Technical Safety Concept

Abstract:

This document contains the Technical Safety Concept for all safety activities in system phase of the eCockpit system.

Original Release Revision Level	
Original Release Date	
Prepared by	
Status	
Approved By	

DOCUMENT REVIEW PROCESS

This document shall be reviewed, approved, and authorized with the following sequential process:

Sequence	Activity	Description	Person(s) Responsible
Step 1	Review	To ensure that the contents of the document are technically correct and complete.	
Step 2	Confirmation Review	To ensure that the documentation is commensurate with the Process & Procedure	
Step 3	Approve	To ensure the correct Functional Safety processes have been followed	
Step 4	Authorize	To formally agree the document and its contents	

DOCUMENT CHANGE HISTORY

REVIEW RECORD

TABLE OF CONTENTS

TABLE OF FIGURES

1 Introduction

This document outlines the Technical Safety Concept (TSC) for eCockpit for . The objective of the TSC is to describe the architecture/design intended for the eCockpit system to meet the functional requirements derived from the safety goals.

1.1 Scope

The scope of this document is to provide the safety concept details for eCockpit system based on the derived functional safety requirements and technical safety requirements, to be compliant with the ISO-26262 standards and align with the safety goals defined.

1.2 Applicable documents

eCockpit Documents

Version	Document Title	Reference
1.7	Functional Safety Requirements	[Ref 01]
1.7	Functional Safety Concept	[Ref 02]
2.2	Hazard Analysis and Risk assessment	[Ref 03]
1.3.7	Technical Safety Requirements	[Ref 04]
0.7	Safety Analysis Report	[Ref 05]
0.5	eCockpit_Project_-_SYS.3_Architectural_Design	[Ref 06]
5.8	DSXVEEP5053_CSUV_SPB_EE_Warning_Message_Catalog-FRS8_SOP_v5.8 29Aug22	[Ref 07]
-	eCockpit_Architect_HW_Design	[Ref 08]

Industry Related Standards

Reference	Document Name/Description
SAE J-2344	Guidelines for Electric Vehicle Safety
ISO 26262- Part 1-10: 2018	Road vehicles — Functional safety

1.3 Terms and definitions

Acronyms/ Abbreviations	Description
ABS	Antilock Braking System
ACC	Accessory
ACM	Airbag Control Module
ASIL	Automotive Safety Integrity Level
CAN	Controller Area Network
CRC	Cyclic Redundancy Check
DDRAM	Double Data Rate Synchronous Dynamic Random Access Memory
DISCOM	Display output Comparison
DTC	Diagnostic Trouble Code
E2EP	End to End Protection
ECU	Electronic Control Unit
ESC	Electronic Stability Control
Ext-MCU	External Microcontroller Unit
FDTI	Fault Detection Time Interval

FHTI	Fault Handling Time Interval
FOTA	Flash Over the Air
FRTI	Fault Reaction Time Interval
FSR	Functional Safety Requirement
FTA	Fault Tree Analysis
FTTI	Fault Tolerance Time Interval
GNSS	Global Navigation Satellite System
HDMI	High-Definition Multimedia Interface
HMI	Human Machine Interface
HUD	Heads Up Display
ID	Identifier
IGN	Ignition
IMG	Intermittent Gong
IPC	Instrument Panel Cluster
LTE	Long-Term Evolution
MCU	Microcontroller Unit
MDU	Media Display Unit
MHU	Multimedia Head Unit
MMC	Multi-Media Card
Ms	Milliseconds
NVM	Non-Volatile memory
PMIC	Power Management Integrated Circuit
QM	Quality Management
RFSO	Renesas Failure Self-Detection Output
RVC	Rear View Camera
SG	Safety Goal
SoC	System on Chip
SVCs	Surround View Cameras
SW	Software
TBD	To Be Defined
TBOX	Telematics BOX
TPMS	Tire Pressure Monitoring System
TSC	Technical Safety Concept
TSR	Technical Safety Requirement
USB	Universal Serial Bus
VIP	Vehicle Input Processor
XGW	Gateway

1.4 System description

1.4.1 System overview

The eCockpit is center of IVI system, which combined 3 main components: IPC (instrument cluster), MHU (Head Unit), TBOX (telematics box) in to one ECU and share 1 display. IPC and MHU, VIP is in one SoC chip. IPC is instrument cluster for showing driving information like telltales, warnings, trip information. MHU is center for infotainments, vehicle control, vehicle settings, phone/tablets mirroring, surround view camera, phone connection and HMI user interaction. TBOX is telematics component that connect to network by LTE and will be the hub for FOTA and emergency call.

