9.12.2.		N/A
H.9.12.4.5.2	In case of software download via remote communication, the cryptographic techniques in H.9.12.4.6 are provided. In addition to the requirements in H.9.12.4.6, identification procedures are provided for the software packages.		N/A
	The cryptographic techniques employed are part of the control, and not rely upon part of the router or similar data transmission device itself, and are performed prior to transmission.		N/A
H.9.12.4.5.3	Each update of software has provisions for authorization by the user and a version ID number which were accessible.		N/A
H.9.12.4.5.4	Installation of class B software or class C software: the control remains in compliance with the requirements of this document during and after the software installation process.		N/A
H.9.12.4.6	Cryptographic techniques		N/A
	In cases where class B control function or class C control function related operating data, configuration parameters and/or software modules are transmitted over a public network, and/or where software updates are provided by the manufacturer via remote communication, cryptographic techniques are employed.		N/A

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

H.13.2	**Fault assessment to ensure functional safety**		
H.13.2.1	Design and construction requirements		P
H.13.2.1.1	Fault avoidance and fault tolerance		P
	Controls incorporating control functions of class B or C are designed according to H.13.2 taking into account the failure modes of Table 14 and H.9.12 for software		P
	Systematic errors are avoided	H.9.12.3	P
	Random faults are dealt with by a proper system configuration	H.9.12.3	P
	Functional analysis of the application resulted in a structured design with:	See H.5,H.6, and H.9.12	P
	-Control flow	See H.5,H.6, and H.9.12	P
	-Data flow	See H.5,H.6, and H.9.12	P
	-Time related functions required by the application	See H.5,H.6, and H.9.12	P
	-For custom-chips special attention is made to minimize systematic errors	Not Applicable	N/A
	System configuration is failsafe or:	Structure to be determined by end use and application.	N/A
	Incorporated components with direct safety-critical functions guarded by safeguards that cause a completely independent safety shut-down in accordance to H.9.12 software class B or C	Structure to be determined by end use and application.	N/A
	- safeguards are built into hardware and,	Structure to be determined by end use and application.	N/A
	- safeguards are supplemented by software	Structure to be determined by end use and application.	N/A
	Time slot monitoring is sensitive to both an upper and a lower limit of the time interval.	IWDG and WWDG provided	P
	Faults resulting in a shift of the upper and/or lower limit are taken into account.	Where applicable to IEC60730_B_STL	P
	In a class C control function when a single fault in a primary safeguard can render the safeguard inoperative, a secondary safeguard is provided	Not Applicable	N/A
	The reaction time of the secondary safeguard is in accordance with Clause H.13.2.3.	Not Applicable	N/A
H.13.2.1.2	Documentation		P
	The documentation was based on H.9.12.3.	See H.9.12.3	P
H.13.2.2	Class B control function		P
H.13.2.2.1	Design and construction requirements		P

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

	Software complies with software class B	Verified by inspection; see applicable Class B clauses of this Report	P
H.13.2.3	Class C control function		N/A
H.13.2.3.1	Design and construction requirements		N/A
	Software complies with software class C		N/A
H.13.2.5	Circuit and construction evaluation		P
H.13.2.5.3	Assessment		P
	Only the safety related software (software class B and C) as identified according to H.13.2.1.2 are subjected to further assessment		P

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

TABLE H.2 – MEASURES TO ADDRESS FAULT/ERRORS (Software Class B)			
Component	Fault/error	Declared measures	Verdict
1. CPU	-	-	-
1.1 Registers	Stuck at	Functional test	P
1.3 Program counter	Stuck at	Time slot monitoring	P
2. Interrupt handling and execution	No interrupt	Not applicable	Not applicable
	Too frequent interrupt	Not applicable	Not applicable
3. Clock	Wrong frequency (for quartz synchronized clock: harmonics/ sub-harmonics only)	Time slot monitoring	P
4. Memory	-	-	-
4.1 Invariable memory	All single bit faults	Periodic 8 or 16-bit CRC	P
4.2 Variable memory	DC fault	Periodic static memory test (March C- or March X test, based on word data)	P
4.3. Addressing (relevant to variable and invariable memory)	Stuck at	See 4.1 and 4.2	P
5. Internal data path	-	-	-
5.1 Data	Stuck at	See 4.1 and 4.2	P
5.2 Addressing	Wrong address	See 4.1 and 4.2	P
6. External communication	-	-	-
6.1 Data	Hamming distance 3	N/A	N/A
6.2 Addressing	Wrong address	N/A	N/A
6.3 Timing	Wrong point in time	N/A	N/A
	Wrong sequence	N/A	N/A
7. Input/output periphery	-	-	-
7.1 Digital I/O	Fault conditions specified in Cl.H.13	N/A	N/A
7.2 Analog I/O	-	-	-
7.2.1 A/D and D/A-convertor	Fault conditions specified in Cl. H.13	N/A	N/A
7.2.2 Analog multiplexer	Wrong addressing	N/A	N/A

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

9. Custom chips e.g. ASIC, GAL, gate array	Any output outside the static and dynamic functional specification	N/A	N/A

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

IEC 60730-1 (Software)			
Clause	Requirement + Test	Result - Remark	Verdict

6.3 Timing	Wrong point in time	N/A	N/A
	Wrong sequence	N/A	N/A
7. Input/output periphery	-	-	-
7.1 Digital I/O	Fault conditions specified in Cl.H.13	N/A	N/A
7.2 Analog I/O	-	-	-
7.2.1 A/D and D/A-convertor	Fault conditions specified in Cl. H.13	N/A	N/A
7.2.2 Analog multiplexer	Wrong addressing	N/A	N/A
8. Monitoring devices and comparators	Any output outside the static and dynamic functional specification	N/A	N/A
9 Custom chips e.g. ASIC, GAL, gate array	Any output outside the static and dynamic functional specification	N/A	N/A

Table: Manufacturer's Documentation Referenced in this TRF (informative)		
Title	Revision (#/Letter)	Date
Mindmotion Software Design Guidance to Compliance with IEC Standards.pdf	/	/
IEC60730_ B_ STL Library Usage Guide.pdf	/	/
Mindmotion self monitoring fault injection test software test report.pdf	/	/
MM_P_SUP_03_02《变更需求Change+Request》V1.0.pdf	/	/

__End__