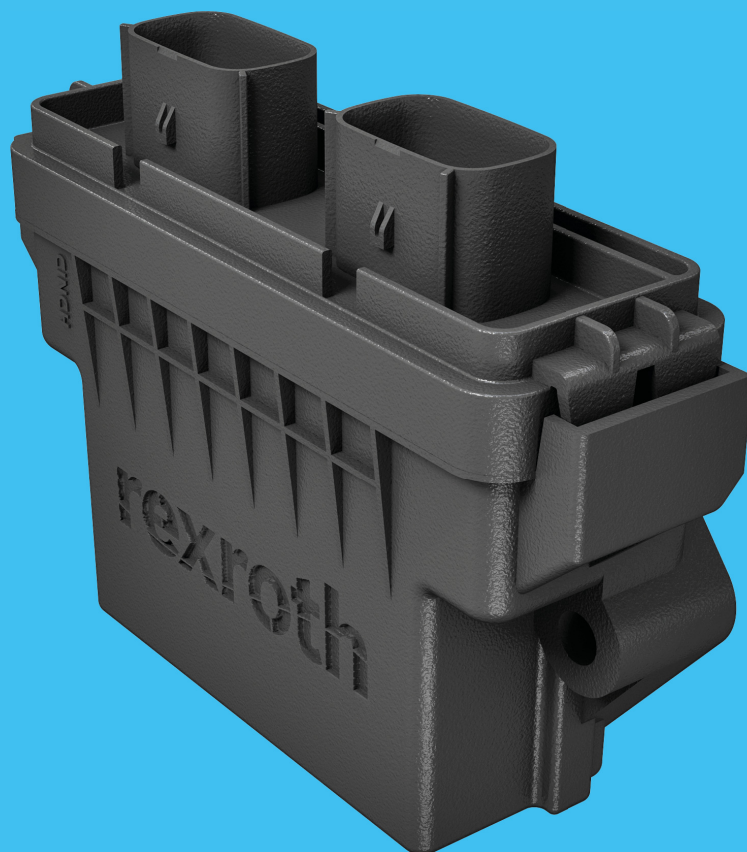


Safety-relevant project planning  
instruction according to  
EN ISO 13849-1:2015

# CHC Controller



Bosch Rexroth Oil Control 2021. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights. The data specified within only serves to describe the product. No statements concerning a certain condition or suitability for a certain application can be derived from our information. The information given does not release the user from the obligation of own judgment and verification. It must be remembered that our products are subject to a natural process of wear and aging.

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

<b>1</b>	<b>Aim and application.....</b>	<b>4</b>
<b>2</b>	<b>Other applicable documents .....</b>	<b>5</b>
<b>3</b>	<b>Abbreviations and definitions.....</b>	<b>5</b>
3.1	Abbreviations .....	5
3.2	Definitions.....	6
<b>4</b>	<b>Operating conditions .....</b>	<b>7</b>
4.1	General operating conditions .....	7
4.2	Temperature profile of the control unit.....	8
4.3	Lifetime .....	8
4.4	Flash/erase cycles .....	8
4.5	Temperature monitoring .....	9
<b>5</b>	<b>Safety-related functions.....</b>	<b>9</b>
5.1	Safety function and safe state .....	9
5.2	System architecture .....	10
<b>6</b>	<b>Safety-related software and software toolchain.....</b>	<b>11</b>
6.1	Data storage in internal data flash .....	11
<b>7</b>	<b>Power supply concept .....</b>	<b>12</b>
<b>8</b>	<b>Safety-related inputs.....</b>	<b>13</b>
8.1	Analog inputs .....	13
<b>9</b>	<b>CAN interface.....</b>	<b>14</b>
<b>10</b>	<b>Safety-related outputs – power outputs in safe output configuration .....</b>	<b>15</b>
10.1	Short circuit to ground .....	15
<b>11</b>	<b>Failure detection possibilities .....</b>	<b>16</b>
11.1	Failure detection capability of different safe output configurations .....	17
<b>12</b>	<b>Reliability parameters.....</b>	<b>18</b>
12.1	Reliability parameters of the safety function “system integrity”.....	18
12.2	Reliability parameters for the CHC .....	18
12.3	Examples of using the reliability parameters .....	19
12.3.1	Example 1: safe current control.....	19
12.3.2	Example 2: safe current control.....	20
<b>13</b>	<b>Using a service tool .....</b>	<b>21</b>

# 1 Aim and application

The CHC12-1/20 control is a control unit with flexible configuration possibilities that are able to support safety functions up to PL d according to EN ISO 13849-1:2015.

This document contains descriptions of the CHC functional safety characteristics and instructions on using the control units for safety-related applications. It can be used as a guideline for the planning of safety related machine system projects.

If not indicated otherwise, the instruction applies for EN ISO 13849-1. Measures that concern only EN ISO 13849-1 are explicitly indicated accordingly.




The information in this document does not cover how to design, install or operate a complete machine, nor does it cover all peripheral equipment that can influence the safety of the complete machine system. The complete system shall be designed and installed in accordance with the safety requirements set forth in the standards and regulations of the country where the machine is operated.

The machine manufacturers that use and configure the CHC control units in the machine systems are responsible for ensuring that the applicable safety laws and regulations in the country concerned are observed and that any significant hazards in the complete machine system application are eliminated. The information in this document will not result in any liability of Bosch Rexroth for a machine that is equipped with the CHC control units.

The configuration of the CHC control units and the integration into the machine safety system shall only be carried out by trained and experienced specialists who have sufficient knowledge of electronic hardware, software programming and functional safety.

This document contains important safety information. It is essential that all relevant instructions and guidance provided in this document are observed, understood and followed by machine manufacturers and machine operators. If necessary, machine manufacturers shall convey relevant safety information mentioned in this document into a more appropriate form such as an operating manual.

Special attention shall be paid to text associated with following symbols.

 <b>DANGER</b>	This indicates a hazardous situation which, if not avoided, death or serious injury could be expected.
 <b>WARNING</b>	This indicate a situation which, if not avoided, damage to the controller could be expected.
 <b>NOTICE</b>	This stands for additional information, which is important to understand the controller and its functionalities functionalities.