Figure 1 HMI Display of eCockpit

1.4.2 Physical view of eCockpit

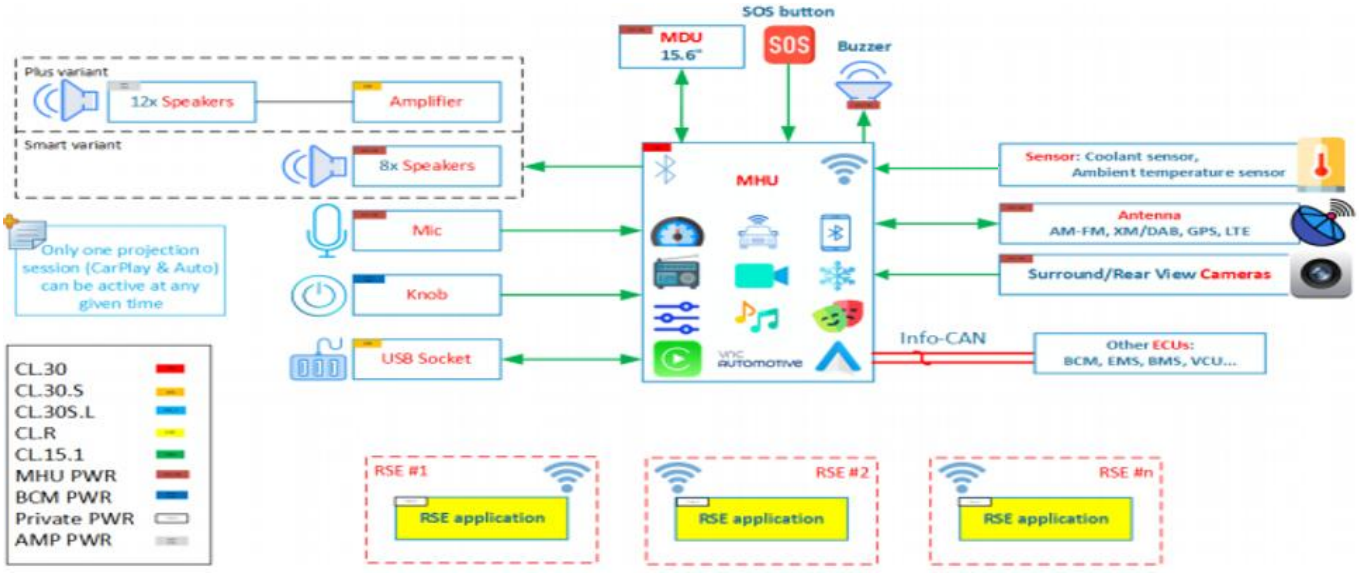


Figure 2 Physical view of eCockpit

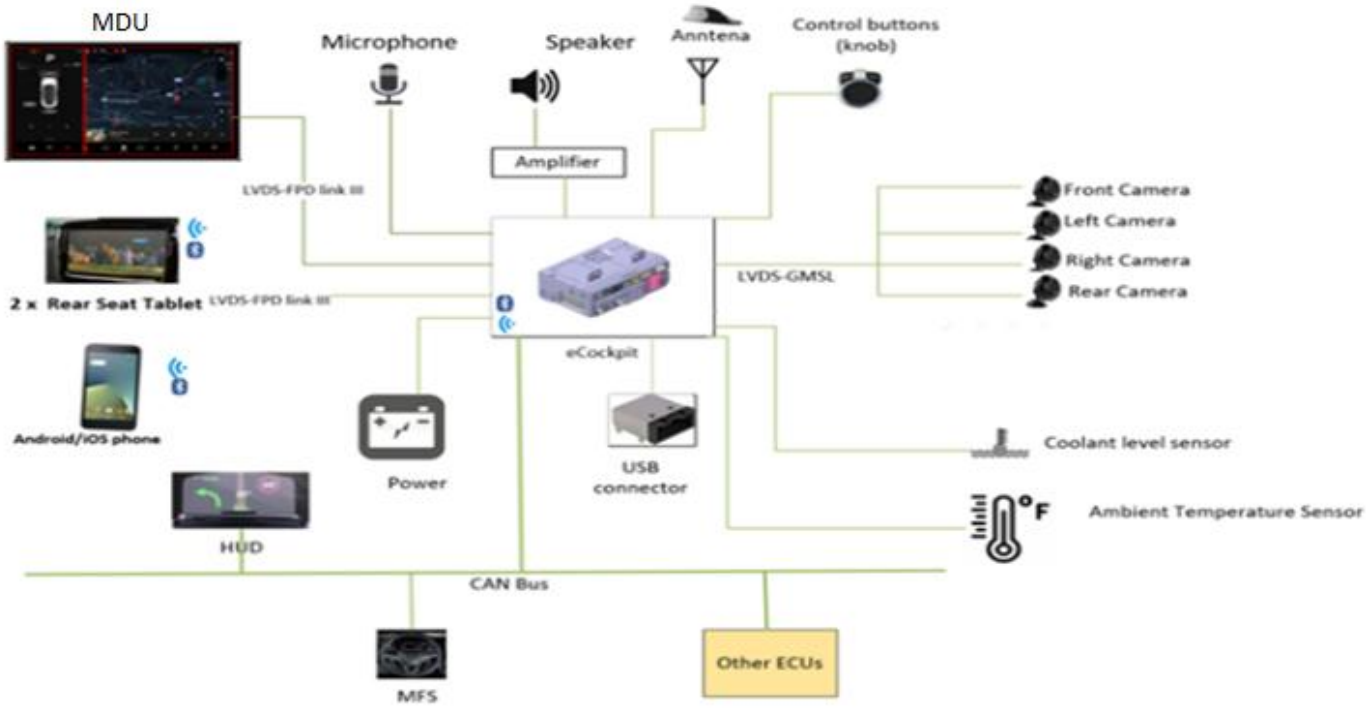


Figure 3 Interfaces of eCockpit system

External Components Interface:

Following illustrates overall interfaces of MHU with various components:

1. Interface with MDU
2. Interface with SVCs
3. Interface with RVC
4. Interface with HUD
5. Interface with Antennas
6. Interface with Microphone
7. Interface with Speaker
8. Interface with Control buttons (knob)
9. Interface with USB hub
10. Interface with CAN bus

1.5 System Architecture Design

The below Safety Architecture Diagram is created based on [Ref 08]

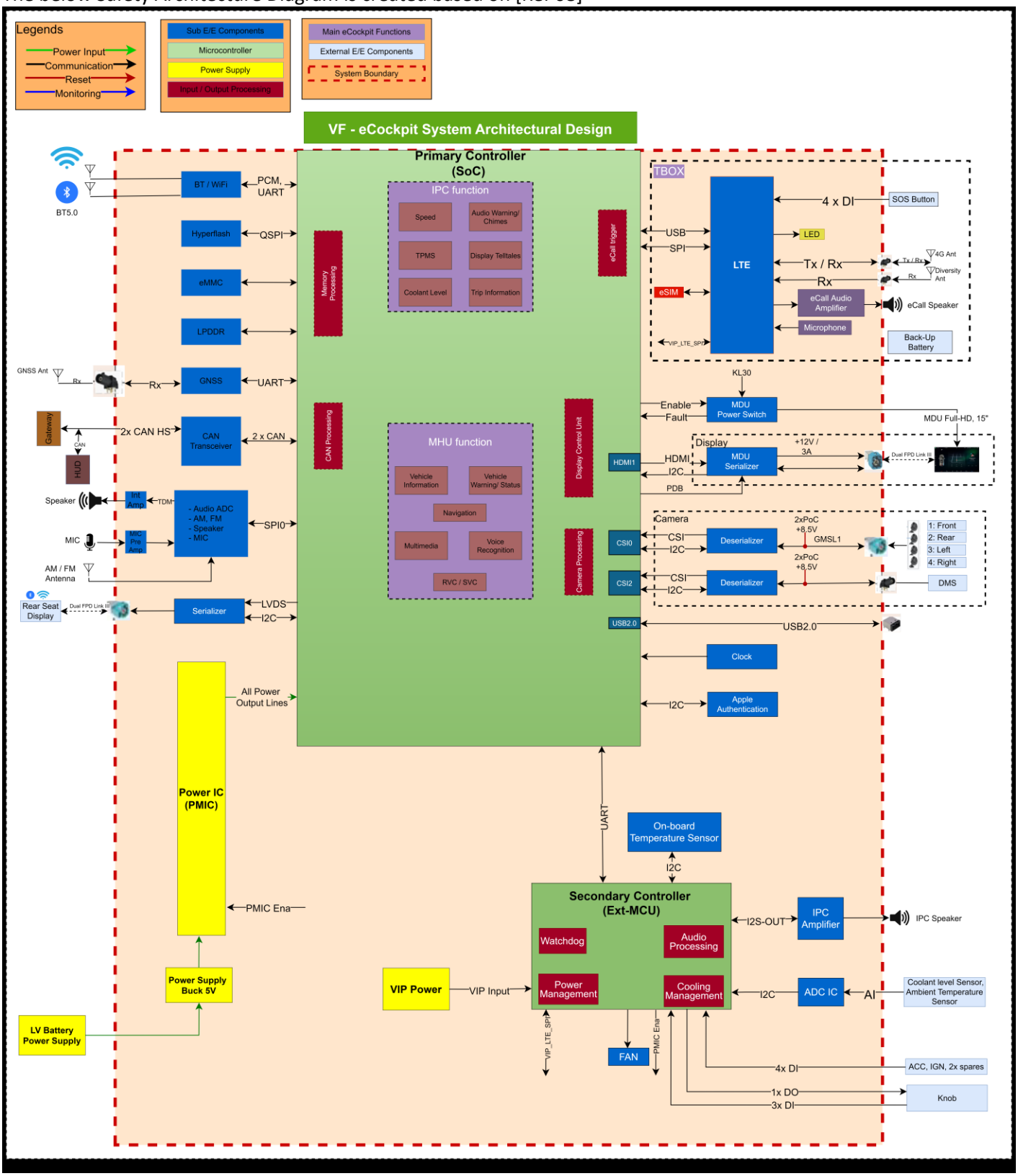
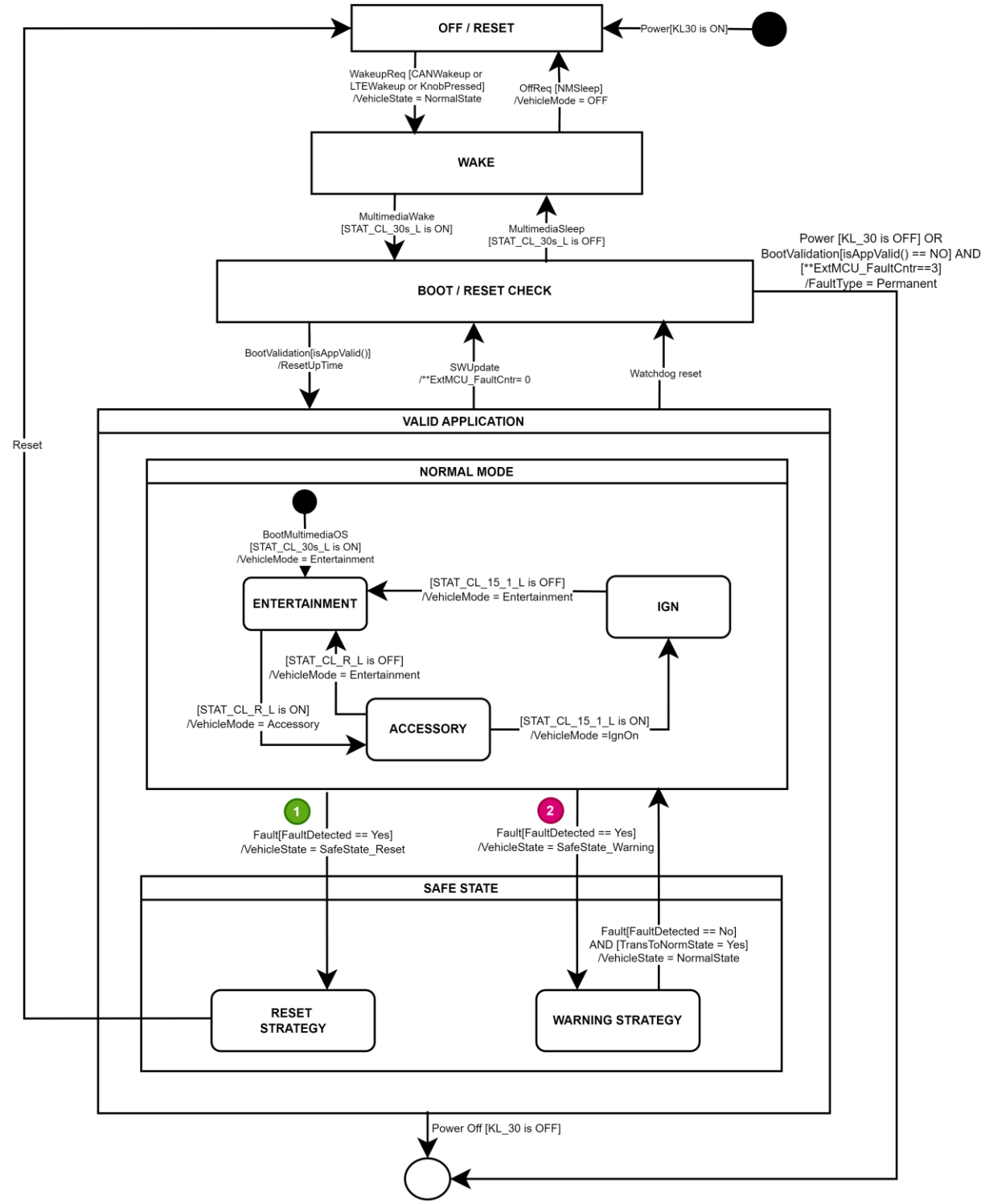


