rexroth
A Bosch Company

Safety-relevant project planning instructions according to EN ISO 13849

Electronic Joystick

4THE5 CAN series 41

RE 29696-02-B/2021-06-22, EN

The cover shows an example application. The product delivered may differ from the image on the cover.

The original instruction manual was created in the English language.

Contents

1 Aim and application

1.1 Context

Bosch Rexroth 4THE5-41 CAN remote controls are versatile control elements with advanced configuration possibilities. They are intended to be integrated into a machine safety chain within the meaning of the ISO13849 (2015-12) standard, by offering safety functions that can reach performance level d or c (PLd or PLc) depending on the versions.

The 4THE5-41 CAN remote controls are available in two variants:
- The 4THED5-41 CAN which reaches a Performance Level d,
- The 4THEC5-41 CAN which reaches a Performance Level c

As such, you will find in this document the information required to calculate the reliability of this safety chain, as well as the various characteristics relating to the safety of the product.

However, this document does not contain any information relating to the design of the machine safety chain, nor to the recommendations for installing the joystick in the machine (whether it is the assembly of the joystick on the armrest or the electrical connections).

For these subjects, the user must comply with the existing standards in the countries of use and the installation recommendations present in the product datasheet.

The machine manufacturer is responsible for the conformity of his machine with the existing laws and regulations. It is also the manufacturer's responsibility to verify that all potential hazards arising from the use of the machine - including actions of the machine in which the 4THE5-41 CAN remote control operates - are correctly identified and neutralized.
None of the information in this document can result in Bosch Rexroth being liable for a machine equipped with a 4THE5-41 CAN remote control.

The configuration of a 4THE5-41 CAN and its integration into the machine's functional safety chain can only be carried out by qualified personnel trained in electronics, software programming, and functional safety.

This document contains important information about functional safety. It is essential that the manufacturer has understood and followed the recommendations in this document and that they indicate in their own manual the recommendations necessary for the safe use of the machine.

1.2 Validity of the documentation

This documentation is valid for the following product:

- Electronic joystick 4THE5 CAN series 41 (4THEC5-41, 4THED5-41)

This documentation is intended for machine manufacturers. It contains important information for machine system development.

1.3 Required and supplementary documentation

Table 1: Required and supplementary documentation

Ref.	Document number	Description
[1]	RE 29696	Data sheet
[2]	RE 29696-01-B	Instruction manual
[3]	ISO 13849-1	Safety of machinery - Parts of control systems relating to security Part 1: General design principles
[4]	ISO 13849-2	Safety of machinery - Parts of control systems relating to security Part 2: Validation
[5]	IEC 61508	Functional safety standard for electrical / electronic / programmable electronic safety-related systems

1.4 Display of information

Standardized safety instructions, symbols, terms and abbreviations are used throughout this documentation so that you can work quickly and safely with your product. To give you a better understanding, these are explained in the sections below.

1.4.1 Safety instructions

Safety instructions are set out as follows:

SIGNAL WORD

Type and source of danger!
Consequences of non-compliance
▶ Measures to prevent danger

- **Warning sign:** draws attention to the danger
- **Signal word:** identifies the degree of danger
- **Type and source of danger:** identifies the type and source of the danger
- **Consequences:** describes what may happen if the safety instructions are not complied
- **Precautions:** states how the danger can be avoided

Table 2: Hazard classes as defined in ANSI Z535.6

Warning sign, signal word	Meaning
DANGER	Identifies a dangerous situation that will result in death or serious injuries if it is not avoided.
WARNING	Identifies a dangerous situation that may result in death or serious injuries if it is not avoided.
CAUTION	Identifies a dangerous situation that may result in minor to moderate injuries if it is not avoided.
NOTICE	Property damage: The product or the environment may be damaged.

1.4.2 Symbols

The following symbols indicate information that is not directly relevant to safety but increases understanding of the documentation.

Table 3: Meaning of the symbols

Symbol	Meaning
	If this information is disregarded, the product cannot be used or operated to its optimum potential.
▶	Single, independent step
1. 2. 3.	Numbered instruction: The numbers indicate that the steps must be completed in a prescribed sequence.

1.4.3 Abbreviations

This documentation uses the following abbreviations:

Table 4: Abbreviations

Abbreviation	Meaning
DC	Diagnostic coverage
$MTTF_d$	Mean time to dangerous failure
PFH_d	Average probability of dangerous failure per hour
PLc	Performance level c
PLd	Performance level d
CCF	Common cause failure
SRP/CS	Safety-related Part of a control system
AMDE	Failure Mode and Effect Analysis
FS	Safety function

1.4.4 Definition of an actuation cycle

Mechanical actuation: "Negative end of stroke → Positive end of stroke → Negative end of stroke" with a torque of 5 Nm applied to the joystick at the end of stroke position.

The above sequence corresponds to a "normalized" cycle.

2 Safety instructions

2.1 About this chapter

The product has been manufactured in accordance with the generally accepted rules of the state of the art. However, there is still a danger of personal injury or damage to equipment if this chapter and the safety instructions in this documentation are not complied with.

- ▶ Read this documentation completely and thoroughly before working with the product.
- ▶ Keep this documentation in a location where it is accessible to all users at all times.
- ▶ Always include the required documentation when you pass the 4THE5 on to third parties.

2.2 Intended use

The intended use of the 4THE5 is stated within the manual [2].

The product can be implemented as a safety-related part of a control system. If the product is implemented to realize safety functions, additional measures shall be defined by the system manufacturer or system planner and realized in the control system of the machine.
Further details can be found in standards governing functional safety such as ISO 13849, IEC 62061 or specific technical guidelines.

2.3 Improper use

Any use other than that described as intended use shall be considered as improper and is therefore impermissible.
Bosch Rexroth AG is not liable for damages resulting from improper use. The user bears all risks from improper use.
The following foreseeable forms of misuse are also considered to be improper (this list does not claim to be exhaustive):

- Use outside the operating parameters approved in the data sheet or in the order confirmation
- Use of non-approved fluids
- Changes to factory settings by unauthorized persons
- Use of add-ons not in combination with the specified Rexroth components
- Using in a potentially explosive environment

2.4 Personnel qualifications

The activities described in this documentation require basic mechanical, electric and software expertise, as well as knowledge of the associated technical terms.
Qualified personnel are those who can recognize possible dangers and take the appropriate safety measures due to their professional training, knowledge, and experience, as well as their understanding of the relevant regulations pertaining to the work to be done. Qualified personnel must follow the rules relevant to their field of operation and have the necessary knowledge.

2.5 General safety instructions

- Observe the applicable accident prevention and environmental protection regulations.
- Observe the safety regulations and provisions of the country in which the product is used/operated.
- Use Rexroth products only when they are in proper working condition.
- Observe all notices on the product.
- Persons who install, operate, remove or maintain Rexroth products must not be under the influence of alcohol, drugs or medication that may affect their reaction time.
- Only use original Rexroth accessories and spare parts.
- Observe the technical data and ambient conditions specified in this documentation.
- If unsuitable products are installed or used in applications that are relevant for safety, unexpected operating conditions may occur in the application, which could result in injury to personnel or damage to equipment. For this reason, only use the product in a safety-related application if this use is explicitly specified and permitted in the product documentation, for example as a safety-related part of a control system (functional safety).
- You may only commission the product if it has been ensured that the end product (e.g., machinery or system) in which the Rexroth products are installed complies with the country-specific provisions, safety regulations and standards for the application.

3 Recommended operating conditions

3.1 Temperature profile

Life-time rate [%]	Temperature [° C]
8	30
64.9	40
25	50
2	60
0.1	70

3.2 Lifetime

The 4THED5-41CAN remote control is designed to function correctly for the time defined in the following table:

Storage	5 years
Number of actuation cycles	5 Million

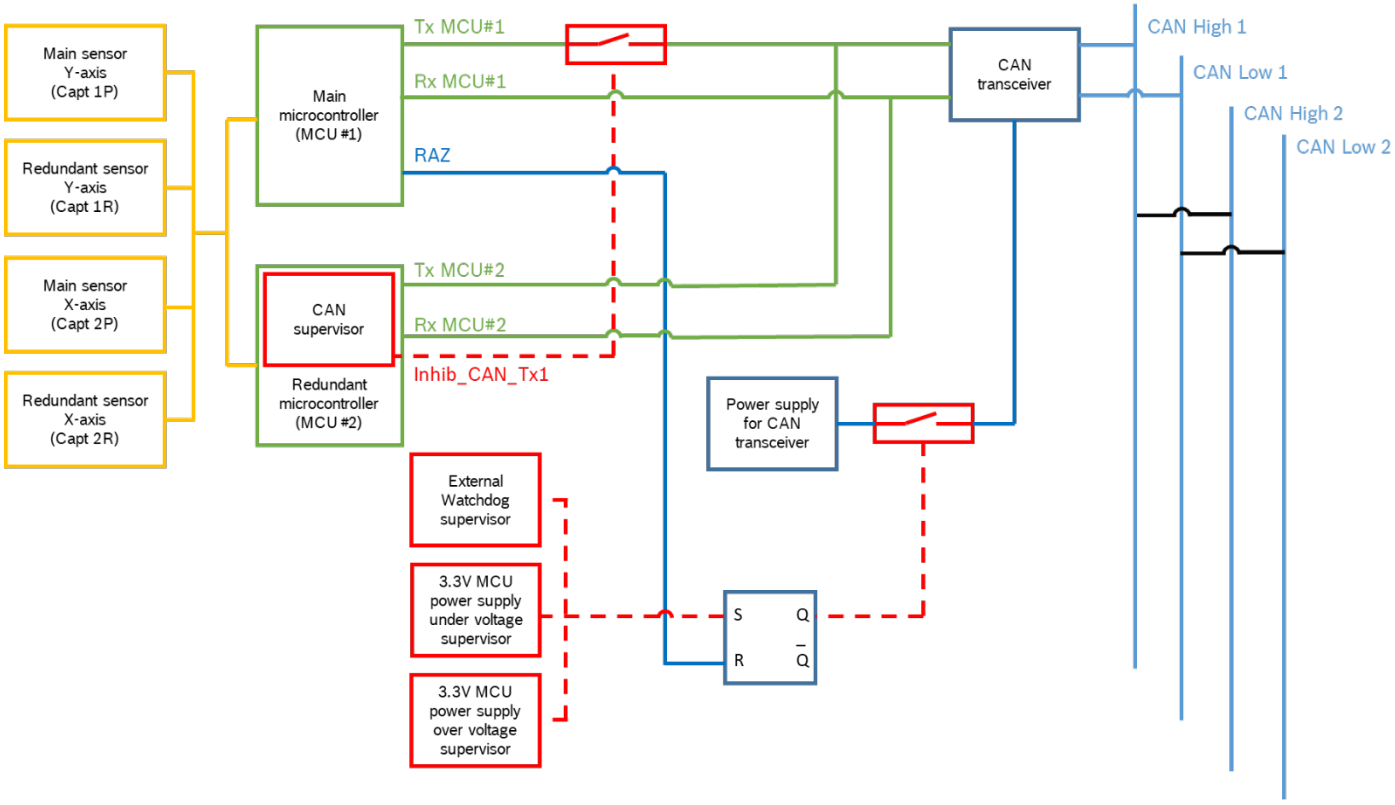
Beyond this lifetime, the probability of product failure is likely to increase, and data relating to functional safety are no longer guaranteed.
If you wish to use a remote control beyond the values given in the table, please contact Bosch Rexroth.

