

	Asr6-Bw16 (BMW-FLM3)	Version main\20	Page 1 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Asr6-Bw16 (BMW-FLM3)

Freedom from interference analysis report

Version main\20

Approval of document

Name	Responsibility	Status	Date
Thomas Reichenecker	SWA/EES3	constructed	

Approval of template

Name	Responsibility	Status	Date
Martin Gottheil	MET	approved	25.4.18
D. Holinstat & R. Gospocic	MET EQM	Checked	25.4.18
Johannes Allgaier	MET	constructed	23.4.18

Revision history of document

Version	Date	Description	Author
main\20	12.05.2021	added StbM/SysMon interface	REICHENECKER
main\19	07.05.2021	1 OS application	REICHENECKER
main\18	14.04.2021	FLMT-5348: update of attribute "AL_ASIL" of decomposed requirements	REICHENECKER
main\17	03.03.2021	released version	REICHENECKER
main\16	03.03.2021	added Cdd to table 2	REICHENECKER
main\15	02.03.2021	- Justification of management of communication - removed decomposition for SysMon/AppM, ...	REICHENECKER
main\14	24.02.2021	- Merged ch. 3.4.8+3.4.11 and removed ch. 3.4.11 - added PduR, PBL	REICHENECKER

© Alle Rechte bei Marelli Automotive Lighting Reutlingen (Germany) GmbH. Jede Verfügungsbefugnis, wie Kopier- und Weitergaberecht, bei uns.

© Marelli Automotive Lighting Reutlingen (Germany) GmbH. All rights of disposal such as copying and passing on to third parties reserved.

 AL AUTOMOTIVE LIGHTING MARELLI ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 2 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Version	Date	Description	Author
main\13	23.02.2021	added - table 3 - references to review reports of KPIT safety documentation	REICHENECKER
main\12	19.02.2021	chapter numbering corrected	REICHENECKER
main\11	19.02.2021	draft chapters for CddSbc, Com, IoHwAb	REICHENECKER
main\10	18.02.2021	draft chapters for CddLed, CddSpi	REICHENECKER
main\9	17.02.2021	draft chapter for IoHwAbUser	REICHENECKER
main\8	16.02.2021	first draft chapter for IoHwAbUser	REICHENECKER
main\7	15.02.2021	added 'draft' watermark&label	REICHENECKER
main\6	12.02.2021	Update after 2nd review Galliano/Ferraro/Reichenecker	REICHENECKER
main\5	10.02.2021	Update after review Galliano/Ferraro/Reichenecker	REICHENECKER
main\4	05.02.2021	added hint for unintended interfaces	REICHENECKER
main\3	05.02.2021	minor extensions	REICHENECKER
main\2	04.02.2021	Draft incl. OS, RTE, SysMon	REICHENECKER
main\1	03.02.2021	First draft	REICHENECKER

File: SWDD_Asr6-Bw16_FFI_Report.docx
Template Version \\main\2

 ALDE-RT/EE	 MARELLI	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 3 von 50
		Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Content

1.	Introduction	5
1.1.	Purpose	5
1.2.	Referenced documents	5
1.3.	Terms and definitions	6
2.	Freedom from interference	8
3.	Analysis.....	8
3.1.	BSW-Module OS: Operating System	11
3.1.1.	Non-safety relevant tasks	11
3.2.	RTE: AUTOSAR Runtime Environment	13
3.2.1.	Non-Safety relevant SW Elements.....	13
3.3.	SWC SysMon: System Monitoring	15
3.3.1.	BSW-Module Dem: Diagnostic Event Manager	15
3.3.2.	SWC Coding (BAC)	15
3.3.3.	SWC DiagM: Diagnostic Manager.....	16
3.3.4.	SWC CodM: Coding Manager	17
3.3.5.	SWC AppM: Application Manager	19
3.3.6.	SWC FctR: Function Router	20
3.3.7.	SWC SysVolt: Supply Voltage Monitoring	21
3.3.8.	SWC LsrSens: Laser Sensor Component.....	22
3.3.9.	SWC SigPrep: Signal Preparation.....	23
3.3.10.	SWC CtrlLed: Control LED	23
3.3.11.	SWC CtrlStp: Control Stepper	24
3.3.12.	SWC LaIntegration: 'Licht Aussen' Integration	25
3.3.13.	BSW-Module StbM: Synchronized Time Base Manager.....	26
3.4.	BSW-Module IoHwAbUser: I/O Hardware Abstraction User Interface.....	27
3.4.1.	Mounting Side Information Interface.....	27
3.4.2.	ECU Supply Voltage.....	28
3.4.3.	BSW-Module NvM: NVRAM Manager.....	29
3.4.4.	CddStp: Stepper Complex Driver	29
3.4.5.	SWC Bs (BAC): Basic Security	30
3.4.6.	SWC Coding (BAC)	31
3.4.7.	SWC CodM: Coding Manager	32
3.4.8.	SWC CtrlHss: High Side Switch Control.....	33
3.4.9.	SWC LsrSens: Laser Sensor Component.....	34
3.4.10.	SWC RSens: Resistor Sensor Component.....	35
3.4.11.	Pb21_PBL: Primary Bootloader.....	36
3.5.	CddLed: LED Complex Driver	38
3.5.1.	SWC CodM: Coding Manager	38
3.5.2.	SWC CtrlLed: Control LED	39
3.5.3.	SWC DiagM: Diagnostic Manager.....	40

 AL AUTOMOTIVE LIGHTING MARELLI ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 4 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.5.4.	SWC LsrSens: Laser Sensor Component	41
3.6.	CddSpi: Serial Peripheral Interface Complex Driver	42
3.6.1.	SWC CodM: Coding Manager	42
3.6.2.	CddStp: Stepper Complex Driver	43
3.7.	CddSbc: System Base Chip Complex Driver	45
3.7.1.	Reset Reason Interface	45
3.7.2.	BSW-Module Dem: Diagnostic Event Manager	46
3.8.	BSW-Module Com: Communication Services.....	48
3.8.1.	SWC SigPrep: Signal Preparation.....	48
3.8.1.	BSW-Module PduR: PDU Router	49
3.9.	BSW-Module IoHwAb: I/O Hardware Abstraction	50
3.9.2.	BSW-Module ADC: Analog/Digital Conversion	50

Illustrations

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

Tables

Table 1: Terms, Definitions and Abbreviations.....	7
Table 2: FLM3 Safety relevant software elements.....	9
Table 3: FLM3 Non-safety relevant software elements, connected to safety relevant software elements	10

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version main\20	Page 5 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

1. Introduction

1.1. Purpose

The purpose of this document is to provide evidence and details about the implementations that assure the freedom from interference between safety relevant and non-safety relevant software elements for the FLM3 Bw16 project.

