| **TECHNICAL SPECIFICATION** | |
| --- | --- |
| System | 45200 HRG\_AxB |
| Document | Functional Requirement Specification |
| Doc. Reference | TS-45200-110-01 |
| Version | 2F |
| Date | 28.04.2020 |
| Prepared by | F. Khemiri |
| Released by | G. Bauer |

Revision history

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No. | Chap. | Date | Author | Revision | Modifications |
|  | All | 26.03.2020 | F. Khemiri | 01E | Preparing the document |
|  | All | 21.04.2020 | D. Jankowsky | 02E | Adoption on HRG requests |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Table 1: Revision history

**Table of content**

[Revision history 2](#_Toc38987070)

[1 Purpose of the document 5](#_Toc38987071)

[2 General task 5](#_Toc38987072)

[3 Functional Overview 6](#_Toc38987073)

[3.1 General structure 8](#_Toc38987074)

[3.1.1 System overview 8](#_Toc38987075)

[3.1.2 Description of the internal and external interfaces 9](#_Toc38987076)

[4 General characteristics 11](#_Toc38987077)

[4.1 Applicable normative 11](#_Toc38987078)

[4.1.1 Normative for functional safety 11](#_Toc38987079)

[4.1.2 Normative for EMC 12](#_Toc38987080)

[4.1.3 Normative for electrical safety and environmental requirements 13](#_Toc38987081)

[4.2 Overall safety-relevant substance data 14](#_Toc38987082)

[4.3 Threshold values for safety and reliability 14](#_Toc38987083)

[4.3.1 Reaction Time 16](#_Toc38987084)

[4.3.2 Planed measures for validation of the safety characteristics 17](#_Toc38987085)

[5 Physical Characteristics 18](#_Toc38987086)

[5.1 Mechanical Characteristics 18](#_Toc38987087)

[5.2 HMI: 18](#_Toc38987088)

[5.3 Environmental Characteristics 19](#_Toc38987089)

[5.4 Electrical and EMI Characteristics 19](#_Toc38987090)

[6 Interface 21](#_Toc38987091)

[6.1 I/O Interface 21](#_Toc38987092)

[6.1.1 Inputs 21](#_Toc38987093)

[6.1.2 Safe Outputs 21](#_Toc38987094)

[6.2 STO 21](#_Toc38987095)

[6.2.1 Safety structure 21](#_Toc38987096)

[6.2.2 Characteristics 22](#_Toc38987097)

[6.3 Safe Brake Control 24](#_Toc38987098)

[6.3.1 SBC implementation 24](#_Toc38987099)

[6.3.2 Characteristics 24](#_Toc38987100)

[6.4 3-phase current measurement 25](#_Toc38987101)

[6.5 Encoder Interface 26](#_Toc38987102)

[6.5.1 External Encoder Interface 26](#_Toc38987103)

[6.5.2 General characteristics 27](#_Toc38987104)

[6.6 Black Channel Sensor Interface 31](#_Toc38987105)

[6.7 Non-safe internal/external Interfaces 32](#_Toc38987106)

[6.8 Data Interface 34](#_Toc38987107)

[6.8.1 Decentral data interface 34](#_Toc38987108)

[6.8.2 Local data interface 35](#_Toc38987109)

[7 Firmware 37](#_Toc38987110)

[7.1 General FW-Requirements 37](#_Toc38987111)

[7.2 OS 38](#_Toc38987112)

[7.3 Data sampling and processing 40](#_Toc38987113)

[7.3.1 Safety-related data sampling and processing 40](#_Toc38987114)

[7.3.2 Non-safety data sampling and processing 41](#_Toc38987115)

[7.4 Local safety functions 42](#_Toc38987116)

[7.4.1 Basic Safety Functions 42](#_Toc38987117)

[7.4.2 Parametrization of the safety functions 43](#_Toc38987118)

[7.5 EtherCAT communication 44](#_Toc38987119)

[7.5.1 EtherCAT basic IP 44](#_Toc38987120)

[7.5.2 EtherCAT cyclic process data exchange 45](#_Toc38987121)

[7.5.3 EtherCAT acyclic service data exchange 46](#_Toc38987122)

[8 Modes of Operation 47](#_Toc38987123)

[8.1 Description of Operational Modes 47](#_Toc38987124)

[8.1.1 Stand alone with external GUI 47](#_Toc38987125)

[8.1.2 Top-level connection mode 48](#_Toc38987126)

[9 Requirements 50](#_Toc38987127)

# Purpose of the document

For a robot application specific data has to be collected on each axis. Part of those data are safety relevant, others not.

The target of this document is the definition of the functionality, performance data and general safety characteristics of a special module for the sampling of axis related data on a robot application. This module becomes hereafter referred to as “HRG\_AxB” (Han’s Robot Germany Axis Board).

# General task

General task is the development of a data sampling and computation board with data interfaces and STO plus brake control output. The board shall deliver several type of safe and non-safe data. It is to be equipped with adequate interfaces for the connection of different types of sensors. The sampled respective generated data are to be forwarded via EtherCAT connection to a non-safe and a safe master. The board shall provide a STO functionality, preferable by interrupting at least 2 phase motorcurrent (STO) and to drive a brake using SBC.

Cyclic non-safe data exchange is by EtherCAT PDO’s, synchronization with the control is based on the Distributed Clock (DC) and safe data communication is by use of the EtherCAT FSoE protocol. Further EtherCAT services like CoE for acyclic data and EoE for parametrization and FW update are to be implemented too. The board is to be equipped with an Ethernet/EtherCAT 2-port interface for the data communication.

The case respective installation space of the board is not part of the development on hand.

The HRG\_AxB is part of the Han’s robot solution and delivers the input data for the Han’s specific control and safe robot solution of this series.

The safety part of the device has to comply with SIL 3 of the EN 61508 and must be suitable for safety functions up to Pl e of EN ISO 13849.

Part of the task-settings is the Examination / validation respective certification of the device by an in accordance to Annex IV – 2006/42/EG approved and listed institution.

# Functional Overview

The objective HRG Axis Board consists in its primarily functionality of a robot axis data sampling and processing unit. The board with its interfaces, connected sensors and the board-specific firmware must generate safe position, speed and torque as well as non-safe space orientation. Further safety related data shall be read via separate SPI interfaces. Design must provide enough resources for a safe local processing of those data as well as for future enhancements.

The board shall be able to interrupt via safe channels the motorcurrent (Direct STO) and to drive a brake using SBC. It shall be connectable to a SBC output of another system as a “sink” for the SBC input. For the Direct STO a feasibility study shell be elaborated first, if not feasible alternatively an adequate control output must be provided.

For signal purposes by use of LED-stripes etc. a serial output and FW-task is to be implemented. An inertial measurement unit (IMU) needs to be included on the board or an interface is to be provided. Furthermore, an interface for temperature sensors needs to be available.

All communication with a top-level unit is by use of EtherCAT services. PDO’s for the cyclic data exchange of non-safe and safe data are to be implemented as well as mandatory and board-specific SDO’s. The cyclic data sampling and communication is to be synchronized with the top-level control by use of the Distributed Clock (DC) service and a time-shift function, accessible by a SDO. The non-cyclic data communication shall be based on the – mandatory – CoE service.

Parametrization of the board shall follow standard EtherCAT mechanism but respect the specific functionality by a tailored profile. For diagnostic purposes a tooling connection must be allowed. The same connection shall be used for a FW-update-service. Preferable EoE will be used for this purpose.

Basic safety functions, as specified in Section 7.4.1 shell be implemented. Implementation of further safety functionality should be respected.

The HRG\_AxB is suitable for applications up to SIL 3 of EN 61508 respective Pl e of EN ISO 13849-1. Part of the task is to implement the prototype test / validation and certification as equipment in accordance with Annex IV 2006/42 / EC – by a respective approved institute.

The primary functions of the device are:

* Safe detection of speed and position for 1 axes
* Provide interface and configuration suitable for two position encoder with BISS-C Interface in slave mode
* Safe detection of torque by use of current sensors for one channel and position input and output difference on gearbox in addition to the gear characteristics as the second diversity channel.
* Provide interface, current sensors, FW-function and configuration for processing of the current and gear/position based data in order to generate actual safe torque. Note: Specification of this FW-function is by HRG
* Provide interface, FW-function and configuration for processing of safety-relevant data for a further data type. Note: Specification and type definition of this FW-function is by HRG
* Safe internal implementation and control of Direct STO (Safe Torque Off) and SBC (Safe Brake Control) for 1 axes.
* Provide interface (or sensor, tbd), FW-function and configuration for non-safe space orientation by use of an adequate internal or external sensor
* Provide interface, FW-function and configuration for a non-safe signaling device
* Provide interface, FW-function and configuration for non-safe temperature sensors
* Ethernet/EtherCAT interface for safe and non-safe communications (FSoE, EoE, CoE)
* Synchronization with top-level control by use of DC service
* Diagnostic interface via EoE.