3.3 Memory write / erase cycles

The user shall not exceed a maximum number of write / erase cycles in the memory of the product of 100 cycles.
Beyond this value, the proper operation of the product is no longer guaranteed.

4 4THED5 (PLd prepared version)

4.1 Architecture



4.2 Safety Functions

4.2.1 FS1

Specification of the functional requirements of the safety function	
Name	Function name: When an axis defect is detected, a "position to neutral" instruction is transmitted on the faulty axis
Required performance level (PLr)	PLd
Activation conditions	Still active
Interface	Input: Inconsistent voltages between primary sensor and redundant sensor Output: CAN message
Function behavior	Trigger status: difference between the two signals greater than software parameterized threshold for 5 successive detections (50ms) Result: Data field of the CAN message set to 0x00 for the faulty axis + emission of an error code specific to this fault on the CAN bus
Priority over other simultaneous functions	Function has a lower priority than FS2, FS3, FS4
Other functions acting on the same actuator	FS2, FS3, FS4
Maximum reaction time of the function	50ms
Function demand rate	N/A
Reaction to faults / restart conditions	Monitoring enabled every time the product is started Disappearing default mode on: - Canceling the error - Returning to the neutral position of the axis concerned
Ambient conditions	The joystick is functional between -20°C and +65°C The joystick is functional when the supply voltage remains within a range from 6.5V to 36V The joystick complies with the IPx7 standard

This safety function can be integrated into a safety chain in the machine.

4.2.2 FS2

Specification of the functional requirements of the safety function	
Name	Function name: When a microcontroller monitoring fault is detected, a "neutral position" setpoint is transmitted on all axes
Required performance level (PLr)	PLd
Activation conditions	Still active
Interface	Input: differences between the CAN messages emitted by the primary microcontroller and the data calculated by the redundant microcontroller Output: “safe” CAN message emitted by the redundant microcontroller
Function behavior	Trigger status: Difference between the object values of the two CAN messages greater than the parameterized threshold in memory of the microcontroller, during 8 successive detections (80ms) OR failure to issue a CAN message for 20 successive detections (200ms) OR Wrong DLC of CAN messages OR unexpected emission of a CAN message (in a silent mode for example) Result: The redundant microcontroller cuts off communication from the main microcontroller and takes control of the CAN bus. It will therefore return: - digital values of the internal axis of the CAN message set to 0x00 (neutral setpoint) - status information + direction forced to neutral position - emission of a fault-specific error code on the CAN bus"
Priority over other simultaneous functions	This function has a higher priority than the safety function FS1
Other functions acting on the same actuator	FS1, FS3, FS4
Maximum reaction time of the function	200ms
Function demand rate	N/A
Reaction to faults / restart conditions	Monitoring enabled at each startup (return to a ""no-fault" functional mode at startup and continue monitoring) Disappearance of the fault mode on resetting of the power supply of the joystick
Ambient conditions	The joystick is functional between -20°C and +65°C The joystick is functional when the supply voltage remains within a range from 6.5V to 36V The joystick complies with the IPx7 standard

This safety function can be integrated into a safety chain in the machine.

4.2.3 FS3

Specification of the functional requirements of the safety function	
Name	Function name: When an internal defect is detected on the microcontroller, transmission of the "neutral position" instruction on all axes and emission of an error code
Required performance level (PLr)	PLd
Activation conditions	Still active
Interface	Input: Microcontroller status Output: CAN message
Function behavior	Trigger status: One of the hardware monitoring routines returned a defect: - ALU test - RAM integrity test - ROM integrity test - Testing output registers - Maintenance test - CPU test Result: Digital values of the CAN message set to 0x00 + status information set to neutral position + emission of a fault-specific error code on the CAN bus
Priority over other simultaneous functions	This function has a higher priority than the safety functions FS1, FS2
Other functions acting on the same actuator	FS1, FS2
Maximum reaction time of the function	3.6 sec
Function demand rate	N/A
Reaction to faults / restart conditions	In some cases, it will be possible to remove the error code as long as all the following points are respected: - Absence of any defect - Product reset - Emission of a diagnostic CAN message to the microcontroller (Rexroth in-house operation only)
Ambient conditions	The joystick is functional between -20°C and +65°C The joystick is functional when the supply voltage remains within a range from 6.5V to 36V The joystick complies with the IPx7 standard

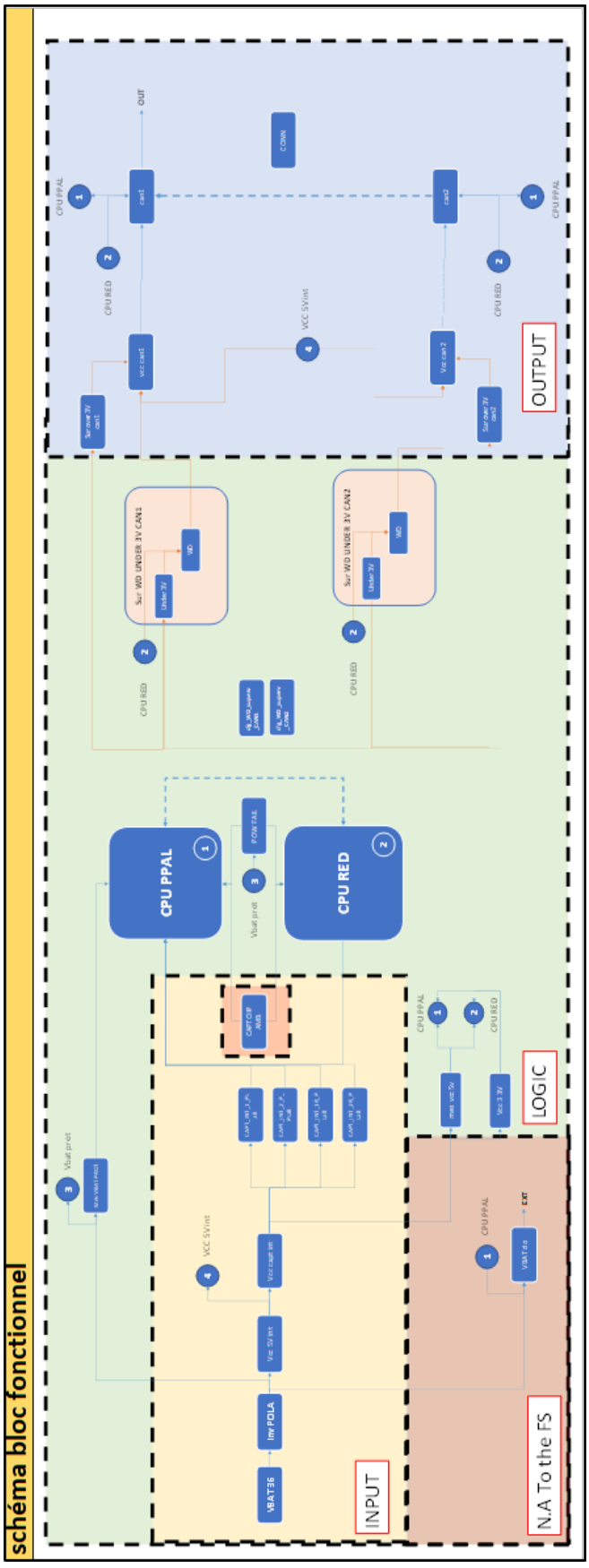
This safety function can be integrated into a safety chain in the machine.

4.2.4 FS4

Specification of the functional requirements of the safety function	
Name	Function Name: When the watchdog supervisor detects a defect on the microcontroller, the CAN output is cut off
Required performance level (PLr)	PLd
Activation conditions	Still active
Interface	Input: Microcontroller status (output watchdog signal active/inactive) Output: Power supply/de-powering the CAN transceiver (CAN Output)
Function behavior	Trigger status: No more active watchdog signal on the microcontroller Result: Anomaly detection via the watchdog supervisor, leading to the CAN output transceiver being cut off
Priority over other simultaneous functions	This function has a higher priority than all other safety functions: FS1, FS2, FS3
Other functions acting on the same actuator	FS1, FS2, FS3
Maximum reaction time of the function	N/A
Function demand rate	N/A
Reaction to faults / restart conditions	- Restarting the product - Presence of the active watchdog on the microcontroller
Ambient conditions	The joystick is functional between -20°C and +65°C The joystick is functional when the supply voltage remains within a range from 6.5V to 36V The joystick complies with the IPx7 standard

This security function is an internal function of the joystick.