1.2. Referenced documents

[ALSwDesignRules] AL Embedded Software Design Rules

[AUTOSAR] AUTOSAR Release 4.2.2, see <https://www.autosar.org> with following parts:

[AUTOSAR_1] AUTOSAR_EXP_FunctionalSafetyMeasures.pdf

[AUTOSAR_2] AUTOSAR_SWS_OS.pdf

[AUTOSAR_3] AUTOSAR_SWS_RTE.pdf

[FLMT-xxxx] Link to JIRA-Ticket no. xxxx of FLM3 project

[ISO] ISO 26262:2018

[KLH_FLM3]: DOORS FLM3_Kapitel_3.5.1_18_January_2019

[KPIT Safety Manual] KPIT Safety Manual with following parts:

[KPIT_SM_1] KPIT_Safety Approach.pdf

[KPIT_SM_2] KPIT Integration_Safety_Architecture_Design_V3.pdf

[KPIT_SM_3] KPIT Safety User Manuals

[MCU Safety Manual] Cypress Safety Manual

[SAR] Safety Analysis Report ECU FLM3

[SBC_DS] Infineon TLE9471 Datasheet

[SWRS] Software Requirement Specification ECU FLM3 with following parts:

[SWRS_1] DOORS SWRS

[SWRS_2] SWDD_Asr6-Bw16_SystemResources.xlsx

[SWRS_3] SWDD_Asr6-Bw16_Mem_Map.xlsx

[SWRS_4] UML model SWRS_Bw16.eapx

[SYRS]: System Requirement Specification ECU FLM3
DOORS SYRS

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 6 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

1.3. Terms and definitions

AL	Automotive Lighting
ASIL	Automotive Safety Integrity Level
AUTOSAR	AUT omotive O pen S ystem A rchitecture
B2CAN	BMW Body 2 CAN
BAC	BMW AUTOSAR Core
BSW	AUTOSAR Basic Software
CAN	Controller Area Network
CDD	Complex Driver Module
CRC	Cyclic Redundancy Check
E2E	End-to-end
ECC	Error correcting code
ECU	Electronic Control Unit
FFI	Freedom from interference
FTTI	Fault Tolerant Time Interval: Time interval where the system can safely tolerate the fault without violation of the system safety goal
HL	Headlight
HW	Hardware
IOS	Inter OS-Application Communication
ISR	Interrupt Service Routine
LB	Low Beam
MCAL	Microcontroller Abstraction Layer
NM	Network Management
OS	Operating system
RTE	AUTOSAR Runtime Environment
SW	Software
SWC	AUTOSAR Software component
SWFMEA	Software failure mode and effect analysis

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 7 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

SWRS	Software requirements specification
SYRS	System requirements specification
TI	Turn Indicator

Table 1: Terms, Definitions and Abbreviations

 AL AUTOMOTIVE LIGHTING MARELLI ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 8 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

2. Freedom from interference

According to ISO 26262 (see [ISO]), if the embedded software consists of software components with different ASIL ratings, then either the entire software must be developed according to the highest ASIL, or freedom from interference shall be ensured for software components with a higher ASIL rating from elements with a lower ASIL rating. Furthermore, the ISO 26262 standard provides faults, which cause interference between software components. The faults are grouped as follows:

- Memory
- Timing and Execution
- Exchange of Information

3. Analysis

In the following sub-chapters, it's going to be detailed what prevention, or detection and mitigation has been implemented based on the general protection mechanisms (see below) for every safety relevant SW-Element that has interfaces with non-safety relevant SW-Elements.

Regarding interference of safety relevant SW-Elements with non-safety relevant SW-Elements, which have no interface (unintended interface), general protection of the safety relevant SW-Elements, provided by the Operating System (OS, see chapter 3.1) , Runtime Environment (RTE, see chapter 3.2) and System Monitoring (SysMon, see chapter 3.3) apply as well.

The general protection mechanisms are

- **Memory protection:**
CRC checks for safety relevant parameters with recovery mechanisms and fail safe reactions offered by SysMon (see [SWRS_1], chapter 4.4.3.4.2.2).
- **Timing protection:**
fixed priority-based preemptive scheduling offered by OS. The FLM3 project OS- and RTE-configuration prevents from blocked execution of safety relevant SW-Elements caused by non-safety relevant SW-Elements because of priority inversion, deadlocks and livelocks e. g. caused by shared resources (background and rationale see [AUTOSAR_2], chapter 7.7.2 and [AUTOSAR_1], KPIT safety approach see [KPIT_SM_2], FLM3 project OS configuration see [SWRS_2]).
In addition, execution of safety relevant SW-Elements blocked by non-safety relevant category 2 ISRs is mitigated by the watchdog concept (see [KPIT_SM_2], [SAR]).
- **Communication protection:**
consistency checks of dependent or redundant information with safe reaction offered by SysMon (see [SWRS_1], chapter 4.4.3.4.2.2). This covers obsolete (not updated), incorrect (within range) or wrong (out of range) information,

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 9 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

caused by loss, delay, insertion, masquerade or corruption of information and generated inside directly connected non-safety relevant software elements as well as indirectly connected non-safety relevant software elements.

Examples might be a diagnostic service input to a non-safety relevant software element or obsolete (not updated) calculations inside a non-safety relevant software element with unwanted impact on safety related target settings.

Because communication protection is covered either in mitigation of data corruption (memory) or mitigation of incorrect synchronization between software elements (timing), there exist no dedicated consideration of incorrect information (communication) within the following sub-chapters.

Table 2 shows the functional safety relevant software elements, their assigned ASIL and whether they are connected to non-safety relevant SW-Elements:

Software Elements	Supplier	ASIL	connected to non-safety relevant elements
OS	KPIT	ASIL B	X
RTE	KPIT	ASIL B	X
WdgM	KPIT	ASIL B	
Com	KPIT	ASIL B	X
WdgIf	KPIT	ASIL B	
IoHwAb_User	AL	ASIL B	X
IoHwAb	KPIT	ASIL B	X
GPT	Cypress	ASIL B	
MCU	Cypress	ASIL B	
DIO	Cypress	ASIL B	
PORT	Cypress	ASIL B	
PWM	Cypress	ASIL B	
CddSbc	AL	ASIL B	X
CddSpi	AL	ASIL B	X
CddLed	AL	ASIL B	X
Cdd	KPIT	ASIL B	
E2E Lib	KPIT	ASIL B	
CRC	KPIT	ASIL B	
SysMon	AL	ASIL B	X

Table 2: FLM3 Safety relevant software elements

Table 3 shows the non-safety relevant software elements, which are connected directly to safety relevant software elements and their assigned ASIL:

Software Elements	Supplier	ASIL
ADC	Cypress	QM / (ASIL B ^{*)})
AppM	AL	QM
Bs (BAC)	BMW	
CddStp	AL	
Coding (BAC)	BMW	
CodM	AL	QM
CtrlHss	AL	
CtrlLed	AL	QM
CtrlPxl	AL	
CtrlStp	AL	
Dem	KPIT	(ASIL B ^{*)})
DiagM	AL	
FctR	AL	QM
LaIntegration	BMW	QM
LsrSens	AL	
NvM	KPIT	QM / (ASIL B ^{*)})
PBL	AL	QM
PduR	KPIT	QM / (ASIL B ^{*)})
PxA	AL	
SensM	AL	QM
SigPrep	AL	
StatM	AL	
StbM	KPIT	QM / (ASIL B ^{*)})
SysVolt	AL	QM
T1	GLIWA	

Table 3: FLM3 Non-safety relevant software elements, connected to safety relevant software elements

^{*)} Because BSW-Modules supplied by KPIT are of safety level ASIL D (see [KPIT_SM_2]) and BSW/MCAL-Modules supplied by Cypress are of safety level ASIL B (see [MCU Safety Manual], [KPIT_SM_2]), ASIL B can be assigned to all BSW-Modules of these suppliers and need not to be considered while freedom from interference analysis (see [ISO], [FLMT5350]).