The HRG\_AxB can be used

* As an axis-related slave in son-safe environment for the HRG specific robot control based on ELMO-Drives.
* Dto. In a safe environment for the HRG specific safe robot solution, based on ELMO-Drives and BBH FSoE safe master devices

## General structure

### System overview



Figure 1: Context diagram HRG\_AxB

### Description of the internal and external interfaces

| **Externals** | **Description** | **Safety requirements** |
| --- | --- | --- |
| External Position / Speed sensors | Interface to an external sensor system for speed and / or position detection for the two axes  Achievable Pl / SIL depends from   1. Safety characteristic of the sensor 2. One or two sensors are used   Interface is of BISS-C type  HRG\_AxB read the data in slave mode, BISS-C master is the inverter. For diagnostic purpose HRG\_AxB may need to act as an additional master | Sensor systems with relevance to safety must be two-channel, non-reactive constructed and installed. Diversity in encoder choice should be respected to reduce CCF, but the technology of the sensors themselves is not necessarily safety relevant. Further internal safety measures are needed to comply with normative requirements for BiSS-C type encoders. |
| Current measurement | Internal measurement of the 3-phase motor current (e.g. with Hall sensors, tbd). This measurement is used in parallel to the torque evaluation by use of the position of the input and output position sensor and the gearbox characteristic.  Achievable Pl / SIL depends from   1. Quality and accuracy of the two diversity systems   Data of the current on the torque is forwarded to the non-safe and to the safe control on different PDO’s. | The torque evaluation is based on a two-channel diversity data input and processing. The technology of the sensors themselves is not safety relevant.  For the safety function criteria like time lag and accuracy are relevant.  Adequate external measures must be taken for limitation of the worst-case signal voltage and impedance. |
| Safety-Relevant Black Channel | Data interface for a further type of safety relevant data. Characteristic of those data will be defined later in the project.  Achievable Pl / SIL depends from   1. Safety characteristic of the sensor 2. Diversity, independency and freedom from feedback of the sensors and their interfaces   Interface is of SPI type  Data is forwarded to the non-safe and to the safe control on different PDO’s. | Interface must be non-reactive. Diagnoses data must be suitable for failure detection.  The interfaces and data processing for the two sensors must be assigned to the two separate channels with a cross-check of the results.  Interface and sensors respective their input signals must be independent and with freedom from feedback |
| Space orientation | Data interface for a space orientation sensor or inclusion of the sensor on the board, tbd. The interface is of non-safe type. Data is to be forwarded to the non-safe control.  Interface is of SPI or I2C type | n.a. |
| EtherCAT | Ethernet / EtherCAT interface to the upper-level non-safe and safe automation systems. From HRG\_AxB the safe and non-safe process data are sent periodically.  Board specific PDO’s for non-safe and safe data.  For safe data communication FSoE is used.  All mandatory and board specific SDO’s are to be provided.  Central parametrization possible in context with the HRG robot control and SCU-safe-master-series.  Diagnostic interface and FW-update service by EoE  DC service used for synchronization with top-level-control | Functional data are non-safety-relevant.  For the transfer of safety-relevant process data FSoE is to be used.  Board-specific profile for safe data is to be implemented.  Transmitting and receiving data to be processed in the two channels of the HRG\_AxB.  Safe parametrization by a board-specific profile and FSoE-parameter. |
| STO | Implementation of Direct Safe Torque Off on the HRG AxB. 3-phase FET circuit for interruption of the motor currents.  Note: In a first step a feasibility study is to be elaborated, if not feasible alternatively adequate STO control output is to be provided. | Two-channel system with internal tests and feedback signals. |
| SBC | Safe Brake Control with internal control as well as with signal from motor drive. Inclusion of PWM for current control – high current for magnetization at the beginning, then low current to keep it open. | Two-channel system as a combination of high side and low side drivers with internal tests and feedback signals. |
| Display/signaling elements | For control of LED signal stripes, a serial interface is to be implemented. Control of this LED stripes by the non-safe PDO | LED stripes are not safety-related |
| Temperature | Data interface for temperature sensors on a 1 wire bus | n.a. |

# General characteristics

The HRG\_AxB unit must be designed to be used for safety-related functions of [machinery](http://dict.leo.org/ende?lp=ende&p=DOKJAA&search=machinery&trestr=0x801) [and](http://dict.leo.org/ende?lp=ende&p=DOKJAA&search=and&trestr=0x801) [equipment](http://dict.leo.org/ende?lp=ende&p=DOKJAA&search=equipment&trestr=0x801) up to SIL 3 of EN 61508 respective Pl e of EN ISO 13849‑1 in accordance to attachment IV of the EC machinery directive 2006/42/EG.

**Remark:**

For devices to be used for safety functions of [machinery](http://dict.leo.org/ende?lp=ende&p=DOKJAA&search=machinery&trestr=0x801) [and](http://dict.leo.org/ende?lp=ende&p=DOKJAA&search=and&trestr=0x801) [equipment](http://dict.leo.org/ende?lp=ende&p=DOKJAA&search=equipment&trestr=0x801) in accordance to attachment IV of the EC machinery directive 2006/42/EG a certification by an acknowledged test laboratory is mandatory.

## Applicable normative

For the definition and validation of the safety demands of the devices the applicable normative have to be used. Especially the listed harmonized normative of the EC machinery directive must be used.

### Normative for functional safety

| Norm /  *Standard* | Titel /  *Title* | Ausgabe /  *Edition* |
| --- | --- | --- |
| IEC 61508 | Teil 1-7: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme  *Part 1-7: Functional safety of electrical/electronic/programmable electronic safety-related systems* | 2011 |
| EN ISO 13849-1 | Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze | 2016 |
| EN ISO 13849-2 | Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 2: Validierung | 2013 |
| EN ISO 13850 | Sicherheit von Maschinen - Not-Halt - Gestaltungsleitsätze | 2016 |
| EN 62061 | Sicherheit von Maschinen - Funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und programmierbarer elektronischer Steuerungssysteme  *Safety of machinery - Functional safety of safety-related electrical, electronic, programmable electronic control systems* | 2016 |
| EN 574 | Sicherheit von Maschinen - Zweihandschaltungen - Funktionelle Aspekte - Gestaltungsleitsätze | 1996 + A1:2008 |
| EN 55011 (Klasse A) | Industrielle, wissenschaftliche und medizinische Geräte - Funkstörungen - Grenzwerte und Messverfahren  *Industrial, scientific and medical equipment – Radio-frequency disturbance characteristics – Limits and methods of measurement* | 2016 + A1:2017 |
| EN 61800-5-1 | Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl – Teil 5-1: Anforderungen an die Sicherheit – Elektrische, thermische und energetische Anforderungen | 2017 |
| EN 61800-5-2 | Elektrische Leistungsantriebssysteme mit einstellbarer Drehzahl - Teil 5-2: Anforderungen an die Sicherheit - Funktionale Sicherheit (IEC 22G/264/CD:2013)  *Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional.* | 2017 |
| EN ISO 12100 | Sicherheit von Maschinen - Allgemeine Gestaltungsleitsätze - Risikobeurteilung und Risikominderung | 2011+  A1:2013 |
| EN 60204-1 | Sicherheit von Maschinen - Elektrische Ausrüstung von Maschinen - Teil 1: Allgemeine Anforderungen | 2006 + A1:2009 |

### Normative for EMC

| Norm /  *Standard* | Titel /  *Title* | Ausgabe /  *Edition* |
| --- | --- | --- |
| EN 61800-3 | Drehzahlveränderbare elektrische Antriebe - Teil 3: EMV-Anforderungen einschließlich spezieller Prüfverfahren  *Adjustable speed electrical power drive systems - Part 3: EMC requirements and specific test methods.* | 2012 + A1:2014 |
| EN 61000-6-2 | Elektromagnetische Verträglichkeit (EMV) – Teil 6-2: Fachgrundnormen - Störfestigkeit für Industriebereiche  *Electromagnetic compatibility (EMC) –*  *Part 6-2: Generic standards - Immunity for industrial environments* | 2006 |
| EN 61000-6-4 | Elektromagnetische Verträglichkeit (EMV) - Teil 6-4: Fachgrundnormen - Störaussendung für Industriebereiche  *Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments* | 2011 |
| EN 61000-6-7 | Elektromagnetische Verträglichkeit (EMV) - Teil 6-7: Fachgrundnormen - Störfestigkeitsanforderungen an Geräte und Einrichtungen, die zur Durchführung von Funktionen in sicherheitsbezogenen Systemen (funktionale Sicherheit) an industriellen Standorten vorgesehen sind | 2015-12 |
| EN 55011 | Industrielle, wissenschaftliche und medizinische Geräte - Funkstörungen - Grenzwerte und Messverfahren | 2016 + A1:2017 |

### Normative for electrical safety and environmental requirements

| Norm /  *Standard* | Titel /  *Title* | Ausgabe /  *Edition* |
| --- | --- | --- |
| EN 50178 | Ausrüstung von Starkstromanlagen mit elektronischen Betriebs | 1997 |
| EN 61800-2 | Drehzahlveränderbare elektrische Antriebe - Teil 2: Allgemeine Anforderungen; Festlegungen für die Bemessung von Niederspannungs-Wechselstrom-Antriebssystemen mit einstellbarer Frequenz | 2015 |
| EN 60721-3-1 | Klassifizierung von Umweltbedingungen - Teil 3: Klassen von Umwelteinflussgrößen und deren Grenzwerte; Hauptabschnitt 1: Langzeitlagerung | 1997 |
| EN 60721-3-2 | Klassifizierung von Umweltbedingungen - Teil 3: Klassen von Umwelteinflussgrößen und deren Grenzwerte; Hauptabschnitt 2: Transport | 1997 |
| EN 60721-3-3 | Klassifizierung von Umweltbedingungen - Teil 3: Klassen von Umwelteinflussgrößen und deren Grenzwerte; Hauptabschnitt 3: Ortsfester Einsatz, wettergeschützt | 1995 + A2:1997 |
| EN 61131-2 | Speicherprogrammierbare Steuerungen - Teil 2: Betriebsmittel-anforderungen und Prüfungen | 2007 |
| EN 60664-1 | Isolationskoordination für elektrische Betriebsmittel in Niederspannungsanlagen - Teil 1: Grundsätze, Anforderungen und Prüfungen. | 2007 |
| EN 60529 | Schutzarten durch Gehäuse (IP-Code)  *Degrees of protection provided by enclosures (IP Code)* | 1991 + A1:2000 + A2:2013 |

## Overall [safety-relevant](http://dict.leo.org/ende?lp=ende&p=Ci4HO3kMAA&search=safety-relevant&trestr=0x8001) [substance](http://dict.leo.org/ende?lp=ende&p=Ci4HO3kMAA&search=substance&trestr=0x8001) [data](http://dict.leo.org/ende?lp=ende&p=Ci4HO3kMAA&search=data&trestr=0x8001)

|  |  |  |
| --- | --- | --- |
| **Substance data** | **Parameter** | **Description** |
| EN/IEC 61508  Target SIL | SIL 3 | Target SIL for certification of the complete device |
| EN ISO 13849-1 architecture | Category 4 | Target category for certification of the complete device – Cat 4 is required to achieve Pl e |
| EN ISO 13849-1 PL | Pl e | Target Pl for certification of the complete device |
| EU-Type certification | yes | EU-type certification requested |
| Basic normative for type certification | EN 61508,  EN 13849-1,  EN 60204,  EN 62061,  EN 50178 | Codes and standards forming the basis of the certification |
| Additional normative for type certification | ISO 13850  EN 61800-5-2,  EN 61800-3,  EN 61000-6-2,  EN 61000-6-7,  EN574 | Additional codes and standards related to specific functionality forming the basis of the certification |
| UL | Type certification | UL Type-certification requested |