4.3 Basic Logical Structure



The joystick features a CAT2 architecture with a PLr (required performance level) d.

Acquisition of instructions and the security environment (Input)
CAT2 architecture via redundant sensors read by a main and redundant microcontroller.

Processing (Logic)
CAT2 architecture provided by a main and a redundant microcontroller having two decision channels:
The CAT2 architecture is insured by:

- 1 main microcontroller whose function is to functionally control the output members transmission of set point positions in CAN format
- 1 redundant (safety) microcontroller whose function is to supervise the output components by inhibiting the transmission of CAN set positions in case of incoherence.

Output
CAT2 architecture provided by a CAN bus transmitting the set point.

4.4 Design of the SRP/CSa (Input)

4.4.1 Specification of the SRP/CSa

SRP/CSb "Input" Specification	
Name	SRP/CSa "Input"
Activation requirements	Always active
Interface	**Input:** Joystick actuation **Output:** Signal from sensors to microcontrollers
Means of interconnection	Copper routing
Description	This SRP/CS is designed by considering redundant sensors re-read by microcontrollers in order to target category 2.
Priority	N/A
Maximum reaction time	0.6ms
Function demand rate	Permanently
Environmental conditions	The joystick is functional between -20°C and +65°C The joystick is functional when the supply voltage remains within a range from 6.5V to 36V The joystick complies with the IPx7 standard

4.4.2 Functional blocks

Name of the functional blocks	**Component type**
VCC_CAPT_INT_PLall	Resistor FET (transistor)
INV_POLA_PLall	Diode
CAPT_INT_1_PLall	Resistor Hall effect sensor Ceramic capacitor
CAPT_INT_1R_PLall	Resistor Hall effect sensor Ceramic capacitor
CAPT_INT_2_PLall	Resistor Hall effect sensor Ceramic capacitor
CAPT_INT_2R_PLall	Resistor Hall effect sensor Ceramic capacitor
VCC_5V_INT_PLall	Transformer (Hypothesis: Inductor and Ferrite) Resistor FET (transistor) Diode Ceramic capacitor
VBAT_36V_PLall	Ceramic capacitor Varistor

4.4.3 Specifying diagnostics and determining the DC

Function block	**Planned diagnosis (based on Annex E of ISO 13849, and IEC 61508-2)**	**DC of each component (according to Annex E of ISO 13849, and IEC 61508-2)**
VCC_CAPT_INT_PLall	Table A13 (IEC 61508-2): Sensors Comparison/majority vote on inputs (1oo2, 2oo3 or better redundancy)	High DC = 99%
INV_POLA_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
CAPT_INT_1_PLall	Table A13 (IEC 61508-2): Sensors Comparison/majority vote on inputs (1oo2, 2oo3 or better redundancy)	High DC = 99%
CAPT_INT_1R_PLall	Table A13 (IEC 61508-2): Sensors Comparison/majority vote on inputs (1oo2, 2oo3 or better redundancy)	High DC = 99%
CAPT_INT_2_PLall	Table A13 (IEC 61508-2): Sensors Comparison/majority vote on inputs (1oo2, 2oo3 or better redundancy)	High DC = 99%
CAPT_INT_2R_PLall	Table A13 (IEC 61508-2): Sensors Comparison/majority vote on inputs (1oo2, 2oo3 or better redundancy)	High DC = 99%
VCC_5V_INT_PLall	Table A3 (IEC 61508-2): Electronic components Monitored redundancy	High DC = 99%
VBAT_36V_PLall	Table A3 (IEC 61508-2) Electronic components Analog signal monitoring	Low DC = 60%

4.4.4 $MTTF_d$ of the functional blocks

The calculation of the $MTTF_d$ of each component is performed by applying reliability calculation benchmarks such as the SN29500.

Function block	**$MTTF_d$ (years)**	**PFH_d**
VCC_CAPT_INT_PLall	55702	2.05E-09
INV_POLA_PLall	105353	1.08E-09
CAPT_INT_2R_PLall	8986	1.27E-08
CAPT_INT_2_PLall	8986	1.27E-08
CAPT_INT_1R_PLall	8986	1.27E-08
CAPT_INT_1_PLall	8986	1.27E-08
VCC_5V_INT_PLall	5858	1.95E-08
VBAT_36V_PLall	31002	3.68E-09
Total (SRP/CSa)	**4467**	**6.76E-04**

4.4.5 Planned actions against CCF and rating

N°	**Rating of the measures against CCF (Annex F- informative of ISO 13849)**		
1	**Separation/ isolation**	**Max**	**JS**
	Physical separation between signal channels	15	0
2	**Diversity**		
	Different design/technologies or physical principles are used	20	0
3	**Design/ application/ experience**		
3.1	Protection against overvoltage, overpressure, overcurrent, overheating, etc.	15	15
3.2	Use of proven components	5	5
4	**Assessment/ analysis**		
	Analysis and consideration of failure modes and their effects to prevent design-related CCF	5	5
5	**Competence/ training**	5	5
6	**Environment**		
6.1	Prevention of contamination and EMC against CCF	25	25
6.2	Other influences (temperature, shock, vibration, humidity, etc.)	10	10
	Total	**100**	**65**
The total score is ≥ 65: the implemented measures allow the joystick to meet the requirements			

4.4.6 Conclusion

SRP/CSa summary		
Data	**Requirements**	**Results**
Requirements for PLd with Category 2 use	Compliance with CAT B requirements	OK
	30 years ≤ $MTTF_d$≤ 100 years (so $MTTF_d$ = **"High")**	$MTTF_d$ channel = 100 years **High $MTTF_d$**
	DC_{avg}≥ 90% (i.e. DC_{avg} ≥ **"Medium")**	DC_{avg} = 97.1% **Medium DC_{avg}**
	CCF score ≥ 65	CCF score = 65
	Proven safety components and principles Single defect = safe state	OK OK
	Tests: if possible, as soon as or before next stress	Tests at each stress
	If defect detected: Drive in safe state (off) or danger warning	If defect detected: Safe state = return to neutral and/or shutdown (see Safety Functions)
	Category 2	Category 2
Conclusion: Is PL "d" attained?		**YES**

4.5 Design of the SRP/CSb (Logic)

4.5.1 Specification of the SRP/CSb

SRP/CSb "Logic" Specification	
Name	SRP/CSb "Logic"
Activation requirements	Always active
Interface	**Input:** Signal from sensors **Output:** Signal from microcontroller to CAN Bus
Means of interconnection	Copper routing
Description	This SRP/CSb is designed by considering two microcontrollers (a primary and a redundant one) having therefore two decision channels in order to target category 2. The function of the main microcontroller is to functionally control the output components and transmit CAN set points. The function of the redundant (safety) microcontroller is to supervise the output components by inhibiting the CAN transmission of set points in case of incoherence.
Priority	N/A
Maximum reaction time	The maximum time for the redundant microcontroller to detect an incoherence of the primary microcontroller is therefore 300ms
Function demand rate	Permanently
Environmental conditions	The joystick is functional between -20°C and +65°C The joystick is functional when the supply voltage remains within a range from 6.5V to 36V The joystick complies with the IPx7 standard

4.5.2 Functional blocks

Functional block	Component type
cfg_WD_superv_CAN1_PLC	Resistor
cfg_WD_superv_CAN1_PLD	Resistor
Surv_WD_under3V_CAN1_PLall	Analog IC
POW_FAIL_PLall	Resistor Analog IC Diode Ceramic capacitor
VCC_3_3V_PLD	Ceramic capacitor
MES_VBAT_PROT_PPAL_PLall	Ceramic capacitor Resistor
MES_VCC_5V_INT_RED_PLD	Resistor Ceramic capacitor
MES_VCC_5V_INT_PPAL_PLall	Resistor Ceramic capacitor
VCC_3_3V_PLall	Resistor Analog IC Ceramic capacitor
CPU_red_PLD	Resistor microcontroller Diode Ceramic capacitor Quartz
CPU_ppal_PLall	Resistor Microcontroller Diode Ceramic capacitor Quartz

4.5.3 Specifying diagnostics and determining the DC

Function block	**Planned diagnosis (based on Annex E of iso 13849, And IEC 61508-2)**	**DC of each component (according to Annex E of ISO 13849, and IEC 61508-2)**
cfg_WD_superv_CAN1_PLC	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
cfg_WD_superv_CAN1_PLD	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
Surv_WD_under3V_CAN1_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
POW_FAIL_PLall	Table A3 (IEC 61508-2) Electronic components Analog signal monitoring	Low DC = 60%
VCC_3_3V_PLD	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
MES_VBAT_PROT_PPAL_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
MES_VCC_5V_INT_RED_PLD	Table A3 (IEC 61508-2) Electronic components Monitored redundancy	High DC = 99%
MES_VCC_5V_INT_PPAL_PLall	Table A3 (IEC 61508-2) Electronic components Monitored redundancy	High DC = 99%
VCC_3_3V_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
CPU_red_PLD	Table A10 (IEC 61508-2) Program sequence Logical monitoring of the program sequence	Average DC = 90%
CPU_ppal_PLall	Table A10 (IEC 61508-2) Program sequence Logical monitoring of the program sequence	Average DC = 90%

4.5.4 $MTTF_d$ of the functional blocks

The calculation of the $MTTF_d$ of each component is performed by applying reliability calculation benchmarks such as the SN29500.

