Technical Report for Functional Safety

Report No.: SHFS220400014571

Jun. 14, 2023

Client / Applicant:	Suzhou Tongyi Automation Technology Co., Ltd. 401 Room 13 Building No. 2 Shuangma Street Suzhou Jiangsu
Manufacturer:	Same as Applicant
Project Title:	Servo Driver
Model No.:	IXL-II-2040, IXL-II-3060, IXL-II-4080, IXL-II-100200, IXL-II-150300
Tested Standards:	ISO 13849-1:2015
Conclusion:	In this report, safety functions of IXL-II-2040, IXL-II-3060, IXL-II-4080, IXL-II-100200, IXL-II-150300 were assessed according to EN 1175:2020, safety related functions requirement, safety architecture and performance level meet PL d with category 3 according to ISO 13849-1:2015, detail information of safety functions item see Table 1.

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

- Proof of systematic safety integrity for defined phases of the life cycle
- Proof of the required safety-related parameters (failure rate, $MTTF_D$, DC, CCF)
- Proof of the techniques and measures according to ISO 13849-1
- Proofs that processes and methods are established at the manufacturer guaranteeing that unexceptionable processes

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

Independent organization for functional safety assessment	Assessor:	Approver:
SGS-CSTC Standards Technical Services (Shanghai) Co., Ltd.	Charles Li	Jerry Zheng

No.588, West Jindu Road, Songjiang District, Shanghai, China 201612 t (86-21) 60125308 f (86-21) 61915678 www.sgsgroup.com.cn
中国・上海・松江区金都西路588号 邮编: 201612 t (86-21) 60125308 f (86-21) 61915678 sgs.china@sgs.com
Member of the SGS Group (SGS SA)

CONTENTS

List of Figures:

List of Tables:

1. Summary of assessment

This technical report summarizes the safety performance evaluation results towards the safety related circuits in **Servo Driver** [Model No.: **See cover page**], provides by **Suzhou Tongyi Automation Technology Co., Ltd.** (consecutively in the report referred as **Tongyi**).

No deviations were found during the assessment acc. to ISO 13849-1:2015 for safety related circuits in **Servo Driver** in terms of systematic performance level.

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

A determination of the safety-related characteristic values ($MTTF_D$, PFH_D, DC_{avg}, Cat., CCF) for the quantitative determination of the performance level, including a supplementary examination of the performance level in corresponding sections of the safety life cycle and determination of Performance Level (PL), based on the results of the safety-related characteristic values, and taking into account the qualitative requirements achievement of PL d with diagnostic measures.

In this report, the below safety functions have been assessed:

Ident. No.	Safety Function Items	Required PL	Assessment Result
SF1	SBC&STO	PL d	PL d / Cat. 3
SF2	Safety encoder	PL d	PL d / Cat. 3

Table 1 Safety functions definition

Supplementary Information:

[1] Safety functions was required according to ISO 13849-1:2015, and PL values were determined by risk assessment.

[2] The above safety functions were assessed, and comply with ISO 13849-1:2015. More detail information please refer to the following report.

This assessment is based on the requirement in ISO 13849-1:2015 towards **Cat. 3 PL d.**

2. Assessment Period

Beginning of project: 2022-04-30

End of project: 2023-05-30

3. References

No. Document Type and Name	Client's Document Name
[D1] Quality Management	通用伺服驱动器质量管理手册
[D2] Safety Plan &Validation Plan	IXL驱动器系统安全计划_v220629
[D3] Evidence of Competency	N/A
[D4] Safety Concept	IXL-II-2040 universal servo driver system safety concept_v20230206

No. Document Type and Name	Client's Document Name
[D5] Safety Requirement Specification	IXL-II-2040型通用伺服驱动器系统安全需求规范 _v20220508
[D6] System Requirement Inspection Report	IXL-II-2040型通用伺服驱动器系统安全需求规范审查报告 _v20220714
[D7] System FMEA Report	IXL-II-2040 safety module-level FMEA report_v20211017
[D8] HW Safety Requirement Specification	IXL-II-2040通用伺服驱动器硬件安全设计要求 _v20220623
[D9] HW Requirement Inspection Report	IXL-II-2040型通用伺服驱动器硬件设计审查报告 _v20220820
[D10] HW Design Description	N/A
[D11] De-rating Design Report	IXL-II-2040 De-Rating Design Report_v20220310
[D12] Schematic	IXL-II-2040-Contral IXL-II-2040-Power
[D13] PCB Layout	IXL-II-2040-Contral-PCB IXL-II-2040-Power-PCB
[D14] PCBA BOM	IXL-II-2040-Contral IXL-II-2040-Power
[D15] HW Inspection Report	IXL-II-2040型通用伺服驱动器硬件设计审查报告 _v20220820
[D16] Component FMEDA Report	IXL-II-2040 safety module-level FMEA report_v20221108
[D17] Safety Analysis Report	IXL-II-2040 Universal Servo Driver system safety analysis report_v20221211
[D18] $MTTF_D$ Calculation Report	IXL-II-2040 Universal Servo Driver MTTFd calculation report_v20230307
[D19] SW Safety Requirement Specification	IXL-II-2040型通用伺服驱动器软件安全需求_v20220620
[D20] SW Architecture Design Specification	IXL-II-2040型通用伺服驱动器_v20230426
[D21] SW Requirement Inspection Report	N/A
[D22] SW Unit Design Specification	IXL-II-2040型通用伺服驱动器_v20220710
[D23] Support Tools Assessment Report	IXL-II-2040型通用伺服驱动器_v20220611
[D24] Coding Guideline	IXL-II-2040型通用伺服驱动器_v20220512
[D25] Code Inspection Report	IXL-II-2040型通用伺服驱动器源代码审查报告 _v20221106
[D26] Code Static Checking Report	IXL-II-2040型通用伺服驱动器源代码静态审查报告 _v20221107
[D27] Safety Data Communication Protocol	IXL-II-2040 Universal Servo Driver system data communication protocol_v2020206
[D28] Safety Parameter Configuration	IXL-II-2040 universal servo driver safety parameter configuration_V20230406
[D29] HW Module Testing Report	IXL-II-2040型通用伺服驱动器硬件模块测试报告 _v20221010