## 2 Other applicable documents

Reference	Document	Content
[1]	RE18324-41	CHC Instruction Manual
[2]	RE18324-40	CHC 12-1/20 Datasheet

## 3 Abbreviations and definitions

### 3.1 Abbreviations

Abbreviation	Meaning
ADC	Analogue digital converter
AI	Analog voltage input
AIC	Analog current input
API	Application programming interface
ASW	Application software
BSW	Basic software
CAN	Controller area network
CLCC	Closed loop current control
CRC	Cyclic redundancy check
DC	Diagnostic coverage
DI	Digital voltage input
D-Flash	Data flash
DO	Digital output
ECC	Error correcting code
ECU	Electronic control unit
FMEDA	Failure modes, effects and diagnostic analysis
FRT	Fault response time
HW	Hardware
HS	High-side
LS	Low-side
MTTFD	Mean time to dangerous failure
N.A.	Not applicable
PL	Performance level
POD	Proportional output used as digital output
PWM	Pulse width modulation
P-Flash	Program flash
SENT	Single edge nibble transmission
SRL	Software requirements level
SPI	Serial peripheral interface
SW	Software

3.2 Definitions

Application software	Application specific user software running on the control unit.										
Basic software	Firmware including HW specific SW drivers and real time operating system.										
Current measurement	A method of the power output current feedback. The current is measured via a shunt and sent directly back to the $\mu$ C. This method provides a high accuracy of the current feedback. Details of current feedback attribute of each power output can be found in [2].										
Current sensing	A method of the power output current feedback. The current is measured via a shunt, and then relayed through the power stage controller to the $\mu$ C. The measurement accuracy of this method is lower than the current measurement method. Details of current feedback attribute of each power output can be found in [2].										
Diagnostic coverage	Measure of the effectiveness of diagnostics, which may be determined as the ratio between the failure rate of detected dangerous failures and the failure rate of total dangerous failures.										
<div> DC according to EN ISO 13849-1, Table 5 </div> <table> <tr> <th>Denotation</th><th>Range</th></tr> <tr> <td>None</td><td>DC &lt; 60%</td></tr> <tr> <td>Low</td><td>60% <math>\leq</math> DC &lt; 90%</td></tr> <tr> <td>Medium</td><td>90% <math>\leq</math> DC &lt; 99%</td></tr> <tr> <td>High</td><td>99% <math>\leq</math> DC</td></tr> </table>		Denotation	Range	None	DC < 60%	Low	60% $\leq$ DC < 90%	Medium	90% $\leq$ DC < 99%	High	99% $\leq$ DC
Denotation	Range										
None	DC < 60%										
Low	60% $\leq$ DC < 90%										
Medium	90% $\leq$ DC < 99%										
High	99% $\leq$ DC										
Functional safety	Part of the overall safety of the machine that depends on the correct function of the control unit and on other installations and measures for minimizing risks.										
Heat dissipation	Possibility / capability to dissipate heat energy by conduction, convection and/or heat radiation.										
Ignition phase	Time from which the control unit is activated (e.g. by the ignition signal or CAN wake-up) until the control unit is deactivated after the ignition is switched off and the after-run functions have been completed.										
Machine	Whole system with all hydraulic and electronic partial components, including the control unit.										
Mean time to dangerous failure	<div>Average value of the expected time to a dangerous failure.</div> <div> MTTF<sub>D</sub> according to EN ISO 13849-1, Table 4 <table> <tr> <td>Low</td><td>3 years <math>\leq</math> MTTF<sub>D</sub> &lt; 10 years</td></tr> <tr> <td>Medium</td><td>10 years <math>\leq</math> MTTF<sub>D</sub> &lt; 30 years</td></tr> <tr> <td>High</td><td>30 years <math>\leq</math> MTTF<sub>D</sub> &lt; 100 years*</td></tr> </table> </div> <div>* limitation of the MTTF<sub>D</sub> for each channel to 100 years is only required by EN ISO 13849.</div>	Low	3 years $\leq$ MTTF <sub>D</sub> < 10 years	Medium	10 years $\leq$ MTTF <sub>D</sub> < 30 years	High	30 years $\leq$ MTTF <sub>D</sub> < 100 years*				
Low	3 years $\leq$ MTTF <sub>D</sub> < 10 years										
Medium	10 years $\leq$ MTTF <sub>D</sub> < 30 years										
High	30 years $\leq$ MTTF <sub>D</sub> < 100 years*										
Operating system	Part of the basic software in the control unit. Its task is to offer a supervisor for the application software, to constitute an interface for the inputs and outputs and for the hardware monitoring software sections. The API function set is the interface between the application software and the operating system.										
Redundancy	Redundancy denotes the presence of an additional functional equivalent or comparable resource of a technical system. This kind of design in a safety function can be used to realize fail-safe and allows error detection through plausibility check between different channels.										
Total service life	Time from delivery to decommissioning of the machine.										

## 4 Operating conditions

### **DANGER**

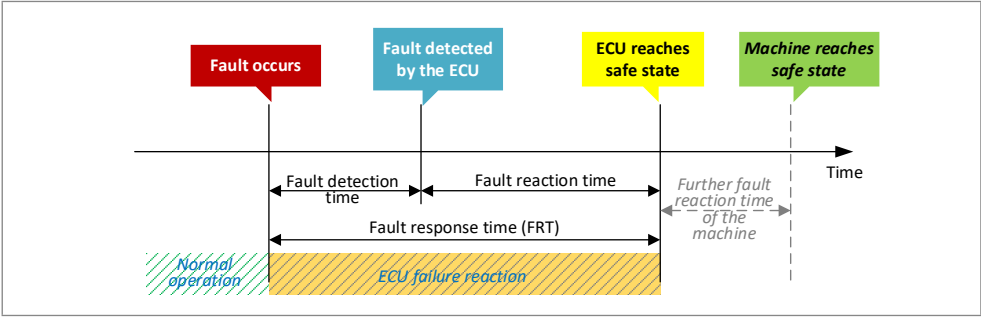
Using the CHC control unit outside the specified boundary conditions or without following the instructions may result in danger to life and/or cause damage to components which could result in consequential damage to the complete system.