Function blocks	**$MTTF_d$ (years)**	**PFH_d**
cfg_WD_superv_CAN1_PLC	1027237	1.11E-10
cfg_WD_superv_CAN1_PLD	1027237	1.11E-10
Surv_WD_under3V_CAN1_PLall	440033	2.59E-10
POW_FAIL_PLall	43260	2.64E-09
VCC_3_3V_PLD	31648	3.61E-09
MES_VBAT_PROT_PPAL_PLall	222213	5.14E-10
MES_VCC_5V_INT_RED_PLD	222213	5.14E-10
MES_VCC_5V_INT_PPAL_PLall	222213	5.14E-10
VCC_3_3V_PLall	15727	7.26E-09
CPU_red_PLD	2118	5.39E-08
CPU_ppal_PLall	2118	5.39E-08
Total (SRP/CSb)	**2492**	**1.08E-03**

4.5.5 Planned actions against CCFs and rating

Nº	**Rating of measures against CCF (Annex F- informative of ISO 13849)**		
1	**Separation/ isolation**	Max	JS
	Physical separation between signal channels	15	0
2	**Diversity**		
	Different design/technologies or physical principles are used	20	0
3	**Design/ application/ experience**		
3.1	Protection against overvoltage, overpressure, overcurrent, overheating, etc.	15	15
3.2	Use of proven components	5	5
4	**Assessment/ analysis**		
	Analysis and consideration of failure modes and their effects to prevent design-related CCFs	5	5
5	**Competence/ training**	5	5
6	**Environment**		
6.1	Prevention of contamination and EMC against CCF	25	25
6.2	Other influences (temperature, shock, vibration, humidity, etc.)	10	10
	Total	100	65
The total score is ≥ 65: the implemented measures allow the joystick to meet the requirements			

4.5.6 Conclusion

SRP/CSb summary		
Data	**Requirements**	**Results**
Requirements for PLd with Category 2	Compliance with CAT B requirements	OK
	30 years ≤ $MTTF_d$≤ 100 years (so $MTTF_d$ = **"High")**	$MTTF_d$ channel = 100 years **High $MTTF_d$**
	DC_{avg}≥ 90% (i.e. DC_{avg} ≥ **"Medium")**	DC_{avg} = 97.1% **Medium DC_{avg}**
	Score ≥ 65	Score = 65
	Proven safety components and principles Single defect = safe state	OK OK
	Tests: if possible, as soon as or before next stress	Tests at each stress
	If defect detected: Drive in safe state (off) or danger warning	If defect detected: Safe state = return to neutral and/or shutdown (see Safety functions)
	Category 2	Category 2
Conclusion: Is PL "d" attained?		**YES**

4.6 Design of the SRP/CSc (Output)

4.6.1 Specification of the SRP/CSc

SRP/CSc "Output" Specification	
Name	SRP/CSc "Output"
Activation requirements	Still active
Interface	Input: Signal from the microcontroller Output: Signal to the CAN Bus
Means of interconnection	Copper routing
Description	See the functional description of the "Output" part
Priority	N/A
Maximum reaction time	100ns
Function demand rate	Permanently
Environmental conditions	Functional joystick between -20°C and +65°C Functional joystick when the supply voltage is between 6.5V and 36V IPx7 compliant joystick

4.6.2 Functional blocks

Functional block	**Component type**
Surv_over3V_CAN1_PLall	Resistor Analog IC CMOS comparator Analog IC Ceramic capacitor
VCC_CAN1_PLall	transistor Resistor Analog IC Ceramic capacitor
CONN_PLall	Connector
CAN1_PLall	Inductor Ceramic capacitor Ceramic capacitor Analog IC Transceiver Varistor

4.6.3 Specifying diagnostics and determining the DC

Function block	Planned diagnosis (based on Annex E of ISO 13849, and IEC 61508-2)	DC of each component (according to Annex E of ISO 13849, and IEC 61508-2)
Surv_over3V_CAN1_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
VCC_CAN1_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
CONN_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
CAN1_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%

4.6.4 $MTTF_d$ of the functional blocks

The calculation of the $MTTF_d$ of each component is performed by applying reliability calculation benchmarks such as the SN29500.

Function block	$MTTF_d$ (years)	PFH_d
Surv_over3V_CAN1_PLall	58171	1.96E-09
VCC_CAN1_PLall	58171	1.96E-09
CONN_PLall	30137	3.79E-09
CAN1_PLall	30137	3.79E-09
Total (SRP/CSc)	**42 332**	**2.05E-04**

4.6.5 Planned actions against CCF and rating

N°	Rating of measures against CCF (Annex F- informative of ISO 13849)		
1	**Separation/ isolation**	Max	JS
	Physical separation between signal channels	15	0
2	**Diversity**		
	Different design/technologies or physical principles are used	20	0
3	**Design/ application/ experience**		
3.1	Protection against overvoltage, overpressure, overcurrent, overheating, etc...	15	15
3.2	Use of proven components	5	5
4	**Assessment/ analysis**		
	Analysis and consideration of failure modes and their effects to prevent design-related CCFs	5	5
5	**Competence/ training**	5	5
6	**Environment**		
6.1	Prevention of contamination and EMC against CCF	25	25
6.2	Other influences (temperature, shock, vibration, humidity, etc.)	10	10
	Total	100	65
The total score is ≥ 65: the implemented measures allow the joystick to meet the requirements			

4.6.6 Conclusion

SRP/CSc summary		
Data	**Requirements**	**Results**
Requirements for PLd with Category 2 use	Compliance with CAT B requirements	OK
	30 years ≤ $MTTF_d$≤ 100 years (so $MTTF_d$ = "High")	$MTTF_d$ channel = 100 years High $MTTF_d$
	DC_{avg}≥ 90% (i.e. DC_{avg}≥ "Medium")	DC_{avg} = 97.1% Medium DC_{avg}
	Score ≥ 65	Score = 65
	Proven safety components and principles Single defect = safe state	OK OK
	Tests: if possible, as soon as or before next stress	Tests at each stress
	If defect detected: Drive in safe state (off) or danger warning	If defect detected: Safe state = return to neutral and/or shutdown (see Safety functions)
	Category 2	Category 2
Conclusion: Is PL "d" attained?		**YES**

4.7 FMEA

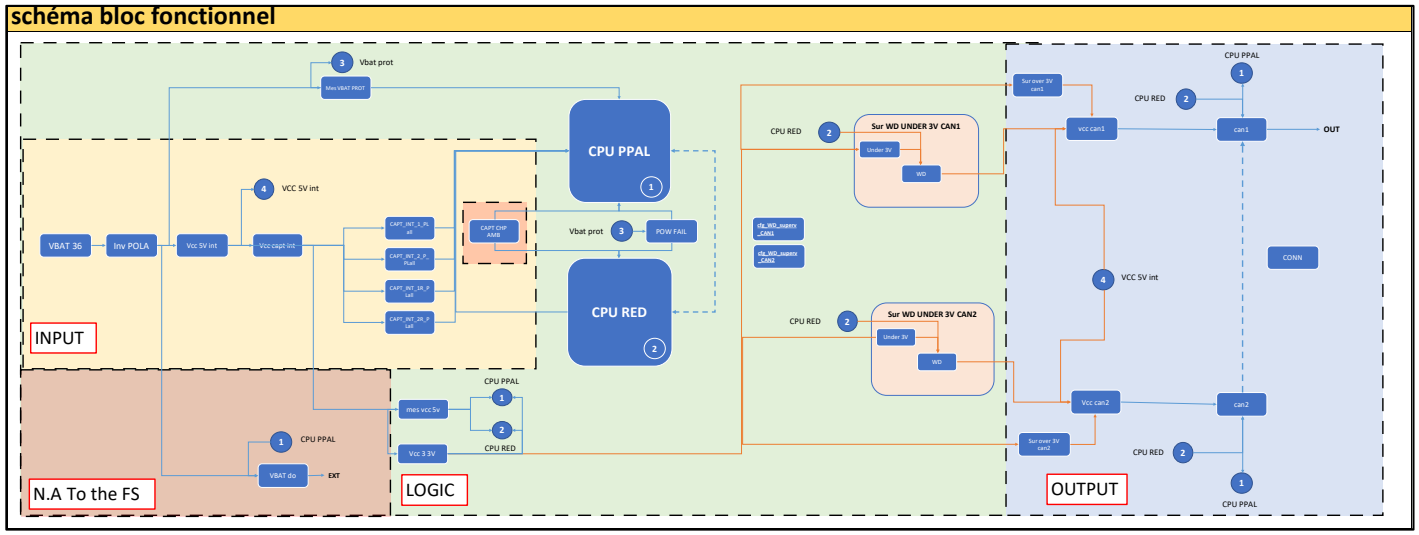
The design FMEA was established to guarantee the quality of the development process of the electronic database 4THE5-41 CAN full.
Please refer to the FMEA T112 CAN cover page for more information.

4.8 Outcomes for the safety functions of the command system

The PL for each SRP/CS has been determined according to the architecture and operation of the system.
The overall PL of the safety function of the command system is determined using Table 11 of ISO 13849-1 2015.

- FS1 "When an axis defect is detected, transmission of the set point "position to neutral" on the axis in default".
- FS2 "When a microcontroller monitoring fault is detected, transmission of the set point "position to neutral" on all axes".

