

	Technical Safety Concept	Draft
		Rev: 1.0

Technical Safety Concept For VCU

Role	Name	Designation	Signature	Date
Author	Brandon Nie	VCU functional safety engineer		
Reviewer				
Reviewer				
Approver				

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

Contents

1. OVERVIEW.....	5
1.1 INTRODUCTION	5
1.2 SCOPE.....	5
1.3 Terms and Abbreviations	6
1.4 System Description	7
2. VCU System Safety Requirements.....	9
2.1 Related Safety Goals 安全目标	9
2.2 Related functional safety requirements 功能安全需求	12
3. General System Safety Strategy	13
3.1 MCU Hardware integrity MCU 硬件完整性	13
3.2 SBC Hardware integrity SBC 硬件完整性	13
3.3 External peripheral parts integrity 外围件完整性	14
3.4 Software integrity 软件完整性	14
3.5 System safe states 安全状态	14
3.5.1 Fail silent 故障静默	15
3.5.2 Switching into neutral gear 切换到空挡	15
3.5.3 No drive output 无扭矩输出	15
3.5.4 limited drive torque 限制驱动扭矩	15
3.5.5 Warning 故障报警	15
4. System Safety Architecture	16
4.1 VCU System Block Diagram	16
4.2 System Block Description	17
5. Detailed Safety mechanisms	20
5.1 P_SG_VH_0002	20
5.2 P_SG_VH_0003	21
5.3 P_SG_VH_0004	22
5.4 P_SG_VH_0005	23
5.5 P_SG_VH_0009	24
5.6 P_SG_VH_0010	24
5.7 P_SG_VH_0012	27
5.8 P_SG_VH_0013	27

	Technical Safety Concept	Draft
		Rev: 1.0

5.9	P_SG_VH_0014.....	28
5.10	P_SG_VH_0017.....	30
5.11	A_SG_VH_0004.....	31
5.12	A_SG_VH_0005.....	33
5.13	A_SG_VH_0006.....	33
5.14	A_SG_VH_0014.....	34
5.15	A_SG_VH_0015.....	35
5.16	C_SG_VH_0002.....	35
5.17	C_SG_VH_0003.....	37
5.18	C_SG_VH_0004.....	38
5.19	C_SG_VH_0007.....	39
6.	Hardware Integrity Concept.....	42
6.1	CPU integrity.....	42
6.2	Interconnect integrity.....	43
6.3	DMA integrity – Reserve.....	43
6.4	Interrupt Router integrity.....	44
6.5	Memory protection.....	44
6.5.1	Volatile memory.....	44
6.5.2	Non Volatile memory.....	45
6.6	Clock Monitoring.....	45
6.7	Temperature Monitoring.....	46
6.8	Power supply monitoring.....	47
6.9	Latent fault strategy.....	49
6.10	Communication protection.....	49
6.11	Register write protection.....	50
6.12	GPIO input protection.....	51
6.13	ADC integrity.....	51
6.14	Watchdog monitoring.....	52
6.15	Safety management.....	53

Revision History

Version	Date	Modified by	Brief history of Changes
1.0	2024/3/5	Brandon Nie	Initial draft

	Technical Safety Concept	Draft
		Rev: 1.0

1. OVERVIEW

1.1 INTRODUCTION

The VCU Technical Safety Concept implements the technical solution to meet functional safety requirements allocated from powertrain, chassis and ADAS system. In this document, the safety strategy, safety state, safety architecture and safety mechanisms are detailed. The safety concept is based on higher level safety concept and system architecture.

VCU 技术安全概念实现了技术解决方案，以满足动力总成、底盘和 ADAS 系统分配的功能安全要求。本文详细介绍了安全策略、安全状态、安全架构和安全机制。技术安全概念的设计基于更高级别的功能安全概念和系统架构设计。

The development of this TSC refers to below list of documents:

技术安全概念的制定参考了以下文件：

- ATOM Powertrain Item Denfinition_V1.1
- ATOM PT Hazard Analysis and Risk Assessment_V1.2
- ATOM Powertrain FSC_V1 (version 1).xlsb
- ATOM_FSR_VCU_V1.11_20240103

1.2 SCOPE

This document is intended for the development of the VCU controller for programs including Family, Taxi, Carsharing and Delivery. The objective of the Technical Safety Concept is to specify the Technical Safety Requirements that are derived from the functional safety concept and to allocate them to the system design. The Technical Safety Concept is developed according to the ISO 26262-Part 4.

本文件旨在开发 VCU 控制器，用于 Family, Taxi, Carsharing 和 Delivery 等项目。技术安全概念的目标是规定源自功能安全概念的技术安全要求，并将其分配给系统设计。技术安全概念是根据 ISO 26262 第 4 部分制定的。

1.3 Terms and Abbreviations

Term	Description
ADC	Analogue digital conversion
ASIL	Automotive safety integrity level
VCU	Application software
BSW	Basic software
CPU	Central processing unit
DBE	Double bit error
DMA	Direct memory access
DSPR	Data scratchpad RAM
DTS	Die temperature sensor
ECC	Error correction code
EDC	Error detection code
ENDINIT	End of initiation
FSC	Functional safety concept
FSR	Functional safety requirement
FTTI	Fault tolerance time interval
GPIO	General purpose input output
HARA	Hazard analysis and risk assessment
ISR	Interrupt service request
IR	Interrupt router
LBIST	Logical built-in self test
LPB	Local PFLASH bank
MBIST	Memory built-in self test
MONBIST	Monitor built-in self test
NVM	Non volatile memory
UV	Under voltage
OV	Over voltage

PBIST	Power built-in self test
PSPR	Program scratchpad RAM
QM	Quality management
SBC	System basic chip
SBE	Single bit error
SG	Safety goal
SMU	Safety management unit
SPB	System peripheral bus
SRI	Shared resource interconnect
TBD	To be determined
TBE	Triple bit error
TSC	Technical safety concept
TSR	Technical safety requirement
WDT	Watchdog timer

1.4 System Description

VCU implements below safety related functionality as part of the whole powertrain system:

作为整个动力传动系统的组成部分，VCU 实现以下安全相关功能：

1. Gear control subsystem 档位控制子系统

Gear control includes automatic gear shift to P/N gear from other gear positons under some conditions, gear shift control and arbitration from different gear shift sources, gear shift control logic and also EPB interface.

档位控制包括在某些条件下从其他档位自动切换到 P/N 档位、来自不同档位来源的换档控制和仲裁、换档控制逻辑以及 EPB 接口。

2. Drive control subsystem 驱动控制子系统


Drive control is composed of pedal analysis, one pedal control, vehicle speed calculation, drive torque calculation, regeneration torque calculation, creep torque control, torque limit, speed limit and torque transition.

驱动控制由踏板分析、单踏板控制、车速计算、驱动扭矩计算、再生扭矩计算、爬行扭矩控制、扭矩限制、速度限制和扭矩转换组成。

3. HV safety 高压安全

HV safety monitor and control the system in a state that risk of electric shock is mitigated.

高压安全监控系统，使其处于降低触电风险的状态。

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

VCU also has non-safety related functions such as charging and discharging, thermal management, energy management, power on/ off management, etc. The functional safety concept allocates the safety monitoring requirements to other controllers like BMS or the function itself is intrinsically safe.

VCU 还有非安全相关功能，如充放电、热管理、能量管理、高压上下电等。对于这些功能，功能安全概念将安全监控要求分配给 **BMS** 等其他控制器，或者功能本身是安全的。

Detailed technical specifications can be found in respective SSTS documents.

详细的技术规范请参考相应的 **SSTS** 文档。

	Technical Safety Concept	Draft
		Rev: 1.0

2. VCU System Safety Requirements

2.1 Related Safety Goals 安全目标


The following SGs are derived from HARA analysis of powertrain system and allocated to VCU, they're the highest level safety requirements.

以下 VCU 相关的安全目标源自于 PWT 系统功能的 HARA 分析，是最高级别的安全要求。

No.	SG_ID	Safety goal description	ASIL	Safe State	FTTI
1	P_SG_VH_0002	Prevent motion in opposite direction due to engaged reverse gear. 防止非预期切入反向的挡位而导致车辆反向移动。	B	Shift to N 切 N 档	500ms
2	P_SG_VH_0003	Prevent unintended deceleration due to engaged reverse gear. 防止非预期切入反向的挡位而导致车辆减速。	B	Shift to N 切 N 档	500ms
3	P_SG_VH_0004	Prevent Gear position display error. 防止挡位显示错误	B	All gear flash 所有档位闪烁	500ms
4	P_SG_VH_0005	Prevent longitudinal motion due to unintended driving gear engaged . 防止进入非预期驱动挡位而导致车辆纵向移动。	B	Shift to N 切 N 档	500ms
6	P_SG_VH_0009	Prevent vehicle from unintended movement due to unintended provide drive torque 防止由于意外提供驱动扭矩而导致车辆意外移动	B	No torque output 无扭矩输出	500ms
7	P_SG_VH_0010	Prevent vehicle acceleration greater than TBD m/s ² for a period greater than 500ms(TBD) caused by provided more drive torque than requested 防止由于提供过大驱动扭矩导致车辆误加速（加速度超过 TBD m/s ² 时间并超过 500ms）	C	No torque output 无扭矩输出	500ms
9	P_SG_VH_0012	Prevent vehicle unintended deceleration for longer than 500ms(TBD) when vehicle speed is above 10km/h(TBD) caused by provide reverse drive torque . 车辆车速超过 10km/h(TBD)时，防止由于提供反向的驱动扭矩导致车辆非预期减速超过 500ms(TBD)。	C	No torque output 无扭矩输出	500ms
10	P_SG_VH_0013	Prevent providing opposite torque against driver's requirements when the vehicle speed is lower than the creep speed, 当车辆速度低于蠕行速度时，防止提供与驾驶员要求相反的扭矩。	B	No torque output 无扭矩输出	500ms

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

11	P_SG_VH_0014	Prevent unintended vehicle deceleration for a period greater than TBD s caused by unintended implement the braking energy regeneration 防止由于非预期执行制动能量回收功能而导致车辆意外减速超过 TBD s。	C	Disable Energy Regeneration 禁用能量回收	500ms
12	P_SG_VH_0017	Prevent high voltage from leaking due to Loss of HV safety Monitor. 防止高压安全检测功能丢失导致高压泄露。	A	interruption of electric HV circuit 断开高压连接器	2S
13	A_SG_VH_0004	Prevent the ADAS from providing unintended drive torque 防止 ADAS 提供意外的驱动扭矩	C	Disable ADAS function & No drive torque output. 禁用 ADAS 功能&无驱动扭矩输出	500ms
14	A_SG_VH_0005	Prevent vehicle unintended deceleration for longer than 500ms(TBD) when vehicle speed is above 10km/h(TBD) caused by provide reverse drive torque 当车辆速度超过 10km/h (TBD) 时, 防止车辆因提供反向驱动扭矩而意外减速超过 500ms (TBD)	C	Disable ADAS function & No drive torque output. 禁用 ADAS 功能&无驱动扭矩输出	500ms
15	A_SG_VH_0006	Prevent providing opposite torque against driver's requirements when the vehicle speed is lower than the creep speed 当车速低于蠕行速度时, 防止提供与驾驶员要求相反的扭矩	B	Disable ADAS function & No drive torque output. 禁用 ADAS 功能&无驱动扭矩输出	500ms
16	A_SG_VH_0014	Avoid unintended drive torque when APA activate with vehicle speed<5kph 当 APA 在车速小于 5 公里/小时的情况下启动时, 避免意外的驱动扭矩	B	Disable APA function & No drive torque output 禁用 APA 功能 &无驱动扭矩输出	500ms
17	A_SG_VH_0015	Avoid unintended drive torque from APA when vehicle speed>5kph	B	Disable APA function & No	500ms

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

		当车速大于 5 公里/小时，避免 APA 产生意外的驱动扭矩		drive torque output 禁用 APA 功能 &无驱动扭矩输出	
18	C_SG_VH_000 2	Avoid unintended provide brake torque or decrease torque 避免意外提供制动扭矩或降低扭矩	C	1>. IBS is disabled; 2>. Brake torque is actuated by hydraulically-mechanical part 3>. Not output drive torque	400ms[TBD]
19	C_SG_VH_000 3	Prevent unintended vehicle acceleration for a period greater than TBD s caused by unintended provide drive torque 防止意外提供驱动扭矩导致的车辆意外加速超过 TBDs	C	Not send drive torque 不发送驱动扭矩	500ms[TBD]
20	C_SG_VH_000 4	Prevent not provide the yaw torque or provide low yaw torque during vehicle destabilization situation 防止在车辆不稳定的情况下不提供横摆力矩或者横摆力矩过低	C	1>. IBS is disabled; 2>. Brake torque is actuated by hydraulically-mechanical part	200ms[TBD]
21	C_SG_VH_000 7	Prevent vehicle unintended movement due to loss/insufficient of holding force 防止车辆因驻车力丢失或者不足而发生意外移动	C	Vehicle Standstill 车辆静止	500ms[TBD]

 ATOM	Technical Safety Concept	Draft
		Rev: 1.0

2.2 Related functional safety requirements 功能安全需求

VCU functional safety requirements includes FSRs derived from safety goals introduced in above chapter and FSRs allocated from other technical fields such as ADAS and Chassis. Detailed requirements are included as an attachment below:

VCU 功能安全要求包括从上一章介绍的安全目标中导出的 **FSR**，以及从 **ADAS** 和底盘等其他域分配的 **FSR**。具体要求包含在以下附件中：



ATOM_FSR_VCU_
V1.11_20240103.