No. Document Type and Name	Client's Document Name
[D30] SW Integration Testing Report	IXL-II-2040型通用伺服驱动器整体软件测试报告_v20221022
[D31] System Safety Validation Report	IXL-II-2040型通用伺服驱动器系统安全验证报告_v20221205
[D32] EMC Testing Report	DSS_SHEM2301000330MD CE Verification DSS_SHEM2301000330MD RPT
[D33] Environmental Testing Report	IXL-II-2040环境测试报告
[D34] Fault Insert Report	IXL-II-2040型通用伺服驱动器故障插入测试报告_v20230105
[D35] Modification Management	IXL-II-2040型通用伺服驱动器变更管理_v20220506
[D36] User Manual	IXL-II系列低压伺服驱动器用户手册5.1
[D37] PCBA Manufacturing Qualification Spec.	PCBA制造技术规范
[D38] Product Declaration of Conformity	Product Declaration of Conformity

Table 2 References and documents

4. Revision Logs

Version	Changes Description
V1.0	Initial Version

5. Rating(s) Definition

Model	IXL-II-2040	IXL-II-3060	IXL-II-4080	IXL-II-100200	IXL-II-150300
Dimensions (mm)	151*100*40	167.5*100*40	182.5*100.7*40.7	250*130*53.8	211.6*155.4*75
Enclosure type	IP20				
Input Voltage	20-80VDC				
Power	960W/1600W	1400W/2100W	1600W/3200W	4800W/9kW	5500W/11kW
Weight	0.72KG	0.8KG	0.8KG	1.86KG	3.0KG

Table 3 Parameters of Servo Driver

6. Critical componment list

No.	Component Name	Type and Specification	Manufacturer
1	MCU	XMC4700	Infineon
2	MOS	NCEP039N10M	无锡新洁能
		NCEP026N10T	

Table 4 Critical Components of Servo Driver

7. Assessment Item Information

Inspection item description .....: See cover page

Model and/or type reference .....: See cover page

Hardware Model and Version.....: IXL-POW-(B7)

IXL-3060SPB-(D5)

IXL-4080SPB-(B)

IXL-100200SPB-(B3)

IXL-2-150-CB(C3)

Firmware Version.....: XMC4700_F196_F144_123030809&2023/03/09

IXL-II-2040

IXL-II-3060

IXL-II-4080

IXL-II-100200

IXL-II-150300

Figure 1 The photos of product

Control PCBA:

IXL-II-2040 /IXL-II-3060 /IXL-II-4080 /IXL-II-100200

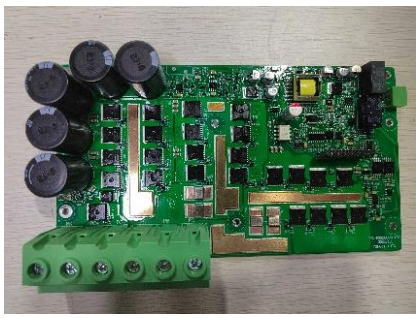
IXL-II-150300

Power PCBA:

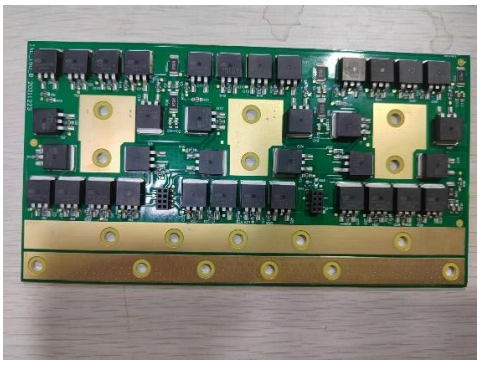
IXL-II-2040

IXL-II-3060

IXL-II-4080



IXL-II-100200



IXL-II-150300

Figure 2 The photos of PCBA

8. Risk Assessment

Per the Figure A.1 of ISO 13849-1:2015

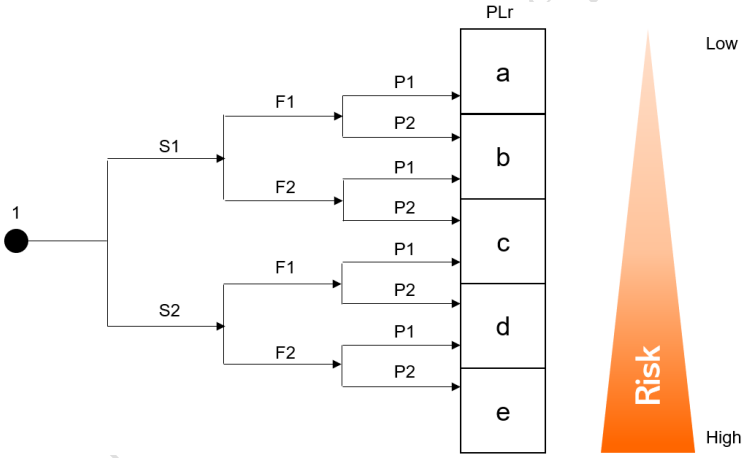


Figure 3 Risk graph of performance level

Risk assessment is applied according to ISO 13849-1:2015.

Safety functions and required performance level is defined in Table 1. Safety functions and all reasonably foreseeable circumstances, including fault conditions are analyzed.

The required performance level of prevention of risk assessment in case of management system failure according to the ISO 13849-1:2015.

9. Safety Function Under Assessment

9.1. General

System architecture

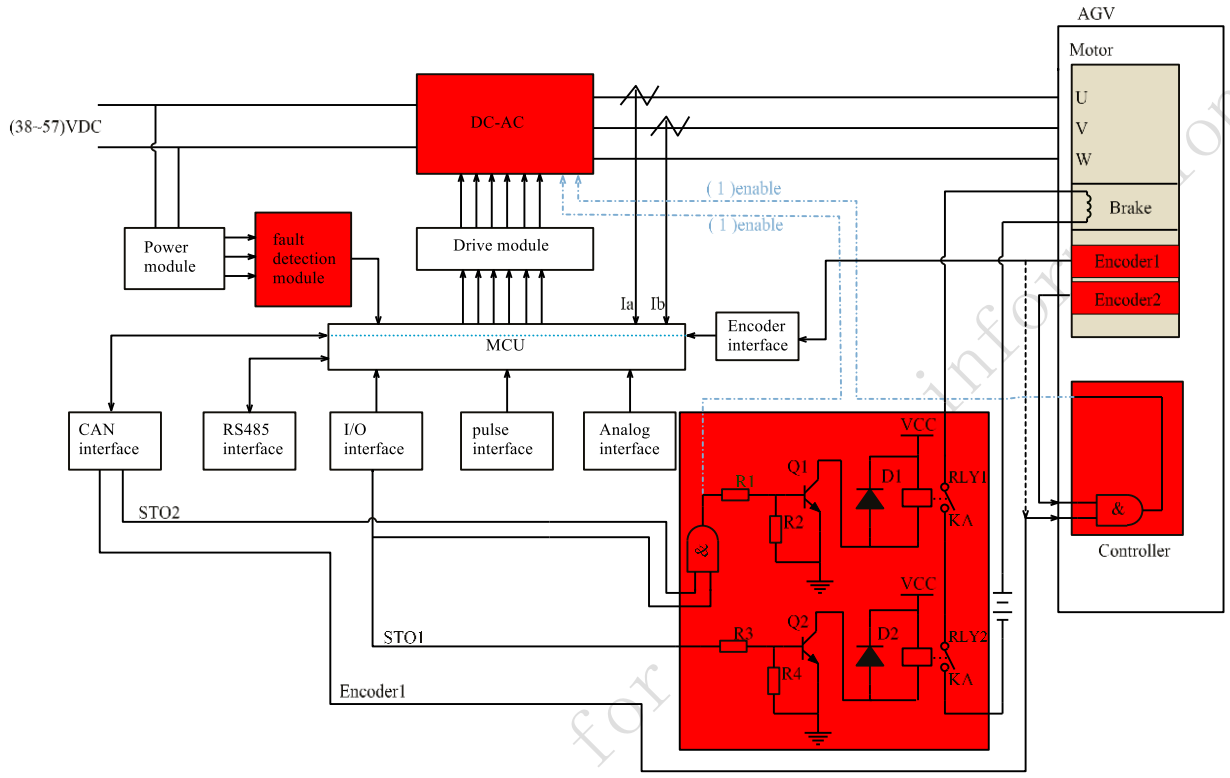


Figure 4 System Architecture

9.2. SBC&STO

9.2.1. Safety Function Definition

When STO1 is damaged and the holding brake cannot be closed, STO2 can be closed. Similarly, when STO2 is damaged and the holding brake cannot be closed, STO1 can close the holding brake.

9.2.2. Safe State

Switch off PWM and brake.

9.2.3. Safety Response Time

Safety response time: 20ms.