Figure 4 System Architecture Design Diagram

1.6 Operating modes



*TransToNormState = Yes, when [Fault Recovered AND Duration of 3 FTTI elapsed] OR IGN transits from OFF to ON
Default Value TransToNormState = No

**ExtMCU_FaultCntr = Counter to indicate fault in Ext-MCU. Upon failure of program flow execution, this counter will be incremented by 1, once in a drive cycle. Recovery from fault in program flow monitoring will lead to decrement in this counter by 1. Default Value of ExtMCU_FaultCntr = 0

Figure 5 Operating modes of eCockpit system

1 Refer eCockpit_TSR105 for details on faults leading to Reset as safe state

2 Refer eCockpit_TSR106 for details on faults leading to Warning strategy as safe state

1.7 Safety Goals

From the HARA Analysis [Ref 03] performed, various safety goals are derived for eCockpit System.

1.8 Safe States

For eCockpit system, various safe states are defined in HARA Analysis [Ref 03]

2 System safety mechanisms

The following sections provide details about the safety measures to be implemented in the system design. The relevant hardware and software interfaces on each of the transition will be provided in hardware-software interface specification.

2.1 CAN input monitoring

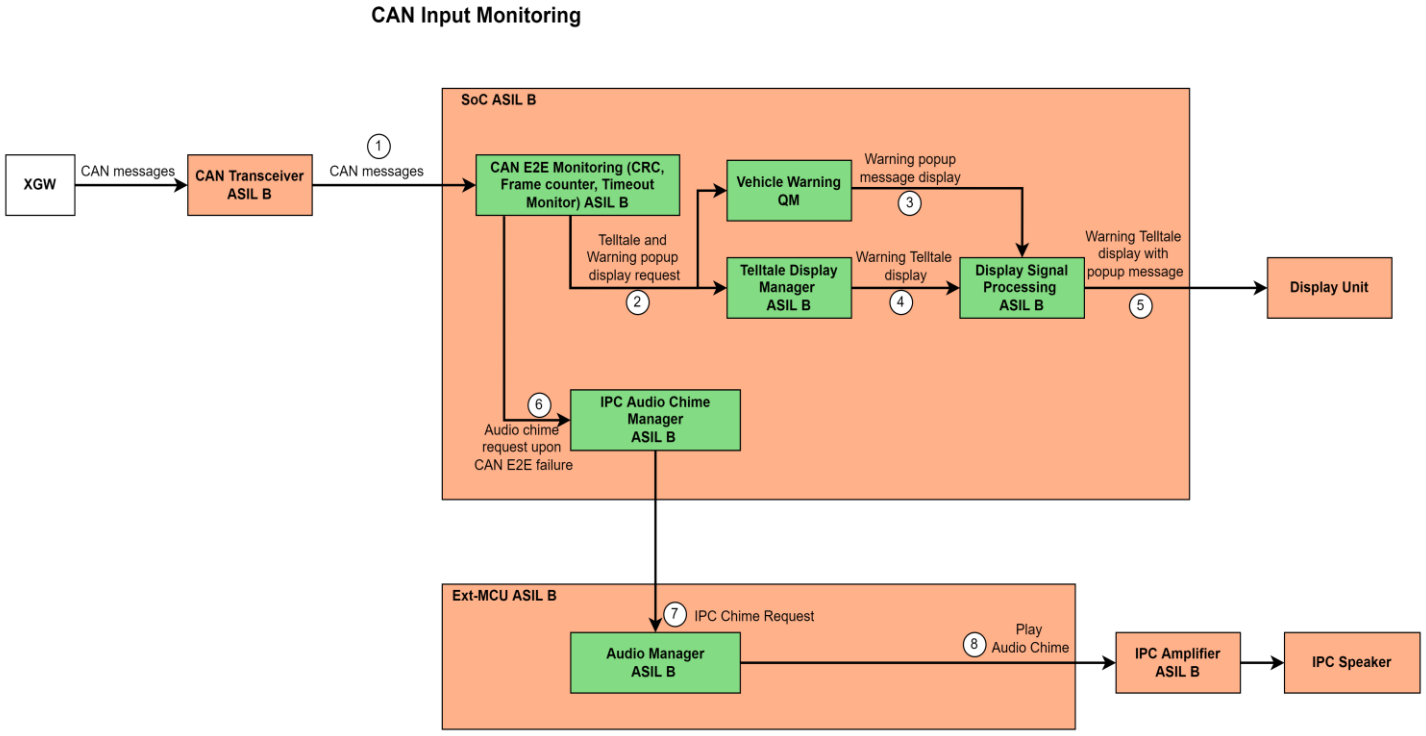


Figure 6 CAN Input monitoring

Faults in CAN inputs and its corresponding safety mechanisms are provided in below table:

Sl. No	Fault	SM ID	Safety Mechanism	Traceability	ASIL	Element Allocated
1.	Faults in Receiving Valid CAN messages	SM_01	**E2EP:** Perform timeout, CRC, and Frame counter check for Safety critical CAN messages	eCockpit_TSR006, eCockpit_TSR007, eCockpit_TSR010, eCockpit_TSR012	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
2.	Failure Modes in CAN transceiver	SM_02	**CAN Bus-off Monitoring:** To monitor the Bus-off state of	eCockpit_TSR019, eCockpit_TSR124,	B	[029] BLK PRIMARY CONTROLLER, [030]

			CAN module	eCockpit_TSR125		BLK SECONDARY CONTROLLER
3.	CAN Transceiver – Power supply faults	SM_03	**Uninterrupted power supply for CAN transceiver** Provide input uninterrupted power supply for CAN transceiver normal operation	eCockpit_TSR020	B	[006] BLK CAN TRANCEIVER
4.	Faults in CAN message processing	SM_01	**E2EP:** Perform timeout, CRC, and Alive counter check for Safety critical CAN messages	eCockpit_TSR006, eCockpit_TSR007, eCockpit_TSR010, eCockpit_TSR012	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
		SM_23	**Q&A watchdog for SoC:** To monitor SoC through Q&A watchdog using Ext-MCU	eCockpit_TSR049, eCockpit_TSR052, eCockpit_TSR051	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
		SM_05	**SoC processing Core Monitoring:** To detect the faults in SoC processing Core executing ASIL rated software functions	eCockpit_TSR039, eCockpit_TSR040	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER

The above shown safety mechanism is a generic mechanism to have CAN E2E protection for all the CAN messages related to safety critical functions such as:

1. Safety relevant telltale display
2. Speedometer Display
3. Tire pressure Display

Safety Concept:

(1) SoC receives cyclic CAN messages from XGW related to safety functions mentioned above

(2) SoC performs integrity check and timeout monitoring on the incoming CAN messages relevant to safety functions for every cycle and provides the E2E result. In case of issues identified during integrity checks or timeout monitoring for missing message cycles as specified in CAN matrix specification, the CAN E2E monitoring block shall trigger request to display warning telltale and corresponding warning popup message.