Detailed description of the software elements can be found in the specification of the software architecture (see [SWRS_1], chapter 4).

An overview about which safety related software elements are connected to which non-safety relevant software elements can be found in the UML diagram 'Functional Safety Chain – Overview' (see [SWRS_4]) or in the chapter structure of this document.

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 11 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.1. BSW-Module OS: Operating System

This ASIL B AUTOSAR Basic Software Module (BSW-Module) is configured to support

- 1 OS-Application comprising different tasks for safety relevant and non-safety relevant SW- Elements.
- stack overflow detection
- preemptive task scheduling
- timing protection for category 2 ISRs

OS provides and schedules different tasks (safety relevant tasks / non-safety relevant tasks) for the runnables of all safety relevant SW- Elements and all non-safety relevant SW- Elements (see [SWRS_2], Table 2, Table 3).). .

All safety relevant tasks are configured with higher priority of any non-safety relevant task .

All category 2 ISRs have higher priority than any task.

In the following sub-chapters, it's going to be detailed what prevention, or detection and mitigation has been implemented for every non-safety relevant software element, which is connected to OS.

3.1.1. Non-safety relevant tasks

- Comprises of all tasks of all non-safety relevant SWCs, BSW-Modules and Complex Driver Modules (CDD), see Table 2..
- Requires preemptive task scheduling by safety relevant BSW-Module OS.

3.1.1.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	- OS will prevent from blocking of execution of safety relevant tasks by means of preemption of low priority tasks [KPIT Safety Manual], [FLMT-1096]. - external watchdog will prevent from blocking category 2 ISRs by means of reset [SAR]. - limited/restricted usage of category 2 ISRs [SWRS] - limited/restricted runtime consumption of category 2 ISRs [ALSwdesignRules]
Incorrect allocation of execution time	- OS will prevent from blocking of execution of safety relevant tasks by means of preemption of low priority tasks [KPIT Safety Manual], [FLMT-1096]. - external watchdog will prevent from blocking category 2 ISRs by means of reset [SAR].

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 12 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

	- limited/restricted usage of category 2 ISRs [SWRS] - limited/restricted runtime consumption of category 2 ISRs [ALSwDesignRules]
Incorrect synchronization between software elements	OS will prevent from incorrect synchronization between safety-relevant and non-safety relevant tasks [KPIT Safety Manual], [FLMT-1096].

3.1.1.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of safety relevant SW-Element internal data	CRC for safety parameters with recovery mechanism [SWRS]. This prevents from corruption of safety relevant SW-Element internal data caused by non-safety relevant tasks.
Stack overflow	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another SW-Element.	CRC for safety parameters with recovery mechanism [SWRS] This prevents from write access other than intended and thus prevents from corruption of safety relevant SW-Element safety relevant input data caused by non-safety relevant SW-Elements.

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 13 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.2. RTE: AUTOSAR Runtime Environment

The ASIL B AUTOSAR Runtime Environment (RTE) is configured to support

- communication between AUTOSAR Software Components (SWCs).
- access of SWCs to AUTOSAR Basic Software Modules (BSW-Modules) and Complex Driver Modules (CDD-Modules).
- End-to-End protection of safety relevant B2CAN communication using the AUTOSAR E2E Library and AUTOSAR CRC Library
- Rte_Read API to select the shutdown mode (ABORT SLEEP/GO TO SLEEP)

In the following sub-chapters, it's going to be detailed what prevention, or detection and mitigation has been implemented for every non-safety relevant software element, which is connected to RTE.

3.2.1. Non-Safety relevant SW Elements

- all non-safety relevant SWCs, BSW-Modules and Complex Driver Modules (CDD) supplied), see Table 2.

3.2.1.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	- RTE/OS will prevent from blocking of execution of safety relevant SW Elements by means of preemption of low priority tasks [KPIT Safety Manual], [FLMT-1096]. - external watchdog will prevent from blocking category 2 ISRs by means of reset [SAR]. - limited/restricted usage of category 2 ISRs [SWRS] - limited/restricted runtime consumption of category 2 ISRs [ALSwDesignRules]
Incorrect allocation of execution time	- RTE/OS will prevent from blocking of execution of safety relevant SW Elements by means of preemption of low priority tasks [KPIT Safety Manual], [FLMT-1096]. - external watchdog will prevent from blocking category 2 ISRs by means of reset [SAR]. - limited/restricted usage of category 2 ISRs [SWRS] - limited/restricted runtime consumption of category 2 ISRs [ALSwDesignRules]

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 14 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Incorrect synchronization between SW-Elements	RTE/OS will prevent from incorrect synchronization between safety relevant and non-safety relevant SW-Elements [KPIT Safety Manual], [FLMT-1096].
---	---

3.2.1.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of safety relevant SW-Element internal data	CRC for safety parameters with recovery mechanism [SWRS]. This prevents from corruption of safety relevant SW-Element internal data caused by non-safety relevant SW-Elements.
Stack overflow	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety parameters with recovery mechanism [SWRS]. This prevents from corruption of safety relevant SW-Element safety relevant input data caused by non-safety relevant SW-Elements.

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 15 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.3. SWC SysMon: System Monitoring

This ASIL B software component (SWC)

- requires input data by asynchronous messages from the following non-safety relevant elements:
AppM, FctR, SysVolt, LsrSens, CodM, Coding, StbM
- provides output data by synchronous calls to the following non-safety relevant element:
Dem
- provides output data by synchronous calls by the following non-safety relevant element:
DiagM
- provides output data by asynchronous messages to the following non-safety relevant elements:
SigPrep, AppM, FctR, CtrlLed, CtrlStp, LaIntegration, DiagM, LsrSens

In the following sub-chapters, it's going to be detailed what prevention, or detection and mitigation has been implemented for every non-safety relevant software element, which is connected to SysMon.

Additional prevention or detection and mitigation has been implemented by means of SysMon for non-safety relevant software elements, which are not directly connected to SysMon, e. g. SPI error fail safe reaction or LED monitoring and fail safe reaction, see ch. 3.6.1.

3.3.1. BSW-Module Dem: Diagnostic Event Manager

- Requires DTC data by synchronous calls from safety relevant SWC SysMon (client/server interface).
- Because the BSW-Module Dem is assigned to safety level ASIL B, Dem is not to be considered while freedom from interference analysis [ISO].

3.3.2. SWC Coding (BAC)

- Provides safety relevant and non-safety relevant coding parameter data by synchronous calls from safety relevant SWC SysMon while startup or recovery of safety relevant coding parameters (client/server interface).

3.3.2.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution, if no return from call	- RTE/OS will prevent from blocking client/server interface [KPIT Safety Manual], [FLMT-1096]. - Coding data evaluated by SysMon while startup or recovery of safety relevant coding parameters only [SWRS].
Incorrect allocation of execution time, if delayed return from call	- RTE/OS will prevent from retarding client/server interface [KPIT Safety Manual], [FLMT-1096].

	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 16 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

	- Coding data evaluated by SysMon while startup or recovery of safety relevant coding parameters only [SWRS].
Incorrect synchronization between software elements	- Return value from call not evaluated by SysMon [SWRS]. - Coding data evaluated by SysMon while startup or recovery of safety relevant coding parameters only [SWRS]. - Status synchronization managed by CodM, see below.