9.2.4. Safety Function Diagram

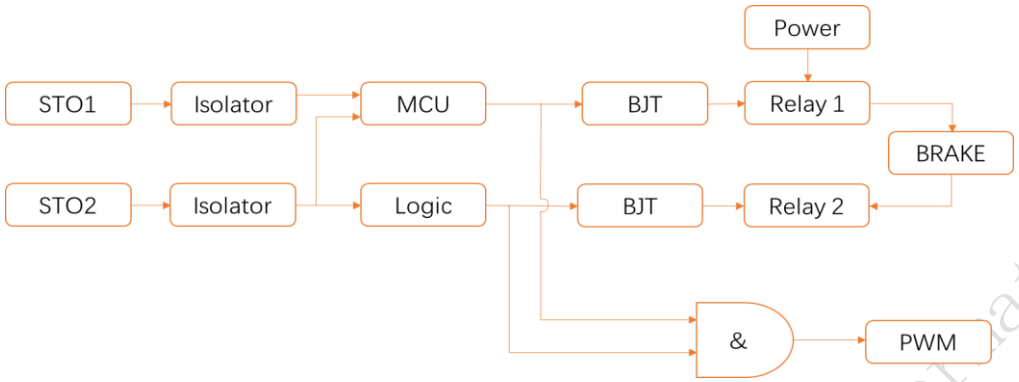


Figure 5 Safety Structure of SBC&STO

9.2.5. Structure Analysis and Estimate the diagnostic coverage (DC)

Annex E of ISO 13849-1:2015 is used as the guideline to estimate the diagnostic coverage (DC) of the system, which in fact is noted as average DC (DC_{avg}).
Category and diagnostic coverage are defined as below table:

Item	Cat.	Diagnostic Measure & Diagnostic Coverage		
		I/L/O	Diagnostic Measure	DC
SF1	Cat. 3	INPUT	**SRP /CS:** STO1, STO2, Isolators	90%
			Monitoring: MCU	
		LOGIC	**SRP/CS:** MCU, Logic	60%
			Monitoring: MCU Self Check	
		OUTPUT	**SRP/CS:** BJT, Relay1, Relay2, BRAKE, PWM	90%
			Monitoring: Monitor the feedback data from STOs	

Table 5 Structure Analysis and Diagnostic Coverage of SBC&STO

According to above analysis and safety structure diagram, the safety function circuit has been designed with category 3.
The minimum of DC for this system is **60%**. Per clause 4.5.3 and Table 5 of ISO 13849-1:2015, the diagnostic coverage (DC) level is determined to be **Low** for this system.

9.2.6. $MTTF_D$ Calculation

The system $MTTF_D$ has been calculated based on schematic and BOM, the $MTTF_D$ calculation report has been checked and confirmed, the system $MTTF_d$ is **2037.165** years. More detail information please refer to [D18] $MTTF_D$ Calculation Report.

Result:

Refer to table 4 of ISO 13849-1:2015, the calculated value for the system $MTTF_D$ of **2037.165** years ($PFH_D = 1.01x10^{-7}$) results in a **High** level of reliability.

9.2.7. Estimate Common Cause Failure

Annex F of ISO 13849-1:2015 is used as the guideline to estimate the common cause failure (CCF) of the system. This is based on the requirements set forth in IEC 61508-6.

No.	Item and Measures Against CCF	Score for control circuit	Maximum possible score	Evidence
1	**Separation/segregation**			
	Physical separation between signal paths	15	15	External input I/O is designed, refer to [D12] Schematic.
2	**Diversity**			
	Different technologies/design or physical principles are used	20	20	One brake control signal is from CAN communication, the other is from external input I/O.
3	**Design/application/experience**			
	Protection against over-voltage, over-pressure, over-current, over-temperature, etc.	15	15	All power supplies of Servo Driver are designed with over-voltage and under-voltage detection and protection, and the safe output channel is designed with over-current protection, which detects the temperature of MCU and the ambient temperature of the controller and carries out over-temperature protection.
	Components used are well-tried.	0	5	
4	**Assessment/analysis**			
	For each part of safety related parts of control system, a failure mode and effect analysis has been carried out and its results considered to avoid common-cause-failures in the design.	5	5	Refer to [D7] System FMEA Report.
5	**Competence/training**			
	Training of designers to understand the causes and consequences of common cause failures.	5	5	All designers involved in the project have been trained to fully understand the mechanism of functional safety and understand the causes and consequences of common failures.
6	**Environmental**			
	The system is designed to meet EMC directive	25	25	Refer to [D30] EMC Testing Report.
	Other influences: Consideration of the requirements for immunity to all relevant environmental influences such as,	10	10	The Servo Driver has passed the environmental test and vibration test. Refer to [D31] Environmental Testing Report.

No.	Item and Measures Against CCF	Score for control circuit	Maximum possible score	Evidence
	temperature, shock, vibration, humidity			
	TOTAL	95	100	

Table 6 Common Cause Failure of SBC&STO

Result:

The estimated CCF for the function is **95**, which is larger than the minimum requirement of 65, thus the calculated CCF meets the requirements set forth in ISO 13849-1:2015.

9.2.8. Conclusions and Recommendations

The performance level is determined in the table below.

Category		B	1	2	2	3	3	4
DC_{avg}		None	None	Low	Medium	Low	Medium	High
$MTTF_D$ of each channel	Low	a	Not covered	a	b	b	c	Not covered
	Medium	b	Not covered	b	c	c	d	Not covered
	High	Not covered	c	c	d	d	d	e

Table 7 PL of SBC&STO

Result:

According to above analysis and evaluation, the performance level has been assessed to achieve **PL d** and meet the requirements ISO 13849-1:2015.