	Technical Safety Concept	Draft
		Rev: 1.0

3. General System Safety Strategy

This section concentrates on high level safety strategy as to how each safety goal is satisfied technically and how faults in the VCU are diagnosed and the initial steps towards reacting to achieve a safe state. Safety mechanisms described here are contained in the following:

本节集中讨论总体安全策略，即如何在技术上满足每个安全目标，如何诊断VCU中的故障，以及为实现安全状态而做出反应的初始步骤。此处描述的安全机制包含在以下内容中

- 1) MCU
- 2) SBC
- 3) External peripheral parts
- 4) EVPT Basic Software
- 5) ATOM Application Software

3.1 MCU Hardware integrity MCU 硬件完整性

The MCU achieves a safe state when a failure is detected within the MCU via the TC377 internal safety mechanisms and is either reported to the VCU or trigger the safe state transition by itself, eg. Application reset or fail silent.

当通过TC377内部安全机制在MCU内检测到故障时，进行故障处理使MCU实现安全状态，包括报告给VCU，触发reset或停止外部通讯。

The safety software runs in the lockstep core to monitor faults of the processing units and internal SMs cover memory including SRAM, flash, and registers. Infrastructure like PMS, clock system, internal bus, timers, DMA, Interrupt Router, etc, are all protected by safety mechanisms provided by Aurix MCU.

安全软件运行在锁步核中，以监测处理单元和内部SM的故障，包括SRAM、FLASH和寄存器。PMS、时钟系统、内部总线、定时器、DMA、中断路由器等都受到Aurix MCU提供的安全机制的保护。

3.2 SBC Hardware integrity SBC 硬件完整性

The SBC TLE8888 has a long service history in the market and proves to be a well trusted design while it's not developed following ISO 26262 process. It contains three parts of functionalities as below:

SBC TLE8888 在市场上有着长久的使用历史，市场数据证明它是一款值得信赖的设计，但它不是按照 ISO 26262 流程开发的。它包含以下三部分功能：

	Technical Safety Concept	Draft
		Rev: 1.0

- 1) Power regulation to supply 3.3v MCU and 5.0v peripherals
- 2) External watchdog timer features window and question answer mechanism
- 3) CAN transceiver
 - a) 为 3.3v MCU 和 5.0v 外围设备供电的电源调节
 - b) 外部看门狗定时器具有窗口和问答机制
 - c) CAN 收发器

Considering its application purpose and safety contribution in this program. The SBC can be covered by MCU safety mechanisms such as external power supply monitoring, watchdog start up self test and E2E communication protection.

考虑到其在本项目中的应用目的和安全贡献。SBC 可以由 MCU 安全机制覆盖，如外部电源监控、看门狗启动自检和 E2E 通信保护。

3.3 External peripheral parts integrity 外围件完整性

The VCU controller achieve a safe state when a failure is detected in the peripheral parts via component self test, MCU diagnostic or End to End communication protection. These detection and mitigation methods are further described in HW integrity section.

当通过部件自检、MCU 诊断或 E2E 通信保护在外围部件中检测到故障时，VCU 控制器实现安全状态。这些检测和缓解方法将在硬件完整性部分中进一步描述。

3.4 Software integrity 软件完整性

Autosar BSW, EVPT BSW and safety related VCU are all developed as per ISO26262 ASIL C process, to ensure that systematic failure is acceptably low. ASIL decomposition is performed between software and memory partitioning for SW with different level is done to ensure independence and ensure the freedom from interference.

Autosar BSW、EVPT BSW 和安全相关 VCU 都是根据 ISO26262 ASIL C 流程开发的，以确保系统故障在可接受的范围内。由于在软件之间存在 ASIL 分解，对不同 ASIL 的软件进行内存分区，以确保独立性和不受干扰。

3.5 System safe states 安全状态

The acceptable system safe states for VCU system include switching into neutral gear, cutting off drive torque, limited provision of drive torque, cutting off high voltage supply, fail silent or warning. The safe state transition can be achieved by the Aurix BSW or VCU depending on the fault class.

对于 VCU 系统而言，可选择的系统安全状态包括切换到空档、切断驱动、限制驱动、停止通信或者故障报警。根据故障类别，Aurix BSW 或 VCU 可以实现安全状态转换。

	Technical Safety Concept	Draft
		Rev: 1.0

3.5.1 Fail silent 故障静默

Fail silent mean the MCU will stop all CAN communication, which is triggered in some cases when MCU internal failure occurs and reset at multiple levels have to be adopted to recover the failures.

故障静默意味着 MCU 将停止所有 CAN 通信，在某些情况下，当 MCU 发生内部故障时，会触发该通信，并且必须采用多级 reset 来恢复故障

3.5.2 Switching into neutral gear 切换到空挡

For faults which might violate the gear control safety goals, when detected mitigation shall be performed to switch the current gear into neutral so that no hazardous drive output can be released.

对于可能违反档位控制安全目标的故障，当检测到缓解措施时，应将当前档位切换到空挡，从而不会释放危险的驱动输出

3.5.3 No drive output 无扭矩输出

No drive output is defined as safe state as the HARA evaluate the loss of propulsion as QM, and when failures potentially resulting in unintended or too much drive torque occur, cutting off drive shall be defined as the safe state.

当前 HARA 将动力丢失评估为 QM，0 驱动扭矩输出被定义为安全状态，当发生可能导致非预期或过大驱动转矩的故障时，可以将 0 驱动扭矩定义为安全状态。

3.5.4 limited drive torque 限制驱动扭矩

Under some circumstances, the fault is not as critical and a limit for the drive to limp home is possible, so the limited drive torque can be used as the safe state here.

在某些情况下，故障并不那么严重，跛行是可行的选项，因此限制扭矩可以用作此处的安全状态。

3.5.5 Warning 故障报警

For latent faults or dual point faults, the commonly used strategy is to issue a warning to HMI as the failure condition is not met until another independent hardware fault occurs.

对于潜伏故障或双点故障等随机硬件故障，通常使用的策略是向 HMI 发出警告，因为直到发生另一个独立的硬件故障时才满足系统失效条件。

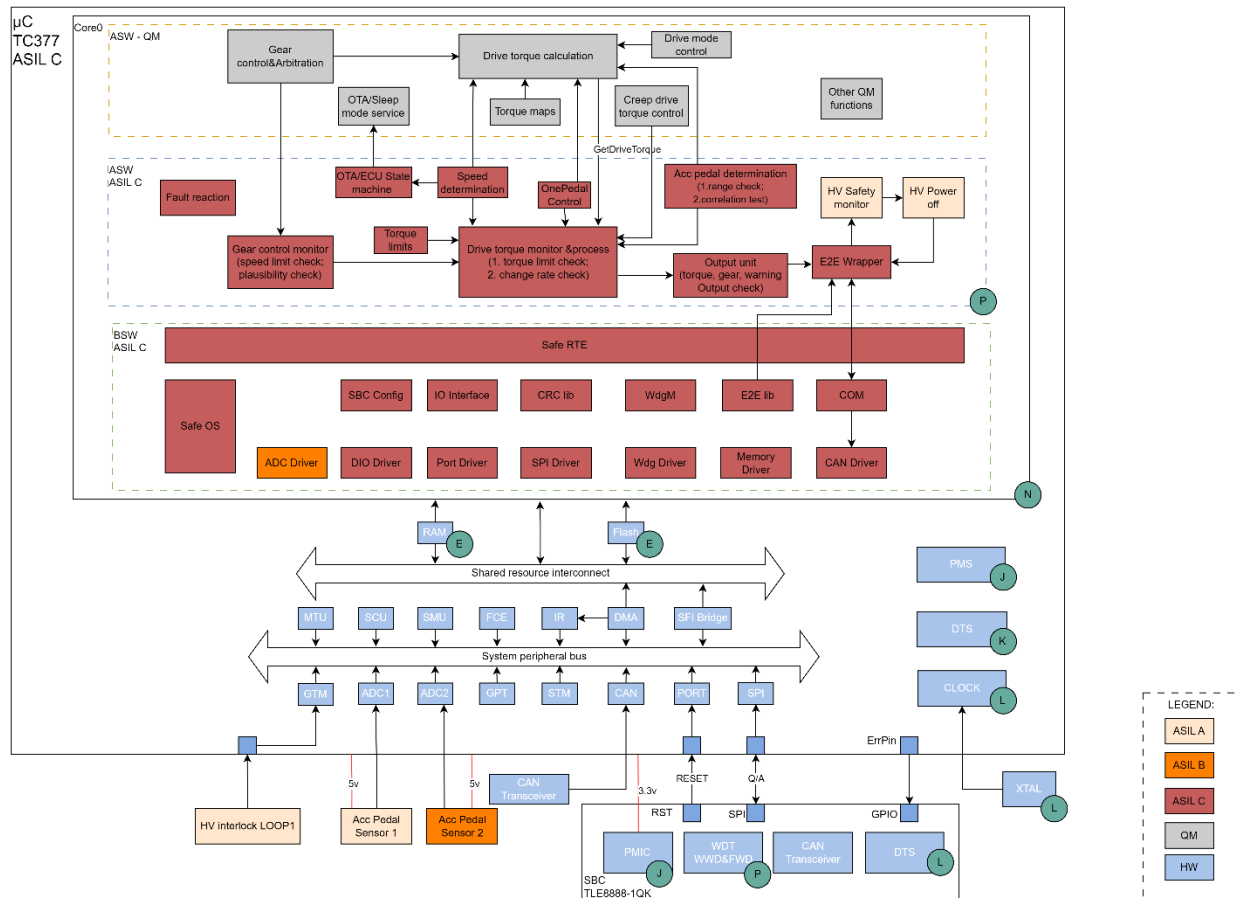


4. System Safety Architecture

4.1 VCU System Block Diagram

The VCU ECU system is mainly composed of a microcontroller and a system basic chip, with SPI and GPIO as their internal interface. Plus, the ECU is externally interfaced with the acceleration pedal position sensors, the high-voltage interlock circuit 1, the brake light switch and the CAN bus.

VCU ECU 系统主要由 MCU，SBC 和 CAN Transceiver 等组成，内部接口为 SPI 和 GPIO。此外，ECU 与加速踏板位置传感器、高压互锁电路 1、制动灯开关和 CAN 总线进行外部接口连接。



	Technical Safety Concept	Draft
		Rev: 1.0

4.2 System Block Description

Below table describes the related blocks, input and output interfaces

下表描述了相关的模块、以及这些模块的输入和输出接口

Block name	Description	Input	Output
MCU	<p>TC377 is Infineon microcontroller which supports up to ASIL D safety application. It features 2 lockstep CPU cores and a non lockstep CPU core.</p> <p>TC377 是英飞凌微控制器，支持高达 ASIL D 的安全应用。它具有 2 个锁步核 CPU 和一个非锁步核 CPU。</p>	CANFD Hw.x Reset Power	CANFD
SBC	<p>The SBC TLE8888-1QK is composed of PMIC, watchdog timer and CAN transiever. The chip is not developed based on ISO 26262 while it's long serviced component and commonly used in the market. It can be classified as CL3 component.</p> <p>SBC TLE8888-1QK 由 PMIC、看门狗定时器和 CAN 收发器组成。该芯片不是基于 ISO 26262 开发的，但它是一种长期服务的组件，在市场上很常用。它可以归类为 CL3 硬件</p>	ERRB SPI Power	Reset SPI
Acceleration pedal sensor	<p>The redundant sensors provides HW analog voltage signal to represent the pedal position. The redundant signals will be processed and checked in MCU side.</p> <p>冗余传感器提供 HW 模拟电压信号以表示踏板位置。冗余信号将在 MCU 侧进行处理和检查。</p>	Power	HW.x
HV interlock LOOP1	<p>MCU monitor the frequency of HW connected pin, abnormal frequency means HV interlock issue</p> <p>MCU 监控 HW 连接引脚的频率，频率异常表示 HV 回路存在互锁问题</p>		HW.x
Gear control &Arbitration	<p>Recieve gear shift requests and arbitrate among different request sources.</p>	PRND, IVI, IBS gear requests Vehicle power status Driver off signals charging status	Gear status;
Gear control monitor	<p>Continuous monitoring of gear shift conditions via speed, brake pedal, and gear shift request signals.</p>	PRND, IVI, IBS gear requests	Gear status;