(3) Vehicle Warning block updates the MHU display buffer with the corresponding warning pop-up message as per the received warning request

(4) Telltale Display Manager block updates the Safety data display buffer with corresponding telltale as per the received warning request

(5) Display Signal Processing block further processes the MHU display buffer and Safety data display buffer to obtain the final blended output. The blended display output is sent to display unit to notify the driver.

Along with displaying the warning telltale and pop-up message as safe state, SoC also triggers (6) IPC audio chime manager to request Ext-MCU to play continuous audio chime as another safe state action.

(7) the audio manager in Ext-MCU would process the audio chime request from SoC and transmit the processed audio output to (8) IPC amplifier to play continuous audio chime in the IPC Speaker

Note: The ASIL decomposition for warning strategy safe state for CAN monitoring is:

1. Acoustic warning through IPC audio chimes – ASIL B [eCockpit_TSR_SS02]
2. Warning telltale + warning popup message display on MDU – ASIL B

Note: The SoC would revoke the safe state of displaying warning telltale and popup message and playing audio chime and transit the system to normal mode if it continues to receive valid CAN signals either for the duration of at least 2 FDTI cycles or transition of vehicle state from OFF to ON is detected, whichever occurs first.
The number of FDTI cycles for considering fault recovery is provided as per assumption ASM_TSC_012.

Note: The list of safety critical CAN messages as provided in [Ref 04]

2.2 Safety Mechanisms related to -eCockpit-CSG01

The monitoring of input CAN messages for displaying safety critical telltales shall follow the generic CAN monitoring mechanism mentioned in section *2.1 CAN input monitoring.*

The list of CAN messages related to the safety critical telltales can be obtained from [Ref 07]

2.2.1 Telltale safety monitor – display output check

[Note: numbering of interfaces continued from Figure 2-1 CAN Input monitoring]

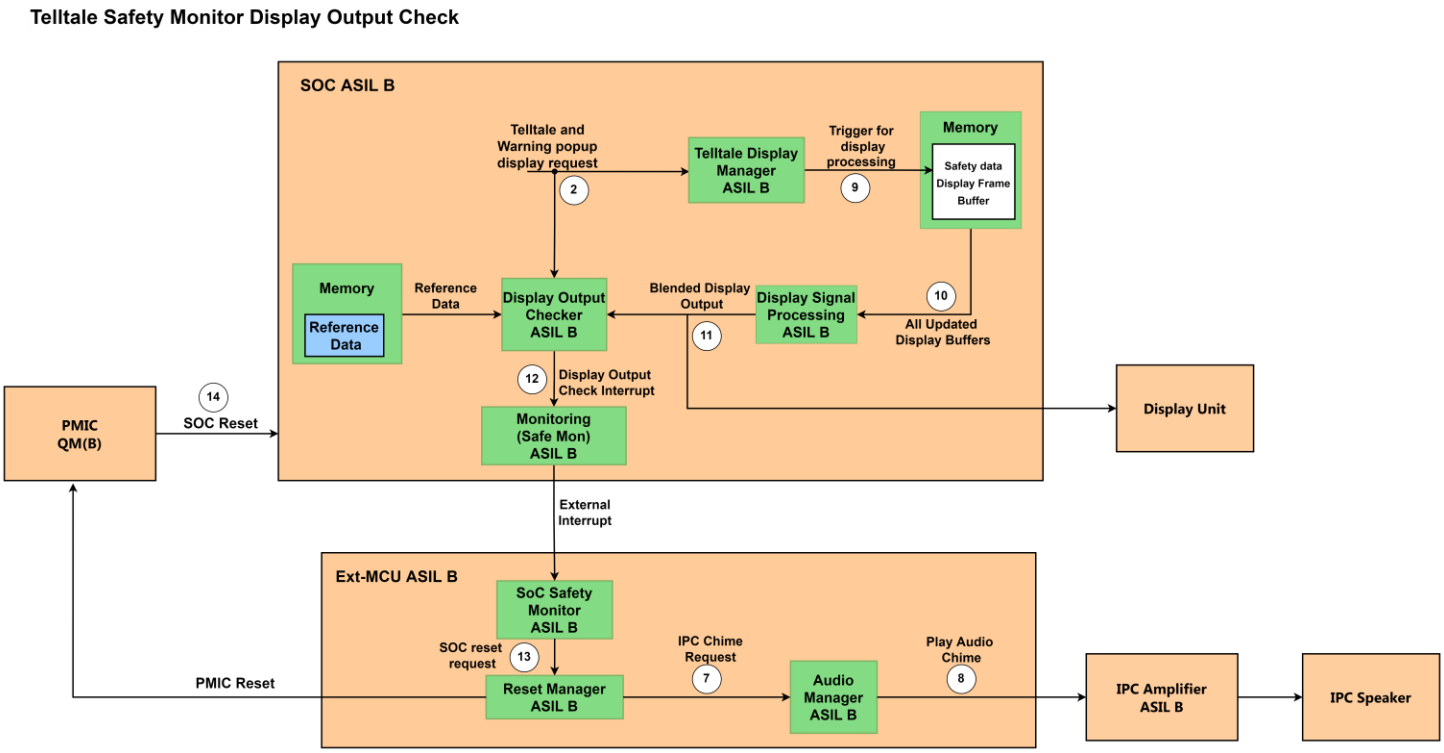


Figure 7 Telltale safety monitor – Display output Check

Faults in telltales display output and its corresponding safety mechanisms are provided in below table:

Sl. No	Fault	SM ID	Safety Mechanism	Traceability	ASIL	Element Allocated
1.	Faults in telltale function processing	SM_06	**Display Output Checker:** To monitor the rendering of safety critical data display	eCockpit_TSR058, eCockpit_TSR059, eCockpit_TSR062, eCockpit_TSR063	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
		SM_05	**SoC processing Core Monitoring:** To detect the faults in SoC processing Core executing ASIL rated software functions	eCockpit_TSR039, eCockpit_TSR040	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
		SM_07	**Memory Access Protection:** To detect illegal access to safety related data memory from non-safety function in SoC	eCockpit_TSR060, eCockpit_TSR061, eCockpit_TSR062, eCockpit_TSR063	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
		SM_08	**Memory Protection:** To protect memory partition related to ASIL rated software functions in SoC	eCockpit_TSR038, eCockpit_TSR123	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
		SM_30	**Memory Integrity Check:** To perform integrity check for the safety content	eCockpit_TSR134, eCockpit_TSR136	B(B)	[029] BLK PRIMARY CONTROLLER, [030] BLK

			written and read from HyperFlash			SECONDARY CONTROLLER
					QM(B)	[002] BLK HYPERFLASH
		SM_31	**Memory Protection for DDRRAM:** To provide memory protection for safety related data stored in DDRRAM	eCockpit_TSR135, eCockpit_TSR136	B(B)	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
					QM(B)	[004] BLK LPDDR
2.	Faults in rendering telltales	SM_06	**Display Output Checker:** To monitor the rendering of safety critical telltales display	eCockpit_TSR058, eCockpit_TSR059, eCockpit_TSR062, eCockpit_TSR063	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER

Safety Concept:

(2) The CAN E2E monitoring, (from *Figure 2-1* CAN Input monitoring) block processes the CAN signal along with its E2E result and decides whether to request to display or clear the display of telltale image and forwards the request along with warning details of the corresponding telltale to Telltale Display Manager block.

(9) Telltale Display Manager block processes the request and prepares the display of corresponding telltale in a safety data display buffer and stores it in DDR RAM. It also triggers further processing for the updated safety critical telltale display data.

(10) Display Signal Processing processes and blends the updated safety data display buffer from DDR RAM in corresponding section of IPC frame along with display buffers for other layers. Further it provides the blended display output to display unit (11).