9.3. Safety encoder

9.3.1. Safety Function Definition

An independent encoder is installed outside the motor. The controller reads the position and speed of the motor through CAN communication. The controller also reads the position and speed of the motor through the external encoder. When the difference is large, the output is closed.

9.3.2. Safe State

Switch off PWM.

9.3.3. Safety Response Time

Safety response time: 10ms.

9.3.4. Safety Function Diagram

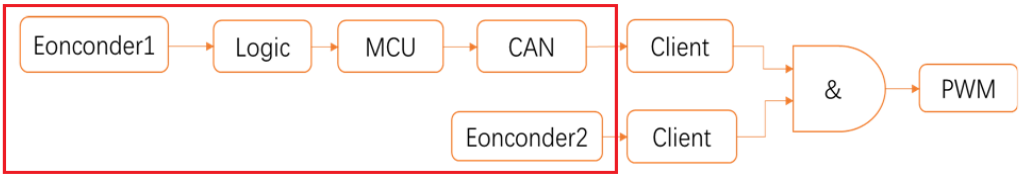


Figure 6 Safety Structure of Safety encoder

9.3.5. Structure Analysis and Estimate the diagnostic coverage (DC)

Annex E of ISO 13849-1:2015 is used as the guideline to estimate the diagnostic coverage (DC) of the system, which in fact is noted as average DC (DC_{avg}).
Category and diagnostic coverage are defined as below table:

Item	Cat.	Diagnostic Measure & Diagnostic Coverage		
		I/L/O	Diagnostic Measure	DC
SF2	Cat. 3	**INPUT**	**SRP /CS:** Encoder1, Encoder2	90%
			Monitoring: MCU	
		LOGIC	**SRP/CS:** MCU	60%
			Monitoring: MCU self check	
		OUTPUT	**SRP/CS:** Client controller, PWM	90%
			Monitoring: Monitor the feedback data from encoders	

Table 8 Structure Analysis and Diagnostic Coverage of Safety encoder

According to above analysis and safety structure diagram, the safety function circuit has been designed with category 3.
The minimum of DC for this system is **60%**. Per clause 4.5.3 and Table 5 of ISO 13849-1:2015, the diagnostic coverage (DC) level is determined to be **Low** for this system.

9.3.6. $MTTF_D$ Calculation

The system $MTTF_D$ has been calculated based on schematic and BOM, the $MTTF_D$ calculation report has been checked and confirmed, the system $MTTF_D$ is **329.364** years. More detail information please refer to [D18] $MTTF_D$ Calculation Report.

Result:

Refer to table 4 of ISO 13849-1, the calculated value for the system $MTTF_D$ of **329.364** years (PFH_D = $1.01x10^{-7}$) results in a **High** level of reliability.

9.3.7. Estimate Common Cause Failure

Annex F of ISO 13849-1:2015 is used as the guideline to estimate the common cause failure (CCF) of the system. This is based on the requirements set forth in IEC 61508-6.

No.	Item and Measures Against CCF	Score for control circuit	Maximum possible score	Evidence
1	**Separation/segregation**			
	Physical separation between signal paths	15	15	External encoder is designed, refer to [D12] Schematic.
2	**Diversity**			
	Different technologies/design or physical principles are used	20	20	One encoder monitoring signal is from CAN communication, the other is from external encoder.
3	**Design/application/experience**			
	Protection against over-voltage, over-pressure, over-current, over-temperature, etc.	15	15	All power supplies of Servo Driver are designed with over-voltage and under-voltage detection and protection, and the safe output channel is designed with over-current protection, which detects the temperature of MCU and the ambient temperature of the controller and carries out over-temperature protection.
	Components used are well-tried.	0	5	
4	**Assessment/analysis**			
	For each part of safety related parts of control system, a failure mode and effect analysis has been carried out and its results considered to avoid common-cause-failures in the design.	5	5	Refer to [D7] System FMEA Report.
5	**Competence/training**			
	Training of designers to understand the causes and consequences of common cause failures.	5	5	All designers involved in the project have been trained to fully understand the mechanism of functional safety and understand the causes and consequences of common failures.
6	**Environmental**			
	The system is designed to meet EMC directive	25	25	Refer to [D30] EMC Testing Report.
	Other influences: Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity	10	10	The Servo Driver has passed the environmental test and vibration test. Refer to [D31] Environmental Testing Report.
	TOTAL	95	100	

Table 9 Common Cause Failure of Safety encoder

Result:

The estimated CCF for the function is **95**, which is larger than the minimum requirement of 65, thus the calculated CCF meets the requirements set forth in ISO 13849-1:2015.

9.3.8. Conclusions and Recommendations

The performance level is determined in the table below.

Category		B	1	2	2	3	3	4
DC_{avg}		None	None	Low	Medium	Low	Medium	High
$MTTF_d$ of each channel	Low	a	Not covered	a	b	b	c	Not covered
	Medium	b	Not covered	b	c	c	d	Not covered
	High	Not covered	c	c	d	d	d	e

Table 10 PL of Safety encoder

Result:

According to above analysis and evaluation, the performance level has been assessed to achieve **PL d** and meet the requirements ISO 13849-1.