1. SIL 3 according to IEC 61508:2010]
2. Architecture categories 4 according to EN ISO 13849-1:2015]
3. Pl e according to EN ISO 13849-1:2015]
4. EU Type certification]
5. EN 61508:2010, EN 13849-1:2015, EN 60204:2006 + A1:2009, EN 62061:2015, EN 50178:1997 Basic normative for type certification]
6. EN 61800-5-2:2016. EN 61800-3:2004 + A1:2012, EN 61000-6-2:2005, EN 61000-6-7:2015, EN574 Additional normative for type certification]
7. UL type certification]

## Threshold values for safety and reliability

|  |  |  |
| --- | --- | --- |
| **Threshold value** | **Parameter** | **Description** |
| Life cycle | 10 years | Life time as used for determination of failure probability |
| Proof test interval | 10 years | Proof test interval in context with determination of failure probability |
| Failure detection and acceptance time device | 3 ms | Max. detection and reaction time for single case failures |

1. Life cycle 10 years]
2. Proof test interval 10 years]
3. Failure detection and acceptance time 3 ms]

|  |  |  |
| --- | --- | --- |
| **Threshold value** | **Parameter** | **Description** |
| Cycle time | 1 ms | Duty cycle time for the complete safety function computation |
| FSoE Communication | 0,5 ms | Cycle time for the FSoE communication  - 2times per cycle required |
| Fast channel time | 1 ms | Fast channel time for the complete safety function computation of specific fast functions |
| EtherCAT communication | 125µs | EtherCAT communication cycle time |
| Completion of self-test routines (Memory + CPU etc.) | 1 h | Max. test time (memory test, CPU test etc.) |
| Monitoring of over- and undervoltage µP-Systems | < 50 ms | Detection time for voltage diagnoses on µP-Core |
| Monitoring of over- and undervoltage of channel A/B | < 50 ms | Detection time for voltage diagnoses on system A/B |
| Operability test of safe outputs | <50 ms | Detection time for operability test of the semiconductor outputs |
| Max output test time | 600 µs | Max cut-off time for dynamic output test |
| Worst case time for false output status | 4 ms | Max. time for output with wrong status (on instead of off) |

1. Cycle time device: 1 ms]
2. Cycle time FSoE: 0,5 ms]
3. Fast channel cycle time 1 ms]
4. EtherCAT communication cycle time 125 µs]
5. Completion of self-test routines 1 h]
6. Monitoring of over- and undervoltage µP-Systems <50 ms]
7. Monitoring of over- and undervoltage of channel A/B <50 ms]
8. Operability test of safe outputs <50 ms]
9. Max cut-off time for dynamic output test 600 µs]
10. Worst case time for false output status 4 ms]

### Reaction Time

|  |  |  |
| --- | --- | --- |
| **Function** | **Response Time** | **Explanation** |
| Cycle time safe Position and speed data | 1 ms | Send out every 1 ms |
| Cycle time Safe Torque | ≥ 1ms\*) | Depending from filter structure and time |
| Mean value filter (for settings see the encoder dialogue in SafePLC2) | 0 – 32 ms | Group runtime of the averager. This runtime affects only the monitoring functions in connection with position / speed / acceleration, but not the logic processing. |
| Black Channel Safe Data | ≥ 1ms\*) | Depending from FW requirement, filter structure and time |
| FSoE Input data to STO, SBC Output | 1,5 ms | Cycle time + internal processing |
| Cycle time non-safe orientation data | ≥ 125 µs | Depending from the sensor / interface clk |
| Cycle time non-safe position of the two encoders | ≥ 125 µs | Depending from the sensor / interface clk |
| Cycle time non-safe current | ≥ 125 µs | Depending from the sensor bandwith |
| Cycle time non-safe serial output | ≥ 250 µs | Depending from the interface clk |

\*) When using a filter, its response time must be added.

1. Cycle time safe Position and speed data: 1 ms]
2. Cycle time Safe Torque: ≥1 ms]
3. Mean value filter (for settings see the encoder dialogue in SafePLC2): 0 – 32 ms]
4. Black Channel Safe Data: ≥ 1ms]
5. FSoE Input data to STO, SBC Output: 1,5 ms]
6. Cycle time non-safe orientation data: ≥ 125 µs]
7. Cycle time non-safe position of the two encoders: ≥ 125 µs]
8. Cycle time non-safe current: ≥ 125 µs]
9. Cycle time non-safe serial output: ≥ 250 µs]

### Planed measures for validation of the safety characteristics

| **Design phase** | **Measure for validation** | **Remark** |
| --- | --- | --- |
| System definition | System-FMEA | System-FMEA for structural analyses of the system and proof to achieve the target Pl / SIL |
| Hardware validation | Hardware FMEA | Hardware-FMEA with analyses for all HW parts of the system in relation to the failure modes, FIT, DC and structure for evaluation of the safety architecture and PFH value |
| Software development | Modification and impact analyses | Analyses of the modifications on re-used SW-modules with predefinition of the hereby required tests |
| Software criticality analyses | Proof for the specified requirements on the SW-architecture and SW-modules characteristics |
| Module tests | Verification of the specified characteristics of the SW-modules. Definition of the module tests within the SW-specification and/or modification analyses |
| Software Design Method and selection of tools | Proof for the correct use of methods and tools in accordance to the SRS respective safety plan. |
| Hardware development | Modification and impact analyses | Analyses of the modifications on re-used HW-circuits with predefinition of the hereby required tests |
| Hardware Review Document | Analyses of the HW based on the schematics in relation to the HW-specification |
| HW performance test | Verification of the HW-performance characteristics by limit value tests |
| EMI and environmental tests | Execution of EMI and environmental tests based on the specified characteristics |
| System validation | Failure Injection tests (FIT) | Failure injection tests for all possible failure scenarios |
|  | System tests | System integration tests for validation of the functional and safety-related characteristics of the device |
|  | Integration tests | Verification of the characteristics of all structural system parts like SW-functions / modules, HW-modules etc. |
| System documentation | Review for system documentation | Verification of the correctness and completeness of the system documentation |
| Production | Review of the measures for production quality assessment | Analyses of the production tests and quality assessment for the production |

# Physical Characteristics

## Mechanical Characteristics

|  |  |  |
| --- | --- | --- |
| **Threshold value** | **Parameter** | **Description** |
| Outline (Main Control Board) | 70 x 40 mm, tbd | Dimension / outline of the Main Control Board |
| Position of interface connectors | tbd | Positions of all interface connectors on the PCB |
| Current sensors - connector | tbd | Latching, reverse polarity protection required |
| Encoder connector | tbd | 2 x encoder connector |
| Orientation sensor | tbd | Latching, reverse polarity protection required |
| Black Channel data connector | tbd | As above |
| LED stripe connector | tbd | As above |
| EtherCAT connector | Tbd, circular or RJ45 | Standard-EtherCAT/Ethernet connectors |
| EtherCAT mandatory LED | Position tbd | Misc. LED are mandatory for EtherCAT and must be visible in operation |

1. Dimension of the Board 70 x 40 mm, tbd]
2. Tbd at a later stage]
3. Type of Current sensors – connector: tbd at a later stage, latching, reverse polarity protection required]
4. Encoder connector: : tbd at a later stage]
5. Type of Orientation sensor – connector: tbd at a later stage, latching, reverse polarity protection required]
6. Type of Black Channel data connector: tbd at a later stage, latching, reverse polarity protection required]
7. Type of LED stripe connector: tbd at a later stage, latching, reverse polarity protection required]
8. EtherCAT connector connector: tbd at a later stage, standard required]

## HMI:

|  |  |  |
| --- | --- | --- |
| **Threshold value** | **Parameter** | **Description** |
| EtherCAT mandatory LED | Position tbd | Misc. LED are mandatory for EtherCAT and must be visible in operation |
| Status RGB LED | Position tbd | RGB LED for easy on-field diagnostics |

1. EtherCAT mandatory LED – position tbd, mandatory, must be visible]
2. Status RGB LED, Position tbd]

## Environmental Characteristics

|  |  |  |
| --- | --- | --- |
| **Threshold value** | **Parameter** | **Description** |
| Environmental temperature | 0-85 °C | Rated environmental temperature of the device inside drive |
| Clime class | 3 K3 EN 60721-3-1 | identification of the clime class |
| Max. appl. Height | ≤ 2000 m | Identification of the maximum application height |
| Pollution class | 1  EN 60664-1 | Rated pollution class |
| Mechanical stress shock | EN 61800-2, IEC 60721-3-3 Klasse 3M1  19,6 m/s² | Specification of the mechanical stress for shock |
| Mechanical stress vibration | IEC 61131-2  5.88 m/s2  10~60Hz | Specification of the mechanical stress for vibration |
| Protection class | IP20; Connectors: IP00 EN 60529 | Degrees of protection provided by enclosures |

1. Environmental temperature -0°C …85°C for board]
2. Clime class 3K3 EN 60721-3-1]
3. Protection class: IP20; Connectors: IP00 according to EN 60529]
4. max appl. height 2000m]
5. Pollution class 1 EN60664-1]
6. Mechanical stress shock level in accordance to EN 61800-2, IEC 60721‑3‑3 Klasse 3M1]
7. Mechanical stress vibration level in accordance to IEC 61131-2, 5.88 m/s2, 10~60Hz]

## Electrical and EMI Characteristics

| **Threshold value** | **Parameter** | **Description** |
| --- | --- | --- |
| Electrical safety standard | EN 61800-5-1  EN 50178 | Specification of the applicable electrical safety standard |
| Supply voltage | 24 VDC ±20% | Specification of the rated supply voltage |
| Worst case supply voltage | 230 V (SELV or PELV) | Specification of the worst-case supply voltage |
| Fuse | 3A (48V) | Rated current and type of fuse for supply |
| EMI standard | EN 61800-3, EN 55011 | Specification of the applicable EMI standard for test execution |
| EMI limit value definition | EN 62061 | Normative for definition of limit values |
| EMI test level | High 4kV | Level for the EMI test |

1. Electrical safety standard EN61800-5-1, EN 50178]
2. Supply voltage 24VDC, tolerance ±20%]
3. Worst case supply voltage 230V (SELV/PELV)]
4. Fuse 3A for the 48V power supply]
5. EMI standard for tests EN 61800, EN 55011]
6. EMI standard for limit value definition EN 62061]
7. EMI test level high, 4 kV]

# Interface

## I/O Interface

### Inputs

#### SBC input

Input for the SBC signal of a motor drive needed to trigger the braking process externally (in addition to internal SBC for safety reasons). See Section 6.3.