3.3.2.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of SysMon internal data	Coding data evaluated by SysMon while startup or recovery of safety relevant coding parameters only [SWRS]. This prevents from corruption of safety relevant SysMon internal data caused by Coding (BAC) [SWRS].
Stack overflow caused by call	- KPIT OS module has designed its own detection mechanism [KPIT Safety Manual]. - Coding data evaluated by SysMon while startup or recovery of safety relevant coding parameters only [SWRS].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of SysMon safety relevant input data caused by Coding (BAC) [KPIT Safety Manual].

3.3.3. SWC DiagM: Diagnostic Manager

- Requests non-safety relevant coding error reasons by synchronous calls to safety relevant SWC SysMon (client/server interface).
- Requires non-safety relevant (for DiagM) vehicle speed cyclically from safety relevant SWC SysMon (sender/receiver interface).
- Requires non-safety relevant (verified) error status of each light source and every internal LED/switch segment cyclically from safety relevant SWC SysMon (sender/receiver interface).
- Requires non-safety relevant target settings for every LED buck channel cyclically from safety relevant SWC SysMon (sender/receiver interface).

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 17 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.3.3.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	- no risk caused by blocking client/server interface, because DiagM calls server operation of SysMon from low priority non-safety relevant task [SWRS_2]. - RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time, if delayed return from call	- no risk caused by blocking client/server interface, because DiagM calls server operation of SysMon from low priority non-safety relevant task [SWRS_2]. - RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements, based on return value from call	RTE/OS will prevent from incorrect synchronization between SysMon and DiagM [KPIT Safety Manual], [FLMT-1096].

3.3.3.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of SysMon internal data	CRC for safety relevant coding parameters with recovery mechanism. This prevents from corruption of SysMon internal data caused by DiagM [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	- CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of SysMon safety relevant input data caused by DiagM [SWRS].

3.3.4. SWC CodM: Coding Manager

- Provides non-safety relevant coding parameter status cyclically to safety relevant SWC SysMon (sender/receiver interface).
- Requests non-safety relevant coding error reasons by synchronous calls to safety relevant SWC SysMon (client/server interface).

 AL AUTOMOTIVE LIGHTING MARELLI ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 18 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.3.4.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution, if no return from call	- No risk, because CodM calls server operation of SysMon from low priority non-safety relevant task [SWRS_2]. - Coding data status evaluated by SysMon while startup only [SWRS].
Incorrect allocation of execution time, if delayed return from call	- No risk, because CodM calls server operation of SysMon from low priority non-safety relevant task [SWRS_2]. - Coding data status evaluated by SysMon while startup only [SWRS].
Incorrect synchronization between software elements	RTE/OS will prevent from incorrect synchronization between SysMon and CodM [KPIT Safety Manual], [FLMT-1096].

3.3.4.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of SysMon internal data	- Coding data status evaluated by SysMon while startup only [SWRS]. - CRC for safety relevant coding parameters with recovery mechanism. This prevents from corruption of SysMon internal data caused by CodM [SWRS]. -
Stack overflow caused by call	- KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	- Coding data status evaluated by SysMon while startup only [SWRS]. - CRC for safety relevant internal communication with fail safe reactions. This prevents from corruption of safety relevant SysMon safety relevant input data caused by CodM [SWRS].

 AL AUTOMOTIVE LIGHTING MARELLI ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 19 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.3.5. SWC AppM: Application Manager

- Provides target settings for onboard light source channels (buck driver channels or onboard bypass switches) incl. safety relevant buck driver channels for TI/LB cyclically to safety relevant SWC SysMon (sender/receiver interface).
- Provides non-safety relevant derating status for buck driver channels cyclically to safety relevant SWC SysMon (sender/receiver interface).
- Requires non-safety relevant (for AppM) vehicle speed cyclically from safety relevant SWC SysMon (sender/receiver interface).

3.3.5.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	RTE/OS will prevent from retarding sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	- RTE/OS will prevent from incorrect synchronization between SysMon and AppM [KPIT Safety Manual], [FLMT-1096]. - SysMon internal plausibility check of safety relevant target settings for buck driver channels with recovery mechanism [SWRS]. - SysMon internal consistency check of safety relevant coding parameters and relevant calibration parameters evaluated by CddLed while startup [SWRS].

3.3.5.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of SysMon internal data	- SysMon internal plausibility check of safety relevant target settings for buck driver channels with recovery mechanism [SWRS]. - CRC for safety relevant coding parameters with recovery mechanism. This prevents from corruption of SysMon internal data caused by AppM [SWRS].

	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 20 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of SysMon safety relevant input data caused by AppM [SWRS].

3.3.6. SWC FctR: Function Router

- Provides light function status incl. safety relevant TI status cyclically to safety relevant SWC SysMon (sender/receiver interface).
- Requires non-safety relevant (for FctR) vehicle speed, vehicle status and light function requests incl. turn indicator timing cyclically from safety relevant SWC SysMon (sender/receiver interface).
- Requires non-safety relevant the (verified) error status of each light source (phys. LED channels) in relation to coding parameters FUSI_DRVxx_NAME_ASIL cyclically from safety relevant SWC SysMon (sender/receiver interface).

3.3.6.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	RTE/OS will prevent from retarding sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	- RTE/OS will prevent from incorrect synchronization between SysMon and FctR [KPIT Safety Manual]. - SysMon internal plausibility check of safety relevant TI status with recovery mechanism [SWRS].

3.3.6.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of SysMon internal data	- SysMon internal plausibility check of safety relevant TI status with recovery mechanism [SWRS]. - CRC for safety relevant coding parameters with recovery mechanism.

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 21 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

	This prevents from corruption of SysMon internal data caused by FctR [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of SysMon safety relevant input data caused by FctR [SWRS].

3.3.7. SWC SysVolt: Supply Voltage Monitoring

- Provides non-safety relevant supply voltage status relevant to the diagnostic supply range cyclically to safety relevant SWC SysMon (sender/receiver interface).

3.3.7.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	RTE/OS will prevent from retarding sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	- RTE/OS will prevent from incorrect synchronization between SysMon and SysVolt [KPIT Safety Manual], [FLMT-1096]. - No plausibility check/recovery is needed, because of no safety relevant input from SysVolt to SysMon [SWRS]

3.3.7.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of SysMon internal data	CRC for safety relevant coding parameters with recovery mechanism [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus

	Asr6-Bw16 (BMW-FLM3)	Version main\20	Page 22 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

	prevents from corruption of SysMon safety relevant input data caused by SysVolt [SWRS].
--	---

3.3.8. SWC LsrSens: Laser Sensor Component

- Provides non-safety relevant status and errors of the laser monitoring cyclically to safety relevant SWC SysMon (sender/receiver interface).
- Requires non-safety relevant status and errors of every LED buck converter channel cyclically from safety relevant SWC SysMon (sender/receiver interface).

3.3.8.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	RTE/OS will prevent from retarding sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	- RTE/OS will prevent from incorrect synchronization between SysMon and LsrSens [KPIT Safety Manual], [FLMT-1096]. - No plausibility check/recovery is needed, because of no safety relevant input from LsrSens to SysMon [SWRS]

3.3.8.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of SysMon internal data	CRC for safety relevant coding parameters with recovery mechanism. [SWRS]. -
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of SysMon safety relevant input data caused by LsrSens [KPIT Safety Manual].