Simultaneously, the (11) blended display output is also fed to Display Output Checker (DOC) block to verify the correctness of the telltale rendered in IPC frame. The DOC verifies each safety critical telltale display by comparing the color of each pixel of telltale image with its corresponding reference data stored in DDR RAM. When mismatch in the color ranges of the telltale between the blended output and reference data is found to be above a certain configurable threshold, DOC indicates the fault to Monitoring block through interrupt (12).

The Monitoring block notifies RFSO manager to trigger an external interrupt through RFSO pin

(13) The SoC safety monitor in the Ext-MCU requests PMIC reset to the reset manager on receiving interrupt from SoC through RFSO pin

the reset manager block in Ext-MCU change the state of reset pin associated with PMIC to trigger a reset in the SoC (14)

Also, whenever there is a reset operation, the Ext-MCU triggers an (7) audio warning.

The audio manager block in the Ext-MCU (8) plays intended audio chime on receiving audio request from the reset manager.

Note: Upon receiving the request to remove the display of safety critical telltales, the SoC shall remove the rendering of corresponding telltale within FDTI duration.

Safe State:

1. Triggering reset of SoC by Ext-MCU [eCockpit_TSR_SS05]
2. Playing Audio chime [eCockpit_TSR_SS02]

2.2.2 MDU safety monitor

[Note: numbering of interfaces continued from Figure 2-2-1 Telltale safety monitor – Display output check]

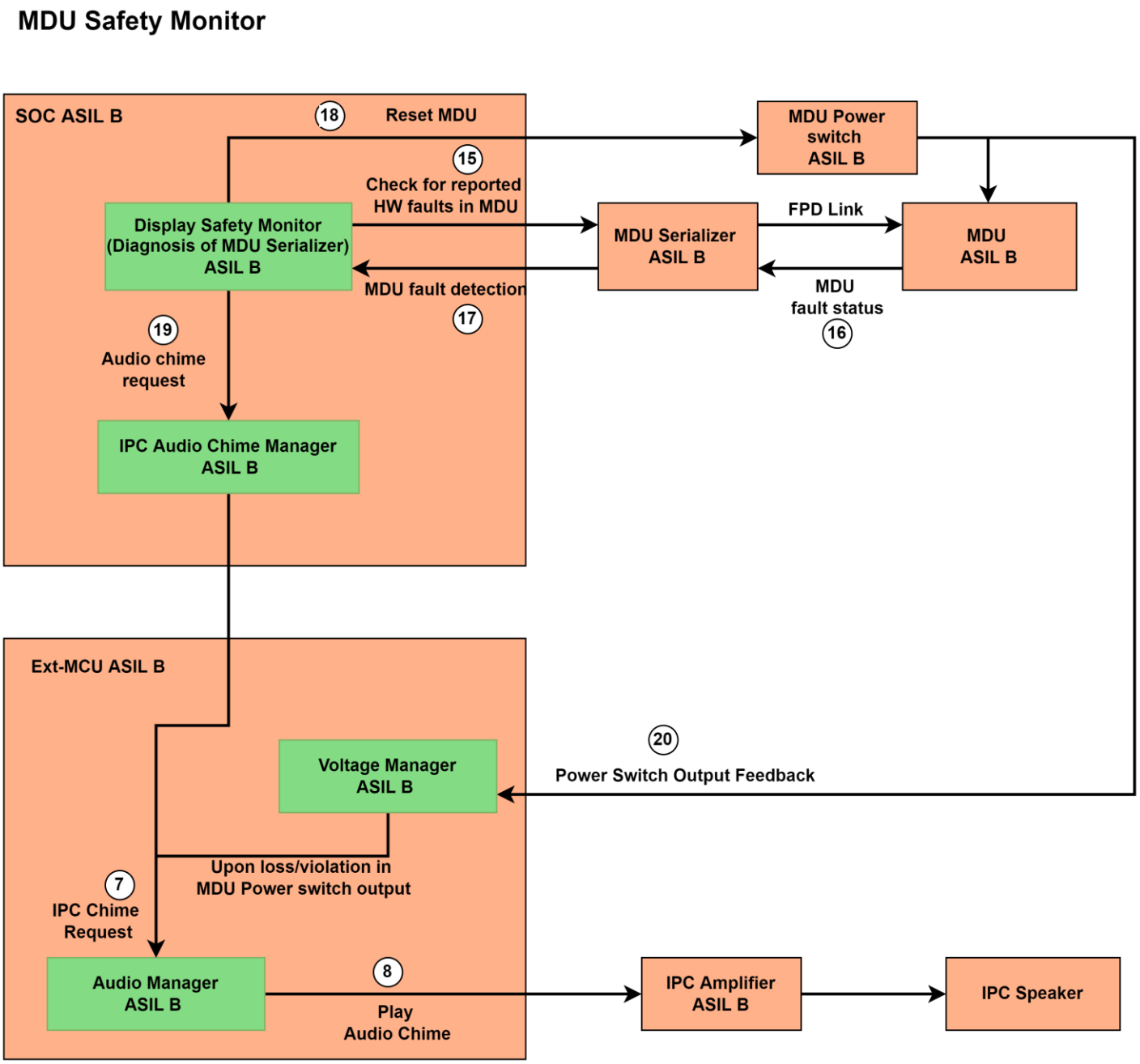


Figure 8 MDU safety monitor

Faults in displaying safety data on MDU and corresponding safety mechanisms are provided in below table:

Sl. No	Fault	SM ID	Safety Mechanism	Traceability	ASIL	Element Allocated
1.	Faults in MDU Power Supply	SM_09	**MDU Power Switch output Monitoring:** To monitor MDU Power switch output	eCockpit_TSR101, eCockpit_TSR102, eCockpit_TSR103	B	[030] BLK SECONDARY CONTROLLER, [018] BLK MDU PWR SWITCH

2.	Faults in MDU	SM_10	**MDU HW Faults Monitoring:** To monitor HW faults (backlight, bias) in MDU	eCockpit_TSR024, eCockpit_TSR025, eCockpit_TSR026, eCockpit_TSR027	B	[029] BLK PRIMARY CONTROLLER, [017] BLK MDU SERIALIZER, [030] BLK SECONDARY CONTROLLER, [018] BLK MDU PWR SWITCH, MDU
3.	Faults in MDU Serializer	SM_11	**MDU Serializer Supply Voltage monitoring:** To monitor supply voltage of MDU Serializer to detect over voltage and under voltage conditions	eCockpit_TSR021, eCockpit_TSR128	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER, [017] BLK MDU SERIALIZER
4.	Fault in FPD Link III connector	SM_12	**FPD Link fault Monitoring:** To monitor FPD link connect through MDU Serializer to detect short circuit and open circuit faults	eCockpit_TSR022, eCockpit_TSR130	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER, MDU Serializer, [018] BLK MDU PWR SWITCH

Safety Concept:

(14) SoC monitors MDU serializer for reported hardware faults from the MDU (15)

(16) on detection of reported fault from MDU (16), the SoC trigger safe state by performing following actions:

- Reset MDU (17)
- Request Ext-MCU through (18) IPC Audio chime manager, (6) to play audio chime in the speaker via IPC amplifier (7)
- Note: In case of recovery of reported HW fault from MDU, The SoC stops resetting MDU and stops playing audio chime in the IPC speaker to transits from safe state to normal state.