The general technical data and instructions regarding transport, storage, installation, wiring and circuitry, as well as operation of the CHC control units are given in [2]. The control units shall only be used within the specified operating conditions and following the given instructions. To use the control units in safety-related applications, some special conditions and instructions that are summarized in this chapter shall be rigidly observed and followed.

### 4.1 General operating conditions

The following operating conditions for the control unit CHC shall be fulfilled for safety-related applications:


- The control units are designed mainly to be used in mobile machine applications. Please consult Bosch Rexroth for the suitability of the control units for other applications.
- The CHC safe state is defined as “power outputs switched off” (details see chapter 10 “Safety-related outputs – power outputs in safe output configuration”). The control unit shall not be used if its safe state cannot support the safe state of the machine safety functions.
- The control units are to be used in applications for intermittent (i.e. not uninterrupted) operations. The maximum uninterrupted operating time is defined as 24 h, i.e. the control unit shall be switched off or reset at least once within 24 h.
- The fault response times are listed in chapter 11 “Failure detection possibilities”. The response time of the “external stop switch” safety function is listed in chapter 5.1 “Safety function and safe state”. The control unit shall not be used if the response time is determined to be insufficient for the machine safety functions. An illustration of the fault response time is given in Fig. 1.
- According to EN ISO 13849-1, for category 2, the test rate should be greater or equal to 100 times of the safety function demand rate. The diagnostic test intervals of the control units can be found in chapter 11 “Failure detection possibilities” (test interval = 1 / test rate). The control unit shall not be used if the test rate is determined to be insufficient for the machine safety functions.
- An efficient field observation process shall be established by the machine manufacturers. Any field failures involving the CHC should be immediately notified to Bosch Rexroth, even if it is not covered by warranty.



**Fig. 1: Illustration of fault detection and fault reaction time**

4.2 Temperature profile of the control unit

The temperature profile and the temperature fluctuation profile that the control unit is subject to have influences on the aging of components.


**DANGER**

CHC control units shall not be used if its temperature and temperature fluctuation profiles do not meet the requirements of the machine applications.

Wisely selected installation location of the control unit will help to reduce the control unit ambient temperature and temperature fluctuations. It is recommended to install the CHC control units as follows:

- Installation at a large cooling area with good heat conductance.
- Installation at a place with good air convection for heat dissipation

4.3 Lifetime

The CHC control unit is designed for a lifetime as shown in the following Table 1:

**Table 1: and lifetime**

Temperature (as per datasheet)	
Storage time	5 years
Service lifetime	20 years operation / 10 000 operating hours, whichever occurs first

Beyond the given lifetime, failure probabilities may increase and the reliability parameters given in chapter 12 “Reliability parameters” cannot be guaranteed. ASW shall therefore control the elapsed operating hours regularly by querying the information from the BSW and inform the machine operator accordingly.

Please contact Bosch Rexroth if a prolonged operating time is required.

4.4 Flash/erase cycles

The microcontroller manufacturer guarantees a maximum number of flash/erase cycles for the program flash of 1000 cycles. For the CHC control units that are to be used for a machine in series production, it is safe to assume that this maximum flash/erase cycles will never be reached.



However, for control units that are used for development and testing purpose (referred to as “development control units”), this maximum flash/erase cycles may be exceeded, and failures may occur. For this reason, development control units shall be marked as such and shall not be used for original series production nor as spare parts.

## 4.5 Temperature monitoring

The control unit monitors periodically the temperature inside the housing. ASW must detect this value to prevent the emergency stop by the BSW.

If the temperature reaches the limit of 120°C internally, all power outputs will be switched off by the BSW to prevent unwanted behavior or concealed damage of the control unit. Reactivation of the power outputs is only possible when the temperature falls below 110 °C.

# 5 Safety-related functions

## 5.1 Safety function and safe state

CHC has safety functions that can be used by the machine manufacturers to support the machine safety functions.

### **Safety function: system integrity**

CHC is designed as universal ECU, where the applications are to be defined by the machine manufacturers and implemented via the application software.

In order to support the broad variety of applications as well as to cover the typical use cases, the safety function is defined as the system integrity, i.e. as demanded by the application software, the control unit shall

- read the safety-related inputs (see chapter 8 “Safety-related inputs”) and messages (see chapter 9 “CAN interfaces”) correctly,
- process the safety-related inputs (see chapter 8 “Safety-related inputs”) and messages (see chapter 9 “CAN interfaces”) correctly, and
- control the corresponding safety-related outputs (see chapter 10 “Safety-related outputs – power outputs in safe output configuration”) without failure.

Depending on the safe output configurations (see chapter 10 “Safety-related outputs power outputs in safe output configuration”), the correct control of the safety-related outputs can be concretized as

- safe current control: the current flow through the actuators shall be set according to ASW demands without failure (including the switch-off command)
- safe deactivation of the actuators: the actuators shall be switched off without failure when demanded by the ASW
- prevention from unintended actuation: actuators shall not be switched on when not demanded by the ASW
- safe switching of the actuators: actuators connected to the switchable power outputs shall be actuated according to ASW demands without failure