### Safe Outputs

No digital outputs

## STO

The STO output must allow the use of an inverter without certified STO function. For this reason two alternatives have to be investigated within the project:

1. Preferable solution - STO on high-voltage / power side internally on the safety device. For the interruption, a 3-phase AC-Switch circuit shall be used (before or after the current measurement).

The switch is safety critical. Diagnoses is demanded for the cut-off function. Minimum 2 phase must be cut-off.

1. Alternative solution – Safe, 2-channel cut-off function for the supply of the pulse shaping unit. Capacitive behavior must be respected, adequate measures must be provided respective coordinated with the supplier of the inverter unit.

### Safety structure

The following figure shows the architecture of the STO circuit.



Figure 2: Architecture of the STO

### Characteristics

| **Naming** | **Value** | **Description** |
| --- | --- | --- |
| Number of outputs | 3 | Safe Torque Off Output |
| Two-channel  SIL 3 Kat. 4 PL e | High Voltage / Power side, 2 of 3 | 3 x Semiconductor switch channels with diagnoses, 2 of 3 principe |
| Leakage current at any condition | Leak current: max. tbd | Rated values |
| Voltage loss | ≤ tbd mV | Voltage loss in active status |
| Capacitive load | ≤ 10nF | Max. capacitive load |
| Ohm load | tbd | Max. load |
| Inductive load | tbd |  |
| Short cut protection < 2Ω | permanent |  |
|  |  |  |
| Protection against strange voltage | Ufremd ≤ +500V | Protection against Overvoltage |
| Test pulse | ≤ 0,5 ms, on stop mode | Test executed only if not in active mode. Test interval tbd => once per shift/8h |
| Diagnoses | Short-cut detection:  Any of the three switches  Diagnoses executed on both channels | Diagnoses required for cut-off function for every channel on all three switches in order to provide 2 of 3 functionality |

1. Number of internal STOchannels: 2 of 3 (high power a) ) or 2 (low power b) )]
2. Two-channel equivalent SIL 3 Kat. 4 PL e]
3. Voltage loss STO ≤ tbd mV]
4. Capacitive load STO ≤ 10nF]
5. Resistive load STO ≥ tbd Ω]
6. Inductive load STO tbd H]
7. Leakage current STO-A < tbd mA]
8. Permanent short-cut protection STO < 2Ω]
9. Protection against other supply voltage STO: Ufremd ≤ +500V]
10. Test pulse duration STO ≤ 0,5ms in stop mode only]
11. Test relation STO 1x every 8h]
12. Detection of STO short cut on all 3 switches by the two safety channel]

## Safe Brake Control

The Safe Brake Control (SBC) is for control of 1 motor brake. The SBC power control has to be included on the HRG AxB.

### SBC implementation

|  |  |  |  |
| --- | --- | --- | --- |
| **Type** |  | **Safety Characteristic** | **Additional requirements** |
| High -Side Combination  The High-Side is a single channel output with internal two cut-off channels |  | SIL 3  Cat. 4 Pl e | Protected wiring |

### Characteristics

|  |  |  |
| --- | --- | --- |
| **Naming** | **Value** | **Description** |
| Semiconductor O | 1 Hi + PWM | High-Side switch + PWM = second channel |
| Output voltage (High Side) | 48 VDC | Rated output voltage |
| Output supply voltage | Min 21V  Max 56 V | Specification of the rated maximum and minimum output supply voltage |
| Worst case output supply voltage | 60V (PELV) | Specification of the worst-case supply voltage, limited by design or the PELV-type etc. |
| Fuse | 3 A | Rated current and type of fuse for supply |
| Rated output current | 1,5 A | Max allowed output current |
| Max. inductive load | 0,8 J | Maximum allowed inductive load |
| Max. capacitive load | 100 nF | Maximum allowed capacitive load |
| Output pulse frequency | 4 kHz | Max. pulse frequency for the outputs |

1. Number of safe brake channels: 1]
2. Characteristic of output: dual channel]
3. Rated voltage 48 VDC]
4. Min. voltage 21 V, max. voltage 56 V]
5. Worst case supply voltage 60 V]
6. Fuse on supply 3 A]
7. Rated output current 1,5 A]
8. Max. inductive load 0,8 J]
9. Max. capacitive load 100nF]
10. Output pulse frequency 125 Hz]
11. Switching time on one channel 200 µs]
12. Switching time all channels 400 µs]

## 3-phase current measurement

Current measurements for torque calculation (1. channel) needs to be implemented on the HRG AxB internally, e.g. with Hall sensors. 3-phase measurement is needed with max. 50 A. Exact implementation needs to be further discussed / tested / investigated.

## Encoder Interface

The HRG\_AxB disposes of two encoder interfaces. The interfaces is of the type BISS-C. The BiSS-C readout has to be transparent (“sniffing” / Slave-Mode) of the communication with the drive controller – the AxB shall function as a BiSS-C slave.

|  |  |  |
| --- | --- | --- |
| **Encoder Interface** | **Connector** | **Encoder Types / Configuration** |
| 1st Encoder | X9A | BISS-C |
| 2nd Encoder | X10A | BISS-C |

The HRG\_AxB has to achieve **Pl e / SIL3** in accordance to EN ISO 13849 / EN 61508 in **dual encoder mode with combination of the two encoder**.

1. SIL 3 / PI e (following EN 61508, EN ISO 13849) has to be achieved with two encoders]

### External Encoder Interface

For the direct connection of encoders, the HRG\_AxB is to be equipped with two external interface. The interface must allow:

* BISS-C

1. Interface for two external encoder]
2. The external interface allows the encoder type BISS-C]
3. Multi-slave = preferable configuration]

#### General characteristic external interface

|  |  |
| --- | --- |
| Encoder | |
| Physical Layer: | RS422 compatible |
| Data interface: | Serial Synchronous interface (SSI) |
| Data format: | Binary or Gray code |
| Overall protocol | BISS-C |
| Data length: | Variable data length from 12 to 32 bit |
| Operation mode: | Slave |
| Clock rate: | Variable: 2000 kHz |

1. SSI input signal level are RS422 compatible]
2. Variable SSI Data length from 12 to 28 bit]
3. Master operation mode for BISS-C]
4. Clock rate: 2000 kHz]
5. Binary or gray code selection]
6. Monitoring of encoder supply voltages required]

### General characteristics

The below listed characteristics must be defined for all related encoder types

| **Designation** | **Parameter** | | **Description** |
| --- | --- | --- | --- |
| Number of external interfaces | 1. 2 | | Number of interfaces with a direct connection to encoder (external interface). BISS-C allows multi-slave connection. If applicable for safe position is subject of safety concept approval |
| Safe Position | yes | | Implementation of safe position computing |
| Type of encoder on external interface | SSI / BISS-C | | List of designated encoder technologies |
| Speed range | 216 | | Range of speed detection |
| Position range | 231 | | Range of position detection |
| Supply voltages encoder | 5V | | Selectable supply voltages for voltage monitoring |
| Supply voltage tolerance | +/- 10% | | Specification of the maximum allowed tolerance |
| Max. Supply current Encoder | 300 mA | |  |
| Encoder combinations for each axis | **1st Encoder** | **2nd Encoder** | Data type combination, e.g. binary + gray-code and resolution range/turn e.g. min ratio is subject of safety concept approval.  Safe-Turn-Counter function with safe referencing |
| BISS-C single-turn absolute on input shaft of gearbox | BISS-C single-turn absolute on output shaft of gearbox |

1. Number of external encoder interface 1 or 2]
2. Safe position and speed computing]
3. Type of encoder on external interface: SSI, BISS-C]
4. HRG\_AxB Resolution on speed signal 216]
5. HRG\_AxB Resolution on position signal 231]
6. Encoder supply voltages on external encoder interface 5V]
7. Encoder supply voltage tolerance on external encoder interface +/- 10%]
8. Encoder supply current: 300 mA]
9. Allowed encoder combinations = 2 x single, data type binary + gray-code, min ratio]

#### Encoder types and their Combinations

For SIL 3 EN 61508 and PL e according to EN ISO 13849-1, two independent, decoupled encoder systems are required.

| **Encoder 1** | **Encoder 2** | **Safe Direction** | **Safe Speed** | **Safe Absolute Position** | **Add. Safety relevant parameter** | **Fault Exclusion:**  *Fault exclusion mech. Shaft fracture, form-locking encoder shaft connection required* | **DC[%]** | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Dual-Channel Subsystem**  **dynamic** | **Dual-Channel Subsystem**  **non-dynamic** |
| SSI/BISS-C  Single-turn | SSI-BISS-C  Single-turn | √ | √ | - | 2 separate interfaces or binary/grey-code + min ratio | √ | 99 | 90 - 95 |
| SSI/BISS-C  Single-turn | SSI-BISS-C  Single-turn | √ | √ | √ | As above + Safe referencing on each POR-cycle + safe turn counter | √ | 99 | 90 - 95 |
| SSI/BISS-C  Single-turn | SSI-BISS-C  Multiturn | √ | √ | √ | As on line 1 + Safe referencing + brake set monitoring on POR + safe turn counter | √ | 99 | 90 - 95 |
| SSI/BISS-C  Multiturn | SSI-BISS-C  Multiturn | √ | √ | √ | As on line 1 + Safe referencing + safe turn counter | √ | 99 | 90 - 95 |

#### Specific diagnostic measures in relation to the encoder type used

The HRG\_AxB implements the following encoder diagnostics depending on encoder type.

|  | **Encoder Type** | **Supply Voltage Monitoring** | **Plausibility Test Position Signal**  **MPUA/MPUB** | **Plausibility Test data type + ratio** | **Encoder Diagnostic According to Corresponding Communication protocol** | **Difference Level Monitoring** | **Safe referencing** | **Safe turn counter** | **Brake monitoring on POR** | **Input Signal Level Monitoring** | **CLK-Frequency Monitoring** | **DATA-Level Monitoring** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Interface**  **X10A/X10B** | SSI/BISS-C | √ | √ | √ | √ |  | √ | √ | √ | √ | √ | √ |
| SSI/BISS-C | √ | √ | √ | √ |  | √ | √ | √ | √ | √ | √ |
|  |  |  |  |  |  |  |  |  |  |  |  |

(For more information please refer to “TS-44400-130-19-01F Encoder diagnosis”)

## Black Channel Sensor Interface

The HRG\_AxB will provide two interfaces for a further safe data processing. There is one type of data derived from the two sensor interfaces.