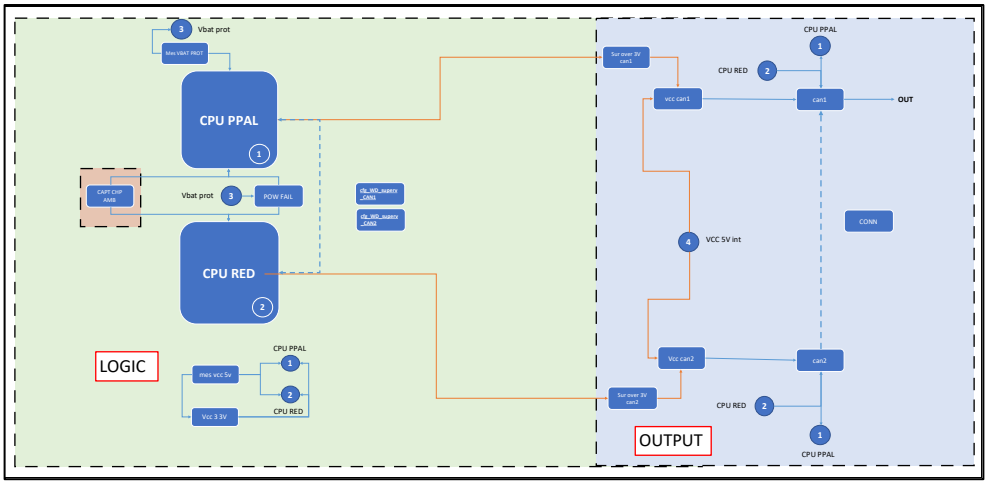
For these two safety functions, the combination of SRP/CS is shown in the figure below:



SRP/CS	$MTTF_d$ (a)		DC (%)		CCF	Category	PL
Input	4 467	High	97	Medium	65	2	d
Logic	2 492	High	90	Medium	65	2	d
Output	42 332	High	99	High	65	2	d

- FS3 "When an internal defect is detected, transmission of the set point "position to neutral" on all axes and emission of an error code".

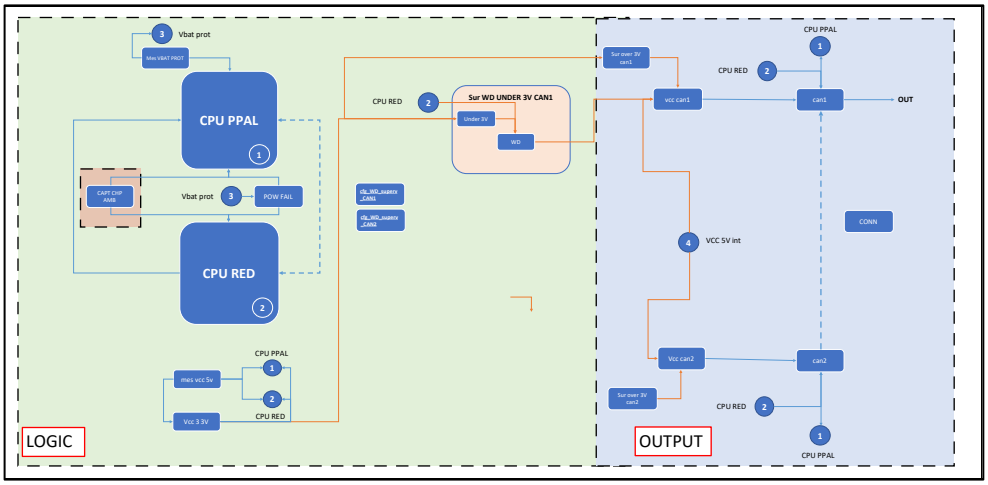
For this safety function, the combination of SRP/CS is shown in the figure below:



SRP/CS	MTTFd (a)		DC (%)		CCF	Category	PL
Logic	2 498	High	90	Medium	65	2	d
Output	42 332	High	99	High	65	2	d

- FS4 "When the watchdog supervisor detects a defect on the microcontroller, hardware transmission CAN cutoff".

For this safety function, the combination of SRP/CS is shown in the figure below:



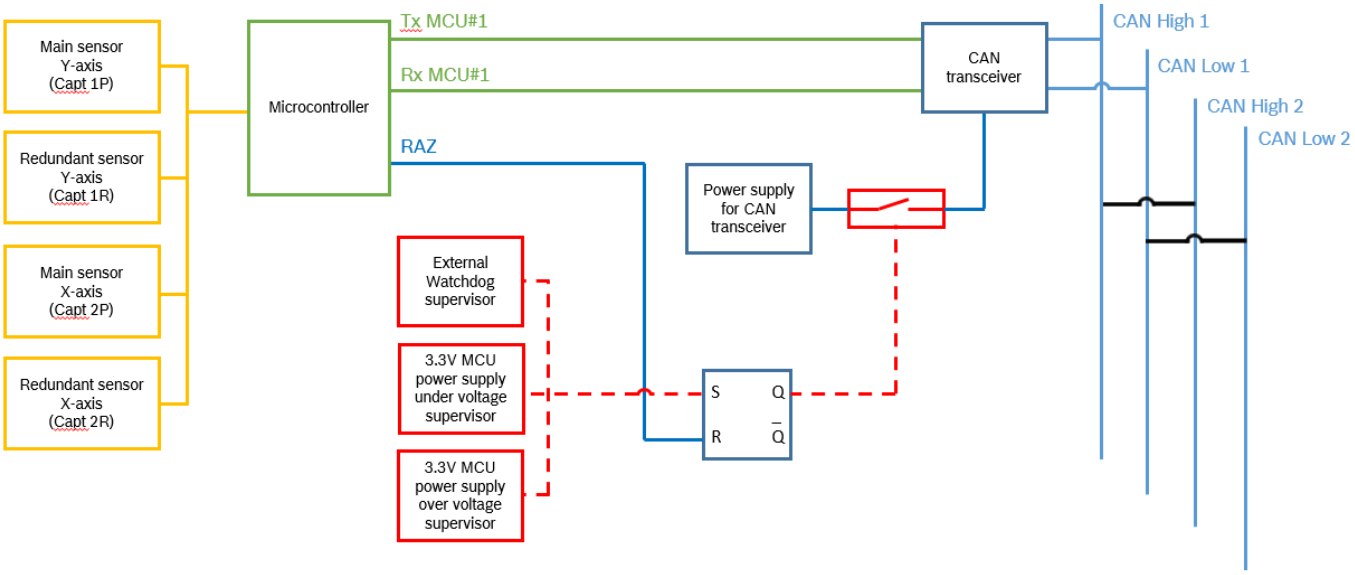
SRP/CS	MTTFd (a)		DC (%)		CCF	Category	PL
Logic	2 492	High	90	Medium	65	2	d
Output	42 332	High	99	High	65	2	d

4.10 Conclusion

	$MTTF_d$ (a)		DC (%)		CCF	PL	PLr
FS1	1541	High	94	Medium	65	**d**	**d**
FS2	1541	High	94	Medium	65	**d**	**d**
FS3	2359	High	92	Medium	65	**d**	**d**
FS4	2353	High	92	Medium	65	**d**	**d**

5 4THEC5 (PLc prepared version)

5.1 Architecture



5.2 Safety Functions

5.2.1 FS1

Specification of the functional requirements of the safety function	
Name	Function name: In case an axis defect is detected, a "position to neutral" instruction is transmitted on the faulty axis
Required performance level (PLr)	PLc
Activation conditions	Still active
Interface	Input: Inconsistent voltages between primary sensor and redundant sensor Output: CAN message
Behavior of the function	Trigger status: difference between the two signals greater than software parameterized threshold for 5 successive detections (50ms) Result: Data field of the CAN message set to 0x00 for the faulty axis + emission of an error code specific to this fault on the CAN bus
Priority over other simultaneous functions	Function lower priority than FS2, FS3, FS4
Other functions acting on the same actuator	FS2, FS3
Maximum reaction time of the function	50ms
Function demand rate	N/A
Reaction to faults / restart conditions	Monitoring enabled every time the product is started Disappearing default mode on: - Canceling the error - Returning to the neutral position of the axis concerned
Ambient conditions	The joystick is functional between -20°C and +65°C The joystick is functional when the supply voltage remains within a range from 6.5V to 36V The joystick complies with the IPx7 standard

This safety function can be integrated into a safety chain in the machine.

5.2.2 FS2

Specification of the functional requirements of the safety function	
Name	Function name: In case an internal defect is detected on the microcontroller, transmission of the neutral position instruction on all axes and emission of an error code
Required performance level (PLr)	PLc
Activation conditions	Still active
Interface	Input: Microcontroller status Output: CAN message
Behavior of the function	Trigger status: One of the hardware monitoring routines returned a defect: - ALU test - RAM integrity test - ROM integrity test - Testing output registers - Maintenance test - CPU test Result: Digital values of the CAN message set to 0x00 + status information set to neutral position + emission of a fault-specific error code on the CAN bus
Priority over other simultaneous functions	This function has a higher priority than the safety function FS1
Other functions acting on the same actuator	FS1
Maximum reaction time of the function	3.6 sec
Function demand rate	N/A
Reaction to faults / restart conditions	In some cases, it will be possible to remove the error code as long as all the following points are respected: - Absence of any defect - Product reset - Emission of a diagnostic CAN message to the microcontroller (Rexroth in-house operation only)
Ambient conditions	The joystick is functional between -20°C and +65°C The joystick is functional when the supply voltage remains within a range from 6.5V to 36V The joystick complies with the IPx7 standard