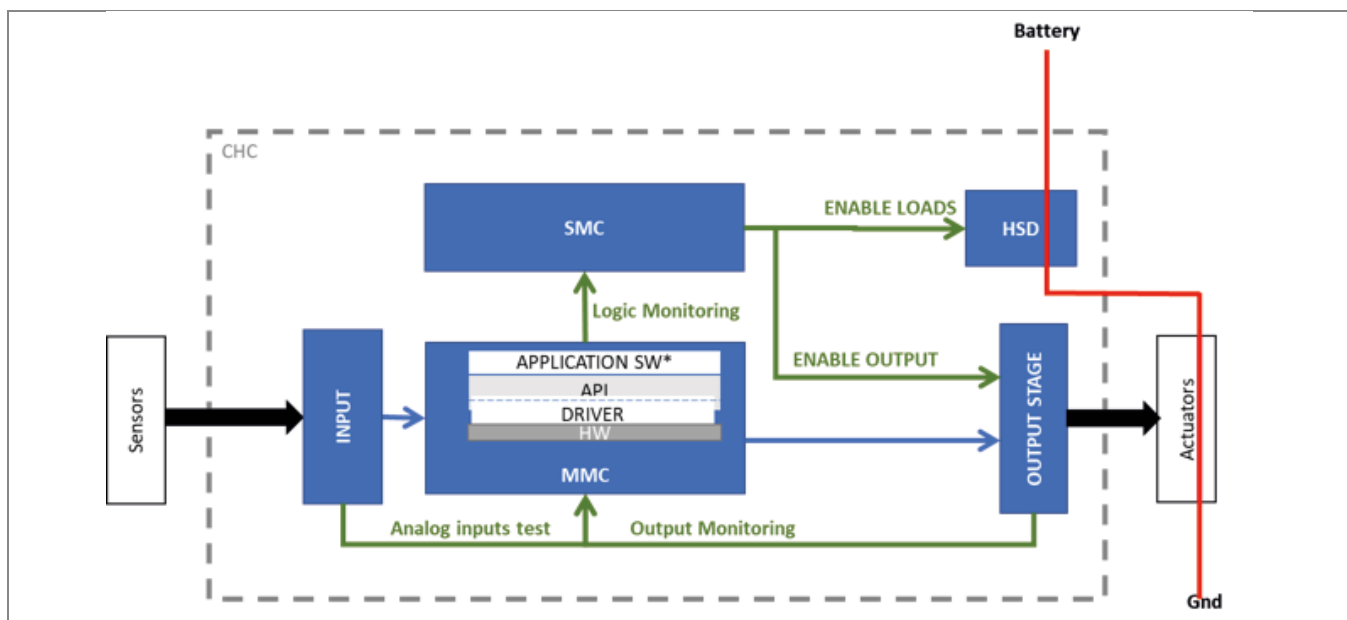
Safe state : correct setting of the safety-related outputs OR all affected safety-related outputs are switched off (details see chapter 11 “Failure detection possibilities”)

## NOTICE

CHC control units are only suitable for supporting fail-safe systems.  
All failures that lead to de-energization of the power outputs are considered as safe failures.

### 5.2 System architecture

The design of the CHC control units adopts the module-based approach. The function groups with safety-related modules of the control unit are illustrated in the following Fig. 2.



**Fig. 2: CHC safety-related modules**

## 6 Safety-related software and software toolchain

The basic software fulfils the requirements of EN ISO 13849-1 up to PL d,

To use the CHC control units for a machine safety function of certain PL, it is the machine manufacturer's responsibility to check if the CHC basic software is able to support the required PL of machine safety functions, and to make sure that the ASW is developed according to the required PL.

The ASW developers shall configure the CHC BSW according to their applications. The configured BSW is then compiled and delivered by the tool in the form of object and header files for download. With the configured, compiled and then downloaded BSW, the ASW is to be developed offline.

If the application software is to be created in C programming language, the ASW developers shall use the same development tools (assembler, compiler, linker) of the same version as those used to create the BSW (the tools and versions are given in [1]).

The toolchain used for the BSW development as well as the software tools provided for the ASW development fulfils the requirement of the EN ISO 13849 to the required level.



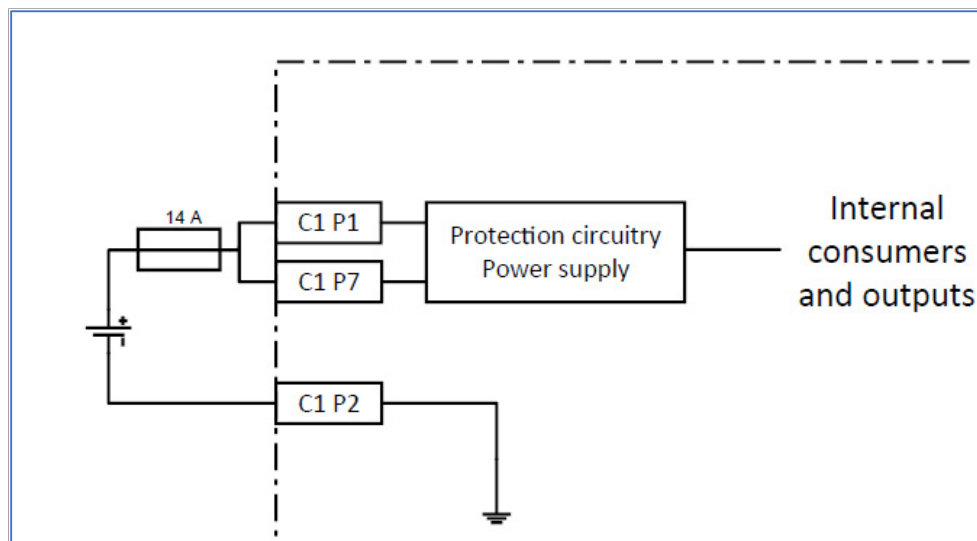
If the wrong tool or the wrong version of the tool is used, the functional safety of the CHC control may not be guaranteed.

### 6.1 Data storage in internal data flash

At power-on, CHC BSW performs a CRC on each block in the data flash in addition to the EEPROM. Failures detected by the CRC will be saved by the BSW. CHC BSW tries again the CRC on block, if the error is present, the CHC goes in SAFOUT mode.

ASW receives a message about the SAFOUT mode and can send on CANbus.

## 7 Power supply concept



**Fig. 3: CHC power supply concept**

The CHC control units monitor periodically the battery voltage, their internal voltages, the sensor supply voltages and take corresponding actions to ensure the functional safety. The various voltages can also be read by the ASW via API functions.

The CHC control units can be used in 12 V or 24 V battery networks within a voltage range for normal operation mode from 9 V to 32 V. Since an allowable supply voltage for 24 V battery network (e.g. 30 V) would be hazardous for a 12 V battery network, it is therefore suggested for the machine manufacturers to define valid voltage supply ranges for their applications and to implement corresponding diagnostic methods in the ASW. Behaviors of the CHC control units regarding supply voltages are given in [2], which could be taken as a reference.