(19) The Ext-MCU also monitors the MDU Power Switch output feedback. Upon detection of voltage violations or unintended loss of power Switch output voltage, the Ext-MCU (6) plays audio chime in the speaker via IPC amplifier (7)

Safe State:

1. SoC triggering reset of MDU through MDU Power switch, upon MDU HW faults detection
2. Playing Audio chime [eCockpit_TSR_SS02]

Design Decision in Display Monitoring:

The Display monitoring functionality is overall rated as ASIL B and following ASIL ratings are considered:

a. MDU Serializer is to be considered ASIL B

b. SoC to be considered as ASIL B

MDU Serializer is considered ASIL B rated as it must:

1. Transmit safety critical display data to MDU for displaying
2. Report back the HW faults of MDU to SoC

2.2.3 Complete Telltale Display Path:

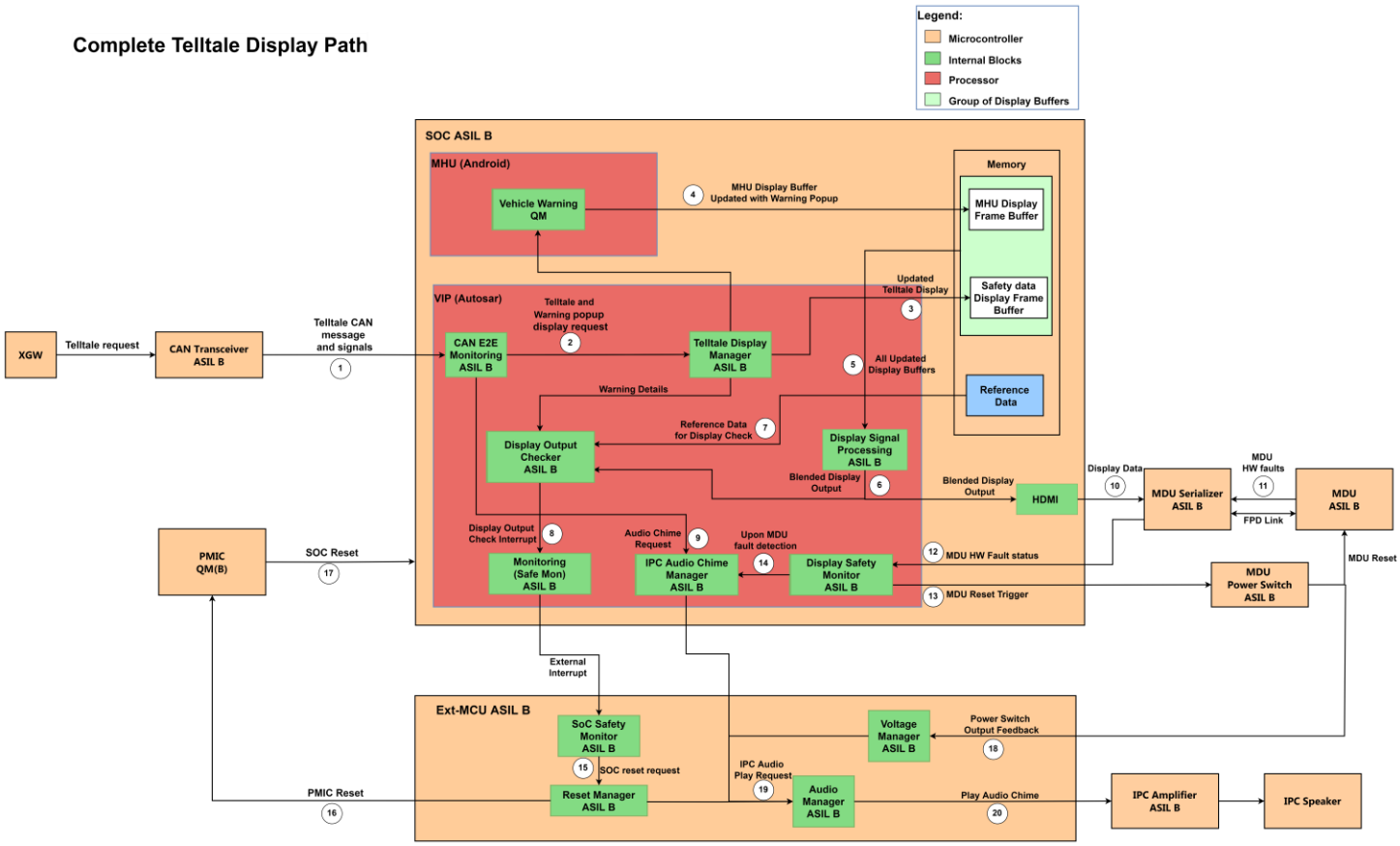


Figure 9 Telltale Display Path

Freedom from Interference for Memory:

Following are the data stored in DDR RAM:

1. Telltale images
2. Safety critical telltale display frame buffer
3. MHU display frame buffer
4. Display frame buffers of other display content
5. Reference data for each telltale for comparison done by DOC

The SoC shall have a restricted memory access to the reference data in DDR RAM used for verifying the correctness of the blended display output by DOC.

Freedom from Interference for Timing:

The DOC will detect any delay in display processing of the telltale data.

2.2.4 IPC speakers monitor

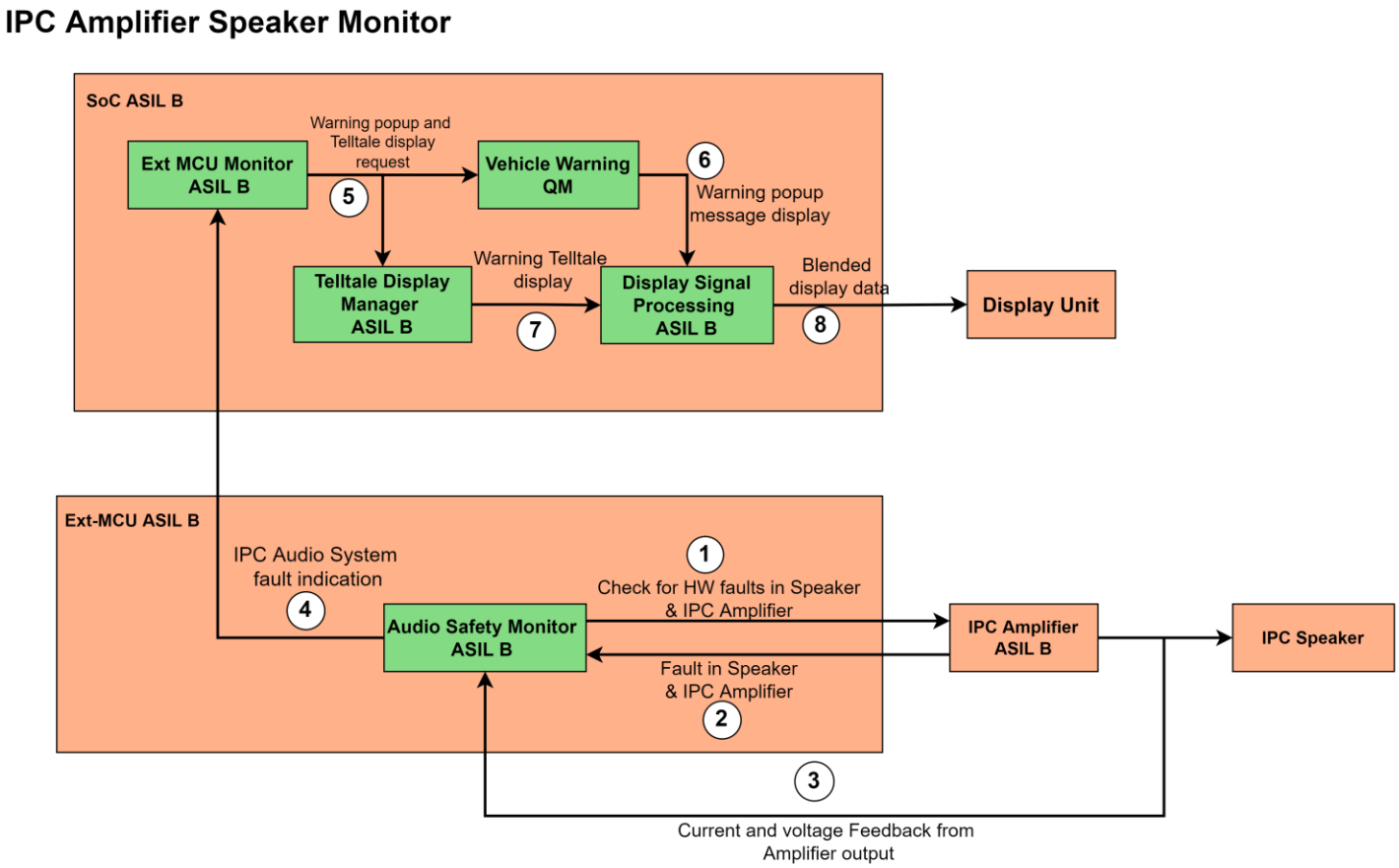


Figure 10 IPC speaker monitor

Sl. No	Fault	SM ID	Safety Mechanism	Traceability	ASIL	Element Allocated
1.	Failure modes in IPC amplifier	SM_13	**IPC Amplifier Supply Voltage monitoring:** To monitor supply voltage of IPC Amplifier to detect over voltage and under voltage conditions	eCockpit_TSR028, eCockpit_TSR132	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER, [013] BLK IPC AMPLIFIER
2.	Failure modes in IPC speaker input	SM_14	**IPC Speaker monitor:** To monitor IPC Amplifier output to detect short circuit and open circuit at output terminals	eCockpit_TSR031, eCockpit_TSR032, eCockpit_TSR033	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER, [013] BLK IPC AMPLIFIER
3.	IPC Communication Failure	SM_15	**IPC Communication monitor:** To detect communication failure between Ext-MCU and IPC Amplifier	eCockpit_TSR054, eCockpit_TSR055, eCockpit_TSR056, eCockpit_TSR133	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER, [013] BLK IPC AMPLIFIER
4.	Failure modes in Audio Processing	SM_16	**Memory Protection for Ext-MCU:** To protect memory partition related to ASIL rated software functions in Ext-MCU	eCockpit_TSR041	B	[030] BLK SECONDARY CONTROLLER