	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 23 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.3.9. SWC SigPrep: Signal Preparation

- Requires non-safety relevant status of the B2CAN channel cyclically from safety relevant SWC SysMon (sender/receiver interface).

3.3.9.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	RTE/OS will prevent from incorrect synchronization between SigPrep and SysMon [KPIT Safety Manual], [FLMT-1096].

3.3.9.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of SysMon internal data	CRC for safety relevant coding parameters with recovery mechanism [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of SysMon safety relevant input data caused by SigPrep [SWRS].

3.3.10. SWC CtrlLed: Control LED

- Requires non-safety relevant status and errors of every LED buck converter channel and every internal LED/switch segment cyclically from safety relevant SWC SysMon (sender/receiver interface).

3.3.10.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 24 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Incorrect allocation of execution time	RTE/OS will prevent from retarding sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	RTE/OS will prevent from incorrect synchronization between CtrlLed and SysMon [KPIT Safety Manual], [FLMT-1096].

3.3.10.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of SysMon internal data	CRC for safety relevant coding parameters with recovery mechanism [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of SysMon safety relevant input data caused by CtrlLed [SWRS].

3.3.11. SWC CtrlStp: Control Stepper

- Requires non-safety relevant (for CtrlStp) vehicle speed cyclically from safety relevant SWC SysMon (sender/receiver interface).

3.3.11.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	RTE/OS will prevent from incorrect synchronization between CtrlStp and SysMon [KPIT Safety Manual], [FLMT-1096].

3.3.11.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of SysMon internal data	CRC for safety relevant coding parameters with recovery mechanism [SWRS].

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 25 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of SysMon safety relevant input data caused by CtrlStp [SWRS].

3.3.12. SWC LaIntegration: 'Licht Aussen' Integration

- Requires non-safety relevant (for LaIntegration) vehicle speed, vehicle status and light function requests cyclically from safety relevant SWC SysMon (sender/receiver interface).

3.3.12.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	RTE/OS will prevent from incorrect synchronization between LaIntegration and SysMon [KPIT Safety Manual].

3.3.12.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of SysMon internal data	CRC for safety relevant coding parameters with recovery mechanism. This prevents from corruption of SysMon internal data caused by LaIntegration [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of SysMon safety relevant input data caused by LaIntegration [SWRS].

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 26 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.3.13. BSW-Module StbM: Synchronized Time Base Manager

- Provides non-safety relevant system time incl. status by synchronous calls from by safety relevant SWC SysMon (client/server interface).
- Because the BSW-Module StbM is assigned to safety level ASIL B, StbM is not to be considered while freedom from interference analysis [ISO].

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 27 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.4. BSW-Module IoHwAbUser: I/O Hardware Abstraction User Interface

This ASIL B Basic Software Module (BSW-Module)

- requires input data by asynchronous messages from the following non-safety relevant elements:
CtrlHss, LsrSens, CddStp, Bs, NvM, CodM, Coding
- provides output data by synchronous calls by the following non-safety relevant elements:
SigPrep, FctR, PxA, SensM, CtrlLed, CtrlPxl CtrlStp, CodM, DiagM, CddStp, T1
- provides output data by asynchronous messages to the following non-safety relevant elements:
AppM, SysVolt, RSens, CtrlHss, DiagM, LsrSens, CddStp
- requires input data by means of shared memory from the following non-safety

relevant elements:

PBL

In the following sub-chapters, it's going to be detailed what prevention, or detection and mitigation has been implemented for every non-safety relevant software element, which is connected to IoHwAbUser.

3.4.1. Mounting Side Information Interface

- The following non-safety relevant SW-Elements request non-safety relevant mounting side information by synchronous call to safety relevant BSW-Module IoHwAbUser while startup (client/server interface):
SigPrep, FctR, PxA, SensM, CtrlLed, CtrlPxl CtrlStp, CodM, DiagM, CddStp, T1
- If the interface to request the mounting side information is the only interface between a non-safety relevant SW-Element and the safety relevant BSW-Module IoHwAbUser, then no separate sub-chapter exist.
- For non-safety relevant SW-Element with additional interfaces to the safety relevant BSW-Module IoHwAbUser, the interface to request the mounting side information is not discussed again (see e. g. CddStp ch. 3.4.4, CodM ch. 3.4.7).

3.4.1.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution, if no return from call	No risk, because call of server operation of IoHwAbUser from low priority non-safety relevant task [SWRS_2].
Incorrect allocation of execution time, if delayed return from call	No risk, because call of server operation of IoHwAbUser from low priority non-safety relevant task [SWRS_2].
Incorrect synchronization between software elements	- RTE/OS will prevent from incorrect synchronization between calling SW-Element and IoHwAbUser [KPIT Safety Manual], [FLMT-1096].

	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 28 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

	- Mounting side data evaluated by calling SW-Element while startup only [SWRS].
--	---

3.4.1.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of IoHwAbUser internal data	- No safety relevant coding parameters used by IoHwAbUser [SWRS]. - Mounting side data evaluated by calling SW-Element while startup only. This prevents from corruption of IoHwAbUser internal data caused by calling SW-Element [SWRS].
Stack overflow caused by call	- KPIT OS module has designed its own detection mechanism [KPIT Safety Manual]. - Mounting side data evaluated by calling SW-Element while startup only [SWRS].
Read or write access to memory allocated to another software element.	- CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of IoHwAbUser safety relevant input data caused by calling SW-Element [SWRS]. - Mounting side data evaluated by calling SW-Element while startup only. This prevents from read or write access other than intended and thus prevents from corruption of IoHwAbUser internal data caused by calling SW-Element [SWRS].

3.4.2. ECU Supply Voltage

- The following non-safety relevant SW-Elements require the non-safety relevant ECU supply voltage cyclically from safety relevant BSW-Module IoHwAbUser (sender/receiver interface).: AppM, SysVolt, DiagM, CddStp
- If the interface to get the ECU supply voltage is the only interface between a non-safety relevant SW-Element and the safety relevant BSW-Module IoHwAbUser, then no separate sub-chapter exist.

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 29 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.4.2.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	RTE/OS will prevent from incorrect synchronization between receiving SW-Element and IoHwAbUser [KPIT Safety Manual], [FLMT-1096].

3.4.2.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of IoHwAbUser internal data	No safety relevant coding parameters used by IoHwAbUser [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of IoHwAbUser safety relevant input data caused by receiving SW-Element [SWRS].

3.4.3. BSW-Module NvM: NVRAM Manager

- provides access for the safety relevant BSW-Module IoHwAbUser to the error status of the NVRAM block "Bs_SecEcuMode" and an operation to write data to the same while startup (client/server interface).
- Because the BSW-Module NvM is assigned to safety level ASIL B, NvM is not to be considered while freedom from interference analysis [ISO].

3.4.4. CddStp: Stepper Complex Driver

- Provides non-safety relevant target settings for enable status/direction/sleep status of the LWR stepper hardware driver by synchronous call to safety relevant BSW-Module IoHwAbUser (client/server interface).
- For mounting side information interface see ch. 3.4.1.

