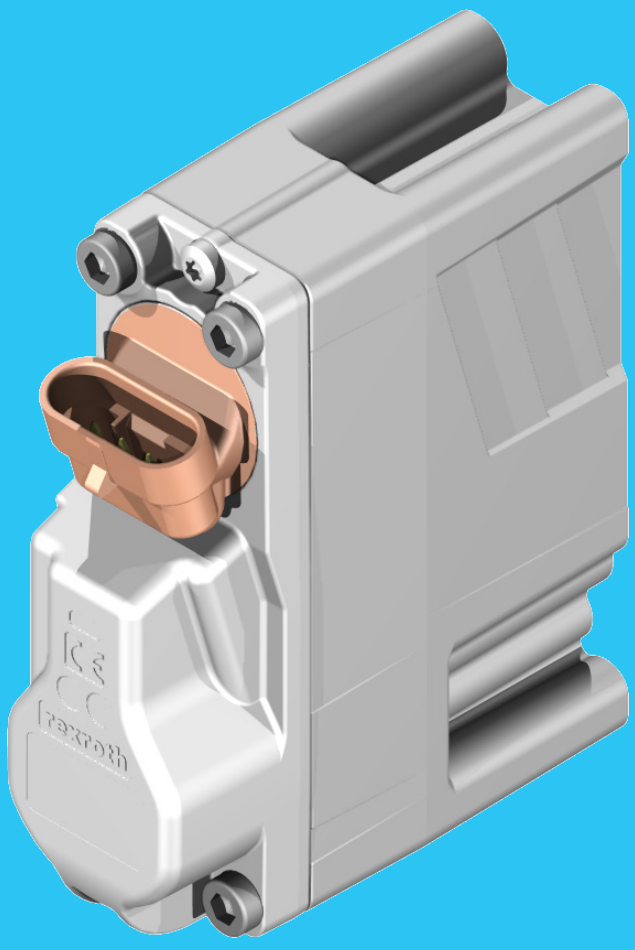
rexroth
A Bosch Company

Safety-relevant
project planning instructions
according to ISO 25119

Pilot Module EHS4



RE 66157-01-B/2022-01-18, replaces: 2021-03-01, EN

The original instruction manual was created in the English language.

Contents

1 About this documentation

1.1 Validity of the documentation

This documentation is valid for the following products:

- Pilot Module EHS4
  - R917012361

As umbrella term for “Pilot Module EHS4” the designation “OBE” will be used in the following.

This safety manual gives instruction on how to safely integrate the SBx4-EHS4 into a safety system, for tractor and machinery for agriculture and forestry (ISO 25119), while ensuring the compliance to the relevant functional safety standards, see [A1].

▶ Read this documentation completely and, in particular, the chapter 2 “Safety instructions” and the chapter 3 “General instructions on property and product damage” in the related instruction manual 66170-B before you start working with the product.

1.2 Required and supplementary documentation

▶ Only commission the Pilot Module if the documentation marked with the book symbol 🕮 is available to you and you have understood and observed it.

Table 1: Applicable standards

	Ref.	Title	Release Date
🕮	[A1]	ISO 25119-1, -2, -3, -4	Part 1, 3, 4: 2018 Part 2: 2019

Table 2: Required and supplementary documentation

	Ref.	Title	Document number	Document type
🕮	[R1]	**Pilot Module EHS4** Technical customer documentation (TKU)	66157-02-B	Instruction manual
🕮	[R2]	**Load-sensing directional valves in sandwich plate design SB24-EHS, SB34-EHS** Contains the permissible technical data, ports, main dimensions and circuit diagrams of standard versions.	66171	Data sheet
🕮	[R3]	**Load-sensing control block SB24/34 for mobile applications** Contains important information on the safe and proper transport, assembly, commissioning, maintenance and removal of the SB24/34 control block.	66170-B	Instruction manual

1.3 Prerequisites

The OBE has been developed according to the relevant safety standard ISO 25119, see [A1].

1.4 Abbreviations

This documentation uses the following abbreviations:

Table 3: Abbreviations

Abbreviation	Meaning
CAT	Category
DC	Diagnostic Coverage
EHS	Pilot operated electrohydraulic actuating unit
FSG	Functional Safety Goal
HW	Hardware
$MTTF_D$	Mean time to dangerous failure
OBE	Pilot Module (On-board electronics)
PWM	Pulse Width Modulation
SF	Safety Function
SRL	Software Requirement Level
SW	Software
SBx4	Control valves SB24 and SB34

2 Aim and application

This manual indicates requirements that need to be satisfied in integrating the OBE to the machine safety system.
This document contains:
1. General description of the OBE
2. OBE safety function and functional safety characteristics

This document contains important safety information. It is essential that all relevant instructions and guidances provided in this document are observed, understood and followed by machine manufacturers to reach the required conformity in accordance with ISO 25119.

The machine manufacturer is responsible for performing a risk analysis of the machine and determining the possible machine safety functions.