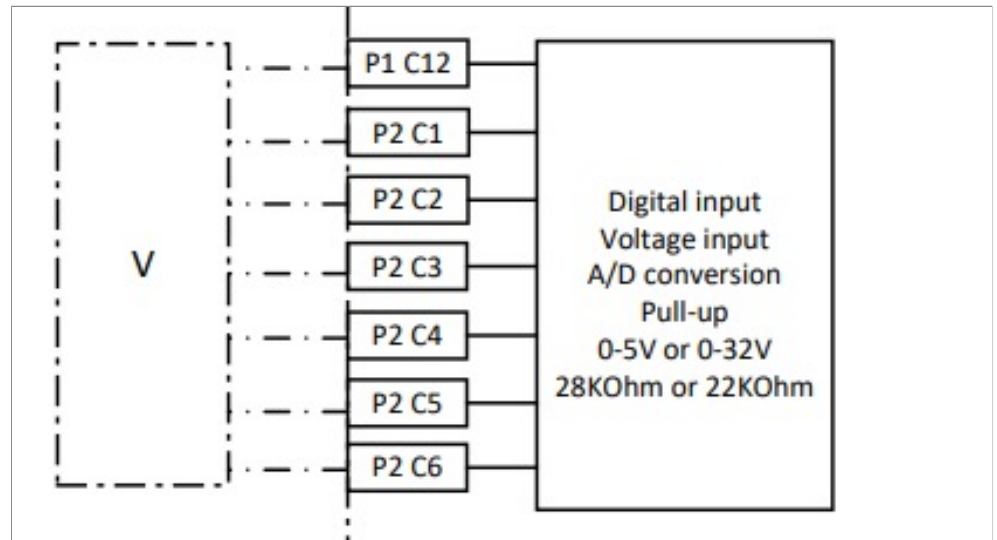
### NOTICE

The measurement of the battery voltage in the control unit has a tolerance of  $\pm 0.5\%$  referred to 32 V. This uncertainty shall to be considered by the ASW monitoring function.

## 8 Safety-related inputs

The CHC control units provide 6 analogue inputs that can be used to read analogue values (refer to [2]). This chapter contains instructions for using the control unit inputs for safety-related applications.

### 8.1 Analog inputs



**Fig. 4: Analog inputs**

The control units CHC provides 6 discrete analogue inputs, where all the signals are fed, after filtering, directly to the ADCs of the  $\mu$ C.

Due to its limited accuracy, it is not suggested to use 32 V-discrete analogue inputs to read analogue sensor signals (0.5-4.5V) with high accuracy requirements. With the thresholds defined by the ASW, these inputs can be used as digital inputs to read for example the state of a switch.

If ASW implements a proper comparison of the two input signals, failures in the input processing circuitry external to and internal of the control unit can be detected with high reliability.

CHC HW and BSW are developed to allow to use redundant sensors in all inputs without restrictions. The comparison of two independent signals could be detected by implementing a signal range check in ASW

Each analog input must be set in the appropriate in ASW: Voltage range: 5V or 32V.

### **DANGER**

Restricted by its limited accuracy, using 32 V-discrete analogue inputs for reading of analogue sensor signals with high accuracy requirements may result in danger to life and/or properties.

Depending on the sensor characteristics, the valid signal reading could be limited to a certain part of the sensor's electrical range.

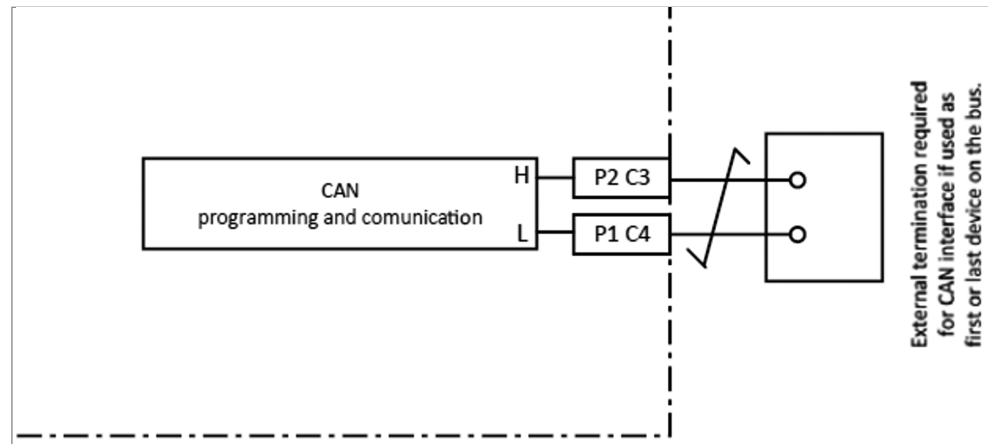
BSW detects the following failures:

- Short circuit to ground
- Short circuit to power supply
- Open circuit

The signal range check can be realized by the ASW. Once implemented correctly, DC of 60% could be achieved by this signal range check method, given the test frequency is 100 times of the demanding rate of the machine safety function.

## 9 CAN interface

The CHC control units provide one CAN-interface (see fig.5).



**Fig. 5: CAN bus pins**

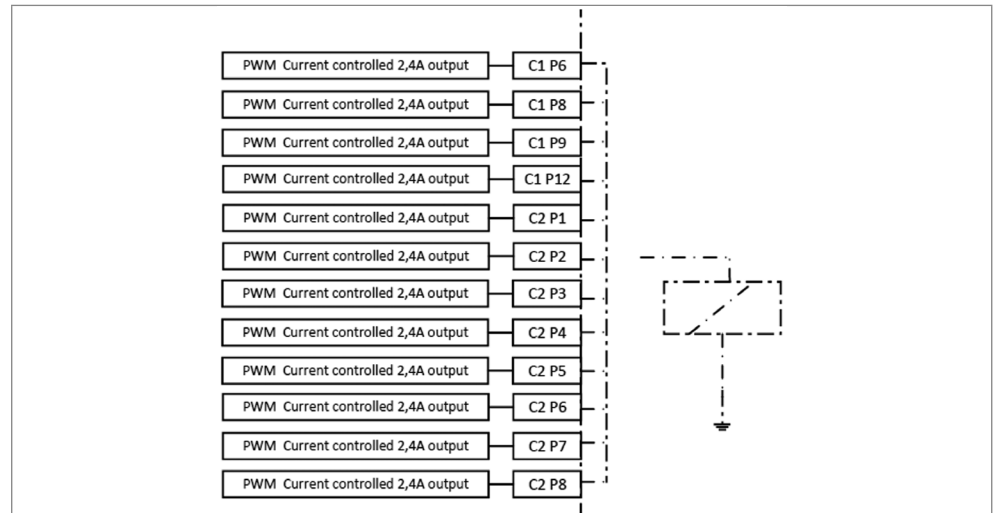
The CAN communication provided by the CHC control units conforms to CAN 2.0 as specified in ISO 11898-1, with all the required safety measures implemented in the data link layer. As a result, the worst case residual error probability for a channel is  $R(P\_CAN)=7 \cdot 10^{-9} \approx 1 \cdot 10^{-8}$ .