 ATOM	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

		Vehicle power status Driver off signals	Error flag
Drive torque calculation	Determine drive torque via drive torque map based on inputs	Vehicle speed, Gear status, Acc pedal position Drive mode OnePedal mode status Brake pedal status	Drive torque
Drive torque monitor & process	Determine drive torque limits based on inputs; Compare drive torque against the limits; Process VDC/TCS/DTC/Regen/ADAS torque requests from IBS and do range check Arbitrate among different torque request sources.	Vehicle speed, Gear status, Acc pedal position Drive mode OnePedal mode status Brake pedal status	Drive torque Error flag
Creep drive torque control	Control the creep drive torque output	Vehicle speed, Gear status, Brake pedal status	Drive torque
Drive mode control	Determine drive mode among Sport/Normal/ECO based on inputs;	IVI request	Drive mode status
Fault reaction	Collect fault flags and transition into safe state	fault flags	Enable flag Warning
OTA/Sleep mode service	Services to perform OTA update or ECU mode transition		
OTA/ECU State machine	State machine to determine the activation/deactivation of OTA update or ECU mode transition	Vehicle speed	activation flag
Acc pedal determination	Sample the acceleration pedal position sensor signals Convert the analog signals into digital signals Verify and determine the Acc pedal position value	Hw.AP1 Hw.AP2	Acc pedal position value
One Pedal control	Determine one pedal mode active or not based on inputs;	IVI request	One pedal mode status
E2E Wrapper	Input CAN message E2E check and validity check; Output CAN signals E2E package	CAN message	CAN message

	Technical Safety Concept	Draft
		Rev: 1.0

HV Safety monitor	High voltage system insulation and interlock monitor	Hw.interlock BMS insulation status BMS interlock status	HMI warning HV power off activation
HV Power off	The procedure to switch the HV power supply off	HV power off activation	
Output unit	Set CAN message including gear, torque, HMI status	gear, torque, HMI status	CAN message
PMIC	Power supply regulators to supply 3.3v MCU and 5v Peripherals	12v Battery power	3.3v and 5v power
Watchdog	Provide window watchdog and functional watchdog, which supports temporal and logical supervision of the operation of MCU	SPI	SPI reset
CAN Transceivers	Tx and Rx of Powertrain CAN, Chassis CAN, charging CAN messages		

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

5. Detailed Safety mechanisms

This section introduces the implementation of safety strategies for each safety goals, including the detailed safety mechanisms to detect and mitigate faults and to achieve a safe state. The hardware integrity is contained in a separate section.

本节介绍了每个安全目标的安全策略的实施，包括检测和缓解故障以及实现安全状态的详细安全机制，硬件完整性包含在单独的章节中。

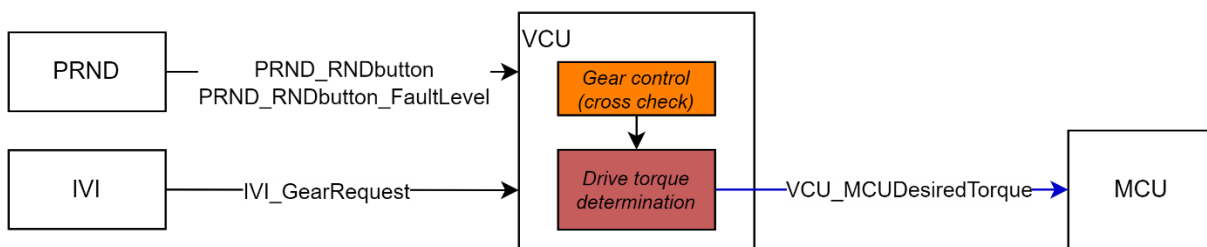
5.1 P_SG_VH_0002

Prevent motion in opposite direction due to engaged reverse gear

Safe state: Shift to N

FTTI: 500ms

ASIL: B



- Data flow for gear shift:

1. PRND sends *PRND_RNDbutton* and *PRND_RNDbutton_FaultLevel*
Or IVI sends gear request *IVI_GearRequest*
2. VCU arbitrates and determines the target gear *int.TargetGear=P/R/N/D*
3. VCU outputs target drive torque *VCU_MCUDesiredTorque* based on *int.TargetGear=P/R/N/D*

- General strategy:

The system "VCU" shall regard the safe state as shift to N

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

- CAN signals input check:

VCU shall ensure the correctness of safety input signals before usage in algorithm, E2E check and validity check will be performed for below signals:

- PRND_RNDbutton
- PRND_RNDbutton_FaultLevel
- IVI_GearRequest

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

VCU shall check the valid request signal shall not be less than 3 frames to avoid disturbance. If the check fails, VCU shall decline the gear shift request, and release a warning to HMI.

- **CAN signals output protection:**

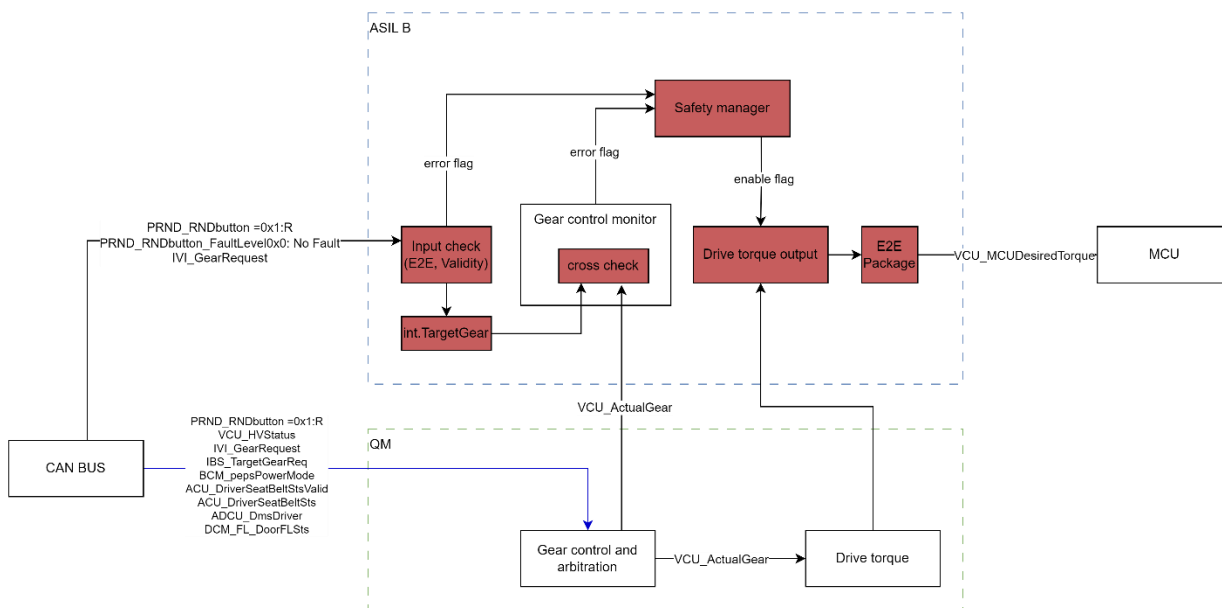
VCU shall ensure the integrity of safety output signals before sending to BUS, E2E protection will be performed for below signals:

- VCU_MCUDesiredTorque

- **R/D shift cross check:**

VCU shall do cross check before gear shift is actually executed. The cross check software shall be independent from the intended functionality.

When R/D shift occurs, but int.TargetGear is not the same for 5 frames, VCU shall shift the current gear to N.



5.2 P_SG_VH_0003

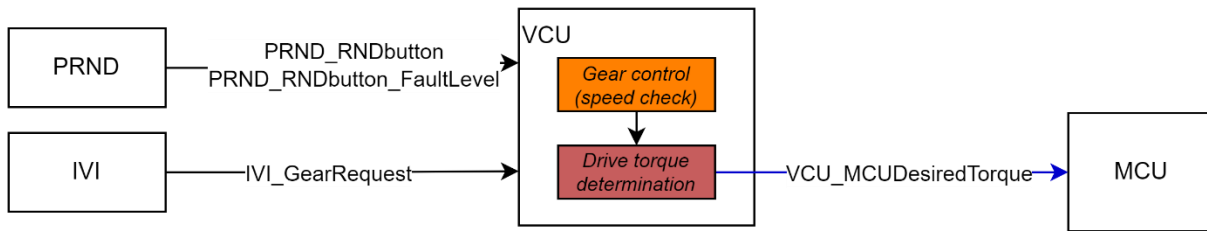
Prevent unintended deceleration due to engaged reverse gear.

Safe state: **Shift to N**

FTTI: 500ms

ASIL: B

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0



- **General strategy:**

The system "VCU" shall regard the safe state as **shift to N**

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

- **Speed check when gear shift from D to R:**

When current gear status is D and the target gear *int.TargetGear=R*, VCU shall check the vehicle speed, if speed is over threshold (18 km/h, tbd), VCU shall decline the gear shift request and release a warning.

5.3 P_SG_VH_0004

Prevent Gear position display error.

Safe state: **All gear flash**

FTTI: 500ms

ASIL: B

- **General strategy:**

The system "VCU" shall regard the safe state as **Report error flag** or **fail silent**

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

- **CAN signals output protection:**

VCU shall ensure the integrity of safety output signals before sending to BUS, E2E protection will be performed for below signals:

- VCU_ActualGear

- **Gear status integrity:**

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

For the integrity of the gear status, the safety strategy can be covered by SG02/ SG03 / SG05, please refer to Chapter 5.6.2 for details.

VCU_ActualGear shall be set as invalid if the gear status is confirmed to be wrong.

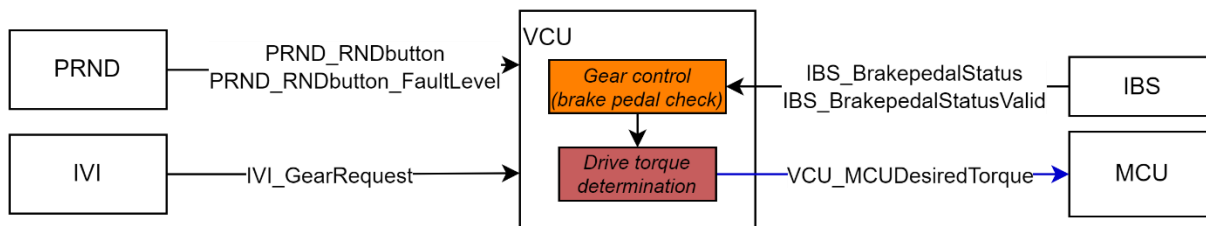
5.4 P_SG_VH_0005

Prevent longitudinal motion due to unintended driving gear engaged.

Safe state: Shift to N

FTTI: 500ms

ASIL: B



● General strategy:

The system "VCU" shall regard the safe state as **shift to N**

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

● CAN signals input check:

VCU shall ensure the correctness of safety input signals before usage in algorithm, E2E check and validity check will be performed for below signals:

- IBS_BrakepedalStatus
- IBS_BrakepedalStatusValid

If the check fails, VCU shall decline the gear shift request and release a warning to HMI.

● N/P shift to D/R integrity:

To avoid unintended gear shift into driving gears, VCU shall only permit to shift into D/R from N/P when the brake pedal is actually pressed. If this check fails, VCU shall decline the gear shift request and release a warning to HMI.

	Technical Safety Concept	Draft
		Rev: 1.0

5.5 P_SG_VH_0009

Prevent vehicle from unintended movement due to unintended provide drive torque

Safe state: No torque output

FTTI: 500ms

ASIL: B

- **General strategy:**

The system "VCU" shall regard the safe state as No Torque Output(0 N.m) defined as below:

- 1, Set the Torque request signal to 0N.m;
- 2, Shut off CAN communication.

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

[The safety strategy of input and output communication protection for SG09 can be covered by C_SG_VH_0010, please refer to Chapter 5.6.2 for details.](#)

- **Drive torque monitoring:**

VCU shall check to ensure no drive torque request if it's N or P gear.

The creep torque control shall be limited to thresholds.