The functionality is not specified yet. Sufficient resources must be reserved for this functionality.

The interface type is of SPI.

The HRG\_AxB has to achieve **Pl e / SIL3** in accordance to EN ISO 13849 / EN 61508 in **dual sensor mode**.

| **Designation** | **Parameter** | | **Description** |
| --- | --- | --- | --- |
| Number of external interfaces | 2 | | 2 interfaces, assigned to channel A and B |
| Type of interface | SPI | | Type to be defined on a later stage, 1 type only |
| Supply voltages sensors | 5V | | Selectable supply voltages for voltage monitoring |
| Supply voltage tolerance | +/- 10% | | Specification of the maximum allowed tolerance |
| Max. Supply current Sensor | 300 mA | |  |
| Sensor combinations | **1st Sensor** | **2nd Sensor** | Type of sensor and data processing defined on a later stage. Safety concept documents and approval by HRG |
| tbd | tbd |

1. Number of external sensor interface for safe black channel 2]
2. Type of encoder on external interface: SPI]
3. Sensor supply voltages on external sensor interface 5V]
4. Sensor supply voltage tolerance on external sensor interface +/- 10%]
5. Sensor supply current: 300 mA]
6. Allowed sensor combinations: tbd by HRG on a later stage]
7. Data processing: tbd by HRG on a later stage]

## Non-safe internal/external Interfaces

There are two further non-safe interfaces to be implemented on the HRG\_AxB:

- Input interface for a space orientation sensor; sensor can also be included on the HRG\_AxB, tbd

- output interface for a LED-stripe

- input interface for temperature sensors, 1 external wire interface for ds18b20 sensor in parasitic power mode and bus operation

There is no further data processing for these interfaces, only forwarding of the dat from/to the non-safe PDO’s.

Input Interface

| **Designation** | **Parameter** | **Description** |
| --- | --- | --- |
| Number of external input interfaces | 1-2 (tbd) | No of external input interfaces for non-safe data |
| Type of interface | SPI | Type to be defined on a later stage, 1 type only |
| Supply voltages sensors | 5V | Supply voltage on connector |
| Supply voltage tolerance | +/- 10% | Specification of the maximum allowed tolerance |
| Max. Supply current Sensor | 300 mA |  |
| Sampling time | ≥ 125 µs | Time between two samples |
| Data forwarding | Mappable on PDO | How to forward the data to the top-level control |

1. Number of external sensor interface for non-safe input data: 1-2, tbd]
2. Type of external interface: SPI or I2C]
3. Sensor supply voltages on external sensor interface: 5V]
4. Sensor supply voltage tolerance on external sensor interface: +/- 10%]
5. Sensor supply current: 300 mA]
6. Sampling cycle time: ≥ 125 µs]
7. Data forwarding: direct mapping to PDO]

Output Interface

| **Designation** | **Parameter** | **Description** |
| --- | --- | --- |
| Number of external output interfaces | 2 | No of external output interfaces for non-safe data |
| Type of interface | UART like, see data sheet | Type of the output interface |
| Supply voltages on output interface | 5V | Supply voltage on connector |
| Supply voltage tolerance | +/- 10% | Specification of the maximum allowed tolerance |
| Max. Supply current Sensor | 3.5 A for both interfaces combined |  |
| Output cycle | ≥ 125 µs, depending from clk-rate | Time between two output samples |
| Data forwarding | Mappable on PDO | How to forward the data from the top-level control to the output |

1. Number of external sensor interface for non-safe output data: 2]
2. Type of external interface: UART like, see data sheet]
3. Supply voltages on external interface: 5V]
4. Supply voltage tolerance on external interface: +/- 10%]
5. Max. supply current: 3.5 A for both interfaces combined]
6. Sampling cycle time: ≥ 125 µs]
7. Data forwarding: direct mapping from PDO to the output interface]

## Data Interface

The data interfaces are separated into external and internal types.

The decentral types are for direct communication with a top-level control for exchange of safe data (sharing of safe inputs, safe output and status data) with a safe master device and non-safe data with the top-level controller,

The local types are used for a data exchange with the connected sensors respective output devices.

### Decentral data interface

|  |  |  |
| --- | --- | --- |
| **Designation** | **Type** | **Description** |
| Technology | EtherCAT | Type of technology used for the interconnection with top-level control device.  The EtherCAT interface is implemented as a slave IP and HW on the HRG\_AxB. |
| Protocol | Non-safe / PDO | Non-safe cyclic data exchange |
| FSoE / PDO | Safe data on EtherCAT |
| CoE | Parameter and diagnose data |
| EoE | Diagnostic and tooling data, FW-update |
|  | DC | Synchronization with top-level control |

1. EtherCAT slave IP and HW on HRG\_AxB]
2. Mappable PDO’s for non-safe data]
3. FSoE for safe data transfer]
4. CoE for parameter and diagnostic data]
5. EoE for diagnostic and tooling data, FW-update]
6. DC for synchronization with top-level control

### Local data interface

#### General data

|  |  |  |
| --- | --- | --- |
| **Designation** | **Type** | **Description** |
| Technology | SPI, UART | Type of technology used for the interconnection HRG\_AxB <-> misc. sensors |
| Modes | Safety relevant and non-safe data | Exchange of non-safe and safe data with local external devices |
| Protocol | Tbd, 1 fixed protocol per sensor interface | Protocol as required for the connected sensors |
| Duty cycle | ≥125 µs | Minimum refresh rate on the interface |

1. Local data interface technology: SPI, I2C and UART]
2. Communication mode on internal data interface = safe / non-safe data exchange]
3. Protocol on local data interface: tbd, 1 fixed protocol per data interface]
4. Duty cycle for data exchange on internal data interface: ≥ 125 µs]

#### SPI-Interface

|  |  |
| --- | --- |
| **SPI system property** | **Value** |
| **Word length** | 16 bits |
| **Word alignment** | tbd |
| **Byte order** | tbd |
| **Baud rate** | 12,5 or 25 Mbps |
| **Length / Protocol** | tbd |
| **Master** | tbd |
| **Slave** | tbd |
| **Telegram cycle** | tbd |
| **Communication mode** | tbd |
| **SPI Mode** | tbd |
| **CLK polarity (CPOL)** | tbd |
| **CLK Phase (CPHA)** | tbd |
| **CS active level** | tbd |

1. SPI parameter tbd on a later stage]

#### I2C-Interface

Interfaces for IMU sensor and temperature sensors

|  |  |
| --- | --- |
| **I2C system property** | **Value** |
| **Baud rate** | 0.4; 1.0; 3.4; oder 5,0 Mbps |
| **Master** | tbd |
| **Slave** | tbd |
| **Telegram cycle** | tbd |
| **Communication mode** | tbd |

1. I2C parameter tbd on a later stage]

#### LED interface

|  |  |
| --- | --- |
| **I2C system property** | **Value** |
| **Baud rate** | 38.4, 57.6, 115.2 kBaud |
| **Word length** | 16 bits |
| **Word alignment** | tbd |
| **Byte order** | tbd |
| **Length / Protocol** | tbd |
| **Telegram cycle** | tbd |
| **Communication mode** | tbd |

1. UART parameter tbd on a later stage]

# Firmware

The functions to be implemented in the FW of the HRG\_AxB are divided into the following sections:

* Input data read and processing for local generation of safe output data for position, speed and torque as well as for black channel data (tbd on a later stage).
* Safe drive monitoring basic functionality = limited to a subset of EN 61800-5-2 list of functions
* Non-safe data read and forwarding from/to local interfaces from/to EtherCAT communication interface
* Services for synchronization, diagnoses, update and parametrization

The functions to be implemented are described in more detail in chapter below

## General FW-Requirements

The general requirements on the FW are defined as follows:

* Runtime system for ensuring time-equidistant treatment of time-critical routines (reading sensors, periodic safety data processing and functions, treatment safe fieldbus etc.)
* All the functionality offered by the FW must be suitable for use in applications up to SIL 3 EN 61508 or Pl e, EN 13849-1
* By appropriate firmware functions / input devices the use of input and output data from standard controls, e.g. data received or sent over non-safe field bus systems must be possible to be used.  
  **Note:** This can, for example, done by forcibly AND operation with safety-related signals.
* Configurable standard FW functions for limited functions (STO, SBC, SS1) according to EN 61800
* Functions and SW tools for configuration / programming, Diagnostics and FW-update
* Configuration / Parametrization external executable under OP WINDOWS

The FW of HRG\_AxB must provide audited functions. These functions can be adjusted within defined limits to the specific characteristics and functionalities of applications with parameters.

The safe data processing is based on the 2-channel inputs and result in the input process image.

1. Safety related run-time system in accordance to the target SIL /Pl]
2. Safety related data sampling and processing adequate to the target SIL /Pl]
3. Parameterization and selection of the functionality in the limits defined for each type of monitoring function]
4. Implementation of the several standard monitoring functions according to the SMX base system]
5. Provision of Functions and SW tools for configuration / programming, Diagnostics and FW-update]

## OS

The operational system of the HRG\_AxB controls the actual state, organize the local data sampling and output, coordinates the two safety channels with each other, ensures the execution of all subprocesses including diagnostic and provides the correct and in-time communication with the top-level control. Therefore, the OS consists of the following modules:

General state machine with at least the following states:

- startup, init

- parameter read and check

- internal sync

- local run

- bus run

- safe data run

- error

The OS takes care of the process image with passivate and active state depending from the actual state and data contend.

For the correct timing in the run states an interrupt timing grid is to be implemented. Data sampling, processing and cross-check with alternate channel is organized by this time grid.

Synchronization with the top-level control is a subset of the OS functionality. The synchronization is based on the DC service. Data sampling is coordinated by a shift time parameter in relation to the timing event.