Safety Concept

(1) The Audio Safety Monitor block in Ext-MCU monitors IPC amplifier for reported hardware faults from the Speaker (2)

(3) Audio Safety Monitor block also receives current and voltages feedback from IPC amplifier output terminals

(4) on detection of fault from IPC amplifier in (2) or (3), the Ext-MCU indicates the fault to SoC

(5) The Ext-MCU monitor block in SoC requests the Vehicle warning and Telltale Display Manager block to display warning popup message and warning telltale.

(6) Vehicle warning block updates the MHU display data buffer with warning message and stores it in DDRRAM memory

(7) Telltale Display Manager block updates the safety data display buffer with warning telltale based on the received request.

(8) The Display Signal processing block processes the display data buffers from DDRRAM and finally obtains a blended display output which is forwarded to display unit to notify driver

The Ext–MCU will detect the communication failure with IPC amplifier. Upon the fault detection the Ext-MCU will reset the IPC amplifier.

Note: The Ext-MCU shall reset IPC amplifier maximum of 3 times only in one ignition cycle. However, SoC shall continue to display warning telltale and warning popup message until the fault in IPC Amplifier is recovered.

Safe State:

1. Warning telltale + Warning popup message display on MDU [eCockpit_TSR_SS06]

2.3 Safety Mechanisms related to -eCockpit-CSG02

2.3.1 Speedometer – CAN monitoring

The safety concept for CAN monitoring of vehicle speed input can be referred from *section 2.1* CAN input monitoring

In case of issues identified during integrity checks or timeout monitoring for missing message cycles as specified in CAN matrix specification, the SoC shall trigger following actions:

- Make speed value as invalid and request the graphic text to be updated as “--”
- Trigger a warning popup on MDU
- Requests Ext-MCU to play continuous audio chime

The CAN messages related to the speedometer display can be obtained from [Ref 07]

2.3.2 Speedometer – Display output Check

Speedometer Display Output Check

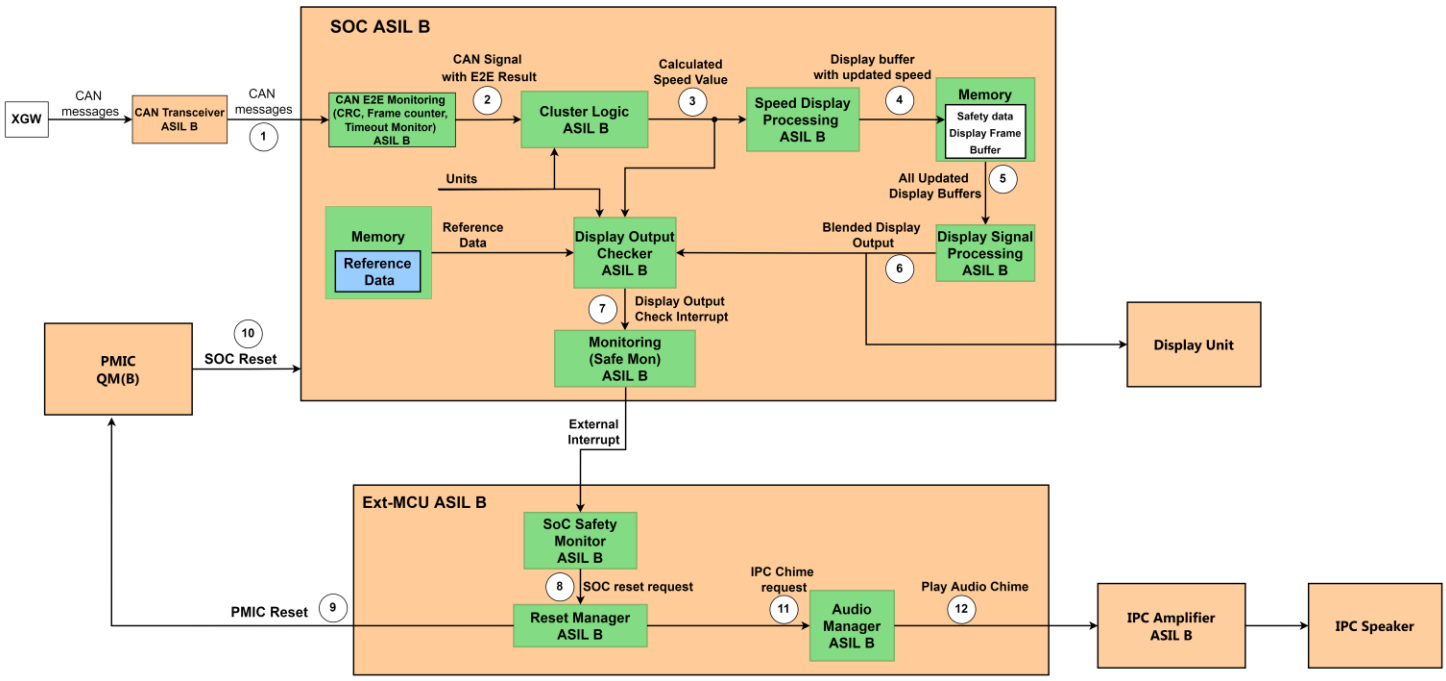


Figure 11 Speedometer - Display output check

Faults in speed display function and related safety mechanisms are provided in the below table:

Sl. No	Fault	SM ID	Safety Mechanism	Traceability	ASIL	Element Allocated
1.	Malfunction in Speed calculation and refreshing	SM_23	**Q&A watchdog for SoC:** To monitor SoC through Q&A watchdog using Ext-MCU	eCockpit_TSR049, eCockpit_TSR052, eCockpit_TSR051, eCockpit_TSR070	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
2.	Fault in Speed display data rendering	SM_06	**Display Output Checker:** To monitor the rendering of safety critical data display	eCockpit_TSR069, eCockpit_TSR071, eCockpit_TSR072, eCockpit_TSR073	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
3.	Fault in speed unit value	SM_17	**Units Interface monitoring:** To monitor the interface used to receive units' values from MDU	eCockpit_TSR065, eCockpit_TSR066	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
		SM_31	**Memory Protection for DDRRAM:** To provide memory protection for safety related data stored in DDRRAM	eCockpit_TSR135, eCockpit_TSR136	B(B)	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
					QM(B)	[004] BLK LPDDR
		SM_30	**Memory Integrity Check:**	eCockpit_TSR134,	B(B)	[029] BLK PRIMARY

			To perform integrity check for the safety content written and read from HyperFlash	eCockpit_TSR136		CONTROLLER, [030] BLK SECONDARY CONTROLLER
					QM(B)	[002] BLK HYPERFLASH

Safety Concept for Display Output Checker:

(1) SoC receives cyclic CAN messages from XGW and CAN E2E Monitoring processes the CAN messages with E2E checks and provide CAN signals along with E2E results.

(2) The Cluster logic block processes the CAN signal along with its E2E result, obtains the calculated obtained vehicle speed, and forwards the vehicle speed value for speed display processing block.

(3) Speed display processing block processes the speed data and prepares the display of speed in a (4) safety data display buffer and stores it in DDR RAM. It also triggers further processing for the updated safety data display buffer

(5) Display signal processing processes and blends the updated safety data display buffer from DDR RAM in corresponding section of IPC frame along with display buffers for other layers. Further it provides the blended display output to display unit (6).