5.6 P_SG_VH_0010

Prevent vehicle acceleration greater than TBD m/s² for a period greater than 500ms(TBD) caused by provided more drive torque than requested

Safe state: No torque output

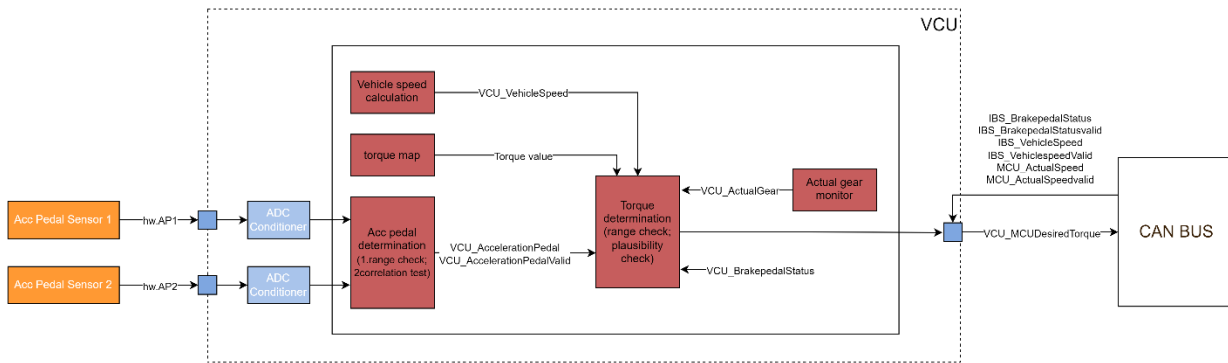
FTTI: 500ms

ASIL: C

- **Data flow for drive torque increase:**

VCU looks up the torque map based on inputs including drive mode, gear status, brake pedal status, acceleration pedal position and vehicle speed.

	<h1>Technical Safety Concept</h1>		Draft
			Rev: 1.0



● General strategy:

The system "VCU" shall regard the safe state as No Torque Output(0 N.m) defined as below:

- 1, Set the Torque request signal to 0N.m;
- 2, Shut off CAN communication.

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

● CAN signals input check:

VCU shall ensure the correctness of safety input signals before usage in algorithm, E2E check and validity check will be performed for below signals:

- IBS_BrakepedalStatus
- IBS_VehicleSpeed
- IBS_VehiclespeedValid
- MCU_ActualSpeed
- MCU_ActualSpeedValid

If the check fails, VCU shall set the drive request to 0Nm and release a warning to HMI.

● CAN signals output protection:

VCU shall ensure the integrity of safety output signals before sending to BUS, E2E protection will be performed for below signals:

- VCU_MCU_DesiredTorque

● Acceleration pedal signal range check:

VCU shall check the range of input signals hw.AP1 and hw.AP2:

If only one signal value is out of 0-5v normal range, the other signal will be used for pedal position calculation and simultaneously set VCU to limp home mode.

In case both hw.AP1 and hw.AP2 are out of range, the drive torque will be degraded to a predefined value(10%, tbd) and trigger the turtle lamp.

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

- **Acceleration pedal signal cross check:**

VCU shall check the difference between input signals hw.AP1 and hw.AP2, if the gap is more than safety threshold, the smaller value shall be used for pedal position calculation and simultaneously set VCU to limp home mode.

VCU shall check whether or not the proportion of hw.AP1 and hw.AP2 is the predefined value, if not, the drive torque will be degraded to a predefined value(10%, tbd) and trigger the turtle lamp.

- **CCF avoidance:**

As ASIL decomposition is performed between hw.AP1 and hw.AP2 channels, the two channels can be implemented as ASIL B(C) and ASIL A(C) respectively and the independence shall be ensured.

VCU shall implement redundant independent analog input channels using different A/D converters for each safety-relevant input signal.

Power supply for sensor1 and sensor2 shall be diagnosable or separate from each other.

The slope of sensor output shall be different and proportional to each other.

- **Vehicle speed calculation:**

In normal situation, VCU will use the speed signal *IBS_VehicleSpeed* from braking system to calculate the drive torque. As a safe state, though, VCU shall use the electric motor speed signal *MCU_ActualSpeed* to calculate a substitute vehicle speed in case of IBS speed signal invalid or communication failure. Warning shall be issued to HMI if such failure is detected.

To ensure the software integrity, the speed calculation inputs shall be E2E protected and the module itself shall be deployed in the ASIL C environment.

- **Torque map integrity:**

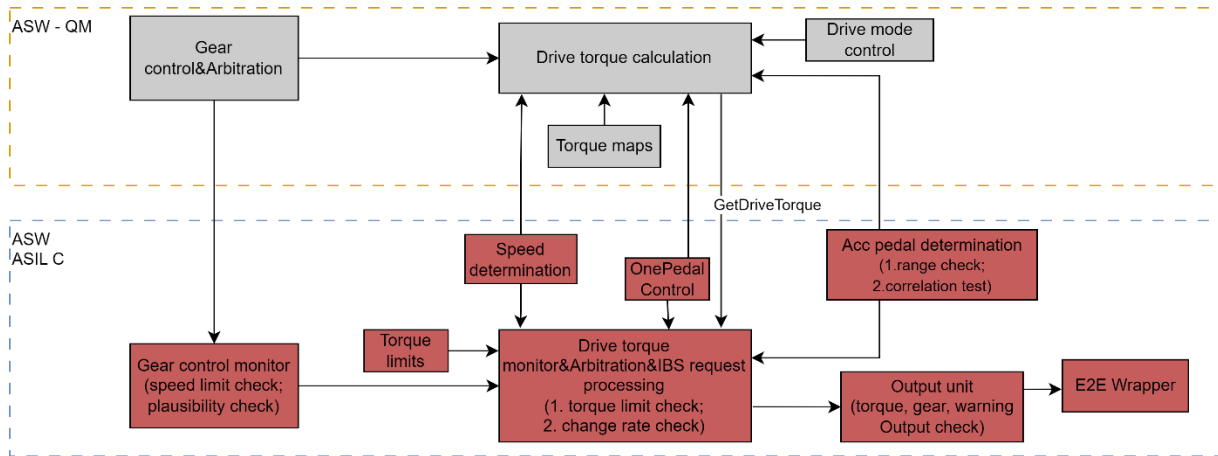
The torque map shall be redundantly checked by the simplified torque limits stored in NVM. The redundancy can facilitate the comparison of drive torque.

- **Drive torque monitoring:**

VCU shall do output check to ensure no abrupt increase in torque more than 50Nm(TBD) occur between two succeeding torque request signals. In case this check fails, *VCU_MCU_DesiredTorque* shall be set 0Nm and an error reported

VCU shall check the value of requested torque against the safety limit in below table under given acceleration pedal position and vehicle speed, if over limit is detected, *VCU_MCU_DesiredTorque* shall be set 0Nm and an error reported.

	AccrPedl	0	10	20	30	40	50	60	70	80	90	100
Max	v < =60km/h	0	50	90	120	150	180	210	240	270	300	300
	v > 60km/h	0	50	90	100	121	147	180	201	221	240	240
Min		-154	-80	-20	0	0	0	0	0	0	0	0



5.7 P_SG_VH_0012

Prevent vehicle unintended deceleration for longer than 500ms(TBD) when vehicle speed is above the creep speed caused by provide reverse drive torque.

Safe state: No torque output

FTTI: 500ms

ASIL: C

The safety strategy for SG12 can be covered by SG10, please refer to the relevant chapter for details.

5.8 P_SG_VH_0013

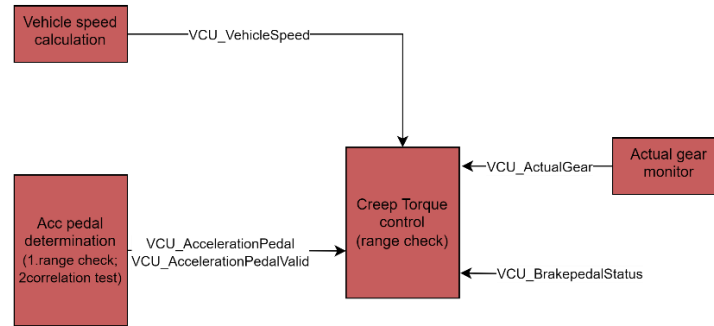
Prevent providing opposite torque against driver's requirements when the vehicle speed is lower than the creep speed.

Safe state: No torque output

FTTI: 500ms

ASIL: B

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0



- **General strategy:**

The system "VCU" shall regard the safe state as No Torque Output(0 N.m) defined as below:

- 1, Set the Torque request signal to 0N.m;
- 2, Shut off CAN communication.

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

- **Range check:**

VCU shall check in D gear, creep drive torque is > 0Nm

VCU shall check in R gear, creep drive torque is < 0Nm

5.9 P_SG_VH_0014

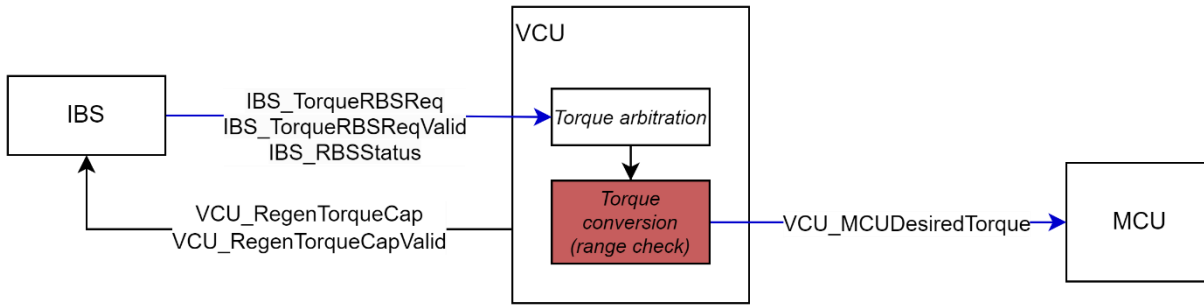
Prevent unintended vehicle deceleration for a period greater than TBD s caused by unintended implement the braking energy regeneration.

Safe state: No torque output

FTTI: 500ms

ASIL: C

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0



- Data flow for regenerative drive torque output:

VCU sends the max. effective regenerative signals *VCU_RegenTorqueCap* and *VCU_RegenTorqueCapValid* to IBS -> IBS sends regenerative request via *IBS_TorqueRBSReq*, *IBS_RBSSStatus* and *IBS_TorqueRBSReqValid*. -> VCU computes negative drive torque request continually -> MCU execute drive torque request *VCU_MCUDesiredTorque* from VCU.

- General strategy:

The system "VCU" shall regard the safe state as No Torque Output(0 N.m) defined as below:

- 1, Set the Torque request signal to 0N.m;
- 2, Shut off CAN communication.

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

- CAN signals input check:

VCU shall ensure the correctness of safety input signals before usage in algorithm, E2E check and validity check will be performed for below signals, if the check fails, VCU shall decline RBS request and feedback the error flag *VCU_RegenTorqueCapValid* to IBS:

- IBS_TorqueRBSReq
- IBS_TorqueRBSReqValid
- IBS_RBSSStatus

- CAN signals output protection:

VCU shall ensure the integrity of safety output signals before sending to BUS, E2E protection will be performed for below signals:

- VCU_RegenTorqueCap
- VCU_RegenTorqueCapValid

- Regenerative torque conversion:

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

VCU shall correctly convert the *IBS_TorqueRBSReq* into *VCU_MCUDesiredTorque*, this shall be developed compliant with ISO 26262 ASIL C

VCU shall ensure that *VCU_MCUDesiredTorque* does not exceed VCU capability
VCU_RegenTorqueCap

The software to convert RBS torque request shall be protected by program flow monitoring

5.10 P_SG_VH_0017

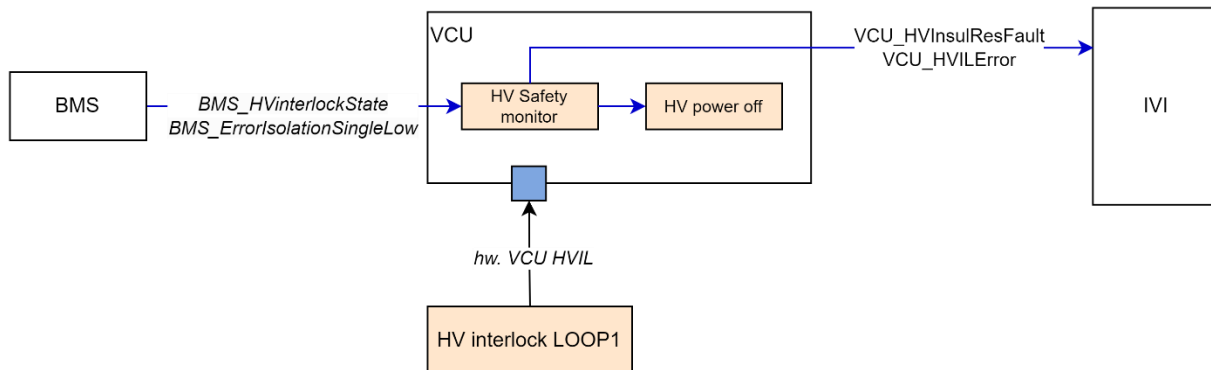
Prevent failure of high voltage monitoring.

Safe state: Turn on the fault indicator light

FTTI: 2000ms

ASIL: A

Safety monitor functions is composed of resistance monitoring and HV interconnect monitoring, for any case of failure in these functions, human body electric shock risk is exposed.