Beside this functional states and processes, the OS is supervising the correct run of all cyclic and non-cyclic processes required to achieve the target SIL / Pl. This includes but is not limited to:

- 2-channel data read and processing with cross-check of results

- check of the correct call of all safety-relevant cyclic processes

- control of the acyclic safety-related diagnoses

- cyclic update of the safe process input and output image

- monitoring of the safe top-level communication task

1. OS state machine with at least the states init, param, sync intern, local run, bus run, safe bus run, error]
2. Timing grid for channel synchronization and time equidistant data sampling]
3. Synchronization IP for coordination with top-level-control]
4. 2-channel data read and processing with cross-check of results]
5. OS provides correct run of all safety-relevant cyclic and acyclic processes]
6. OS controls the complete and correct run of all safety-related diagnoses]
7. OS controls cyclic update of process input and output image]
8. OS monitors the communication with top-level control]

## Data sampling and processing

Data sampling and processing is divided into the safety-related part and the non-safe part. Both are coordinated by the OS and time equidistant data sampling is ensured.

### Safety-related data sampling and processing

The below listed safety-related data sampling and processing to be implemented in the first stage of the HRG\_AxB project.

| **Description** | **Description** | **Input data** | **Reference document/**  **Base specification** |
| --- | --- | --- | --- |
| Safe position | Generation of safe position by parallel data sampling, normalizing and cross-check of the derived values. One data will be used as process data. | Encoder position | TS-37300-220-62-XF |
| Safe speed | Generation of safe speed based on the time-equidistant position data sampling, normalizing and cross-check of the derived values. Frequency or time based method, depending from the number of increments diff read. One data will be used as process data. | Encoder position | TS-37300-220-62-XF |
| Safe Torque | 2-channel diversity method by read of the actual current plus use of the motor model in one channel and position difference on in- and output of gearbox plus gearbox characteristic on the other channel. The adjusted result is used as process data. Filter time on current and gearbox effects like backlash etc. must be respected. Detailed specification required. | Motor current  Position on in- and output side of gearbox | Tbd, to be delivered by HRG |
| Safety Black channel | Special processing based on 2 channel input data. Not known yet. | 2 input data | Tbd, to be delivered by HRG |

1. Safe position data sampling and processing function]
2. Safe speed data sampling and processing function]
3. Safe torque data sampling and processing function]
4. Safety Black Channel data sampling and processing function]

### Non-safety data sampling and processing

The non-safety data are sampled and forwarded to the communication unit as native data only. The below listed data are sampled by the HRG\_AxB.

| **Description** | **Description** | **Input data** | **Reference document/**  **Base specification** |
| --- | --- | --- | --- |
| Actual current | Actual current of the 3 phases. Data is sampled on a fast AD-unit and can be mapped to a non-safe PDO | Current sensing | tbd |
| Orientation | Orientation is read in by a adequate sensor. Data can be mapped to a non-safe PDO | Orientation sensor data | tbd |
| Temperature | Temperature is read from max. 10 sensors on a 1 wire bus | Temperature sensor data | tbd |

1. 3-phase current data sampling and processing function]
2. Orientation data sampling and processing function]
3. Temperature data sampling and processing function]

## Local safety functions

### Basic Safety Functions

The below listed functions build the basic set of safe monitoring functions to be implemented in the first stage of the HRG\_AxB project.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Designation** | | **Description** | **Instance** | **Reference document/ Base specification** |
| STO | Safe torque Off | Stop function (Cat. 0) and monitoring of STO activation | 1 | TS-44400-130-07-XF |
| SS1 | Safe Stop 1 | Monitoring of stop ramps by comparison of target and actual course of the speed (Cat. 1) | 1 (\*) | TS-37000-400-12-XF |
| SS2 | Safe Stop 2 | Monitoring of stop ramps by comparison of target and actual course of the speed (Cat. 2) | 1 (\*) | TS-37000-400-12-XF |
| SBC | Safe Brake Control | Control of the Brake Output | 2 | TS-44400-130-07-XF |
| SOS | Safe Operating Stop | Standstill monitoring by comparing tolerance threshold velocity or position actual values | 1 per axis | TS-37350-110-01-XF |
| SREF | Safe Referencing | Setup of the encoder position reference by special input activation | 1 per axis | TS-37500-110-30-01F TS-37350-110-51-XF |

1. Implementation of the standard safe monitoring function STO in accordance to the definition in TS-44400-130-07-XF with instance 2]
2. Implementation of the standard safe monitoring function SS1 in accordance to the definition in TS-37350-110-01-XF with instance 4 per axis]
3. Implementation of the standard safe monitoring function SS2 in accordance to the definition in TS-37350-110-01-XF with instance 4 per axis]
4. Implementation of the standard safe monitoring function SBC in accordance to the definition in TS-37350-110-01-XF with instance 2]
5. Implementation of the standard safe monitoring function SOS in accordance to the definition in TS-37350-110-01-XF with instance 1 per axis]
6. Implementation of the standard safe monitoring function SREF in accordance to the definition in TS-37500-110-30-XF with instance 1 per axis]

**Note:**

The results of the safe monitoring functions are defined as follows:

* Compliance with limits and ranges = TRUE
* Limits and ranges excited = FALSE

### Parametrization of the safety functions

Safe monitoring functions can be configured and scaled during configuration and during commissioning of the module. The parameters are set by the configuration tool (Windows program) via appropriate input masks. Parameter ranges are limited by the configuration program in the possible and meaningful areas. Basically, the configuration tool is no safe program in the sense of SIL3 / EN61508.

Programmed parameters and activated functions must be validated on the target system

1. Validation of the application parameter]

The transfer of parameter data between the PC and the HRG\_AxB-system is via the system interface (USB or tunneling over EtherCAT). It is the responsibility of the commissioning engineer to verify that the selected USB port or Tooling port match the configuration program and the target module HRG\_AxB. For checking appropriate firmware functions are made available.

1. Correct transfer of the parameter data from programming system to target system]

The requirements according to EN 62061 are met

1. Requirement parameterization of safety functions according to EN62601]

## EtherCAT communication

The EtherCAT communication FW is divided into the

- cyclic part with non-safe and safe (FSoE) PDO’s

- acyclic part with SDO’s respective CoE objects and the EoE service for diagnoses and FW-update

### EtherCAT basic IP

In order to allow different communication cycles for the safe and non safe data a total of two sync units are foreseen for the cyclic communication and a further one for the mailbox/acyclic communication.

The EtherCAT slave stack of Beckhoff is used and implemented in a separate µP unit in order to achieve independence between the data sampling and processing process, general state machine and the bus state.

Data exchange with the sync units is time critical, a DMA IP connected to DPRAM units assigned to the two safety channels is to be used to allow parallel read and write of process data.

Non-safe data exchange shall although be executed preferable by fast parallel processing with DMA IP.

The DC signal output is to be used for synchronization; the signal must be readable on both safety channels.

1. Two sync units for PDO’s, one sync unit for mailbox]
2. EtherCAT slave stack independent from time critical implementation]
3. DMA IP via DPRAM used for process data exchange with the EtherCAT IP]
4. Non-safe data exchange between interface and EtherCAT IP by direct DMA process ]
5. DC signal used for synchronization with top-level control]

### EtherCAT cyclic process data exchange

The cyclic process data exchange is organized by PDO’s. For the non-safe part two mappable PDO’s are foreseen, for the safe part two PDO with fixed assigned data is to be implemented. The table below show the size and content of this PDO’s. The non-safe ones are connected äwith sync unit 0, the safe PDO with snyc unit 1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PDO** | **Size** | **Sync** | **Input** | **Output** |
| PDO 0 | 8 Byte input and 8 byte output, mappable to the available non-safe data | Sync 0 | STO Enable  Brake Enable  SS1 Enable  SS2 Enable | Act. Current  Position Enc 1  Position Enc 2  Orientation  Status  Torque |
| PDO 1 | 8 Byte input and 8 byte output, mappable to the available non-safe data | Sync 0 | STO Enable  Brake Enable  SS1 Enable  SS2 Enable | Act. Current  Position Enc 1  Position Enc 2  Orientation  Status  Torque |
| PDO 3 | 1 Byte input and 14 byte output | Sync 1 | STO  SBC  SS1 active  SS2 active  SREF active | Safe Position  Safe Speed |
| PDO 4 | 1 Byte input and 14 byte output | Sync 1 | Status | Safe Torque  Safe Black Channel |

1. PDO organization as in table under 7.5.1]
2. 2 mappable PDO for non-safe data]
3. 2 PDO for safe date with fixed content]

### EtherCAT acyclic service data exchange

For service data the acyclic CoE service is to be used. The below table show the total of CoE objects foreseen for implementation.

|  |  |  |
| --- | --- | --- |
| **Objects** | **Size** | **Content** |
| Tbd | All FSoE mandatory objects are to be implemented | Process data  Parameter  Status  Misc. |
| 10 | Device status and data | Status  FW-version  HW-version  Addresses  Serial number  Production date |
| 32 | Objects to be defined on a later stage, number is limited | Process data  Status  Encoder data  Sensor data  Tbd |

1. CoE objects to be implemented]
2. Mandatory objects for FSoE]
3. Total of 10 objects for device status and data]
4. Total of 32 objects for non-safe process and service data]

# Modes of Operation

Below the different possible modes of operation are listed and at the end of this chapter to be specified.

## Description of Operational Modes

### Stand alone with external GUI

In this mode the device runs still in stand-alone mode but is to be programmed and parametrized by use of the Safe-PLC respective Safe-PMT (see description in the chapter above) running on a PC. Access to the device can is by tunneling through the tooling interface of the main device and the internal data link main device / HRG\_AxB.

This mode is for diagnoses only. All sensor inputs are read and the data, including the safety data, are produced and accessible via the diagnoses interface. The maximum status is “Run Intern”.



Figure 3: Stand-alone operation mode

1. Local Mode = Stand-alone mode for parametrization and diagnoses]

### Top-level connection mode

This mode requires a active EterCAT connection with a host device. It enables the use of HRG\_AxB-slaves on the HRG robot controller for non-safe data exchange and on third party safe master devices such as the BBH FSoE master for safety functions.

The non-safe data to be exchanged can be selected by mapping the possible data to the non-safe PDO’s. Data is visible in the states “Bus RUN” and “SAFE BUS RUN”.

Parameters for the non-safe data are accessible via CoE objects and forwarded to the drive as start-up parameter.

The profiles of the safe data link is fixed. Te safe data are available in state “SAFE BUS RUN”. Activation of the internal monitoring functions by the FSoE master is by the safe input (output from the host side) and a reaction on the result is part of the output data.

Changeable safe parameters will be selected on the Safe-PLC application and build an integral part of the profile, allowing the parametrization to be adapted and executed through the FSoE master.

Safe parameter will be transferred during the start-up phase from the FSoE master to the HRG\_AxB using the standard FSoE process.