To use the CAN interface for safety-related communications, it is machine manufacturer's responsibility that the safety communication layer is implemented as required by the corresponding standards. ASW must be programmed, verified and tested to be conformed with customer requested standard.

For the conformity with EN ISO 13849-1, all relevant requirements of EN 61784-3 shall be fulfilled by the communication channel.

## 10 Safety-related outputs – power outputs in safe output configuration

All the outputs provided by the CHC control units are allowed to be used for safety-related applications. Detailed description of functions and characteristics of the power outputs can be found in [2].



**Fig. 6: Control concept of power outputs**

CHC uses only high-side outputs. For each output is available on ASW the voltage and current on the output.

BSW detects and reacts with API message to be manage by ASW, the following failures:

- Short circuit to power supply
- Open circuit.

### 10.1 Short circuit to ground

Short circuit to ground failure must be detected by ASW using the voltage measure: if the output is not driven, the voltage on the output must be equal to ground, if different a short circuit to ground is detected! If requested by functional safety function, ASW must be designed to react to short circuit to ground failure in according with machine system.

## **! DANGER**

For safety-related applications, the voltage on outputs must be detected and managed if different to GND.

## **! WARNING**

It shall be ensured that the accumulated current of the multiple power outputs does not exceed the maximum current limit of the single power output (for details see [2]).

# 11 Failure detection possibilities

In order to ensure the safety integrity, the CHC control units are equipped with various diagnostic methods that monitor the hardware and the execution of the software. These diagnostic methods as well as the corresponding failure reactions are summarized in the following Table 2.

**Table 2: CHC diagnostic methods and failure reactions**

Diagnostic method	Reaction	Worst case diagnostic test interval [ms]	Worst case FRT [ms]
<b>Power-on test</b>			
Switch-off capability of the watchdog	Disabling of the power outputs	Every time at power-on	–
Switch-off capability of the power monitoring circuits	Disabling of the power outputs	Every time at power-on	–
CRC check of each block in the D-Flash	Failure message on ASW	Every time at power-on	–
CRC check of the ASW blocks in the P-Flash	Prevention of the ASW start-up	At power-on if a ECC error is recorded in the last operation cycle	–
<b>Runtime µC and memory test</b>			
µC build-in self-tests: – Peripheral core monitoring – RAM ECC – P-Flash, EEPROM ECC – Prevention from unauthorized RAM access – Memory addressing error monitoring – Internal bus error monitoring– Clock error monitoring – Core temperature monitoring – Core voltage monitoring	SW reset	Neglectable	< 200
RAM & stack pattern test	Switching-off of all power outputs + SW reset	40	2000
CRC of the hardware monitoring modules in the P-Flash	Switching-off of all power outputs + SW reset	10	5000
<b>Program execution monitoring</b>			
Temporal monitoring of the program execution with internal watchdog	SW reset	Same as the task time	200
Temporal and logical monitoring of the program execution of the BSW hardware monitoring modules with external windowed-watchdog	Switching-off of all power outputs + SW Reset	33	200
<b>ADC test</b>			
ADC tests	Switching-off of all power outputs	20	160



**Table 2: CHC diagnostic methods and failure reactions**

Diagnostic method	Reaction	Worst case diagnostic test interval [ms]	Worst case FRT [ms]
<b>Runtime voltage monitoring</b>			
Monitoring of internal power supply – Over-voltage – Under-voltage	Switching-off of all power outputs	10	120
Over-voltage monitoring of the control unit power supply – over 36 V for 1000 ms – over 32 V for 300 000 ms	Switching-off of all power outputs	10	1000 (over 36 V) 300000 (over 32 V)
Monitoring of sensor power supply – Over-voltage – Under-voltage	Switching off of the erroneous sensor power supply	10	80
<b>Runtime temperature monitoring</b>			
Over-temperature monitoring	Switching-off of all power outputs	10	120
<b>Runtime output failure detection</b>			
See chapter 11.1 “Failure detection capability of different safe output configurations”.			
<b>External switch function failure detection</b>			
Monitoring of the external switch status	Switching-off of all power outputs	10	11

### 11.1 Failure detection capability of different safe output configurations

The output status of the power outputs are monitored periodically by following methods:

- Diagnostic methods implemented by the output control devices
- Current feedback (current measure or current sensing) of proportional High-sides
- High-side current comparison to detect HS current deviations

In addition, the API is provided to be used by ASW to monitor the close-loop current control.

Upon failure detection, all power outputs belonging to the same safe output configuration will be switched off.

“Reliability parameters of the safety function “system integrity”” on par. 12 are only valid under following conditions:

- CLCC deviation monitoring is used by the ASW with proper configured maximal deviations, which shall correspond to the dangerous current deviation for the application, and the ASW monitors the related error message and reacts to it by bringing the machine into safe state, i.e. switching off the power outputs.
- A proper threshold is set for the HLCC function

If all the above pre-conditions are fulfilled, the fault response time (FRT) of all safe output configurations is less than 150 ms.

Failure detection interval of all safe output configurations is 50 ms for HLCC.

## **DANGER**

For diagnostic purpose, there are test pulses generated by the output control devices and diagnosis current of the power outputs (for details see [1], [2]). It shall be ensured that the test pulses and diagnosis current will not cause unintended actuation of the actuators.

## 12 Reliability parameters

### 12.1 Reliability parameters of the safety function “system integrity”

For safety function (system integrity), the reliability parameters MTTFD, DCavg and CCF are provide the complete controller calculation.

The full hardware has been divided in functional block (See sheet HW Blocks par. 5.2).