- Data flow for HV Insulation monitor:

BMS detects insulation status and periodically provides insulation fault signal to VCU *BMS_ErrorIsolationSingleLow* -> In case of isolation fault, VCU will perform the high voltage power-off process by sending *VCU_ModeRequestDCDC* = 0x2: Disabled to POD and release a warning *VCU_HVInsulResFault* to IVI

- Data flow for HV InterLock monitor:

BMS detects interlock faults at interface of the battery and motor and periodically provides interlock fault signal to VCU *BMS_HVinterlockState* -> VCU detects interlock faults via hardware signal *hw. VCU HVIL* through PIN21 and PIN70 at the charging interface of POD, in case of fault, VCU will perform the high voltage power-off process and release a warning *VCU_HVILError* to IVI

- General strategy:

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

The system "VCU" shall regard the safe state as indicate error to HMI.

The system "VCU" shall define the fault handling time interval as 1000ms for single point fault and one driving cycle for dual point fault.

- **CAN signals input check:**

VCU shall ensure the correctness of safety input signals before usage in algorithm, E2E check and validity check will be performed for below signals:

- BMS_ErrorIsolationSingleLow
- BMS_HVinterlockState

- **CAN signals output protection:**

VCU shall ensure the integrity of safety output signals before sending to BUS, E2E protection will be performed for below signals:

- VCU_HVInsulResFault
- VCU_HVILError
- VCU_ModeRequestDCDC

- **Interlock fault detection:**

VCU shall protect input signal using Safety GPIO input protection safety mechanism introduced in Chapter 7.8, in case of an error, VCU shall set *VCU_ModeRequestDCDC* = 0x2: Disabled

VCU VCU shall periodically read *BMS_ErrorIsolationSingleLow* and *BMS_HVinterlockState* to check if fault exists, if yes, VCU shall set *VCU_ModeRequestDCDC* = 0x2: Disabled

VCU hardware and OS shall provide ASIL A memory partition for VCU.

5.11 A_SG_VH_0004

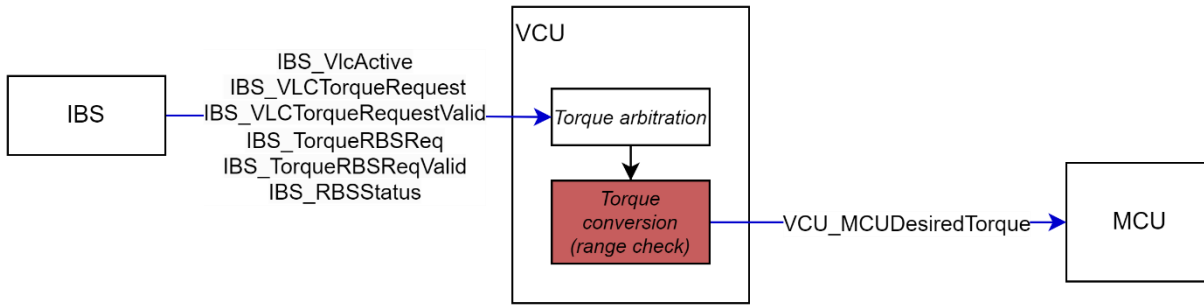
Prevent the ADAS from providing unintended drive torque.

Safe state: Disable ADAS function & No drive torque output.

FTTI: 500ms

ASIL: C

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0



- **Data flow for ADAS drive torque execution:**

1. IBS VLC module sends ADAS torque request *IBS_VlcActive*=0x1: ACTIVE, *IBS_VLCTorqueRequest* and *IBS_VLCTorqueRequestValid*=0x1: Active signals to VCU OR IBS CDD module sends ADAS torque request *IBS_RBSSStatus*=0x1: ACTIVE, *IBS_TorqueRBSReq* and *IBS_TorqueRBSReqValid*=0x1: Active signals to VCU
2. VCU arbitrates and converts $VCU_MCUDesiredTorque = \frac{IBS_VLCTorqueRequest \text{ or } IBS_TorqueRBSReq}{i(10.418) / n(0.96)}$

- **General strategy:**

The system "VCU" shall regard the safe state as ignoring ADAS torque request.

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

- **CAN signals input check:**

VCU shall ensure the correctness of safety input signals before usage in algorithm, E2E check and validity check will be performed for below signals:

- IBS_VlcActive
- IBS_VLCTorqueRequest
- IBS_VLCTorqueRequestValid
- IBS_TorqueRBSReq
- IBS_TorqueRBSReqValid
- IBS_RBSSStatus

VCU shall ignore ADAS request and set *VCU_VLCTorqueRequestAvailable* = 0x0: Not Available if the check fails.

- **CAN signals output protection:**

~~VCU shall ensure the integrity of safety output signals before sending to BUS, E2E protection will be performed for below signals:~~

- ~~■ VCU_VLCTorqueRequestAvailable~~

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

- **ADAS torque range check:**

VCU shall check the value of the converted VLC and CDD torque request against the upper and lower limits, if it's outside the range, the Request shall be neglected and error shall be reported to IBS

VCU shall set *VCU_VLCTorqueRequestAvailable* = 0x0: Not Available when any related fault is detected.

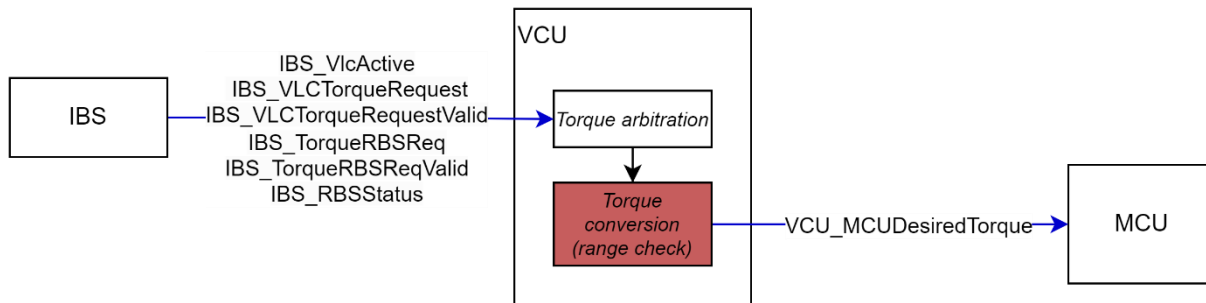
5.12 A_SG_VH_0005

Prevent vehicle unintended deceleration for longer than 500ms(TBD) when vehicle speed is above 10km/h(TBD) caused by provide reverse drive torque.

Safe state: Disable ADAS function & No drive torque output.

FTTI: 500ms

ASIL: C



The safety strategy for this safety goal can be covered by A_SG_VH_0004, please refer to related chapters for details.

5.13 A_SG_VH_0006

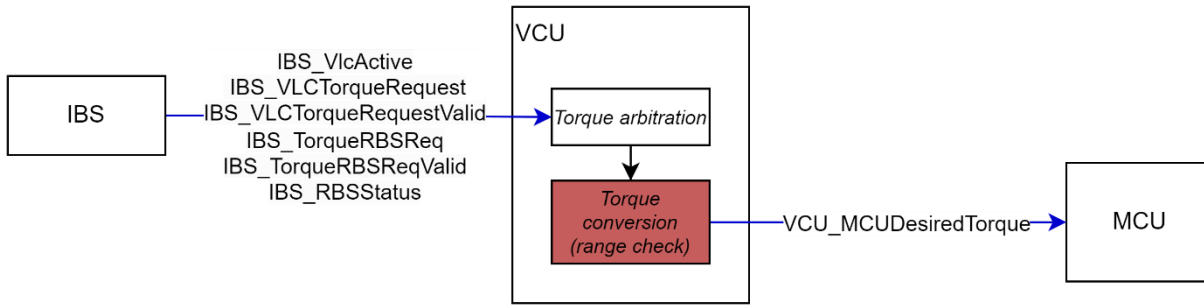
Prevent providing opposite torque against driver's requirements when the vehicle speed is lower than the creep speed.

Safe state: Disable ADAS function & No drive torque output.

FTTI: 500ms

ASIL: C

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0



The safety strategy for this safety goal can be covered by A_SG_VH_0004, please refer to related chapters for details.

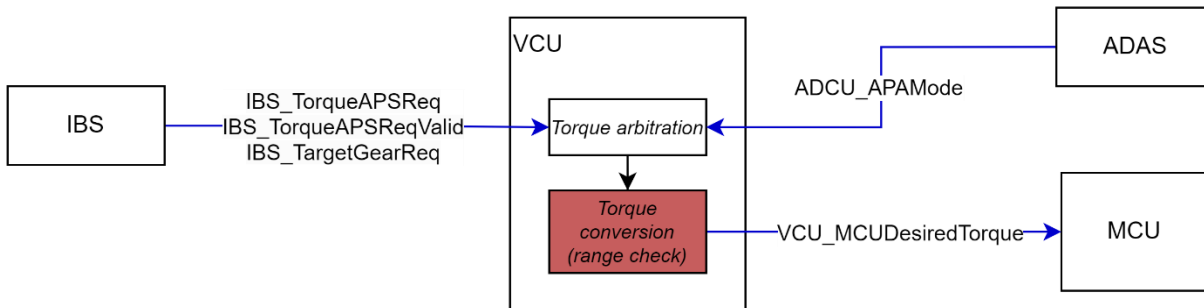
5.14 A_SG_VH_0014

Avoid unintended drive torque when APA activate with vehicle speed<5kph.

Safe state: Disable APA function & No drive torque output.

FTTI: 500ms

ASIL: B



- Data flow for APA drive torque execution:

1. IBS sends APA torque request $ADCU_APAMode = 0x4$: Guidance active/ $0x5$: Recovery interrupt, $IBS_TorqueAPSReq$, $IBS_TorqueAPSReqValid = 0x1$: Normal signals $IBS_TargetGearReq = D/R$
2. VCU arbitrates and converts $VCU_MCUDesiredTorque = IBS_VLCTorqueRequest$ or $IBS_TorqueRBSReq / i(10.418) / n(0.96)$

- General strategy:

The system "VCU" shall regard the safe state as ignoring ADAS torque request.

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

● CAN signals input check:

VCU shall ensure the correctness of safety input signals before usage in algorithm, E2E check and validity check will be performed for below signals:

- ADCU_APAMode
- IBS_TorqueAPSReq
- IBS_TorqueAPSReqValid
- IBS_TargetGearReq

● APA torque range check:

VCU shall check the value of *IBS_TorqueAPSReq* against the upper and lower limits for corresponding gear status, if it's outside the range, the request shall be neglected and error shall be reported to IBS

VCU shall set *VCU_VLCTorqueRequestAvailable* = 0x0: Not Available when any related fault is detected.

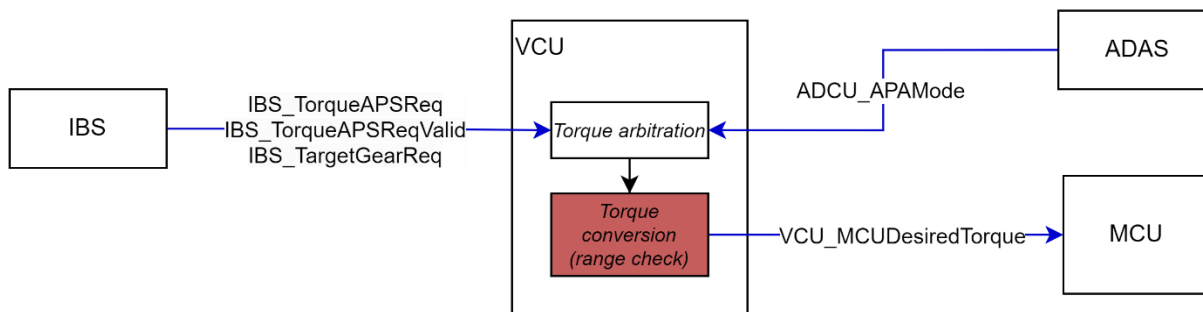
5.15 A_SG_VH_0015

Avoid unintended drive torque from APA when vehicle speed>5kph.

Safe state: Disable APA function & No drive torque output.

FTTI: 500ms

ASIL: C




The safety strategy for this safety goal can be covered by A_SG_VH_0014, please refer to related chapter for details.

5.16 C_SG_VH_0002

Avoid unintended provide brake torque.