3.4.4.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
--------	---

	Asr6-Bw16 (BMW-FLM3)	Version main\20	Page 30 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Blocking of execution, if no return from call	No risk, because CddStp calls server operation of IoHwAbUser from low priority non-safety relevant task [SWRS_2].
Incorrect allocation of execution time, if delayed return from call	No risk, because CddStp calls server operation of IoHwAbUser from low priority non-safety relevant task [SWRS_2].
Incorrect synchronization between software elements	RTE/OS will prevent from incorrect synchronization between CddStp and IoHwAbUser [KPIT Safety Manual], [FLMT-1096].

3.4.4.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of IoHwAbUser internal data	No safety relevant coding parameters used by IoHwAbUser [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of IoHwAbUser safety relevant input data caused by CddStp [SWRS].

3.4.5. SWC Bs (BAC): Basic Security

- Provides the current ECU mode to the safety relevant BSW-Module IoHwAbUser (mode interface).

3.4.5.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking mode interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time, if delayed return from call	RTE/OS will prevent from retarding mode interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	- RTE/OS will prevent from incorrect synchronization between IoHwAbUser and Bs [KPIT Safety Manual], [FLMT-1096]. - No plausibility check/recovery is needed, because of no safety relevant input from Bs to IoHwAbUser [SWRS].

	Asr6-Bw16 (BMW-FLM3)	Version main\20	Page 31 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.4.5.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of IoHwAbUser internal data	No safety relevant coding parameters used by IoHwAbUser [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of IoHwAbUser safety relevant input data caused by Bs [SWRS].

3.4.6. SWC Coding (BAC)

- Provides non-safety relevant coding parameter data by synchronous calls from safety relevant BSW-Module IoHwAbUser while startup (client/server interface).

3.4.6.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution, if no return from call	- RTE/OS will prevent from blocking client/server interface [KPIT Safety Manual], [FLMT-1096]. - Coding data evaluated by IoHwAbUser while startup only [SWRS].
Incorrect allocation of execution time, if delayed return from call	- RTE/OS will prevent from retarding client/server interface [KPIT Safety Manual], [FLMT-1096]. - Coding data evaluated by IoHwAbUser while startup only [SWRS].
Incorrect synchronization between software elements	- Return value from call not evaluated by SysMon [SWRS]. - Coding data evaluated by IoHwAbUser while startup only [SWRS]. - Status synchronization managed by CodM, see below.

3.4.6.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
--------	---

	Asr6-Bw16 (BMW-FLM3)	Version main\20	Page 32 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Corruption of content of IoHwAbUser internal data	- No safety relevant coding parameters used by IoHwAbUser [SWRS]. - Coding data evaluated by IoHwAbUser while startup only [SWRS].
Stack overflow caused by call	- KPIT OS module has designed its own detection mechanism [KPIT Safety Manual]. - Coding data evaluated by SysMon while startup only [SWRS].
Read or write access to memory allocated to another software element.	- CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of IoHwAbUser safety relevant input data caused by Coding (BAC) [KPIT Safety Manual]. - Coding data evaluated by IoHwAbUser while startup only [SWRS].

3.4.7. SWC CodM: Coding Manager

- Provides non-safety relevant calibration parameter data by synchronous calls from safety relevant BSW-Module IoHwAbUser (client/server interface).
- Provides non-safety relevant coding- and calibration parameter status cyclically to safety relevant BSW-Module IoHwAbUser (sender/receiver interface).
- For mounting side information interface see ch. 3.4.1.

3.4.7.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	- RTE/OS will prevent from blocking client/server interface [KPIT Safety Manual], [FLMT-1096]. - Calibration data evaluated by IoHwAbUser while startup only [SWRS].
Incorrect allocation of execution time	- RTE/OS will prevent from blocking client/server interface [KPIT Safety Manual], [FLMT-1096]. - Calibration data evaluated by IoHwAbUser while startup only [SWRS].
Incorrect synchronization between software elements	- RTE/OS will prevent from incorrect synchronization between CodM and IoHwAbUser [KPIT Safety Manual], [FLMT-1096].

	Asr6-Bw16 (BMW-FLM3)	Version main\20	Page 33 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

	- Coding data status and calibration data incl. status evaluated by IoHwAbUser while startup only [SWRS].
--	---

3.4.7.2. Memory failures and implemented preventions, or detections and mitigations:

3.4.7.3.

Faults	Prevention, or detection and mitigation
Corruption of content of IoHwAbUser internal data	- No safety relevant coding parameters used by IoHwAbUser [SWRS]. - Coding data status and calibration data incl. status evaluated by IoHwAbUser while startup only [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of IoHwAbUser safety relevant input data caused by CodM [SWRS].

3.4.8. SWC CtrlHss: High Side Switch Control

- Provides non-safety relevant target settings to enable/disable the sense feedback of the high side switches of the HSS hardware driver by synchronous call to safety relevant BSW-Module IoHwAbUser (client/server interface).
- Provides non-safety relevant target settings for the state of every high side switch by synchronous call to safety relevant BSW-Module IoHwAbUser (client/server interface).
- Requires non-safety sense feedback of every high side switch cyclically from safety relevant BSW-Module IoHwAbUser (sender/receiver interface).

3.4.8.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	- No risk caused by blocking client/server interface, because CtrlHss calls server operation of IoHwAbUser from low priority non-safety relevant task [SWRS_2]. - RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	- No risk caused by blocking client/server interface, because CtrlHss calls server

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 34 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

	operation of IoHwAbUser low priority non-safety relevant task [SWRS_2]. - RTE/OS will prevent from retarding sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	- RTE/OS will prevent from incorrect synchronization between CtrlHss and IoHwAbUser [KPIT Safety Manual], [FLMT-1096].

3.4.8.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of IoHwAbUser internal data	No safety relevant coding parameters used by IoHwAbUser [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS].

3.4.9. SWC LsrSens: Laser Sensor Component

- Provides non-safety relevant target setting for enable status status of the laser by synchronous call to safety relevant BSW-Module IoHwAbUser (client/server interface).
- Requires non-safety inputs from laser sensors cyclically from safety relevant BSW-Module IoHwAbUser (sender/receiver interface).

3.4.9.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	- no risk caused by blocking client/server interface, because LsrSens calls server operation of IoHwAbUser low priority non-safety relevant task [SWRS_2]. - RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual].
Incorrect allocation of execution time	- no risk caused by blocking client/server interface, because LsrSens calls server operation of IoHwAbUser from low priority non-safety relevant task [SWRS_2].

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 35 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

	- RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual].
Incorrect synchronization between software elements	RTE/OS will prevent from incorrect synchronization between IoHwAbUser and LsrSens [KPIT Safety Manual], [FLMT-1096].

3.4.9.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of IoHwAbUser internal data	No safety relevant coding parameters used by IoHwAbUser [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS].

3.4.10. SWC RSens: Resistor Sensor Component

- Requires non-safety inputs from ECU internal sensors and external sensors connected to the ECU cyclically from safety relevant BSW-Module IoHwAbUser (sender/receiver interface).

3.4.10.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	RTE/OS will prevent from incorrect synchronization between RSens and IoHwAbUser [KPIT Safety Manual], [FLMT-1096].

3.4.10.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of IoHwAbUser internal data	No safety relevant coding parameters used by IoHwAbUser [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version main\20	Page 36 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS].
---	---

3.4.11. Pb21_PBL: Primary Bootloader

- Provides non-safety relevant input from mounting side identification of headlamp wiring harness connected to the ECU to safety relevant BSW-Module IoHwAbUser (shared memory interface).