The controller MTTFd is provided for functional safety function in years.

MTTF of simple components are calculated using SN29500-1. For Integrated circuits, or for components which Manufacturer data is available, the Manufacturer values are used.

About DCavg and CCF values, also this value are calculated using SN29500-1.

DCavg and CCF values are supply only the controller worst cases.

### NOTICE

The reliability parameters provided are merely for CHC control units and are only valid, if the control units are used following all relevant instructions of this document.

For each individual machine safety function, it is the responsibility of the machine manufacturer to calculate the reliability parameters of the complete safety-related system (sensors, control unit, actuators) and evaluate its conformity with the relevant standards.

### 12.2 Reliability parameters for the CHC

As above explained, the tables below are the MTTFD values of the complete controller: including common components, controllers and input/output iterations.

The calculation of DCavg and CCF, are calculated by the worst case:

DCavg = 97,63%

CCF =75

Depending by CHC uses (in hours/years) the MTTFd values change.

Hour/day: 8 - Working days/year: 260			
Inputs	CAN	Outputs	MTTFd (y)
0	Y	1 pair	1614
0	Y	2 pairs	1423
0	Y	3 pairs	1272
0	Y	4 pairs	1150
0	Y	5 pairs	1050
0	y	6 pairs	966
1	N	1 pair	1626
2	N	2 pairs	1393
3	N	3 pairs	1218
4	N	4 pairs	1083
5	N	5 pairs	974
6	N	6 pairs	886
6	Y	6 pairs	867

Hour/day: 16 - Working days/year: 320			
Inputs	CAN	Outputs	MTTFd (y)
0	Y	1 pair	656
0	Y	2 pairs	578
0	Y	3 pairs	517
0	Y	4 pairs	467
0	Y	5 pairs	427
0	y	6 pairs	392
1	N	1 pair	660
2	N	2 pairs	566
3	N	3 pairs	495
4	N	4 pairs	440
5	N	5 pairs	395
6	N	6 pairs	360
6	Y	6 pairs	352

Hour/day: 24 - Working days/year: 360			
Inputs	CAN	Outputs	MTTFd (y)
0	Y	1 pair	389
0	Y	2 pairs	343
0	Y	3 pairs	306
0	Y	4 pairs	277
0	Y	5 pairs	253
0	y	6 pairs	232
1	N	1 pair	391
2	N	2 pairs	335
3	N	3 pairs	293
4	N	4 pairs	261
5	N	5 pairs	235
6	N	6 pairs	213
6	Y	6 pairs	209

## NOTICE

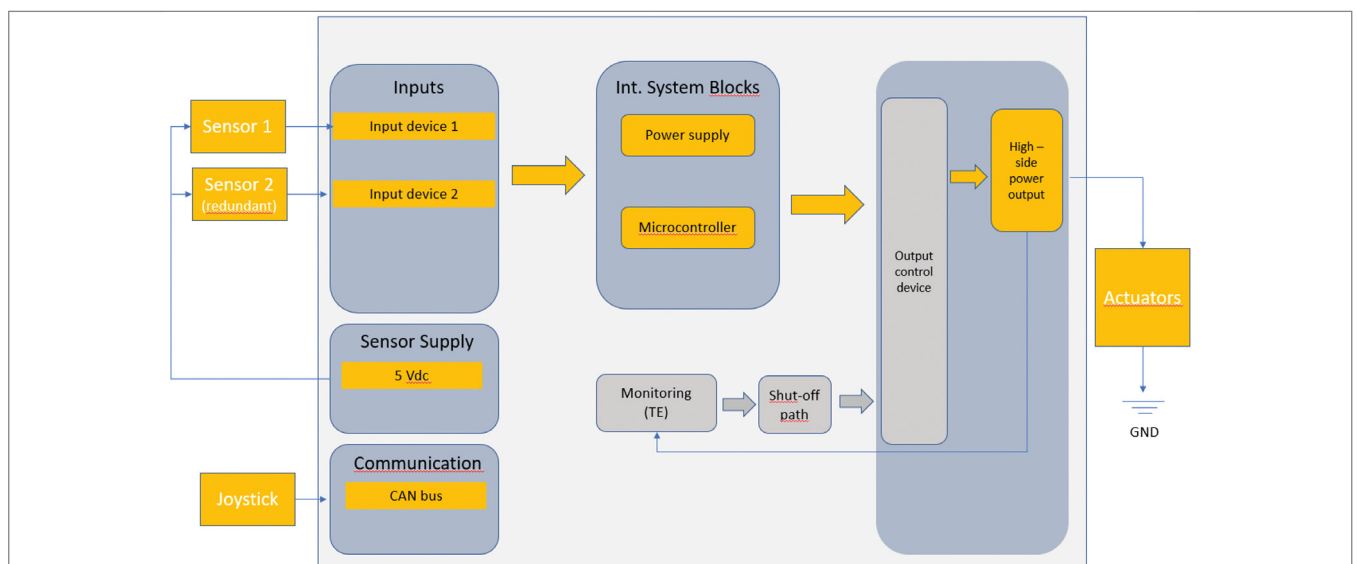
The reliability parameters provided are merely for CHC control units and are only valid, if the control units are used following all relevant instructions of this document.

For each individual machine safety function, it is the responsibility of the machine manufacturer to calculate the reliability parameters of complete safety-related system (external stop switch, control unit, actuators) and evaluate its conformity with the relevant standards.

### 12.3 Examples of using the reliability parameters

This chapter uses examples to explain how to calculate the corresponding MTTFD and DC of the control unit using the information given in tables in Par. 12.2.

#### 12.3.1 Example 1: safe current control



**Fig. 7: First example for using the reliability parameters of the safety function “system integrity”**

In this first example, CHC is wired, configured and programmed (application software) to read periodically 2 sensor (redundant value) and 1 joystick commands via CAN bus, and to control 1 actuators operating in High-side mode. CHC “system integrity” safety function ensures that all the required inputs are read and processed correctly as required by the ASW as well as the corresponding outputs are set correctly as required by the ASW.

The MTTFD, DCavg and CCF values for this system are easily determined into the tables at par.12.2 depending by machine working hours, in this example 360day/y, 24h/day.