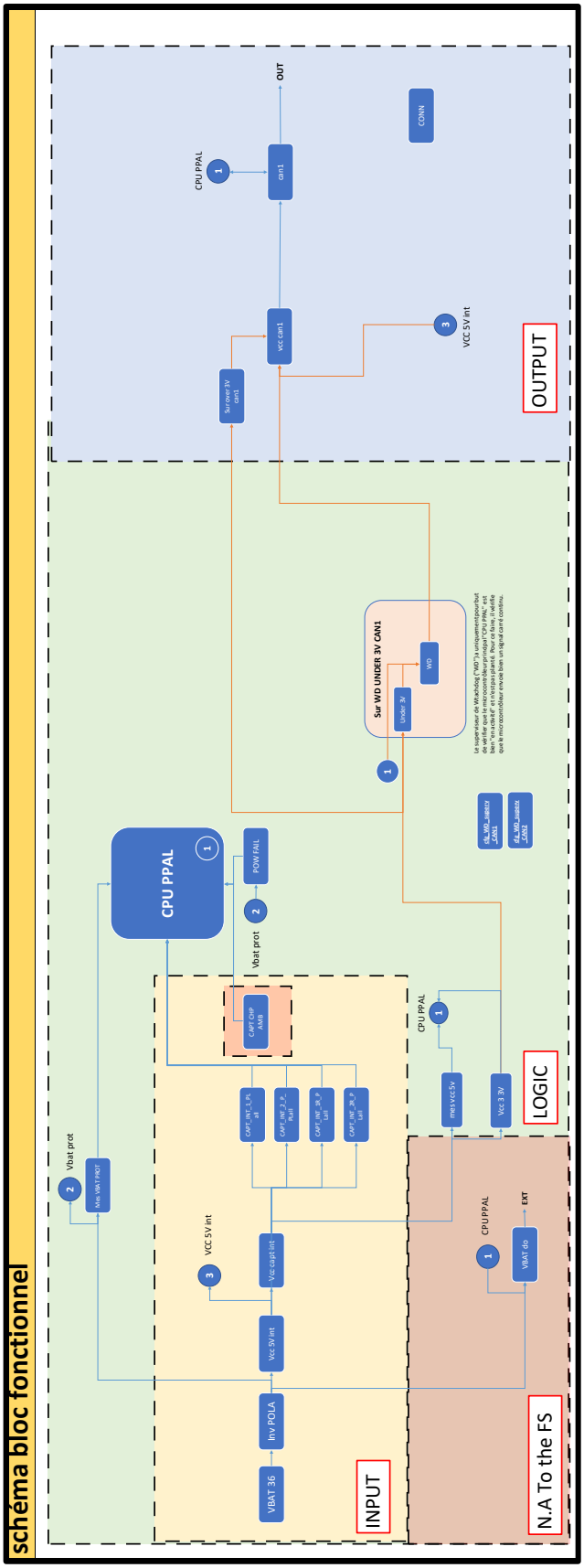
This safety function can be integrated into a safety chain in the machine.

5.2.3 FS3

Specification of the functional requirements of the safety function	
Name	Function Name: In case the watchdog supervisor detects a defect on the microcontroller, the CAN output is cut off
Required performance level (PLr)	PLc
Activation conditions	Still active
Interface	Input: Microcontroller status (output watchdog signal active/inactive) Output: Power supply/de-powering the CAN transceiver (CAN Output)
Behavior of the function	Trigger status: No more active watchdog signal on the microcontroller Result: Anomaly detection via the watchdog supervisor, leading to the CAN output transceiver being cut off
Priority over other simultaneous functions	This function has a higher priority than all other safety functions: FS1, FS2
Other functions acting on the same actuator	FS1, FS2
Maximum reaction time of the function	N/A
Function demand rate	N/A
Reaction to faults / restart conditions	- Restarting the product - Presence of the active watchdog on the microcontroller
Ambient conditions	The joystick is functional between -20°C and +65°C The joystick is functional when the supply voltage remains within a range from 6.5V to 36V The joystick complies with the IPx7 standard

This security function is an internal function of the joystick.

5.3 Basic Logical Structure



The mixed architecture combining CAT2-like operation with a PLr (required performance) type c

Acquisition of instructions and the security environment (Input)
CAT2 type via redundant sensors read by a primary and redundant microcontroller.

Mixed Processing (Logic)
Cat2 type provided by a microcontroller with a decision canal: Cat2 type insured by :
1 primary microcontroller whose function is to functionally control the output members
Transmission of setpoint positions in CAN format

Output
Cat2 type provided by a CAN bus transmitting the set positions.

5.4 Design of the SRP/CSa (Input)

5.4.1 Specification of the SRP/CSa

SRP/CSb "Input" Specification	
Name	SRP/CSa "Input"
Activation requirements	Always active
Interface	**Input:** Joystick actuation **Output:** Signal from sensors to microcontrollers
Means of interconnection	Copper routing
Description	This SRP/CS is designed by considering redundant sensors re-read by microcontrollers in order to target category 2.
Priority	N/A
Maximum reaction time	0.6ms
Function demand rate	Permanently
Environmental conditions	The joystick is functional between -20°C and +65°C The joystick is functional when the supply voltage remains within a range from 6.5V to 36V The joystick complies with the IPx7 standard

5.4.2 Functional Blocks

Functional block	**Component type**
VCC_CAPT_INT_PLall	Resistor FET (transistor)
INV_POLA_PLall	Diode
CAPT_INT_1_PLall	Resistor Hall effect sensor Ceramic capacitor
CAPT_INT_1R_PLall	Resistor Hall effect sensor Ceramic capacitor
CAPT_INT_2_PLall	Resistor Hall effect sensor Ceramic capacitor
CAPT_INT_2R_PLall	Resistor Hall effect sensor Ceramic capacitor
VCC_5V_INT_PLall	Transformer (Hypothesis: Inductor and Ferrite) Resistor film FET (transistor) Diode Ceramic capacitor
VBAT_36V_PLall	Ceramic capacitor Varistor

5.4.3 Specifying diagnostics and determining the DC

Function block	**Planned diagnosis (based on Annex E of ISO 13849, and IEC 61508-2)**	**DC of each component (according to Annex E of ISO 13849, and IEC 61508-2)**
VCC_CAPT_INT_PLall	Table A13 (IEC 61508-2): Sensors Analog signal monitoring	Low DC = 60%
INV_POLA_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
CAPT_INT_1_PLall	Table A13 (IEC 61508-2): Sensors Comparison/majority vote on inputs (1oo2, 2oo3 or better redundancy)	High DC = 99%
CAPT_INT_1R_PLall	Table A13 (IEC 61508-2): Sensors Comparison/majority vote on inputs (1oo2, 2oo3 or better redundancy)	High DC = 99%
CAPT_INT_2_PLall	Table A13 (IEC 61508-2): Sensors Comparison/majority vote on inputs (1oo2, 2oo3 or better redundancy)	High DC = 99%
CAPT_INT_2R_PLall	Table A13 (IEC 61508-2): Sensors Comparison/majority vote on inputs (1oo2, 2oo3 or better redundancy)	High DC = 99%
VCC_5V_INT_PLall	Table A13 (IEC 61508-2): Sensors Signal monitoring analog	Low DC = 60%
VBAT_36V_PLall	Table A3 (IEC 61508-2) Electronic components Analog signal monitoring	Low DC = 60%

5.4.4 $MTTF_d$ Functional Blocks

The calculation of the $MTTF_d$ of each component is performed by applying reliability calculation benchmarks such as the SN29500.

Function block	$MTTF_d$ (years)	PFH_d
VCC_CAPT_INT_PLall	55702	2.05E-09
INV_POLA_PLall	105353	1.08E-09
CAPT_INT_2R_PLall	8986	1.27E-08
CAPT_INT_2_PLall	8986	1.27E-08
CAPT_INT_1R_PLall	8986	1.27E-08
CAPT_INT_1_PLall	8986	1.27E-08
VCC_5V_INT_PLall	5858	1.95E-08
VBAT_36V_PLall	31002	3.68E-09
Total (SRP/CSa)	**4467**	**6.76E-04**

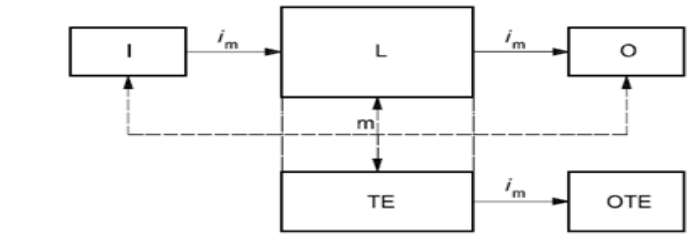
5.4.5 Planned actions against CCFs and rating

Nº	Rating of the measures against CCF (Annex F- informative of ISO 13849)		
1	**Separation/ isolation**	Max	JS
	Physical separation between signal channels	15	0
2	**Diversity**		
	Different design/technologies or physical principles are used	20	0
3	**Design/ application/ experience**		
3.1	Protection against overvoltage, overpressure, overcurrent, overheating, etc.	15	15
3.2	Use of proven components	5	5
4	**Assessment/ analysis**		
	Analysis and consideration of failure modes and their effects to prevent design-related CCF	5	5
5	**Competence/ training**	5	5
6	**Environment**		
6.1	Prevention of contamination and EMC against CCF	25	25
6.2	Other influences (temperature, shock, vibration, humidity, etc.)	10	10
	Total	100	65
The total score is ≥ 65: the implemented measures allow the joystick to meet the requirements			

5.4.6 Conclusion

<table>
<tr><th colspan="4">SRP/CSa summary</th></tr>
<tr><th>Data</th><th colspan="2">Requirements</th><th>Results</th></tr>
<tr><td rowspan="8">Requirements for PLc with Category 2 use</td><td colspan="2">Compliance with CAT B requirements</td><td>OK</td></tr>
<tr><td>10 years ≤ $MTTF_d$≤ 100 years (so $MTTF_d$≥ "Medium")</td><td>30 years ≤ $MTTF_d$≤ 100 years (so $MTTF_d$ = "High")</td><td>$MTTF_d$ channel = 100 years

$MTTF_d$ High</td></tr>
<tr><td>DCavg ≥ 60%
(so DC_{avg}≥ "Low")</td><td>DC_{avg}≥ 90%
(i.e. DC_{avg}≥ "Medium")</td><td>DC_{avg} = 86.2%
Medium DC_{avg}</td></tr>
<tr><td colspan="2">Score ≥ 65</td><td>Score = 65</td></tr>
<tr><td colspan="2">Proven safety components and principles
Single defect = safe state</td><td>OK</td></tr>
<tr><td colspan="2">Tests: if possible, as soon as or before next stress</td><td>Tests at each stress</td></tr>
<tr><td colspan="2">If defect detected: Drive in safe state (off) or danger warning</td><td>If a defect is detected:

Safe state = return to neutral and/or shutdown (see safety functions)</td></tr>
<tr><td colspan="2"> 
</td><td>Category 2</td></tr>
<tr><td colspan="3">Conclusion: Is PL "c" attained?</td><td>YES</td></tr>
</table>