10. Safety-related Software

The colour legend applicated for both Safety-related Software and Systematic Failure.

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

Table 11 Colour legend used in following tables

Requirement + Test	Result - Remark
All lifecycle activities of safety-related embedded or application software shall primarily consider the avoidance of faults introduced during the software lifecycle. The main objective of the following requirements is to have readable, understandable, testable and maintainable software.	Requirements fulfilled. Refer to [D19] SW Safety Requirement Specification.
Safety-related embedded software (SRESW)	
For SRESW for components with PLr a to d, the following basic measures shall be applied:	
— software safety lifecycle with verification and validation activities	Requirement not applicable.
— documentation of specification and design;	Requirements fulfilled. Refer to [D19] SW Safety Requirement Specification, [D20] SW Architecture Design Specification, [D22] SW Unit Design Specification.

Requirement + Test	Result - Remark
— modular and structured design and coding;	Requirements fulfilled. Refer to [D20] SW Architecture Design Specification, [D22] SW Unit Design Specification.
— control of systematic failures	Requirements fulfilled. Refer to [D5] Safety Requirement Specification, [D19] SW Safety Requirement Specification.
— where using software-based measures for control of random hardware failures, verification of correct implementation;	Requirements fulfilled. Refer to [D5] Safety Requirement Specification.
— functional testing, e.g. black box testing;	Requirements fulfilled. Refer to [D30] SW Integration Testing Report, [D34] Fault Insert Report.
— appropriate software safety lifecycle activities after modifications.	Requirement not applicable.
For SRESW for components with PLr c or d, the following additional measures shall be applied:	
— project management and quality management system comparable to, e.g., IEC 61508 or ISO 9001;	Requirements fulfilled. Refer to [D1] Quality Management.
— documentation of all relevant activities during software safety lifecycle;	Requirements fulfilled. Refer to [D2] Safety Plan.
— configuration management to identify all configuration items and documents related to a SRESW release;	Requirement not applicable.
— structured specification with safety requirements and design;	Requirements fulfilled. Refer to [D5] Safety Requirement Specification.
— use of suitable programming languages and computer-based tools with confidence from use;	Requirements fulfilled. Refer to [D23] Support Tools Assessment Report, [D24] Coding Guideline.
— modular and structured programming, separation from non-safety-related software, limited module sizes with fully defined interfaces, use of design and coding standards;	Requirements fulfilled. Refer to [D19] SW Safety Requirement Specification, [D24] Coding Guideline.
— coding verification by walk-through/review with control flow analysis;	Requirements fulfilled. Refer to [D25] Code Inspection Report, [D26] Code Static Checking Report.
— extended functional testing, e.g. grey box testing, performance testing or simulation;	Requirement not applicable.
— impact analysis and appropriate software safety lifecycle activities after modifications.	Requirement not applicable.
Safety-related application software (SRASW)	

Requirement + Test	Result - Remark
For SRASW for components with PLr from c to e, the following additional measures with increasing efficiency (lower effectiveness for PLr of c, medium effectiveness for PLr of d, higher effectiveness for PLr of e) are required or recommended.	
a) The safety-related software specification shall be reviewed (see also Annex J), made available to every person involved in the lifecycle and shall contain the description of:	
safety functions with required PL and associated operating modes	Requirement not applicable SRASW has not applicated in this project
performance criteria, e.g., reaction times,	Requirement not applicable See above.
hardware architecture with external signal interfaces,	Requirement not applicable See above.
detection and control of external failure.	Requirement not applicable See above.
b) Selection of tools, libraries, languages:	
Suitable tools with confidence from use: for PL = e achieved with one component and its tool, the tool shall comply with the appropriate safety standard; if two diverse components with diverse tools are used, confidence from use may be sufficient. Technical features which detect conditions that could cause systematic error (such as data type mismatch, ambiguous dynamic memory allocation, incomplete called interfaces, recursion, pointer arithmetic) shall be used. Checks should mainly be carried out during compile time and not only at runtime. Tools should enforce language subsets and coding guidelines or at least supervise or guide the developer using them.	Requirement not applicable See above.
Whenever reasonable and practicable, validated function block (FB) libraries should be used — either safety-related FB libraries provided by the tool manufacturer (highly recommended for PL = e) or validated application specific FB libraries and in conformity with this part of ISO 13849.	Requirement not applicable See above.
A justified LVL-subset suitable for a modular approach should be used, e.g., accepted subset of IEC 61131‑3 languages. Graphical languages (e.g., function block diagram, ladder diagram) are highly recommended.	Requirement not applicable See above.
c) Software design shall feature:	
semi-formal methods to describe data and control flow, e.g., state diagram or program flow chart,	Requirement not applicable See above.
modular and structured programming predominantly realized by function blocks deriving from safety-related validated function block libraries,	Requirement not applicable See above.
function blocks of limited size of coding,	Requirement not applicable See above.