3.4.11.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	- no risk caused by blocking shared memory interface, because of fixed execution order PBL/Application (CM0+)/Application (CM4F) without handshake or feedback - Mounting side data evaluated by PBL and Application (CM4F) while startup only [SWRS]. - external watchdog will prevent from blocking PBL by means of reset [SAR].
Incorrect allocation of execution time	- no risk caused by retarding shared memory interface, because of fixed execution order PBL/Application (CM0+)/Application (CM4F) without handshake or feedback - Mounting side data evaluated by PBL and Application (CM4F) while startup only [SWRS]. - external watchdog will prevent from blocking PBL by means of reset [SAR].
Incorrect synchronization between software elements	- fixed execution order PBL/Application (CM0+)/Application (CM4F) without handshake or feedback

3.4.11.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of IoHwAbUser internal data	- fixed shared memory location is used as interface. This prevents from corruption of IoHwAbUser internal data caused by PBL [SWRS_3].

 AL AUTOMOTIVE LIGHTING MARELLI ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 37 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

	- Mounting side data evaluated by PBL and Application (CM4F) while startup only [SWRS].
Stack overflow caused by call	- KPIT OS module has designed its own detection mechanism [KPIT Safety Manual]. - Mounting side data evaluated by PBL and Application (CM4F) while startup only [SWRS].
Read or write access to memory allocated to another software element.	- fixed execution order PBL/Application (CM0+)/Application (CM4F) without handshake or feedback. - fixed shared memory location is used as interface. This prevents from corruption of IoHwAbUser internal data caused by PBL [SWRS_3]. - Mounting side data evaluated by PBL and Application (CM4F) while startup only [SWRS].

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 38 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.5. CddLed: LED Complex Driver

This ASIL B Complex Driver Module (CDD-Module)

- requires input data by asynchronous messages from the following non-safety relevant elements:
CtrlLed, CodM
- provides output data by asynchronous messages to the following non-safety relevant elements:
DiagM, LsrSens

In the following sub-chapters, it's going to be detailed what prevention, or detection and mitigation has been implemented for every non-safety relevant software element, which is connected to CddLed.

3.5.1. SWC CodM: Coding Manager

- Provides non-safety relevant calibration parameter data by synchronous calls from safety relevant CDD-Module CddLed (client/server interface).
- Provides non-safety relevant calibration parameter status cyclically to safety relevant CDD-Module CddLed (sender/receiver interface).

3.5.1.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	- RTE/OS will prevent from blocking client/server interface [KPIT Safety Manual], [FLMT-1096]. - Calibration data evaluated by CddLed while startup only [SWRS].
Incorrect allocation of execution time	- RTE/OS will prevent from blocking client/server interface [KPIT Safety Manual], [FLMT-1096]. - Calibration data evaluated by CddLed while startup only [SWRS].
Incorrect synchronization between software elements	- RTE/OS will prevent from incorrect synchronization between CodM and CddLed [KPIT Safety Manual], [FLMT-1096]. - Calibration data incl. status evaluated by CddLed while startup only [SWRS]. - consistency check of safety relevant coding parameters and relevant calibration parameters see ch. 3.3.5

3.5.1.2. Memory failures and implemented preventions, or detections and mitigations:

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 39 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Faults	Prevention, or detection and mitigation
Corruption of content of CddLed internal data	- No safety relevant coding parameters used by CddLed [SWRS]. - Calibration data incl. status evaluated by CddLed while startup only [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions [SWRS]. This prevents from read or write access other than intended and thus prevents from corruption of CddLed safety related input data caused by CodM [KPIT Safety Manual].

3.5.2. SWC CtrlLed: Control LED

- Provides non-safety relevant link information of parallel buck drivers and onboard bypass switches by synchronous call to safety relevant CDD-Module CddLed (client/server interface).

3.5.2.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution, if no return from call	- No risk, because CtrlLed calls server operation of CddLed from low priority non-safety relevant task [SWRS_2]. - Buck driver link information evaluated by CddLed while startup only [SWRS].
Incorrect allocation of execution time, if delayed return from call	- No risk, because CtrlLed calls server operation of CddLed from low priority non-safety relevant task [SWRS_2]. - Buck driver link information evaluated by CddLed while startup only [SWRS].
Incorrect synchronization between software elements	- RTE/OS will prevent from incorrect synchronization between CtrlLed and CddLed [KPIT Safety Manual], [FLMT-1096]. - Buck driver link information evaluated by CddLed while startup only [SWRS].

3.5.2.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
--------	---

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 40 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Corruption of content of CddLed internal data	No safety relevant coding parameters used by CddLed [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions This prevents from read or write access other than intended and thus prevents from corruption of CddLed safety related input data caused by CtrlLed [SWRS].

3.5.3. SWC DiagM: Diagnostic Manager

- Requires non-safety relevant (for DiagM) status and faults of every LED buck channel cyclically from safety relevant CDD-Module CddLed (sender/receiver interface).

3.5.3.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	RTE/OS will prevent from incorrect synchronization between DiagM and CddLed [KPIT Safety Manual], [FLMT-1096].

3.5.3.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of CddLed internal data	No safety relevant coding parameters used by CddLed. [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions . This prevents from read or write access other than intended and thus prevents from corruption of CddLed safety related input data caused by DiagM [SWRS].

 AL AUTOMOTIVE LIGHTING MARELLI ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 41 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.5.4. SWC LsrSens: Laser Sensor Component

- Requires non-safety relevant (for LsrSens) status and faults of every LED buck channel cyclically from safety relevant CDD-Module CddLed (sender/receiver interface).

3.5.4.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	RTE/OS will prevent from incorrect synchronization between LsrSens and CddLed [KPIT Safety Manual], [FLMT-1096].

3.5.4.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of CddLed internal data	No safety relevant coding parameters used by CddLed. This prevents from corruption of CddLed internal data caused by LsrSens [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions. This prevents from read or write access other than intended and thus prevents from corruption of CddLed safety related input data caused by LsrSens [KPIT Safety Manual].

 AL AUTOMOTIVE LIGHTING MARELLI ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 42 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.6. CddSpi: Serial Peripheral Interface Complex Driver

This ASIL B Complex Driver Module (CDD-Module)

- requires input data from the following non-safety relevant elements:
CddStp, CodM

In the following sub-chapters, it's going to be detailed what prevention, or detection and mitigation has been implemented for every non-safety relevant software element, which is connected to CddSpi.

3.6.1. SWC CodM: Coding Manager

- Provides non-safety relevant calibration parameter data by synchronous calls from safety relevant CDD-Module CddSpi (client/server interface).
- Provides non-safety relevant calibration parameter status cyclically to safety relevant CDD-Module CddSpi (sender/receiver interface).

3.6.1.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	- RTE/OS will prevent from blocking client/server interface [KPIT Safety Manual], [FLMT-1096]. - Calibration data evaluated by CddSpi while startup only [SWRS].
Incorrect allocation of execution time	- RTE/OS will prevent from blocking client/server interface [KPIT Safety Manual], [FLMT-1096]. - Calibration data evaluated by CddSpi while startup only [SWRS].
Incorrect synchronization between software elements	- RTE/OS will prevent from incorrect synchronization between CodM and CddSpi [KPIT Safety Manual], [FLMT-1096]. - Calibration data incl. status evaluated by CddSpi while startup only [SWRS]. - consistency check of safety relevant coding parameters and relevant calibration parameters see ch. 3.3.5 - SPI error monitoring by CddLed and fail safe reaction by SysMon [SWRS]. - LED status monitoring and fail safe reaction by SysMon [SWRS].