Figure 4: External safe master mode

1. BUS RUN and SAFE BUS RUN for cyclic non-safe data exchange with EtherCAT host]
2. SAFE BUS RUN for cyclic safe data exchange with FSoE master]
3. Parametrization by CoE objects or SafePLC tool]
4. Parameter download using the FSoE Safe Parameters]

# Requirements

[[110.01.001: SIL 3 according to IEC 61508:2010] 14](#_Toc38986873)

[[110.01.002: Architecture categories 4 according to EN ISO 13849-1:2015] 14](#_Toc38986874)

[[110.01.003: Pl e according to EN ISO 13849-1:2015] 14](#_Toc38986875)

[[110.01.004: EU Type certification] 14](#_Toc38986876)

[[110.01.005: EN 61508:2010, EN 13849-1:2015, EN 60204:2006 + A1:2009, EN 62061:2015, EN 50178:1997 Basic normative for type certification] 14](#_Toc38986877)

[[110.01.006: EN 61800-5-2:2016. EN 61800-3:2004 + A1:2012, EN 61000-6-2:2005, EN 61000-6-7:2015, EN574 Additional normative for type certification] 14](#_Toc38986878)

[[110.01.007: UL type certification] 14](#_Toc38986879)

[[110.01.008: Life cycle 10 years] 14](#_Toc38986880)

[[110.01.009: Proof test interval 10 years] 14](#_Toc38986881)

[[110.01.010: Failure detection and acceptance time 3 ms] 14](#_Toc38986882)

[[110.01.011: Cycle time device: 1 ms] 15](#_Toc38986883)

[[110.01.012: Cycle time FSoE: 0,5 ms] 15](#_Toc38986884)

[[110.01.013: Fast channel cycle time 1 ms] 15](#_Toc38986885)

[[110.01.014: EtherCAT communication cycle time 125 µs] 15](#_Toc38986886)

[[110.01.015: Completion of self-test routines 1 h] 15](#_Toc38986887)

[[110.01.016: Monitoring of over- and undervoltage µP-Systems <50 ms] 15](#_Toc38986888)

[[110.01.017: Monitoring of over- and undervoltage of channel A/B <50 ms] 15](#_Toc38986889)

[[110.01.018: Operability test of safe outputs <50 ms] 15](#_Toc38986890)

[[110.01.019: Max cut-off time for dynamic output test 600 µs] 15](#_Toc38986891)

[[110.01.020: Worst case time for false output status 4 ms] 15](#_Toc38986892)

[[110.01.021: Cycle time safe Position and speed data: 1 ms] 16](#_Toc38986893)

[[110.01.022: Cycle time Safe Torque: ≥1 ms] 16](#_Toc38986894)

[[110.01.023: Mean value filter (for settings see the encoder dialogue in SafePLC2): 0 – 32 ms] 16](#_Toc38986895)

[[110.01.024: Black Channel Safe Data: ≥ 1ms] 16](#_Toc38986896)

[[110.01.025: FSoE Input data to STO, SBC Output: 1,5 ms] 16](#_Toc38986897)

[[110.01.026: Cycle time non-safe orientation data: ≥ 125 µs] 16](#_Toc38986898)

[[110.01.027: Cycle time non-safe position of the two encoders: ≥ 125 µs] 16](#_Toc38986899)

[[110.01.028: Cycle time non-safe current: ≥ 125 µs] 16](#_Toc38986900)

[[110.01.029: Cycle time non-safe serial output: ≥ 250 µs] 16](#_Toc38986901)

[[110.01.030: Dimension of the Board 70 x 40 mm, tbd] 18](#_Toc38986902)

[[110.01.031: Tbd at a later stage] 18](#_Toc38986903)

[[110.01.032: Type of Current sensors – connector: tbd at a later stage, latching, reverse polarity protection required] 18](#_Toc38986904)

[[110.01.033: Encoder connector: : tbd at a later stage] 18](#_Toc38986905)

[[110.01.034: Type of Orientation sensor – connector: tbd at a later stage, latching, reverse polarity protection required] 18](#_Toc38986906)

[[110.01.035: Type of Black Channel data connector: tbd at a later stage, latching, reverse polarity protection required] 18](#_Toc38986907)

[[110.01.036: Type of LED stripe connector: tbd at a later stage, latching, reverse polarity protection required] 18](#_Toc38986908)

[[110.01.037: EtherCAT connector connector: tbd at a later stage, standard required] 18](#_Toc38986909)

[[110.01.038: EtherCAT mandatory LED – position tbd, mandatory, must be visible] 18](#_Toc38986910)

[[110.01.039: Status RGB LED, Position tbd] 18](#_Toc38986911)

[[110.01.040: Environmental temperature -0°C …85°C for board] 19](#_Toc38986912)

[[110.01.041: Clime class 3K3 EN 60721-3-1] 19](#_Toc38986913)

[[110.01.042: Protection class: IP20; Connectors: IP00 according to EN 60529] 19](#_Toc38986914)

[[110.01.043: max appl. height 2000m] 19](#_Toc38986915)

[[110.01.044: Pollution class 1 EN60664-1] 19](#_Toc38986916)

[[110.01.045: Mechanical stress shock level in accordance to EN 61800-2, IEC 60721‑3‑3 Klasse 3M1] 19](#_Toc38986917)

[[110.01.046: Mechanical stress vibration level in accordance to IEC 61131-2, 5.88 m/s2, 10~60Hz] 19](#_Toc38986918)

[[110.01.047: Electrical safety standard EN61800-5-1, EN 50178] 20](#_Toc38986919)

[[110.01.048: Supply voltage 24VDC, tolerance ±20%] 20](#_Toc38986920)

[[110.01.049: Worst case supply voltage 230V (SELV/PELV)] 20](#_Toc38986921)

[[110.01.050: Fuse 3A for the 48V power supply] 20](#_Toc38986922)

[[110.01.051: EMI standard for tests EN 61800, EN 55011] 20](#_Toc38986923)

[[110.01.052: EMI standard for limit value definition EN 62061] 20](#_Toc38986924)

[[110.01.053: EMI test level high, 4 kV] 20](#_Toc38986925)

[[110.01.054: Number of internal STOchannels: 2 of 3 (high power a) ) or 2 (low power b) )] 23](#_Toc38986926)

[[110.01.055: Two-channel equivalent SIL 3 Kat. 4 PL e] 23](#_Toc38986927)

[[110.01.056: Voltage loss STO ≤ tbd mV] 23](#_Toc38986928)

[[110.01.057: Capacitive load STO ≤ 10nF] 23](#_Toc38986929)

[[110.01.058: Resistive load STO ≥ tbd Ω] 23](#_Toc38986930)

[[110.01.059: Inductive load STO tbd H] 23](#_Toc38986931)

[[110.01.060: Leakage current STO-A < tbd mA] 23](#_Toc38986932)

[[110.01.061: Permanent short-cut protection STO < 2Ω] 23](#_Toc38986933)

[[110.01.062: Protection against other supply voltage STO: Ufremd ≤ +500V] 23](#_Toc38986934)

[[110.01.063: Test pulse duration STO ≤ 0,5ms in stop mode only] 23](#_Toc38986935)

[[110.01.064: Test relation STO 1x every 8h] 23](#_Toc38986936)

[[110.01.065: Detection of STO short cut on all 3 switches by the two safety channel] 23](#_Toc38986937)

[[110.01.066: Number of safe brake channels: 1] 24](#_Toc38986938)

[[110.01.067: Characteristic of output: dual channel] 25](#_Toc38986939)

[[110.01.068: Rated voltage 48 VDC] 25](#_Toc38986940)

[[110.01.069: Min. voltage 21 V, max. voltage 56 V] 25](#_Toc38986941)

[[110.01.070: Worst case supply voltage 60 V] 25](#_Toc38986942)

[[110.01.071: Fuse on supply 3 A] 25](#_Toc38986943)

[[110.01.072: Rated output current 1,5 A] 25](#_Toc38986944)

[[110.01.073: Max. inductive load 0,8 J] 25](#_Toc38986945)

[[110.01.074: Max. capacitive load 100nF] 25](#_Toc38986946)

[[110.01.075: Output pulse frequency 125 Hz] 25](#_Toc38986947)

[[110.01.076: Switching time on one channel 200 µs] 25](#_Toc38986948)

[[110.01.077: Switching time all channels 400 µs] 25](#_Toc38986949)

[[110.01.078: SIL 3 / PI e (following EN 61508, EN ISO 13849) has to be achieved with two encoders] 26](#_Toc38986950)

[[110.01.079: Interface for two external encoder] 26](#_Toc38986951)

[[110.01.080: The external interface allows the encoder type BISS-C] 26](#_Toc38986952)

[[110.01.081: Multi-slave = preferable configuration] 26](#_Toc38986953)

[[110.01.082: SSI input signal level are RS422 compatible] 26](#_Toc38986954)

[[110.01.083: Variable SSI Data length from 12 to 28 bit] 26](#_Toc38986955)

[[110.01.084: Master operation mode for BISS-C] 26](#_Toc38986956)

[[110.01.085: Clock rate: 2000 kHz] 26](#_Toc38986957)

[[110.01.086: Binary or gray code selection] 26](#_Toc38986958)

[[110.01.087: Monitoring of encoder supply voltages required] 26](#_Toc38986959)

[[110.01.088: Number of external encoder interface 1 or 2] 28](#_Toc38986960)

[[110.01.089: Safe position and speed computing] 28](#_Toc38986961)

[[110.01.090: Type of encoder on external interface: SSI, BISS-C] 28](#_Toc38986962)

[[110.01.091: HRG\_AxB Resolution on speed signal 216] 28](#_Toc38986963)

[[110.01.092: HRG\_AxB Resolution on position signal 231] 28](#_Toc38986964)

[[110.01.093: Encoder supply voltages on external encoder interface 5V] 28](#_Toc38986965)

[[110.01.094: Encoder supply voltage tolerance on external encoder interface +/- 10%] 28](#_Toc38986966)

[[110.01.095: Encoder supply current: 300 mA] 28](#_Toc38986967)

[[110.01.096: Allowed encoder combinations = 2 x single, data type binary + gray-code, min ratio] 28](#_Toc38986968)

[[110.01.097: Number of external sensor interface for safe black channel 2] 31](#_Toc38986969)

[[110.01.098: Type of encoder on external interface: SPI] 31](#_Toc38986970)