5.5 Design of the SRP/CSb (Logic)

5.5.1 Specification of the SRP/CSb

SRP/CSa "Logic" Specification	
Name	SRP/CSb "Logic"
Activation requirements	Always active
Interface	**Input:** Signal from sensors **Output:** Signal from microcontroller to CAN Bus
Means of interconnection	Copper routing
Description	This SRP/CSb is designed by considering a microcontroller in order to target category 2. The function of the primary microcontroller is to functionally control the output components and transmit set positions in CAN format.
Priority	N/A
Maximum reaction time	30ms
Function demand rate	Permanently
Environmental conditions	The joystick is functional between -20°C and +65°C The joystick is functional when the supply voltage remains within a range from 6.5V to 36V The joystick complies with the IPx7 standard

5.5.2 Functional Blocks

Functional block	**Component type**
cfg_WD_superv_CAN1_PLC	Resistor
Surv_WD_under3V_CAN1_PLall	Analog IC
POW_FAIL_PLall	Resistor Analog IC Diode Capacitor Ceramic
VCC_3_3V_PLD	Ceramic capacitor
MES_VBAT_PROT_PPAL_PLall	Ceramic capacitor Resistor
MES_VCC_5V_INT_PPAL_PLall	Resistor Ceramic capacitor
VCC_3_3V_PLall	Resistor Analog IC Ceramic capacitor
CPU_ppal_PLall	Resistor Microcontroller Diode Ceramic capacitor Quartz
cfg_WD_superv_CAN1_PLC	Resistor
Surv_WD_under3V_CAN1_PLall	Analog IC
POW_FAIL_PLall	Resistor Analog IC Diode Capacitor Ceramic

5.5.3 Specifying diagnostics and determining the DC

Function block	**Planned diagnosis (based on Annex E of ISO13849, and IEC61508-2)**	**DC of each component (according to Annex E of ISO13849, and IEC61508-2)**
cfg_WD_superv_CAN1_PLC	Table A10 (IEC 61508-2) Program sequence Logical monitoring of the program sequence	DC Average = 90%
Surv_WD_under3V_CAN1_PLall	Table A10 (IEC 61508-2) Program sequence Logical monitoring of the program sequence	DC Average = 90%
POW_FAIL_PLall	Table A3 (IEC 61508-2) Electronic components Analog signal monitoring	Low DC = 60%
VCC_3_3V_PLD	Table A3 (IEC 61508-2) Electronic components Analog signal monitoring	Low DC = 60%
MES_VBAT_PROT_PPAL_PLall	Table A3 (IEC 61508-2) Electronic components Analog signal monitoring	Low DC = 60%
MES_VCC_5V_INT_PPAL_PLall	Table A3 (IEC 61508-2) Electronic components Monitored redundancy	High DC = 99%
VCC_3_3V_PLall	Table A3 (IEC 61508-2) Electronic components Analog signal monitoring	Low DC = 60%
CPU_ppal_PLall	Table A10 (IEC 61508-2) Program sequence Logical monitoring of the program sequence	DC Average = 90%
cfg_WD_superv_CAN1_PLC	Table A10 (IEC 61508-2) Program sequence Logical monitoring of the program sequence	DC Average = 90%
Surv_WD_under3V_CAN1_PLall	Table A10 (IEC 61508-2) Program sequence Logical monitoring of the program sequence	DC Average = 90%
POW_FAIL_PLall	Table A3 (IEC 61508-2) Electronic components Analog signal monitoring	Low DC = 60%

5.5.4 $MTTF_d$ Functional Blocks

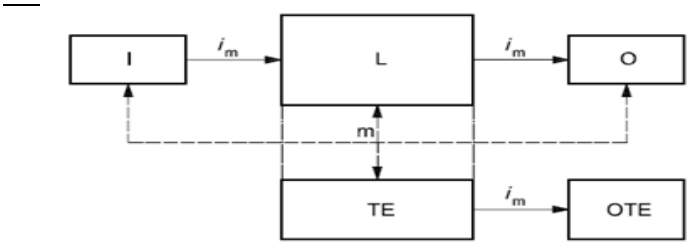
The calculation of the $MTTF_d$ of each component is performed by applying reliability calculation benchmarks such as the SN29500.

Function block	**$MTTF_d$ (years)**	**PFH_d**
cfg_WD_superv_CAN1_PLC	1027237	1.11E-10
Surv_WD_under3V_CAN1_PLall	440033	2.59E-10
POW_FAIL_PLall	43260	2.64E-09
VCC_3_3V_PLD	31648	3.61E-09
MES_VBAT_PROT_PPAL_PLall	222213	5.14E-10
MES_VCC_5V_INT_PPAL_PLall	222213	5.14E-10
VCC_3_3V_PLall	15727	7.26E-09
CPU_ppal_PLall	2118	5.39E-08
Total (SRP/CSb)	**60266**	**6.88E-08**

5.5.5 Planned actions against CCFs and rating

N°	**Rating of the measures against CCF (Annex F- informative of ISO 13849)**		
1	**Separation/ isolation**	Max	JS
	Physical separation between signal channels	15	0
2	**Diversity**		
	Different design/technologies or physical principles are used	20	0
3	**Design/ application/ experience**		
3.1	Protection against overvoltage, overpressure, overcurrent, overheating, etc.	15	15
3.2	Use of proven components	5	5
4	**Assessment/ analysis**		
	Analysis and consideration of failure modes and their effects to prevent design-related CCF	5	5
5	**Competence/ training**	5	5
6	**Environment**		
6.1	Prevention of contamination and EMC against CCF	25	25
6.2	Other influences (temperature, shock, vibration, humidity, etc.)	10	10
	Total	100	65
The total score is ≥ 65: the implemented measures allow the joystick to meet the requirements			

5.5.6 Conclusion

<table>
<tr><th colspan="4">SRP/CSb summary</th></tr>
<tr><th>Data</th><th colspan="2">Requirements</th><th>Results</th></tr>
<tr><td rowspan="8">Requirements for PLc with Category 2 use</td><td colspan="2">Compliance with CAT B requirements</td><td>OK</td></tr>
<tr><td>10 years ≤ $MTTF_d$≤ 100 years (so $MTTF_d$≥ "Medium")</td><td>30 years ≤ $MTTF_d$≤ 100 years (so $MTTF_d$ = "High")</td><td>$MTTF_d$ channel = 100 years
$MTTF_d$ High</td></tr>
<tr><td>DC_{avg} ≥ 60%
(so DC_{avg}≥ "Low")</td><td>DC_{avg}≥ 90%
(i.e. DC_{avg}≥ "Medium")</td><td>DC_{avg} = 84%
Medium DC_{avg}</td></tr>
<tr><td colspan="2">Score ≥ 65</td><td>Score = 65</td></tr>
<tr><td colspan="2">Proven safety components and principles
Single defect = safe state</td><td>OK</td></tr>
<tr><td colspan="2">Tests: if possible, as soon as or before next stress</td><td>Tests at each stress</td></tr>
<tr><td colspan="2">If defect detected: Drive in safe state (off) or danger warning</td><td>If a defect is detected:
Safe state = return to neutral and/or shutdown (see safety functions)</td></tr>
<tr><td colspan="2"> 
</td><td>Category 2</td></tr>
<tr><td colspan="3">Conclusion: Is PL "c" attained?</td><td>YES</td></tr>
</table>

5.6 Design of the SRP/CSc (Output)

5.6.1 Specification of the SRP/CSc

SRP/CSc "Output" Specification	
Name	SRP/CSc "Output"
Activation requirements	Always active
Interface	Input: Signal from the microcontroller Output: Emission of a message on the CAN Bus
Means of interconnection	Copper routing
Description	See the functional description of the "Output" part
Priority	N/A
Maximum reaction time	100ns
Function demand rate	Permanently
Environmental conditions	The joystick is functional between -20°C and +65°C The joystick is functional when the supply voltage remains within a range from 6.5V to 36V The joystick complies with the IPx7 standard

5.6.2 Functional Blocks

Functional block	**Component type**
Surv_over3V_CAN1_PLall	Resistor Analog IC CMOS comparator Ceramic capacitor
VCC_CAN1_PLall	Transistor Resistor Analog IC Ceramic capacitor
CONN_PLall	Connector
CAN1_PLall	Inductor Ceramic capacitor Analog IC Transceiver Varistor

5.6.3 Specifying diagnostics and determining the DC

Function block	Planned diagnosis (based on Annex E of ISO13849, and IEC61508-2)	DC of each component (according to Annex E of ISO 13849, and 61508-2)
Surv_over3V_CAN1_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
VCC_CAN1_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
CONN_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%
CAN1_PLall	Table A14 (IEC 61508-2) Final elements (actuators) Testframe	High DC = 99%

5.6.4 $MTTF_d$ Functional Blocks

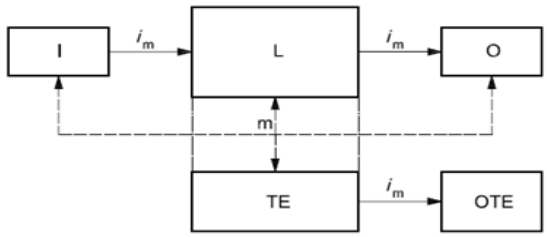
The calculation of the $MTTF_d$ of each component is performed by applying reliability calculation benchmarks such as the SN29500.