Requirement + Test	Result - Remark
code execution inside function block which should have one entry and one exit point,	Requirement not applicable See above.
architecture model of three stages, Inputs ⇒ Processing ⇒ Outputs	Requirement not applicable See above.
assignment of a safety output at only one program location, and	Requirement not applicable See above.
use of techniques for detection of external failure and for defensive programming within input, processing and output blocks which lead to safe state.	Requirement not applicable See above.
d) Where SRASW and non-SRASW are combined in one component:	
SRASW and non-SRASW shall be coded in different function blocks with well-defined data links;	Requirement not applicable See above.
there shall be no logical combination of non-safety-related and safety-related data which could lead to downgrading of the integrity of safety-related signals, for example, combining safety- related and non-safety-related signals by a logical “OR” where the result controls safety related signals.	Requirement not applicable See above.
e) Software implementation/coding:	
code shall be readable, understandable and testable and, because of this symbolic variable (instead of explicit hardware addresses) should be used;	Requirement not applicable See above.
justified or accepted coding guidelines shall be used	Requirement not applicable See above.
data integrity and plausibility checks (e.g., range checks.) available on application layer (defensive programming) should be used;	Requirement not applicable See above.
code should be tested by simulation;	Requirement not applicable See above.
verification should be by control and data flow analysis for PL = d or e.	Requirement not applicable See above.
f) Testing:	
the appropriate validation method is black box testing of functional behaviour and performance criteria (e.g., timing performance);	Requirement not applicable See above.
for PL = d or e, test case execution from boundary value analysis is recommended;	Requirement not applicable See above.
test planning is recommended and should include test cases with completion criteria and required tools;	Requirement not applicable See above.
I/O testing shall ensure that safety-related signals are correctly used within SRASW.	Requirement not applicable See above.

Requirement + Test	Result - Remark
g) Documentation:	
all lifecycle and modification activities shall be documented;	Requirement not applicable See above.
documentation shall be complete, available, readable, and understandable;	Requirement not applicable See above.
code documentation within source text shall contain module headers with legal entity, functional and I/O description, version and version of used library function blocks, and sufficient comments of networks/statement and declaration lines.	Requirement not applicable See above.
h) Verification:	
i) Configuration management:	
It is highly recommended that procedures and data backup be established to identify and archive documents, software modules, verification/validation results and tool configuration related to a specific SRASW version.	Requirement not applicable See above.
j) Modifications	
After modifications of SRASW, impact analysis shall be performed to ensure specification. Appropriate lifecycle activities shall be performed after modifications. Access rights to modifications shall be controlled and modification history shall be documented.	Requirement not applicable See above.
Software-based parameterization	
The integrity of all data used for parameterization shall be maintained. This shall be achieved by applying measures to	
— control the range of valid inputs,	Requirement not applicable. Parameterization is not applicated in this project.
— control data corruption before transmission,	Requirement not applicable.
— control the effects of errors from the parameter transmission process,	Requirement not applicable.
— control the effects of incomplete parameter transmission, and	Requirement not applicable.
— control the effects of faults and failures of hardware and software of the tool used for parameterization.	Requirement not applicable.
This procedure shall include confirmation of input parameters to the SRP/CS by either	
— retransmission of the modified parameters to the parameterization tool, or	Requirement not applicable.
— other suitable means of confirming the integrity of the parameters,	Requirement not applicable.
The following verification activities shall be applied for software-based parameterization:	

Requirement + Test	Result - Remark
— verification of the correct setting for each safety-related parameter (minimum, maximum and representative values);	Requirement not applicable.
— verification that the safety-related parameters are checked for plausibility, for example by use of invalid values, etc.;	Requirement not applicable.
— verification that unauthorized modification of safety-related parameters is prevented;	Requirement not applicable.
— verification that the data/signals for parameterization are generated and processed in such a way that faults cannot lead to a loss of the safety function.	Requirement not applicable.

11. Systematic Failure

11.1. Introduction

When electrical systems are used in conjunction with other technologies, then relevant tables for basic safety and well–tried safety principles should also be taken into account.

11.2. List of basic safety principles

Requirement + Inspection	Result - Remark
G.1 General	
ISO 13849-2 gives a comprehensive list of measures against systematic failure which should be applied, such as basic and well-tried safety principles.	Requirement not applicable.
G.2 Measures for the control of systematic failures	
The following measures should be applied.	
— Use of de-energization (see ISO 13849-2) The safety-related parts of the control system (SRP/CS) should be designed so that with loss of its power supply a safe state of the machine can be achieved or maintained.	Requirements fulfilled Power supply circuit was taken into consideration. in case of power loss, the Servo Driver will enter safe state. Refer to [D7] System FMEA Report.
— Measures for controlling the effects of voltage breakdown, voltage variations, overvoltage, undervoltage SRP/CS behaviour in response to voltage breakdown, voltage variations, overvoltage, and undervoltage conditions should be predetermined so that the SRP/CS can achieve or maintain a safe state of the machine (see also IEC 60204-1 and IEC 61508-7:2000, A.8).	Requirements fulfilled Refer to [D5] Safety Requirement Specification, [D8] HW Safety Requirement Specification.