It leads to the result that MTTFD of the main channel is 352 years and the DCavg of the control unit for this safety function is 97,63%.

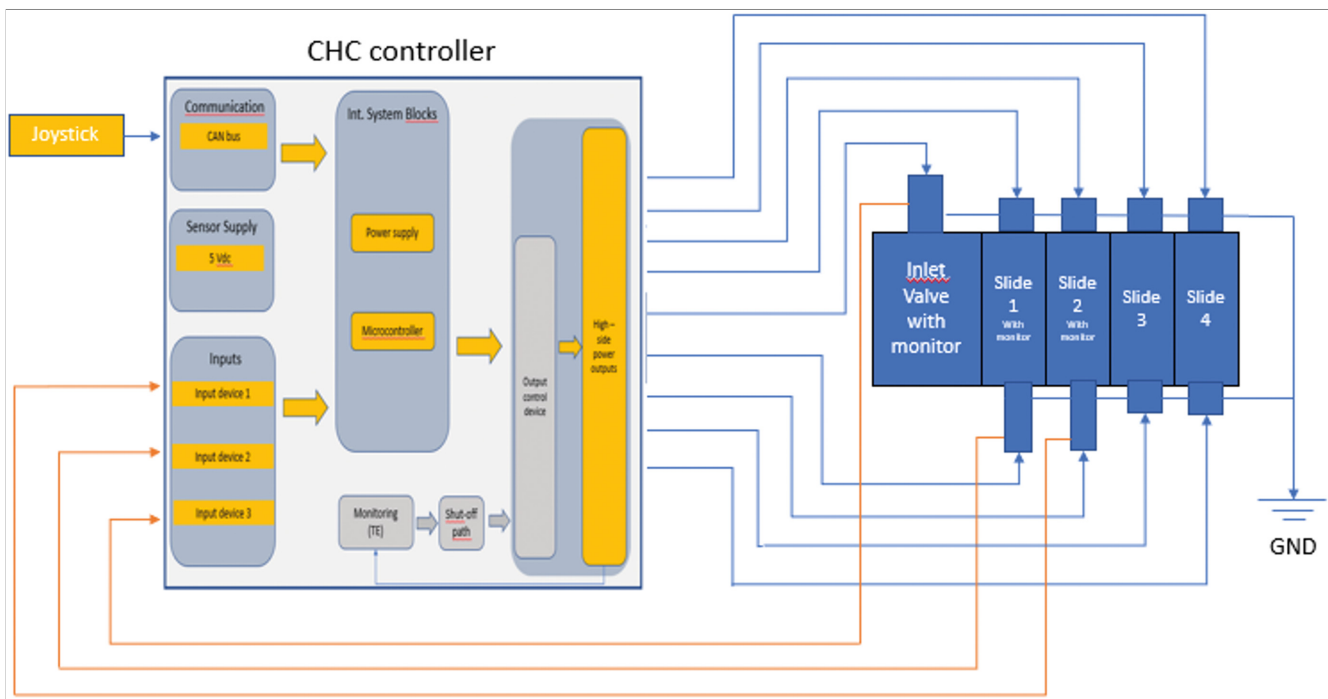
This result could be used further by the machine manufacturer, together with the safety-related parameters of the sensors, actuators to calculate the MTTFD and DCavg of the whole safety function, and therefore provide the required evidence of PL conformity. This configuration can reach PL d following ISO 13849 standard.

### 12.3.2 Example 2: safe current control

In the second example, CHC is wired, configured and programmed (application software) to drive a hydraulic distributor. CHC reads 3 sensors and 1 joystick commands via CAN bus, and controls 9 actuators operating in High-side mode. The system must to reach the PLd in function in slide 1 and slide 2 following the ISO 13849, to obtain this result the system needs monitors on slide 1 and slide 2 and also on inlet valve. CHC is designed to receive the sensors in all analog inputs without specific order. ASW must manage the inputs.

The short circuit to ground must be manage by ASW (see par. 10.1). CHC can read the voltage on outputs, if voltage is different to GND when the valve is de-energize, a fault is active and ASW must de-energize the outputs. By ASW is possible to send the fault detection on CANbus to fix the fault.

CHC “system integrity” safety function ensures that all the required inputs are read and processed correctly as required by the ASW as well as the corresponding outputs are set correctly as required by the ASW



**Fig. 8: Second example for using the reliability parameters of the safety function “system integrity”**

The MTTFd, DCavg and CCF values for this system are easily determined into the tables at par.12.2 depending by machine working hours, in this example 360day/y, 24h/day.

It leads to the result that MTTFD of the main channel is 209 years and the DCavg of the control unit for this safety function is 97,63%.

This result could be used further by the machine manufacturer, together with the safety-related parameters of the sensors, actuators, command unit and communication channels to calculate the MTTFD and DCavg of the whole safety function, and therefore provide the required evidence of PL conformity.

## 13 Using a service tool

Service tools can be used for parameterization, flashing and diagnostics of the CHC control units.

In order to ensure the functional safety according to EN ISO 13849-1, machine manufacturers shall make sure that following requirements are strictly followed.

### **General**

- The machine shall go into the safe state before the communication of the CHC control units and a service tool begins and stay in the safe state as long as the communication is established.
- The disconnection of the communication shall not lead to automatic initiation of machine movement.

### **Flashing**

- After flashing, it shall be validated with sufficient testing that the correct software with the correct version is flashed to the correct CHC control unit.

### **Parameterization of safety-related parameters**

- Parameterization of safety-related parameters shall fulfill the requirements of EN ISO 13849-1:2015, Chapter 4.6.4 (e.&. prevention from unauthorized modification, input range control, transmission error control, etc.).
- After safety-related parameterization, it shall be validated with sufficient testing that the correct CHC control unit is correctly parameterized.

**Bosch Rexroth AG**

Robert-Bosch-Straße 2  
71701 Schwieberdingen  
Germany  
Service Tel. +49 9352 40 50 60  
[info.bodas@boschrexroth.de](mailto:info.bodas@boschrexroth.de)  
[www.boschrexroth.com](http://www.boschrexroth.com)

**Your local contact can be found at:**

<https://addresses.boschrexroth.com>