Function block	$MTTF_d$ (years)	PFH_d
Surv_over3V_CAN1_PLall	58171	1.96E-09
VCC_CAN1_PLall	58171	1.96E-09
CONN_PLall	30137	3.79E-09
CAN1_PLall	30137	3.79E-09
Total (SRP/CSc)	**42 332**	**2.34E-08**

5.6.5 Planned actions against CCFs and rating

N°	Rating of the measures against CCF (Annex F- informative of ISO 13849)		
1	**Separation/ isolation**	Max	JS
	Physical separation between signal channels	15	0
2	**Diversity**		
	Different design/technologies or physical principles are used	20	0
3	**Design/ application/ experience**		
3.1	Protection against overvoltage, overpressure, overcurrent, overheating, etc.	15	15
3.2	Use of proven components	5	5
4	**Assessment/ analysis**		
	Analysis and consideration of failure modes and their effects to prevent design-related CCF	5	5
5	**Competence/ training**	5	5
6	**Environment**		
6.1	Prevention of contamination and EMC against CCF	25	25
6.2	Other influences (temperature, shock, vibration, humidity, etc.)	10	10
	Total	100	65
The total score is ≥ 65: the implemented measures allow the joystick to meet the requirements			

5.6.6 Conclusion

<table>
<tr><th colspan="4">SRP/CSc summary</th></tr>
<tr><th>Data</th><th colspan="2">Requirements</th><th>Results</th></tr>
<tr><td rowspan="8">Requirements for PLc with Category 2 use</td><td colspan="2">Compliance with CAT B requirements</td><td>OK</td></tr>
<tr><td>10 years ≤ $MTTF_d$≤ 100 years (so $MTTF_d$≥ "Medium")</td><td>30 years ≤ $MTTF_d$≤ 100 years (so $MTTF_d$ = "High")</td><td>$MTTF_d$ channel = 100 years
$MTTF_d$ High</td></tr>
<tr><td>DC_{avg} ≥ 60%
(so DC_{avg}≥ "Low")</td><td>DC_{avg}≥ 90%
(i.e. DC_{avg}≥ "Medium")</td><td>DC_{avg} = 99%
Medium DC_{avg}</td></tr>
<tr><td colspan="2">Score ≥ 65</td><td>Score = 65</td></tr>
<tr><td colspan="2">Proven safety components and principles
Single defect = safe state</td><td>OK</td></tr>
<tr><td colspan="2">Tests: if possible, as soon as or before next stress</td><td>Tests at each stress</td></tr>
<tr><td colspan="2">If defect detected: Drive in safe state (off) or danger warning</td><td>If a defect is detected:
Safe state = return to neutral and/or shutdown (see safety functions)</td></tr>
<tr><td colspan="2"> 
</td><td>Category 2</td></tr>
<tr><td colspan="3">Conclusion: Is PL "c" attained?</td><td>YES</td></tr>
</table>

5.7 FMEA

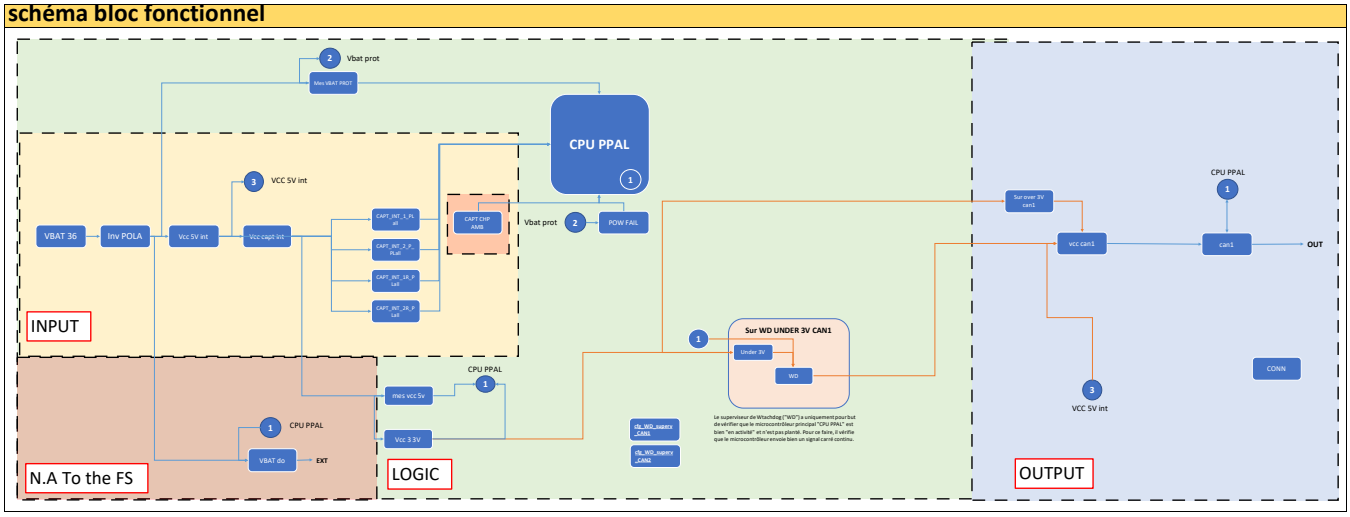
The design FMEA was established to guarantee the quality of the development process of the electronic database 4THE5-41CAN.
Please refer to the FMEA T112 CAN cover page for more information.

5.8 Outcomes for the safety functions of the command system

The PL for each SRP/CS has been determined according to the architecture and operation of the system.
The overall PL of the safety function of the command system is determined using Table 11 of ISO 13849-1 2015

- FS1 "In case an axis defect is detected, a "position to neutral" instruction is transmitted on the faulty axis"

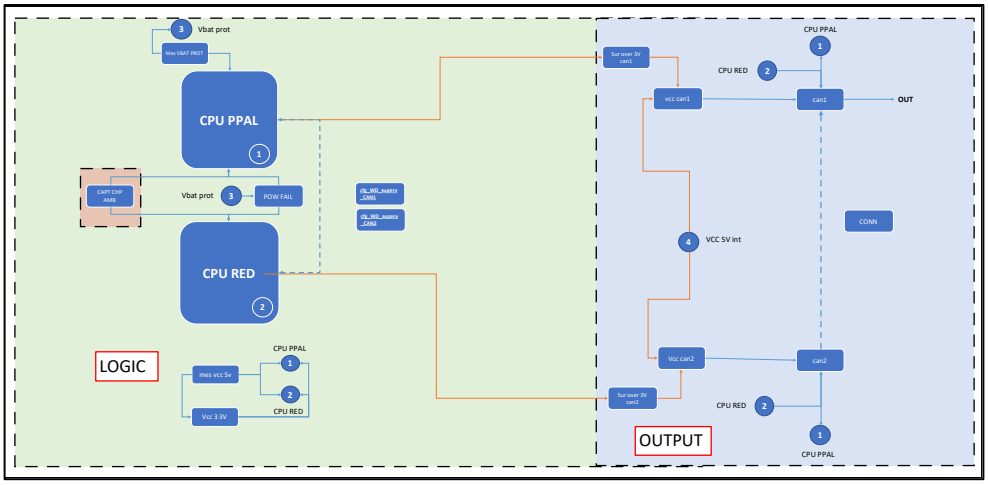
For this safety function, the combination of SRP/CS is shown in the figure below:



SRP/CS	MTTF$_d$ (years)		DC (%)		CCF	Category	PL
Input	4 467	High	86	Low	65	2	c
Logic	60 266	High	84	Low	65	2	c
Output	42 332	High	99	High	65	2	d

- FS2 " In case an internal defect is detected on the microcontroller, transmission of the neutral position instruction on all axes and emission of an error code”

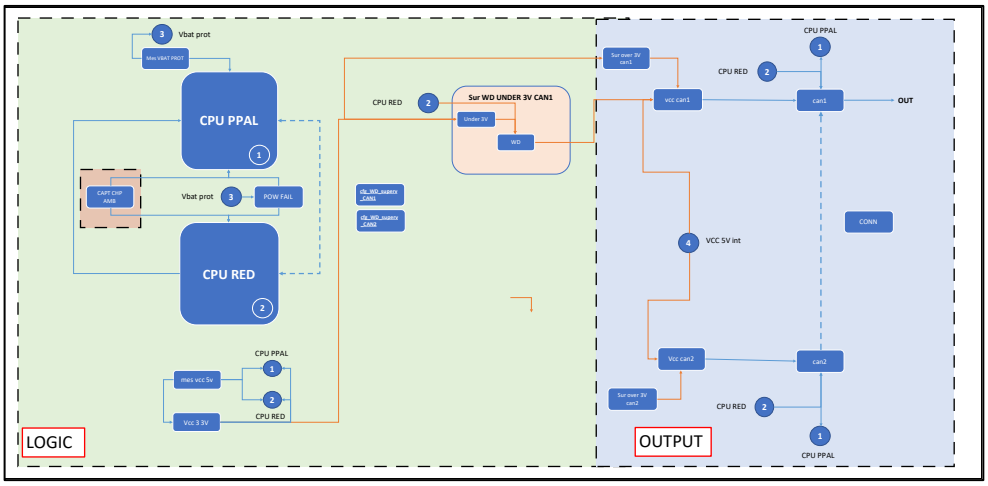
For this safety function, the combination of SRP/CS is shown in the figure below:



SRP/CS	MTTFd (years)		DC (%)		CCF	Category	PL
Logic	4 467	High	86	Low	65	2	c
Output	60 266	High	84	Low	65	2	c

- FS3 " In case the watchdog supervisor detects a defect on the microcontroller, the CAN output is cut off "

For this safety function, the combination of SRP/CS is shown in the figure below:



SRP/CS	MTTFd (years)		DC (%)		CCF	Category	PL
Logic	**4 467**	**High**	**86**	**Low**	**65**	**2**	**c**
Output	60 266	High	84	Low	65	2	c

5.10 Conclusion

	$MTTF_d$ (years)		**DC (%)**		**CCF**	**PL**	**PLr**
FS1	3787	High	94	Medium	65	c	c
FS2	27085	High	92	Medium	65	c	c
FS3	24866	High	93	Medium	65	**c**	**c**

Bosch Rexroth AG
BP 101
91, bd Irène Joliot-Curie
69634 Vénissieux Cedex
France
Tel. +33 47878 5252
www.boschrexroth.com

Subject to change
RE 29696-02-B/2021-06-22