[[110.01.099: Sensor supply voltages on external sensor interface 5V] 31](#_Toc38986971)

[[110.01.100: Sensor supply voltage tolerance on external sensor interface +/- 10%] 31](#_Toc38986972)

[[110.01.101: Sensor supply current: 300 mA] 31](#_Toc38986973)

[[110.01.102: Allowed sensor combinations: tbd by HRG on a later stage] 31](#_Toc38986974)

[[110.01.103: Data processing: tbd by HRG on a later stage] 31](#_Toc38986975)

[[110.01.104: Number of external sensor interface for non-safe input data: 1-2, tbd] 32](#_Toc38986976)

[[110.01.105: Type of external interface: SPI or I2C] 32](#_Toc38986977)

[[110.01.106: Sensor supply voltages on external sensor interface: 5V] 32](#_Toc38986978)

[[110.01.107: Sensor supply voltage tolerance on external sensor interface: +/- 10%] 32](#_Toc38986979)

[[110.01.108: Sensor supply current: 300 mA] 32](#_Toc38986980)

[[110.01.109: Sampling cycle time: ≥ 125 µs] 32](#_Toc38986981)

[[110.01.110: Data forwarding: direct mapping to PDO] 32](#_Toc38986982)

[[110.01.111: Number of external sensor interface for non-safe output data: 2] 33](#_Toc38986983)

[[110.01.112: Type of external interface: UART like, see data sheet] 33](#_Toc38986984)

[[110.01.113: Supply voltages on external interface: 5V] 33](#_Toc38986985)

[[110.01.114: Supply voltage tolerance on external interface: +/- 10%] 33](#_Toc38986986)

[[110.01.115: Max. supply current: 3.5 A for both interfaces combined] 33](#_Toc38986987)

[[110.01.116: Sampling cycle time: ≥ 125 µs] 33](#_Toc38986988)

[[110.01.117: Data forwarding: direct mapping from PDO to the output interface] 33](#_Toc38986989)

[[110.01.118: EtherCAT slave IP and HW on HRG\_AxB] 34](#_Toc38986990)

[[110.01.119: Mappable PDO’s for non-safe data] 34](#_Toc38986991)

[[110.01.120: FSoE for safe data transfer] 34](#_Toc38986992)

[[110.01.121: CoE for parameter and diagnostic data] 34](#_Toc38986993)

[[110.01.122: EoE for diagnostic and tooling data, FW-update] 34](#_Toc38986994)

[[110.01.123: DC for synchronization with top-level control 34](#_Toc38986995)

[[110.01.124: Local data interface technology: SPI, I2C and UART] 35](#_Toc38986996)

[[110.01.125: Communication mode on internal data interface = safe / non-safe data exchange] 35](#_Toc38986997)

[[110.01.126: Protocol on local data interface: tbd, 1 fixed protocol per data interface] 35](#_Toc38986998)

[[110.01.127: Duty cycle for data exchange on internal data interface: ≥ 125 µs] 35](#_Toc38986999)

[[110.01.128: SPI parameter tbd on a later stage] 35](#_Toc38987000)

[[110.01.129: I2C parameter tbd on a later stage] 36](#_Toc38987001)

[[110.01.130: UART parameter tbd on a later stage] 36](#_Toc38987002)

[[110.01.131: Safety related run-time system in accordance to the target SIL /Pl] 38](#_Toc38987003)

[[110.01.132: Safety related data sampling and processing adequate to the target SIL /Pl] 38](#_Toc38987004)

[[110.01.133: Parameterization and selection of the functionality in the limits defined for each type of monitoring function] 38](#_Toc38987005)

[[110.01.134: Implementation of the several standard monitoring functions according to the SMX base system] 38](#_Toc38987006)

[[110.01.135: Provision of Functions and SW tools for configuration / programming, Diagnostics and FW-update] 38](#_Toc38987007)

[The operational system of the HRG\_AxB controls the actual state, organize the local data sampling and output, coordinates the two safety channels with each other, ensures the execution of all subprocesses including diagnostic and provides the correct and in-time communication with the top-level control. Therefore, the OS consists of the following modules: 38](#_Toc38987008)

[General state machine with at least the following states: 38](#_Toc38987009)

[- startup, init 38](#_Toc38987010)

[- parameter read and check 38](#_Toc38987011)

[- internal sync 38](#_Toc38987012)

[- local run 38](#_Toc38987013)

[- bus run 38](#_Toc38987014)

[- safe data run 38](#_Toc38987015)

[- error 38](#_Toc38987016)

[The OS takes care of the process image with passivate and active state depending from the actual state and data contend. 38](#_Toc38987017)

[For the correct timing in the run states an interrupt timing grid is to be implemented. Data sampling, processing and cross-check with alternate channel is organized by this time grid. 38](#_Toc38987018)

[Synchronization with the top-level control is a subset of the OS functionality. The synchronization is based on the DC service. Data sampling is coordinated by a shift time parameter in relation to the timing event. 39](#_Toc38987019)

[Beside this functional states and processes, the OS is supervising the correct run of all cyclic and non-cyclic processes required to achieve the target SIL / Pl. This includes but is not limited to: 39](#_Toc38987020)

[- 2-channel data read and processing with cross-check of results 39](#_Toc38987021)

[- check of the correct call of all safety-relevant cyclic processes 39](#_Toc38987022)

[- control of the acyclic safety-related diagnoses 39](#_Toc38987023)

[- cyclic update of the safe process input and output image 39](#_Toc38987024)

[- monitoring of the safe top-level communication task 39](#_Toc38987025)

[[110.01.136: OS state machine with at least the states init, param, sync intern, local run, bus run, safe bus run, error] 39](#_Toc38987026)

[[110.01.137: Timing grid for channel synchronization and time equidistant data sampling] 39](#_Toc38987027)

[[110.01.138: Synchronization IP for coordination with top-level-control] 39](#_Toc38987028)

[[110.01.139: 2-channel data read and processing with cross-check of results] 39](#_Toc38987029)

[[110.01.140: OS provides correct run of all safety-relevant cyclic and acyclic processes] 39](#_Toc38987030)

[[110.01.141: OS controls the complete and correct run of all safety-related diagnoses] 39](#_Toc38987031)

[[110.01.142: OS controls cyclic update of process input and output image] 39](#_Toc38987032)

[[110.01.143: OS monitors the communication with top-level control] 39](#_Toc38987033)

[Data sampling and processing is divided into the safety-related part and the non-safe part. Both are coordinated by the OS and time equidistant data sampling is ensured. 40](#_Toc38987034)

[The below listed safety-related data sampling and processing to be implemented in the first stage of the HRG\_AxB project. 40](#_Toc38987035)

[[110.01.144: Safe position data sampling and processing function] 40](#_Toc38987036)

[[110.01.145: Safe speed data sampling and processing function] 40](#_Toc38987037)

[[110.01.146: Safe torque data sampling and processing function] 40](#_Toc38987038)

[[110.01.147: Safety Black Channel data sampling and processing function] 40](#_Toc38987039)

[The non-safety data are sampled and forwarded to the communication unit as native data only. The below listed data are sampled by the HRG\_AxB. 41](#_Toc38987040)

[[110.01.148: 3-phase current data sampling and processing function] 41](#_Toc38987041)

[[110.01.149: Orientation data sampling and processing function] 41](#_Toc38987042)

[[110.01.150: Temperature data sampling and processing function] 41](#_Toc38987043)

[[110.01.151: Implementation of the standard safe monitoring function STO in accordance to the definition in TS-44400-130-07-XF with instance 2] 42](#_Toc38987044)

[[110.01.152: Implementation of the standard safe monitoring function SS1 in accordance to the definition in TS-37350-110-01-XF with instance 4 per axis] 42](#_Toc38987045)

[[110.01.153: Implementation of the standard safe monitoring function SS2 in accordance to the definition in TS-37350-110-01-XF with instance 4 per axis] 42](#_Toc38987046)

[[110.01.154: Implementation of the standard safe monitoring function SBC in accordance to the definition in TS-37350-110-01-XF with instance 2] 42](#_Toc38987047)

[[110.01.155: Implementation of the standard safe monitoring function SOS in accordance to the definition in TS-37350-110-01-XF with instance 1 per axis] 42](#_Toc38987048)

[[110.01.156: Implementation of the standard safe monitoring function SREF in accordance to the definition in TS-37500-110-30-XF with instance 1 per axis] 42](#_Toc38987049)

[[110.01.157: Validation of the application parameter] 43](#_Toc38987050)

[[110.01.158: Correct transfer of the parameter data from programming system to target system] 43](#_Toc38987051)

[[110.01.159: Requirement parameterization of safety functions according to EN62601] 43](#_Toc38987052)

[[110.01.160: Two sync units for PDO’s, one sync unit for mailbox] 44](#_Toc38987053)

[[110.01.161: EtherCAT slave stack independent from time critical implementation] 44](#_Toc38987054)

[[110.01.162: DMA IP via DPRAM used for process data exchange with the EtherCAT IP] 44](#_Toc38987055)

[[110.01.163: Non-safe data exchange between interface and EtherCAT IP by direct DMA process ] 44](#_Toc38987056)

[[110.01.164: DC signal used for synchronization with top-level control] 44](#_Toc38987057)

[[110.01.165: PDO organization as in table under 7.5.1] 45](#_Toc38987058)

[[110.01.166: 2 mappable PDO for non-safe data] 45](#_Toc38987059)

[[110.01.167: 2 PDO for safe date with fixed content] 45](#_Toc38987060)

[[110.01.168: CoE objects to be implemented] 46](#_Toc38987061)

[[110.01.169: Mandatory objects for FSoE] 46](#_Toc38987062)

[[110.01.170: Total of 10 objects for device status and data] 46](#_Toc38987063)

[[110.01.171: Total of 32 objects for non-safe process and service data] 46](#_Toc38987064)

[[110.01.172: Local Mode = Stand-alone mode for parametrization and diagnoses] 47](#_Toc38987065)

[[110.01.173: BUS RUN and SAFE BUS RUN for cyclic non-safe data exchange with EtherCAT host] 49](#_Toc38987066)

[[110.01.174: SAFE BUS RUN for cyclic safe data exchange with FSoE master] 49](#_Toc38987067)

[[110.01.175: Parametrization by CoE objects or SafePLC tool] 49](#_Toc38987068)

[[110.01.176: Parameter download using the FSoE Safe Parameters] 49](#_Toc38987069)