Safe state:

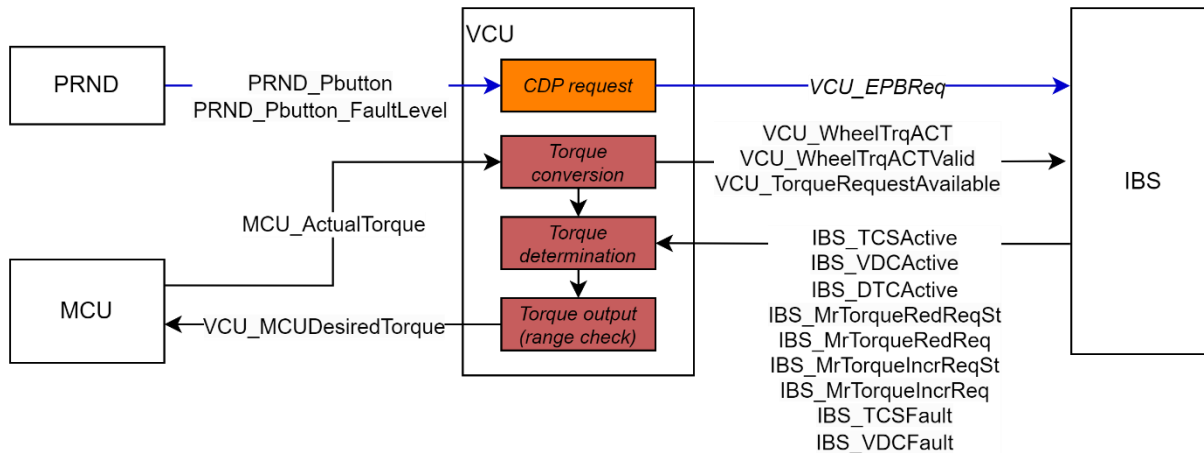
- 1>. IBS is disabled;
- 2>. Brake torque is actuated by hydraulically-mechanical part

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

3>. Not output drive torque

FTTI: 500ms

ASIL: C



- **Data flow for CDP request:**

1. P button pressed $PRND_Pbutton = 0x1$: Pressed for more than 400ms
2. VCU confirms an effective CDP request $VCU_EPBReq = 0x3$: CDP Request

- **Data flow for IBS torque control request:**

1. VDC/TCS/DTC send torque control request signals
2. VCU arbitrates and converts $VCU_MCU_DesiredTorque = IBS_MrTorqueRedReq / i(10.418) / n(0.96)$

- **General strategy:**

The system "VCU" shall regard the safe state as

1. Decline IBS drive torque request
2. NOT send CAN message.

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

- **CAN signals input check:**

VCU shall ensure the correctness of safety input signals before usage in algorithm, E2E check and validity check will be performed for below signals:

- IBS_TCSActive
- IBS_VDCActive
- IBS_DTCAActive
- IBS_MrTorqueRedReqSt

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

- IBS_MrTorqueRedReq
- IBS_MrTorqueIncrReqSt
- IBS_MrTorqueIncrReq
- IBS_TCSFault
- IBS_VDCFault

In case CRC/AliveCounter/Timeout detect an error, VCU shall neglect the IBS request and set *VCU_TorqueRequestAvailable* = 0x0: Not Available

● CAN signals output protection:

This is covered by C_SG_VH_0007

● IBS request output range check:

CDP request shall be correctly confirmed compliant with at least ASIL B

IBS torque request shall be correctly converted compliant with ASIL C

VCU shall perform range check for IBS requested torque

- $tbd < VDC/TCS \text{ requested torque} < \text{MCU_ActualTorque}$
- $\text{MCU_ActualTorque} < DTC \text{ requested torque} < tbd$

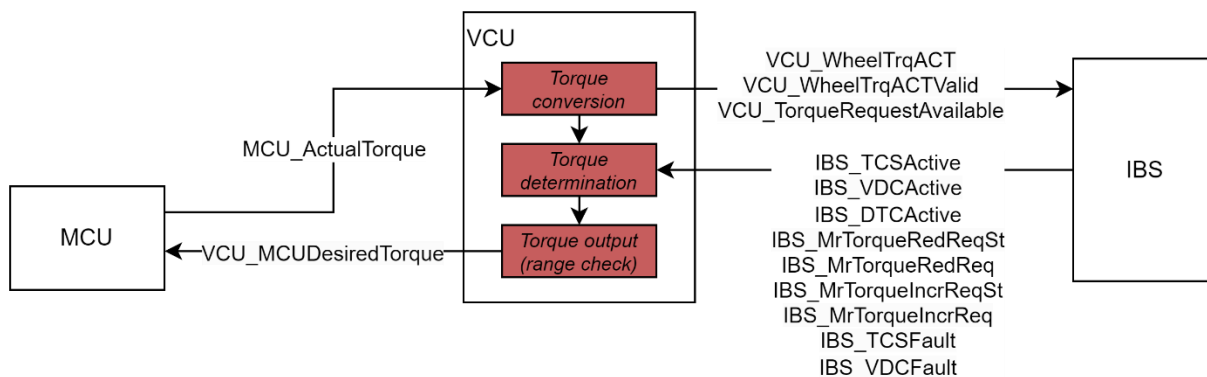
5.17 C_SG_VH_0003

Prevent unintended vehicle acceleration for a period greater than TBD s caused by unintended provide drive torque.

Safe state: Not send drive torque

FTTI: 500ms

ASIL: C



The safety strategy for this safety goal can be covered by C_SG_VH_0003, please refer to related chapter for details.

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

5.18 C_SG_VH_0004

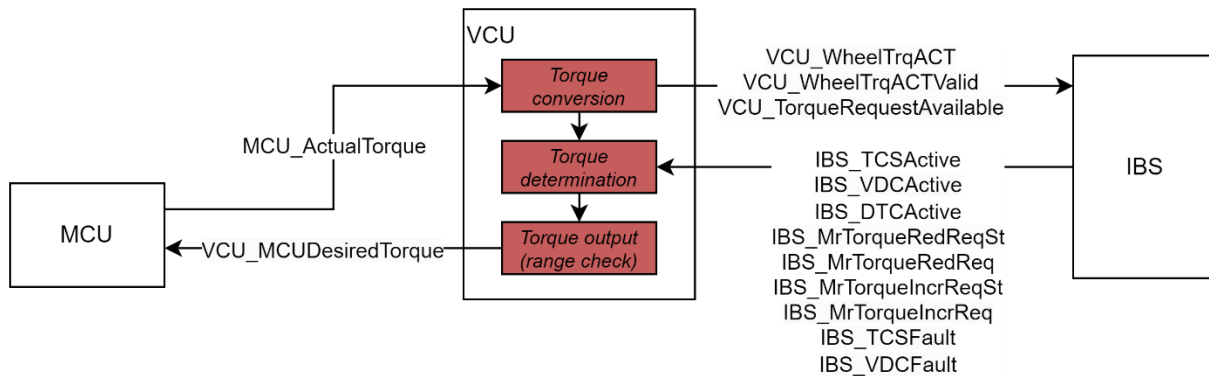
Prevent not provide the yaw torque or provide low yaw torque during vehicle destabilization situation

Safe state: 1>. IBS is disabled;

2>. Brake torque is actuated by hydraulically-mechanical part.

FTTI: 200ms

ASIL: C



- Data flow for IBS stability control:

VCU executes drive torque request or regenerative braking continually and transmits the *VCU_TorqueRequestAvailable* signal to IBS -> IBS monitors the stability situation and request VCU to reduce or increase torque if necessary, via

1. *IBS_TCSActive=0x1:Active* or *IBS_VDCActive=0x1:Active* and
2. *IBS_MrTorqueRedReqSt=0x1:ACTIVE* and *IBS_MrTorqueRedReq*,

at the same time, to execute braking stability control function via braking actuators -> VCU arbitrates multiple request and perform according to priority, among which IBS request is the highest.

- General strategy:

The system "VCU" shall regard the safe state as below:

- 1, Decline the IBS Torque request;
- 2, Report error flag.

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

- CAN signals input check:

VCU shall ensure the correctness of safety input signals before usage in algorithm, E2E check and validity check will be performed for below signals:

 ATOM	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

- IBS_TCSActive
- IBS_VDCActive
- IBS_MrTorqueRedReqSt
- IBS_MrTorqueRedReq
- IBS_TCSFault
- IBS_VDCFault
- IBS_ABSFault

If the check detects any communication error, VCU shall neglect IBS drive request and release an error flag to IBS.

If the check detects any invalid status of TCS, VDC or ABS, VCU shall degrade by limiting the vehicle speed below 20km/h.

● CAN signals output protection:

VCU shall ensure the integrity of safety output signals before sending to BUS, E2E protection will be performed for below signals:

- VCU_TorqueRequestAvailable
- VCU_WheelTrqACT
- VCU_WheelTrqACTValid

● Torque request arbitration:

IBS torque request shall be given the highest priority among all torque requests, and this logic shall be developed compliant with ASIL C

● MCU Actual torque conversion:

VCU shall ensure the correctness of the conversion of *MCU_ActualTorque*, and output *VCU_WheelTrqACT&VCU_WheelTrqACTValid* to IBS

5.19 C_SG_VH_0007

Prevent vehicle unintended movement due to loss/insufficient of holding force.

Safe state: Vehicle Standstill


FTTI: 500ms

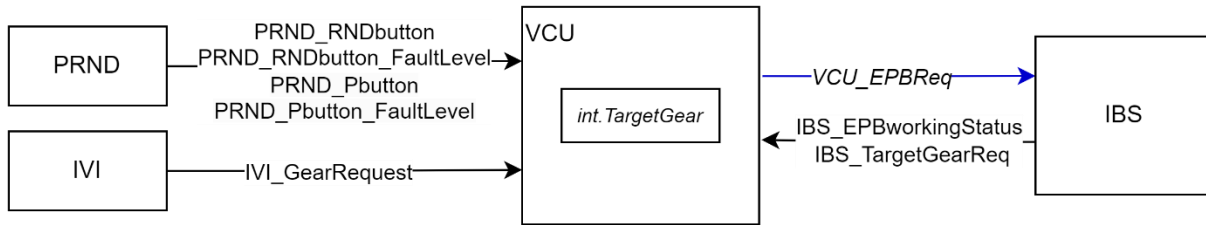
ASIL: C

● Data flow for EPB apply and release requested from VCU:

When current gear is R/N/D and target gear changes (*int.TargetGear* =P), VCU sends *VCU_EPBReq* = 0x1: Apply Request

When current gear is P and target gear changes (*int.TargetGear* =R/N/D), VCU sends *VCU_EPBReq* = 0x2: Release Request

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

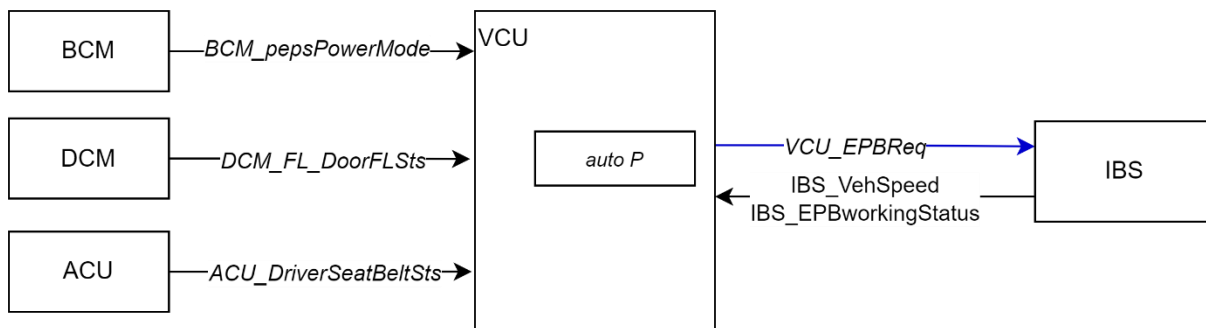


● Data flow for Auto P from VCU:

When any of following event occur, VCU will request EPB to apply

1. *VCU_Chargestatus* = Plug Detected ||
2. *BCM_pepsPowerMode* = 0x1: OFF_POWERMODE ||
3. Drive off detected, *ACU_DriverSeatBeltStsValid*= 0x1: VALID & *ACU_DriverSeatBeltSts*= 0x1: Tied & *DCM_FL_DoorFLSts* = 0x1: Opened

& Vehicle speed < 3km/h



● General strategy:

The system "VCU" shall regard the safe state as below:

- 1, Set acceleration pedal status as Invalid; OR
- 2, NOT send CAN message.

The system "VCU" shall define the fault handling time interval as 200ms for single point fault and one driving cycle for dual point fault.

● CAN signals input check:

VCU shall ensure the correctness of safety input signals before usage in algorithm, E2E check and validity check will be performed for below signals:

- BCM_pepsPowerMode
- ACU_DriverSeatBeltStsValid
- ACU_DriverSeatBeltSts
- DCM_FL_DoorFLSts

 ATOM	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

- IBS_VehSpeed
- IBS_EPBworkingStatus

If the check fails, VCU shall stop sending out the message including *VCU_EPBReq*.

- CAN signals output protection:

VCU shall ensure the integrity of safety output signals before sending to BUS, E2E protection will be performed for below signals:

- VCU_AccelerationPedal
- VCU_AccelerationPedalValid
- VCU_EPBReq

- EPB apply plausibility check:

When the conditions to apply EPB are confirmed, VCU shall check the EPB status, if *IBS_EPBworkingStatus* is not “Applied or applying” within FTTI, VCU shall stop sending out the message including *VCU_EPBReq* and trigger a HMI warning.

