

	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)

无干扰分析报告

主要V版本\ \ 20

Approval of document

Name	Responsibility	Status	Date
Thomas Reichenecker	SWA/EES3	constructed	

模板审批

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

文件修订历史

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

 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

文件:SWDD_Asr6-Bw16_FF1_Report.docx
模板版本\main\2

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

内容

1.	介绍	5
1.1.	目的	5
1.2.	引用文件	5
1.3.	术语和定义	6
2.	不受干扰	8
3.	分析	8
3.1.	BSW-Module OS:操作系统	11
3.1.1.	非安全相关任务	11
3.2.	RTE: AUTOSAR运行环境	13
3.2.1.	非safety相关SW元素	13
3.3.	SWC SysMon:系统监控	15
3.3.1.	BSW-Module Dem:诊断事件管理器	15
3.3.2.	SWC Coding(后台)	15
3.3.3.	SWC DiagM:诊断管理器	16
3.3.4.	SWC CodM:编码管理器	17
3.3.5.	SWC AppM:应用管理器	19
3.3.6.	SWC FctR:功能路由器	20
3.3.7.	SWC SysVolt:电源电压监测	21
3.3.8.	SWC LsrSens:激光传感器组件	22
3.3.9.	SWC SigPrep:信号准备	23
3.3.10.	SWC CtrlLed:控制LED	23
3.3.11.	SWC CtrlStp:控制步进器	24
3.3.12.	SWC集成: “light Aussen” 集成	25
3.3.13.	BSW-Module StbM:同步时基管理器	26
3.4.	BSW-Module IoHwAbUser: I/O硬件抽象用户界面	27
3.4.1.	安装侧信息界面	27
3.4.2.	ECU供电电压	28
3.4.3.	BSW-Module NvM: NVRAM管理器	29
3.4.4.	CddStp:步进复杂驱动	29
3.4.5.	SWC Bs (BAC):基本安全	30
3.4.6.	SWC Coding(后台)	31
3.4.7.	SWC CodM:编码管理器	32
3.4.8.	SWC CtrlHss:高位侧开关控制	33
3.4.9.	SWC LsrSens:激光传感器组件	34
3.4.10.	SWC RSens:电阻传感器组件	35
3.4.11.	Pb21_PBL:主引导程序	36
3.5.	CddLed: LED复合驱动	38
3.5.1.	SWC CodM:编码管理器	38
3.5.2.	SWC CtrlLed:控制LED	39
3.5.3.	SWC DiagM:诊断管理器	40

©Alle Rechte bei Marelli Automotive Lighting Reutlingen (Germany) GmbH. Jede Vergungsbefugnis, 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.

	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:激光传感器组件	41
3.6.	CddSpi:串行外设接口复杂驱动	42
3.6.1.	SWC CodM:编码管理器	42
3.6.2.	CddStp:步进复杂驱动	43
3.7.	CddSbc: System Base Chip复杂驱动程序	45
3.7.1.	复位原因接口	45
3.7.2.	BSW-Module Dem:诊断事件管理器	46
3.8.	BSW-Module Com:通信服务	48
3.8.1.	SWC SigPrep:信号准备	48
3.8.1.	BSW-Module PduR: PDU Router	49
3.9.	BSW-Module IoHwAb: I/O硬件抽象	50
3.9.2.	bsw模块ADC:模拟/数字转换	50

Illustrations

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

表

表1:术语、定义和缩写	7
表2:FLM3安全相关软件要素	9
表3:FLM3非安全相关软件要素, 与安全相关软件要素相连	10

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

1. 介绍

1.1. 目的

本文件的目的是提供有关确保FLM3 Bw16项目安全相关和非安全相关软件元素不受干扰的实现证据和细节。

1.2. 引用文件

[ALSwDesignRules] AL嵌入式软件设计规则

(AUTOSAR)]AUTOSAR Release 4.2.2, 参见<https://www.autosar.org>
 (AUTOSAR_1) 包含以下部分:
 (AUTOSAR_2) AUTOSAR_EXP_FunctionalSafetyMeasures.pdf
 [AUTOSAR_3 AUTOSAR_SWS_OS.pdf
 AUTOSAR_SWS_RTE.pdf

(FLMT-xxxx) M3]:链接到jira -机票号。FLM3项目的xxxx
 (ISO) ISO 26262:2018

[KLH_FL]FLM3_Kapitel_3.5.1_18_January_2019

[KPIT安全手册]KPIT安全手册
 包含以下部分:

[KPIT_SM_1] KPIT_Safety Approach.pdf
 [KPIT_SM_2] KPIT Integration_Safety_Architecture_Design_V3.pdf [KPIT_SM_3]
 KPIT安全用户手册

[MCU安全手册]Cypress安全手册

安全分析报告ECU FLM3

(SBC_DS) Infineon TLE9471 Datasheet

[SWRS]软件需求规范ECU FLM3
 包含以下部分:

[swrs_1]]SWRS
 [SWRS_2] SWDD_Asr6-Bw16_SystemResources.xlsx [SWRS_3] SWDD_
 Asr6-Bw16_Mem_Map.xlsx [SWRS_4] UML模型SWRS_Bw16.eapx

(锡): 系统需求规格ECU FLM3
 门湖浆

 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. 术语和定义

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

表1:术语、定义和缩写

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

2. 不受干扰

根据ISO 26262(参见[ISO]), 如果嵌入式软件由不同ASIL等级的软件组件组成, 那么要么整个软件必须按照最高的ASIL进行开发, 要么从ASIL等级较低的元素中确保ASIL等级较高的软件组件不受干扰。此外, ISO 26262标准还提供了故障, 故障会导致软件组件之间的干扰。故障分为以下几类:

- 记忆
- 定时和执行
- 信息交流

3. 分析

在接下来的子章节中, 将详细介绍基于一般保护机制(见下文)对每个与非安全相关的SW-Element有接口的安全相关SW-Element实施了哪些预防或检测和缓解措施。

对于与安全相关的sw - element与没有接口(意外接口)的非安全相关sw - element的干扰, 操作系统(OS, 见3.1章)、运行时环境(RTE, 见3.2章)和系统监控(SysMon, 见3.3章)提供的与安全相关的sw - element的一般保护也适用。

一般的保护机制是

-内存保护:

CRC检查安全相关参数与恢复机制和失败

SysMon提供的安全反应(参见[SWRS_1], 第4.4.3.4.2.2章)。-定时保护:

OS提供的固定优先级抢占式调度。FLM3项目的操作系统和操作系统配置防止了由于优先级反转、死锁和活动锁(例如由共享资源引起的)而导致的与安全相关的SW-Elements的执行阻塞(背景和基本原理参见[AUTOSAR_2], 第7.7.2章和[AUTOSAR_1], KPIT安全方法参见[KPIT_SM_2], FLM3项目的操作系统配置参见[SWRS_2])。

此外, 通过看门狗概念(参见[KPIT_SM_2], [SAR]), 可以减轻由非安全相关的第2类isr阻塞的安全相关sw - element的执行。

-通信保护:

SysMon提供的安全反应的依赖或冗余信息的一致性检查(参见[SWRS_1], 第4.4.3.4.2.2章)。这包括过时(未更新), 不正确(在范围内)或错误(超出范围)的信息,