It is machine manufacturer’s responsibility to evaluate the complete safety-related system and to determine the suitability of OBE for any machine safety functions.

The OBE is 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 OBE must be switched off or reset at least once within 24 h.

3 Description of the OBE

The block diagram of the OBE is shown in Fig. 1.

The functionality of the software contains:
- Control of EHS pilot valve
- Control loop for the main spool
- CAN interface
- Diagnostics and error management

The OBE is installed in SBx4 valve slices to provide the right amount of pilot oil to move the spool of the main stage into the right position. Therefor a closed loop control circuit is realized with the Pilot valve itself powered by the OBE control board and the position sensor for the main spool.

The OBE processes the input signal of the position sensor, compares it with the setpoint sent by the main controller of the machine via CAN bus, performs a position control algorithm and actuates the pilot valve accordingly.

The mentioned software libraries are flashed to the OBE. The operational specification is described in [R1].

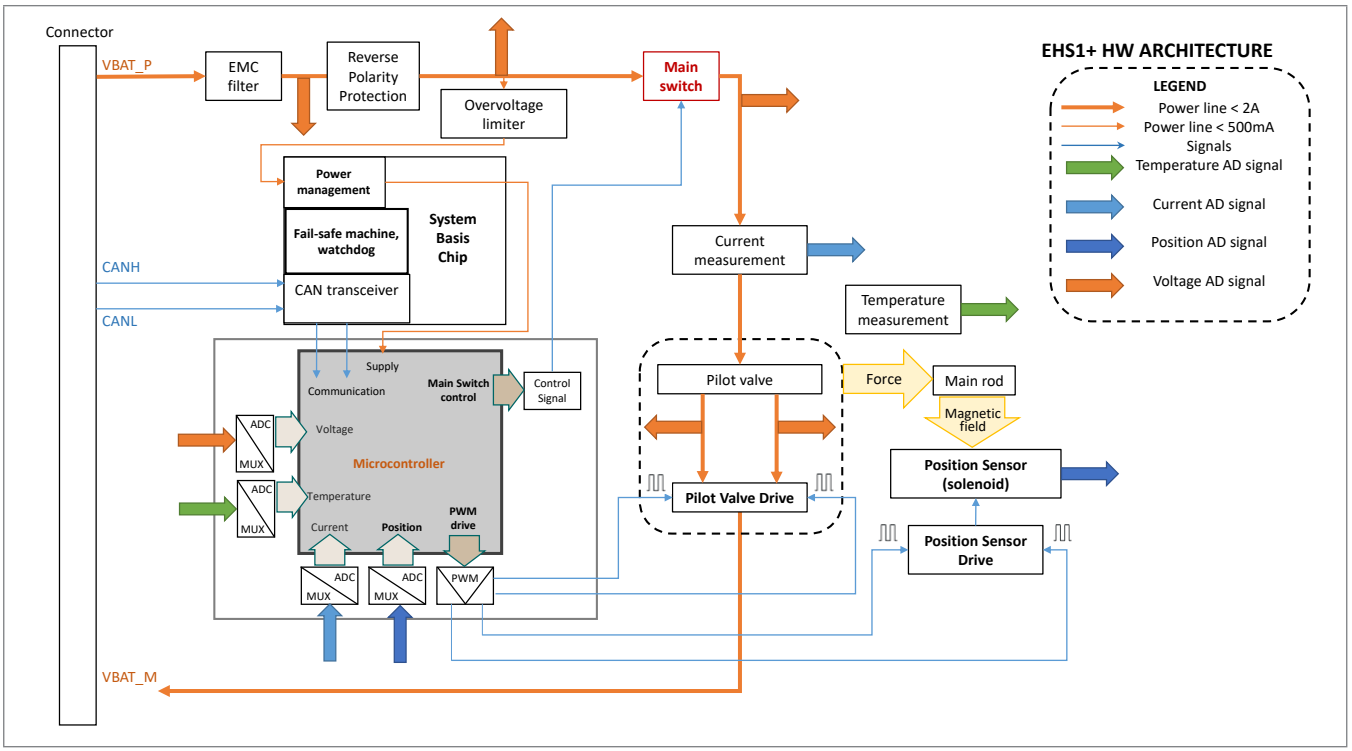


Fig. 1: System overview of the OBE

4 Safety concept

4.1 Hazardous events

Hazardous events identified for the OBE within the the safety system, for tractor and machinery for agriculture and forestry (ISO 25119), are:

1. The pilot module applies force which prevents the spool to move in neutral position, when the neutral position is commanded.
2. The pilot module applies force to move the spool out of its neutral position although it's not commanded to do so.
3. The pilot module applies force to move the spool into wrong direction.
4. The pilot module applies force to move the spool out of its neutral position in one direction as commanded but with too much deviation.

4.2 Safety functions of the OBE

The safety concept for the OBE covers the following four Functional Safety Functions.