When the EPB actual status is “releasing”, VCU shall check the PRND and IVI status, if neither EPB releasing conditions are met, VCU shall stop sending out the message including *VCU_EPBReq* within FTTI

	Technical Safety Concept	Draft
		Rev: 1.0

6. Hardware Integrity Concept

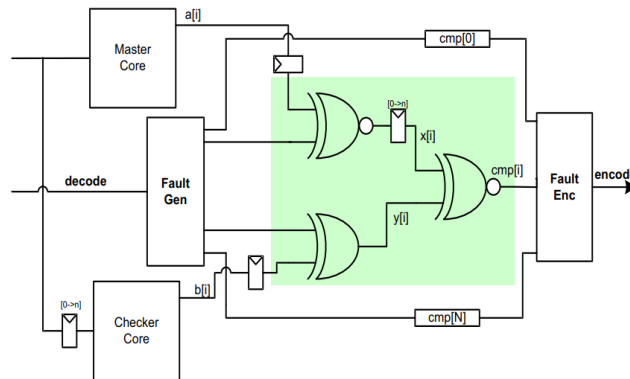
The hardware modules are building blocks of the infrastructure of functional operation and the random failures or soft errors of critical HW components can result in critical failure violating safety goals.

6.1 CPU integrity

TC377 is composed of 3 CPUs, among which CPU0 and CPU1 are lockstep CPUs and CPU2 is a non-lockstep CPU. As safety software is running on the lockstep CPU0 (TBD), so only safety mechanisms to protect CPU0 are configured.

The lockstep monitoring function is based on hardware redundancy and will compare the outputs from the master and checker core and report that a failure has occurred to the SMU. This mechanism can make sure high coverage of random hardware faults, transient faults of ALU, registers. In case error is reported, SMU will bring the VCU into safe state, ie. CPU reset or system reset.

Each core capable of lockstep also has a continuously running background self test of the lockstep comparator. The self test function will inject faults into both inputs of each of the monitored nodes and verify that the fault is correctly detected by the monitoring logic.



The CPU is a slave node of SRI bus, so the registers are protected by the internal mechanisms.

Plus, there's logical built in self test running at start up to diagnose any digital logic error of the processing unit so that latent faults are covered.

Failure mode including CPU addressing faults, ALU output incorrect or stuck at or register corruption or stuck at wrong value can be effectively detected by above mentioned SMs, so that the high DC is achieved for MCU processor parts.

Safety related software shall be operated in CPU1, which shall be configured to be running in lockstep state via *LCLCON1* register.

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

The lockstep logic shall be monitored via fault injection of LCLTEST register in LBIST, if error is detected, warning lamp shall be triggered.

~~Safety related software shall be allocated to different core from the one running it's monitored function.~~

~~VCU shall ensure that lockstep comparison mode is used for CPU0/1~~

VCU shall reset when lockstep comparison error is detected

The OS shall run core test at start up and trigger MCU reset when it fails 3 times in a row.

6.2 Interconnect integrity

The SRI Fabric connects the CPU, the DMA module, and other high bandwidth requestors to high bandwidth memories and other resources for instruction fetches and data accesses. Any R/W operation can be affected by several faults during the address phase or the data phase, resulting in incorrect or missing data, wrong addressing and so on.

The SPB connects the high speed peripherals (CPU and DMA) to the medium and low bandwidth peripherals.

Address check - The slave agent check if incoming bus transaction address belongs to the agent address space. If the slave agent does not match, an alarm is generated.

Integrity check - All SRI nodes (masters and slaves) are protected against integrity errors. If the SRI interface detects an integrity error during the address or data phases of an SRI transaction, the SRI interface triggers an alarm.

Error handling - If the SRI triggers an error interrupt service request, the SW shall evaluate the type of SRI error and trigger the most appropriate reaction.

For alarms generated from bus transaction of the safety core CPU1 and safety related memory, reset shall be triggered

6.3 DMA integrity – Reserve

The DMA moves data from source modules to destination modules without the intervention of CPU. DMA is composed of Move engine, DMARAM, and DMA channels. During DMA operations, transactions can be subject to permanent or transient faults that can affect the success of the data moves, such as data or address corruption, delay or loss of data. For these failure modes, CRC or timestamp are used to detect errors.

The DMA channel moving safety data shall be independent from channels moving non safety data and resource partition shall be configured to set master tag ID and supervisor mode.

CRC of DMA move address for safety data shall be compared with the expected value in DMA memory, if the checksums don't match, an error shall be reported.

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

CRC of DMA moved data for safety data shall be compared with the expected value in DMA memory, if the checksums don't match, an error shall be reported.

Timestamp of DMA moved data for safety data shall be checked with the previous value in DMA memory, if no update or delay more than 100ms occurs, an error shall be reported.

If any error reported from DMA safety mechanisms, VCU shall reschedule the data transfer from a redundant channel and if error still exists, system reset shall be applied.

6.4 Interrupt Router integrity

The IR is responsible for scheduling interrupt service requests to the correct service provider. A service request can be raised by internal peripherals, external hardware or Application SW. The service providers are all CPU and the DMA.

The IR is connected to all internal functional blocks, so potentially a failure in a peripheral can generate malfunctions in the IR and propagate to (CPU or DMA). And ISR in some cases function as the fault reaction, so the correct behaviour of the IR and its monitoring functions during runtime are a crucial part of the safety concept.

6.5 Memory protection

For this program, no external non volatile or volatile memory are used, so only TC377 internal memory protection is needed. The ECU platform shall provide sufficient protection when performing data transfer and read/ write access to ensure data integrity.

6.5.1 Volatile memory

The volatile memory can be affected by transient or permanent faults that can corrupt data, several blocks in the MCU have one or more dedicated SRAM, for example, CPU DSPR, LMU, GTM RAM, CAN RAM, etc .

Data in SRAM may be corrupted by permanent hardware faults such as bit stuck-at and transient hardware faults such as soft errors caused by a neutron or alpha particle. Errors during a write, caused for example by a fault in the addressing logic, may also corrupt the data in SRAM, while errors during read can lead to a wrong or corrupted loaded data. Several safety mechanisms are allocated to each [SRAM] module and monitor the correct R/W operations.

Different fault categories are monitored and detected by SRAM safety mechanisms.

- Data integrity for SRAM is ensured by an ECC/EDC mechanism, which performs SBE correction and DBE detection.
- Address failures due to wrong address generation or decoding during both read and write operation are also detected

	Technical Safety Concept	Draft
		Rev: 1.0

Error handling:

For single bit error alarm, there can be no additional reaction.

For DBE, address error and about the ASIL partitions, MCU shall trigger application reset

6.5.2 Non Volatile memory

NVM is composed of data flash(DF0 and DF1), program flash, UCB, CFS and BOOTROM.

The ECC checksum is calculated over 256 data bits and the address bits

Each NVM block storing safety data or code shall be protected by an enhanced EDC/ECC monitor which is able to detect up to TBE and correct SBE and DBE.

EDC/ECC logic shall be monitored continuously and if error detected, an alarm shall be triggered.

The NVM read path shall be protected from corruption, in case of failure an alarm shall be reported.

6.6 Clock Monitoring

The clock system consists of the clock generation unit, system PLL, peripheral PLL, CCU (clock control unit) and their control registers. Clock faults including frequency out of range or jitter can cause faulty operation of CPU, DMA, on chip buses or peripheral devices and thus impact safety. The MCU implements the primary clock system on an external crystal oscillator and uses independent back up clock source as its monitoring. When critical faults are detected, MCU shall trigger reaction to bring system into reset state.

The main clock and backup clock monitoring shall be both configured to function effectively after reset.

Register protection:

The clock control registers are write access protected by MCU internal safety mechanisms, including supervisor mode protection, ENDINIT protection and access source check.

Glitch filtering:

The clock hardware is designed that glitch above or below thresholds will be filtered, in this way the glitches of clock frequency is protected.

Loss of lock detection:

	Technical Safety Concept	Draft
		Rev: 1.0

The PLL may become unlocked, caused by a break of the crystal/ceramic resonator or the external clock line. In case of loss-of-lock, the Clock Control Unit (CCU) switches to the back-up clock, this is called the Clock Emergency Behavior.

If the system or peripheral PLL loss of lock is detected, MCU shall switch the main clock into the backup clock system and report to VCU about the error.

VCU shall trigger the fault lamp in case of the error reported from the clock monitoring system.

Frequency out of range detection:

The external crystal and the internal backup oscillator are both monitored to detect failures related to abnormal frequency. The fOSC is monitored by the oscillator watchdog to compare between crystal frequency and the backup oscillator frequency. The fBACK is monitored by counting cycles within a configured window, if cycles exceeds the thresholds, alarm will be reported.

The frequency of the system external clock source shall be monitored, if frequency out of range is detected, MCU system reset shall be triggered

The frequency of the system Backup clock shall be monitored, if frequency out of range is detected, BSW shall report to VCU about the error.

VCU shall trigger the fault lamp in case of the error reported from the clock monitoring system.

Aliveness detection:

The aliveness of the external oscillator, PLL0/1/2 and backup oscillator are monitored, if no toggling of the clock signal occur within 512 monitoring clock cycles, SMU will be notified.

MCU system shall enable clock sytem aliveness detection and reset if fault is detected.

In case the clock monitoring still reports error after reset for once, MCU shall reset once again and shut down MCU immediately if then the clock monitoring error still exists

MCU BSW shall report the error flag to VCU in case of clock related faults.

6.7 Temperature Monitoring

When operating outside the specified temperature range, the correct processing and output of many on chip devices can not be guaranteed. In the VCU system, additional temperature sensor is not deployed to measure housing temperature, while both critical heat source TC377 and TLE8888 adopt internal mechanism to handle the over temperature detection and indication.

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

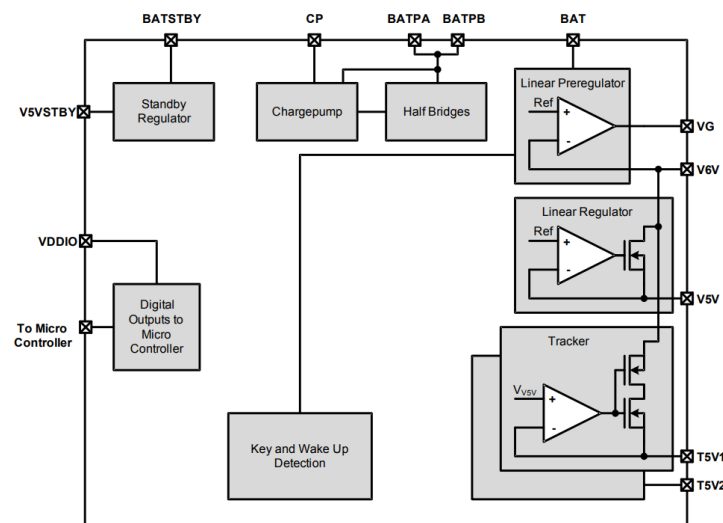
The TC377 DTS is composed by two sensors which measure the die temperature DTS and core die temperature DTSC, which generate a measurement result that indicate directly the current temperature and stored in the register. When the DTS comparator checks that threshold of range is crossed, related DTS alarm will be generated to SMU, as such TC377 shall inhibit the system output by reset or system shutdown and indicate a warning to HMI. The threshold shall be configured such that the safety output cannot be corrupted. A plausibility check between DTS and DTSC is performed at runtime to detect single and latent faults, a difference more than 9 degree(TBD) will switch into the safe state.

The TLE8888-1QK features internal temperature protection, and shut down the power supply when over temperature is detected.

6.8 Power supply monitoring

Please refer to EVPT power tree for detailed power management design.

TLE8888-1QK converts the 12v vehicle battery into 3.3v and 5v output rails so that it can supply the ECU components including the MCU and its peripherals respectively. Plus, TLE8888 provides functionality of HW-based power supply monitoring of the battery over voltage and 5v output OV/UV. When OV or UV events of BAT, 3.3v or 5v output occur, the microcontroller will be reset and the cause of the reset will be available in the status register.



For Aurix TC377 in this program, the external nominal system supply from external regulator is 3.3 V. The Embedded Voltage Regulators (EVR) in turn generate the VDDP3 and VDD supply voltages required internally for the core, flash and port domains. These output supply rails and also the external supply are monitored regarding under voltage and over voltage events via MCU

 ATOM	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

internal safety mechanisms. TC377 offers a primary and a secondary monitor based on two independent bandgap references to implement safety requirements. The primary monitor ensures that the micro controller is put into a cold PORST rest state when the UV condition is satisfied, while the secondary monitor detects UV and OV events and triggers alarms to SMU. Monitors are realized via dedicated 8 bit ADC converters and result comparators.

Aside from monitoring during operation, TC377 features PBIST and MONBIST to test the monitors and improve latency faults coverage. The PBIST allows the testing of supply levels, power functions and voltage monitors before cold PORST reset release. And after reset release, MONBIST for the secondary monitors and alarm generation path can be carried out via configuration registers.