3.6.1.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
--------	---

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 43 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Corruption of content of CddSpi internal data	- No safety relevant coding parameters used by CddSpi. [SWRS]. - Calibration data incl. status evaluated by CddSpi while startup only [SWRS].
Stack overflow caused by call	- KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions. This prevents from read or write access other than intended and thus prevents from corruption of CddSpi internal data caused by CodM [SWRS].

3.6.2. CddStp: Stepper Complex Driver

- Provides SPI Tx data by synchronous calls to non-safety relevant Complex Driver Module CddStp by safety relevant Complex Driver Module CddSpi (callback API function).
- Requires SPI Rx data by synchronous calls to non-safety relevant Complex Driver Module CddStp by safety relevant Complex Driver Module CddSpi (callback API function).

3.6.2.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution, if no return from call	OS will prevent from blocking callback API functions [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time, if delayed return from call	OS will prevent from retarding callback API functions [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	OS will prevent from incorrect synchronization between CddSpi and CddStp caused by callback API functions [KPIT Safety Manual], [FLMT-4399]

3.6.2.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of CddSpi internal data	No safety relevant coding parameters used by CddSpi[SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\\20	Page 44 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions[SWRS].
---	--

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 45 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.7. CddSbc: System Base Chip Complex Driver

This ASIL B Complex Driver Module (CDD-Module)

- requires input data from the following non-safety relevant elements:
CddStp, CodM

In the following sub-chapters, it's going to be detailed what prevention, or detection and mitigation has been implemented for every non-safety relevant software element, which is connected to CddSpi.

3.7.1. Reset Reason Interface

- The following SW-Elements request non-safety relevant reset reason by synchronous call to safety relevant CDD-Module CddSbc while startup (client/server interface):
CodM, DiagM, StatM
- If the interface to request the reset reason is the only interface between a non-safety relevant SW-Element and the safety relevant CDD-Module CddSbc, then no separate sub-chapter exist.

3.7.1.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution, if no return from call	No risk, because call of server operation of CddSbc from low priority non-safety relevant task [SWRS_2].
Incorrect allocation of execution time, if delayed return from call	No risk, because call of server operation of CddSbc from low priority non-safety relevant task [SWRS_2].
Incorrect synchronization between software elements	- RTE/OS will prevent from incorrect synchronization between calling SW-Element and CddSbc [KPIT Safety Manual], [FLMT-1096]. - Reset reason evaluated by calling SW-Element while startup only [SWRS].

3.7.1.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of CddSbc internal data	- No safety relevant coding parameters used by CddSbc. [SWRS]. - Reset reason evaluated by calling SW-Element while startup only [SWRS].
Stack overflow caused by call	- KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 46 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

	- Reset reason evaluated by calling SW-Element while startup only [SWRS].
Read or write access to memory allocated to another software element.	- CRC for safety relevant internal communication with fail safe reactions. This prevents from read or write access other than intended and thus prevents from corruption of CddSbc safety related input data caused by calling SW-Element [SWRS]. - Reset reason evaluated by calling SW-Element while startup only [SWRS].

3.7.2. BSW-Module Dem: Diagnostic Event Manager

- Requires DTC data by synchronous calls from safety relevant CDD-Module CddSbc (client/server interface).

3.7.2.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution, if no return from call	RTE/OS will prevent from blocking client/server interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time, if delayed return from call	RTE/OS will prevent from retarding client/server interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements, based on return value from call	Return value from call not evaluated by SysMon [SWRS].

3.7.2.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of CddSbc internal data	No safety relevant coding parameters used by CddLed. This prevents from corruption of CddSbc internal data caused by BSW-Module Dem [SWRS].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	CRC for safety relevant internal communication with fail safe reactions. This prevents from read or write access other than intended and thus prevents from corruption of CddSbc safety related input data caused by BSW-Module Dem [SWRS].

  MARELLI ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 47 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version main\20	Page 48 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.8. BSW-Module Com: Communication Services

This ASIL B Basic Software Module (BSW-Module)

- requires input data by asynchronous messages from the following non-safety relevant elements:
SigPrep
- provides output data by asynchronous messages to the following non-safety relevant elements:
SigPrep

In the following sub-chapters, it's going to be detailed what prevention, or detection and mitigation has been implemented for every non-safety relevant software element, which is connected to Com.

3.8.1. SWC SigPrep: Signal Preparation

- Provides non-safety relevant status information, which has to be sent in B2CAN Tx-PDUs cyclically to safety relevant BSW-Module Com (sender/receiver interface).
- Requires non-safety relevant data for all B2CAN Rx-PDUs cyclically from safety relevant BSW-Module Com (sender/receiver interface).

3.8.1.1. Timing and execution failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Blocking of execution	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect allocation of execution time	RTE/OS will prevent from blocking sender/receiver interface [KPIT Safety Manual], [FLMT-1096].
Incorrect synchronization between software elements	RTE/OS will prevent from incorrect synchronization between SigPrep and Com [KPIT Safety Manual], [FLMT-1096].

3.8.1.2. Memory failures and implemented preventions, or detections and mitigations:

Faults	Prevention, or detection and mitigation
Corruption of content of Com internal data	No safety relevant coding parameters used by Com. This prevents from corruption of Com internal data caused by SigPrep [KPIT Safety Manual].
Stack overflow caused by call	KPIT OS module has designed its own detection mechanism [KPIT Safety Manual].
Read or write access to memory allocated to another software element.	E2E protection for safety relevant B2CAN communication with fail safe reactions. This prevents from read or write access other than intended and thus prevents from

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 49 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

	corruption of Com safety related data caused by SigPrep [KPIT Safety Manual].
--	--

3.8.1. BSW-Module PduR: PDU Router

- Provides analog services for routing of I-PDUs (Interaction Layer Protocol Data Units) using the BSW-Module Com [AUTOSAR].
- Because the BSW-Module PduR is assigned to safety level ASIL B, PduR is not to be considered while freedom from interference analysis [ISO].

 ALDE-RT/EE	Asr6-Bw16 (BMW-FLM3)	Version \\main\20	Page 50 von 50
	Freedom from interference analysis report	Author ret2rt	Date 2021-05-12

3.9. BSW-Module IoHwAb: I/O Hardware Abstraction

This ASIL B Basic Software Module (BSW-Module)

- requires input data from the following non-safety relevant elements:
ADC

In the following sub-chapters, it's going to be detailed what prevention, or detection and mitigation has been implemented for every non-safety relevant software element, which is connected to CddSpi.

3.9.2. BSW-Module ADC: Analog/Digital Conversion

- Provides analog input raw data by synchronous calls to safety relevant BSW-Module ADC by safety relevant BSW-Module IoHwAb (API function).
- Requires configuration data for the ADC unit by synchronous calls to non-safety relevant BSW-Module ADC by safety relevant BSW-Module IoHwAb (API function).
- Because the BSW-Module ADC is assigned to safety level ASIL B, ADC is not to be considered while freedom from interference analysis [ISO].