Requirement + Inspection	Result - Remark
— Measures for controlling or avoiding the effects of the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances, electromagnetic interference and its effects) SRP/CS behaviour in response to the effects of the physical environment should be predetermined so that the SRP/CS can achieve or maintain a safe state of the machine (see also, for example, IEC 60529, IEC 60204-1).	Requirements fulfilled Refer to [D31] System Safety Validation Report.
— Program sequence monitoring shall be used with SRP/CS containing software in order detect defective program sequences A defective program sequence exists if the individual elements of a program (e.g., software modules, subprograms or commands) are processed in the wrong sequence or period of time or if the clock of the processor is faulty (see EN 61508-7:2001, A.9).	Requirements fulfilled Refer to [D7] System FMEA Report, [D19] SW Safety Requirement Specification
— Measures for controlling the effects of errors and other effects arising from any data communication process (see IEC 61508-2:2000, 7.4.8)	Requirements fulfilled Refer to [D7] System FMEA Report.
In addition, one or more of the following measures should be applied, taking into account the complexity of the SRP/CS and its PL:	/
— failure detection by automatic tests;	Requirement not applicable
— tests by redundant hardware;	Requirement not applicable
— diverse hardware;	Requirement not applicable
— operation in the positive mode;	Requirements fulfilled Mechanical components are designed in the positive mode.
— mechanically linked contacts;	Requirement not applicable
— direct opening action;	Requirement not applicable
— oriented mode of failure;	Requirement not applicable
— over-dimensioning by a suitable factor, where the manufacturer can demonstrate that derating will improve reliability — where over-dimensioning is appropriate, an over-dimensioning factor of at least 1,5 should be used. See also ISO 13849-2:2012, D.3.	Requirement not applicable
G.3 Measures for avoidance of systematic failures	/
The following measures should be applied.	/
— Use of suitable materials and adequate manufacturing Selection of material, manufacturing methods and treatment in relation to, e.g. stress, durability, elasticity, friction, wear, corrosion, temperature, conductivity, dielectric rigidity.	Requirements fulfilled Safety related components information see [D14] PCBA BOM.

Requirement + Inspection	Result - Remark
— Correct dimensioning and shaping Consideration of, e.g. stress, strain, fatigue, temperature, surface roughness, tolerances, manufacturing.	Requirements fulfilled Safety related components information see [D14] PCBA BOM.
— Proper selection, combination, arrangements, assembly and installation of components, including cabling, wiring and any interconnections, Apply appropriate standards and manufacturer's application notes, e.g. catalogue sheets, installation instructions, specifications, and use of good engineering practice.	Requirements fulfilled Safety related components information see [D14] PCBA BOM.
— Compatibility Use components with compatible operating characteristics. NOTE 1 Components such as hydraulic or pneumatic valves can require cyclic switching to avoid failure by non-switching or unacceptable increase in switching times. In this case a periodic test is necessary.	Requirements fulfilled Safety related components information see [D14] PCBA BOM.
— Withstanding specified environmental conditions Design the SRP/CS so that it is capable of working in all expected environments and in any foreseeable adverse conditions, e.g., temperature, humidity, vibration and electromagnetic interference (EMI) (see ISO 13849-2:2012, D.2).	Requirements fulfilled Refer to [D32] EMC Testing Report, [D33] Environmental Testing Report.
— Use of components designed to an appropriate standard and having well-defined failure modes To reduce the risk of undetected faults by the use of components with specific characteristics (see IEC 61508-7:2000, B.3.3).	Requirement not applicable
In addition, one or more of the following measures should be applied, taking into account the complexity of the SRP/CS and its PL.	/
— Hardware design review (e.g. by inspection or walk-through) To reveal by reviews and analysis discrepancies between the specification and implementation (see IEC 61508-7:2000, B.3.7 and B.3.8).	Requirements fulfilled Refer to [D15] HW Inspection Report.
— Computer-aided design tools capable of simulation or analysis Perform the design procedure systematically and include appropriate automatic construction elements that are already available and tested (see IEC 61508-7:2000, B.3.5).	Requirements fulfilled Refer to [D23] Support Tools Assessment Report.

Requirement + Inspection	Result - Remark
— Simulation Perform a systematic and complete inspection of an SRP/CS design in terms of both the functional performance and the correct dimensioning of their components (see IEC 61508-7:2000, B.3.6). NOTE 2 IEC 61508–2:2010, Annex F specifies techniques and measures for avoidance of systematic failures during design and development of application-specific integrated circuits (ASICs), field programmable gate arrays (FPGAs), programmable logic devices (PLDs) etc.	Requirement not applicable
G.4 Measures for avoidance of systematic failures during SRP/CS integration	/
The following measures should be applied during integration of the SRP/CS:	/
— functional testing;	Requirements fulfilled Refer to [D31] System Safety Validation Report, [D34] Fault Insert Report.
— project management;	Requirements fulfilled Refer to [D2] Safety Plan.
— documentation.	Requirements fulfilled Refer to [D2] Safety Plan.
In addition, black-box testing should be applied, taking into account the complexity of the SRP/CS and its PL.	Requirements fulfilled Refer to [D34] Fault Insert Report.

Table 12 Basic safety principles

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