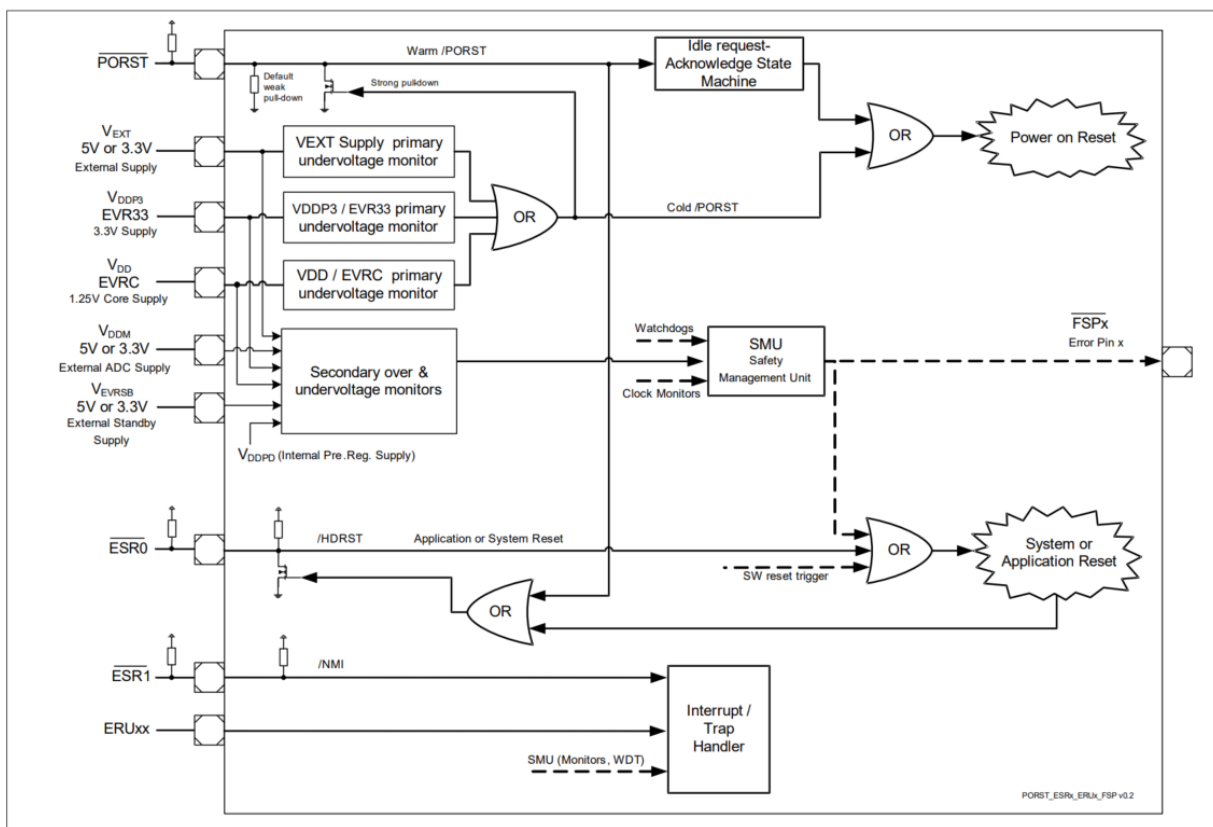


Figure 111 Monitoring and Reset Pins

An buffer capacitor shall be designed to reduce power spikes and stabilize the power supply from the vehicle battery.

The external voltage supply for MCU shall be monitored regarding the overvoltage and undervoltage violation, the thresholds of voltage range can refer to the datasheet. If OV or UV occur, the power shall be cut off.

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

The external voltage supply shall be monitored regarding the overvoltage and undervoltage violation, the thresholds of voltage range can refer to the datasheet. If OV or UV occur, the power shall be cut off.

6.9 Latent fault strategy

Details of the methodology for covering latent faults are elaborated in the TC3XX safety manual, the majority of the identified latent failure modes are detected via the BIST mechanism. BIST is executed as part of the power up process after OS has been initiated. In case any test fails, error flag is notified to BSW and it will mature the fault over a configurable number of clock cycles.

TC377 offers four different HW based self tests including PBIST, MBIST, LBIST and MONBIST to deal with external power supply, SRAM, digital logic and secondary voltage monitor separately.

- **PBIST** is to test the primary power supply and executed before cold PORST release and allows the testing of supply levels, power functions and voltage monitors. PBIST is enabled by default and can't be disabled by configuration.
- **LBIST** applies pseudo-random patterns generated by a PRPG (Pseudo-Random Pattern Generator) to a full-scan circuit in parallel and compacts the test responses into a signature with a MISR. During this test, MCU functionality is not available and at the end of the test, LBIST terminates with a system reset.

LBIST shall be configured to be enabled according to the user manual

LBIST results from MISR shall be compared against the expected value to detect any latent fault, in case of 3 consecutive LBIST failures, MCU shall not boot up

- **MONBIST** detects faults on secondary voltage monitors and associated alarm paths and FSP error pin routed to the stand-by SMU

MONBIST shall be configured to be enabled according to the user manual

MONBIST results shall be checked in MONBISTSTAT register after test is done and indicates a signal to warning in case of error.

- **MBIST** detects faults for SRAM at start up to detect any potential memory cell faults

6.10 Communication protection

To protect safety related CAN signals from corruption, loss, delay and other failure modes when transmitting over the CAN bus, the end to end protection mechanism is used, including CRC/

	Technical Safety Concept	Draft
		Rev: 1.0

counter/ timeout, which can cover failures from components such as CAN transceivers or connectors.

TSR_VCU_COM_01

The following CAN signals received/Transmitted by VCU shall be protected according to ATOM E2E specification.

TSR_VCU_COM_02

AliveCounter and checksum shall be calculated in the Application layer, to ensure corresponding application alive and working correctly.

TSR_VCU_COM_03

For the received signals, if checksum or AliveCounter error is detected in 5(TBD) consecutive frames or timeout occurs, the error shall be reported to the corresponding safety management module

TSR_VCU_COM_04

MCU shall enter into the safe state depending on the signal case by case.

TSR_VCU_COM_05

The VCU shall check the error status and data range of safety related signals.

6.11 Register write protection

TC377 provides several safety mechanisms to protect safety related control registers and status registers from corruption.

- **The master tag id** is checked before a write access to the safety register and only the configured source of ids are allowed to write
- **Supervisor privilege level check** – Critical module registers are defined with an access privilege level that restricts the modification to master functions with supervisor privilege level.
- **ENDINIT**- including system ENDINIT and safety ENDINIT, driven by the CPU watchdog timer and safety watchdog timer respectively. The ENDINIT have to be activated before the write access to be performed, otherwise any attempt to write a Safety ENDINIT protected SFR will be discarded , the SFR is not changed, and an alarm is generated.
Furthermore, the timeout of ENDINIT feature is monitored by the CPU watchdogs or the safety watchdog, if timeout occurs, an error is reported.
- **Flipflop Detection** – MCU provides flipflop detection for safety related modules, which need to be configured and results shall be checked by software and trigger reaction when the error is reported.

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0

Register flipflop monitoring shall be enabled for safety related modules including MTU, IR, SCU, PMS, DMA, SMU_Core, PLL and CCU.

In case error is reported by protection features including master ID tag, supervisor mode and ENDINIT, MCU shall record a DTC. In case error is reported by the flipflop detection, reset shall be performed.

6.12 GPIO input protection

To protect safety related GPIO signals from corruption, hardware shall design two redundant channels for signal transmission. This design can detect failures from pins, wiring, GTMs and so on.

The pins selected for safety GPIO shall not be adjacent to avoid common cause failure.

The GTM channels used to trigger GPIO shall be independent from each other to avoid common cause failure.

The redundant GPIO signal shall be transmitted as inverted as the main one from the sender side.

MCU software shall read both GPIO signal information and compare, in case the comparison doesn't match, an error shall be reported so that a warning shall be triggered.

6.13 ADC integrity

Redundant safety-related analog signals are delivered by the system and redundantly processed by internal resources of the EVADC. The results of the redundant processing are transported from the EVADC to a system volatile memory via the CPU or the DMA and compared by the CPU.

Assumption 1: The System Integrator shall avoid the use of adjacent pins and ADC channels belonging to the same group for the acquisition of redundant input signals. These are measures against common cause failures.

Assumption 2: The common cause failure outside the MCU due to faults in analog signals acquisition HW circuitry are detected by the system-level safety measures, e.g. design of diverse and dynamic analog inputs

 ATOM	Technical Safety Concept	Draft
		Rev: 1.0

6.14 Watchdog monitoring

VCU system has both internal and external watchdogs equipped while they function differently to protect the integrity of ECU. The internal watchdog can be enabled to monitor the code sequence and timeout but this is covered by the external watchdog, so internal watchdog timers only act as timeout monitoring of the ENDINIT, in case ENDINIT does not terminate until the timeout period, a failure will be set.

The external watchdog is a subsystem of SBC chip, which is totally independent of the MCU and can monitor the program flow via the window watchdog and functional watchdog. The window watchdog detects if it's triggered within the defined time window, if not, this'll be regarded as a failure and reset of MCU will be requested.

An external watchdog timer with question-answer protocol shall be designed to monitor the aliveness and code sequence of MCU

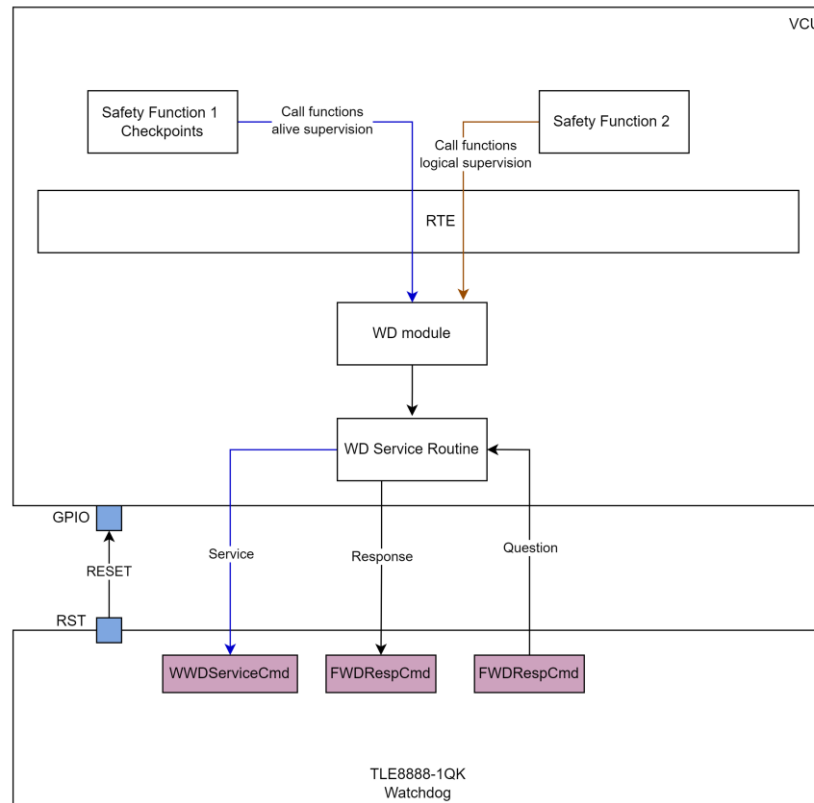
MCU BSW shall provide interface to monitor the program flow of critical VCU.

MCU BSW shall timely trigger the external watchdog and feedback correct ANSWER to SBC.

MCU shall design a SPI interface to receive the question of functional watchdog and a GPIO to set reset signal.

MCU VCU shall set appropriate checkpoints in safety related codes via provided interfaces.

	<h1>Technical Safety Concept</h1>	Draft
		Rev: 1.0



MCU shall check the functionality of watchdog at startup self test by injecting an error.

6.15 Safety management

For random hardware faults detected by internal safety mechanisms, TC377 provides a safety management module SMU to deal with, which is composed of a core SMU part and a standby SMU part. The core SMU can respond to most of alarms and the standby SMU can respond to the alarms reported from modules supplied with the standby clock.

SMU features 2 recovery timers to detect the time out of ISR or NMI response, if the consumed time exceeds the defined threshold, an alarm will be generated.

MCU software shall configure the safety management module so that the detected faults are responded properly. The configuration shall be done based on each safety mechanism.

SMU core domain aliveness can be monitored by the SMU standby domain, if Alive alarm is detected, it asserts a configured Error Pin. Then the SBC shall monitor the Error Pin and reset the MCU when necessary.

MCU software shall configure the Error Pin to be asserted in case the aliveness alarm is reported.

	Technical Safety Concept	Draft
		Rev: 1.0

MCU software shall perform a self test at start up of the SMU aliveness monitoring function according to the user manual. In case the test fail, MCU shall indicate to HMI via telltale.

FSP monitor may not be enabled as FSP is only used when the core SMU triggered ISR or NMI is not responded.