4.2.1 SF1: Safe shutdown of the oil flow, if stop is requested

The main spool shall move back to neutral position within the specified time, if requested. If the main spool does not move back to neutral position on time or if a failure is detected, the main spool will be forced back to neutral position via safety measures (details see chapter 5).

NOTICE! Neutral position is reached, if the main spool enters the neutral coverage zone and does not leave it again.

Safe state: The pilot solenoids are de-energized.

4.2.2 SF2: Avoid oil flow, if no oil flow is requested

The main spool shall not move out of neutral position, if not intended. If the main spool moves out of the neutral position unintendedly or if a failure is detected, the main spool shall be brought back to neutral position. (details see chapter 5)

NOTICE! Neutral position is left, if the main spool moves out of the neutral coverage zone into any direction.

Safe state: Main spool in neutral position.

4.2.3 SF3: Avoid oil flow into unintended direction, if oil flow is requested

The main spool shall move into the intended direction, if deflection is requested out of neutral position. If the main spool is in the wrong direction or if a failure is detected, the main spool shall be brought back to neutral position. (details see chapter 5)

NOTICE! Deflection starts by leaving the neutral coverage zone of the valve.

Safe state: Main spool in neutral position.

4.2.4 SF4: Avoid higher oil flow than requested

If deflected, the main spool shall not deflect more than 10% over setpoint in any direction. This is to avoid an unexpected high speed of an implement. If the deflection is more than 10% over the setpoint (over-deflected), or if a failure is detected, the main spool shall be brought back to neutral position (details see chapter 5).

Safe state: The pilot solenoids are de-energized.

4.3 Safety related characteristics of the OBE

This chapter shows safety-related characteristics of the OBE (Category, $MTTF_D$, DCavg, and SRL) in order to support the design of the safety system, for tractor and machinery for agriculture and forestry (ISO 25119).

According to ISO 25119-2:2019, the design of the OBE corresponds to Category 2 for the safety function 1 to 3 (SF1 – 3) and Category 1 for the safety function 4 (SF4). The $MTTF_D$ and DC_{avg} of all safety functions for the given temperature profile are as follows:

Temperature [°C]	Self heating [°C]	Working hours [%]	$MTTF_D$ [1] [years]	DC_{avg} [%]
–35...59	15	10	210	72
59...80	15	79		
80...97	15	10		
97...110	15	1		

[1] Assumption on mission profile
OBE can be powered on for 24 hours per day @ 16 V.
Life time of OBE is 10000 hours.

The OBE software fulfills the requirements of SRL 1 according to ISO 25119-3:2018.

OBE is able to support a safety level up to AgPL c for SF1 to SF3 and AgPL b for SF4, if integrated properly into a safety system, for tractor and machinery for agriculture and forestry (ISO 25119), following all the relevant instructions of this document.

5 OBE reaction on failure detection

If an OBE detects a serious failure that can lead to a safety risk, it cuts the power line to the power stages of the pilot valve solenoids via a built-in switch.

Consequently, the centering springs force the main spool to move into its neutral position and prevent the oil flow to the attached hydraulic consumer.

The power stages will stay unpowered until the OBE gets reset and detects no failure.

The OBE remains in this state even if the main control unit of the machine commands a movement of the corresponding hydraulic consumer.

On failure detection, the OBE sends an error message via CAN bus in order to inform other participants of the CAN communication system about its current status.

CAUTION! In certain failure cases, it is impossible for OBE to enter the safe state. The machine controller shall closely monitoring the CAN error messages and react to these failures to bring the machine into safe state depending on machine use cases (details see chapter 4 of [R1]).

6 Timing behaviour in normal operating mode

Trigger Event	Diagnostic trouble code	Fault description	Internal Trigger to separate power stages from power supply after failure detection	Electrical current in power stages is sufficiently low	Valve spool in neutral position (if not sticking)
Internal electrical or electronic failure	4085.12	NVM/checksum error, output stage fault, position transducer fault	30 msec	Depends on setpoint! Worst case is in float (highest current). Current = 0 mA in 35 msec (measured with connected pilot valve @25°C) (Note: plus chosen ramp time if configured)	Actuation time float to neutral (worst case) Oil SAE 10W40 @–30°C = 5000 msec @0°C = 130 msec @60°C = 60 msec (Note: plus chosen ramp time if configured)
Valve failure	4085.07	Main spool not in neutral at power up	30 msec		
		Main spool can't return to neutral	@>20°C 1500 msec; @–30°C 6000 msec (Note: Detection adapted over temperature because of oil viscosity)		
External CAN command "neutral"	–	–	4 ms (Note: plus chosen ramp time if configured)		
CAN command missing	2034.09	CAN command message not received within timeout counter	500 msec (Note: plus switch off ramp time; if ramp time is configured)		

Bosch Rexroth AG
Robert-Bosch-Straße 2
71701 Schwieberdingen
Germany
Phone +49 711 811-8481
info.ma@boschrexroth.de
www.boschrexroth.com

Your local contact person can be found at:
www.boschrexroth.com/addresses

Subject to change
RE 66157-01-B/2022-01-18