Simultaneously, the (6) blended display output is also fed to Display Output Checker (DOC) block to verify the correctness of the vehicle speed along with its unit rendered in IPC frame. When any deviation between the blended output and reference data is found, the DOC indicates the fault to Monitoring block.

The (7) Monitoring block notifies RFSO manager to trigger an external interrupt through RFSO pin

(8) The SoC safety monitor in the Ext-MCU requests PMIC reset to the reset manager on receiving interrupt from SoC through RFSO pin

the (9) reset manager block in Ext-MCU change the state of reset pin associated with PMIC to trigger a reset in the SoC (10)

Also, whenever there is a reset operation, the Ext-MCU triggers an (11) audio warning.

The audio manager block in the Ext-MCU (12) plays intended audio chime on receiving audio request from the reset manager

The SoC shall also update the vehicle speed value every 200ms on the display.

Safe State:

1. Triggering reset of SoC by Ext-MCU [eCockpit_TSR_SS05]
2. Playing Audio chime [eCockpit_TSR_SS02]

2.4 Safety Mechanisms related to -eCockpit-CSG03

2.4.1 TPMS – CAN monitoring

The safety concept for CAN monitoring of tire pressures input can be referred from section 2.1 CAN input monitoring

(2) SoC performs timeout monitoring on the incoming CAN signals on TPMS information for every cycle

(3) on timeout of the required CAN message(s), the SoC shall trigger following actions:

- Make TPMS value as invalid and request the graphic text to be updated as “--”
- Trigger a warning popup on MDU
- Requests Ext-MCU to play continuous audio chime

The CAN messages related to the tire pressures display can be obtained from [Ref 07]

2.4.2 TPMS – Display output Check

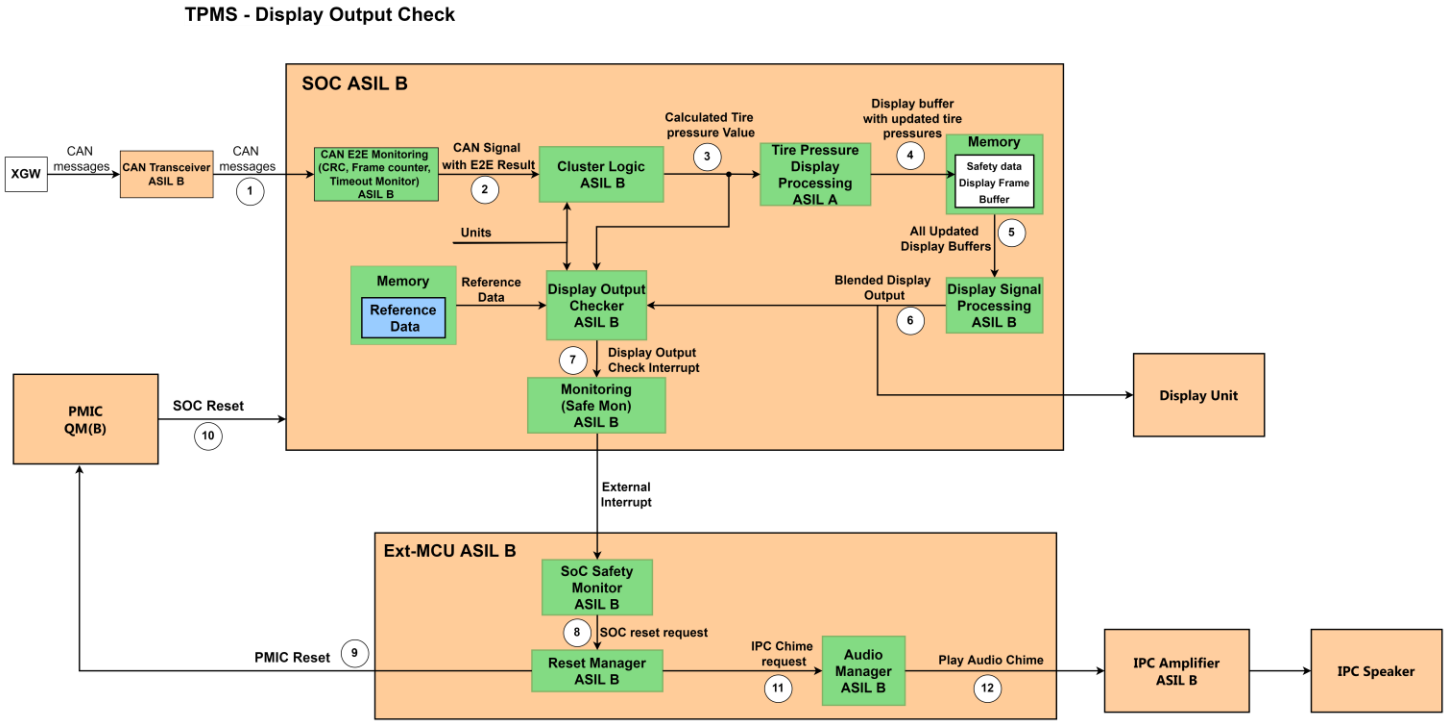


Figure 12 TPMS - Display output check

Faults in tire pressure values display function and related safety mechanisms are provided in the below table:

Sl. No	Fault	SM ID	Safety Mechanism	Traceability	ASIL	Element Allocated
1.	Faults in tire pressure conversion	SM_23	**Q&A watchdog for SoC:** To monitor SoC through Q&A watchdog using Ext-MCU	eCockpit_TSR049, eCockpit_TSR052, eCockpit_TSR051	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
		SM_05	**SoC processing Core Monitoring:** To detect the faults in SoC processing Core executing ASIL rated software functions	eCockpit_TSR039, eCockpit_TSR040	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
2.	Fault in tire pressure display data rendering	SM_06	**Display Output Checker:** To monitor the rendering of safety critical data display	eCockpit_TSR075, eCockpit_TSR076, eCockpit_TSR077	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
3.	Fault in tire pressures unit value	SM_17	**Units Interface monitoring:** To monitor the interface used to receive units' values from MDU	eCockpit_TSR065, eCockpit_TSR066	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER

		SM_31	**Memory Protection for DDRRAM:** To provide memory protection for safety related data stored in DDRRAM	eCockpit_TSR135, eCockpit_TSR136	B(B)	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
					QM(B)	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
		SM_30	**Memory Integrity Check:** To perform integrity check for the safety content written and read from HyperFlash	eCockpit_TSR134, eCockpit_TSR136	B(B)	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
					QM(B)	[002] BLK HYPERFLASH

Safety Concept for Display Output Checker:

(1) SoC receives cyclic CAN messages from XGW and CAN E2E Monitoring processes the CAN messages with E2E checks and provide CAN signals along with E2E results

The Cluster logic block processes the (2) CAN signal along with its E2E result, obtains the calculated tire pressure values, and forwards the (3) tire pressures value for tire pressure display processing block.

Tire pressure display processing block processes the tire pressure data and prepares the display of tire pressures in a (4) safety data display buffer and stores it in DDR RAM. It also triggers further processing for the updated safety data display buffer

(5) Display signal processing processes and blends the updated safety data display buffer from DDR RAM in corresponding section of IPC frame along with display buffers for other layers. Further it provides the blended display output to display unit (6).

Simultaneously, the (6) blended display output is also fed to Display Output Checker (DOC) block to verify the correctness of the tire pressures values along with its unit rendered in IPC frame. When any deviation between the blended output and reference data is found, the DOC indicates the fault to Monitoring block (7).

The Monitoring block notifies RFSO manager to trigger an external interrupt through RFSO pin

(8) The SoC safety monitor in the Ext-MCU requests PMIC reset to the reset manager on receiving interrupt from SoC through RFSO pin

the reset manager block in Ext-MCU change the state of (9) reset pin associated with PMIC to trigger a reset in the SoC (10) Also, whenever there is a reset operation, the Ext-MCU triggers an audio warning.

The (11) audio manager block in the Ext-MCU plays intended (12) audio chime on receiving audio request from the reset manager

Safe State:

1. Triggering reset of SoC by Ext-MCU [eCockpit_TSR_SS05]

2. Playing Audio chime [eCockpit_TSR_SS02]

2.5 Safety Mechanisms related to -eCockpit-CSG04

2.5.1 eCall safety monitor – Input monitoring

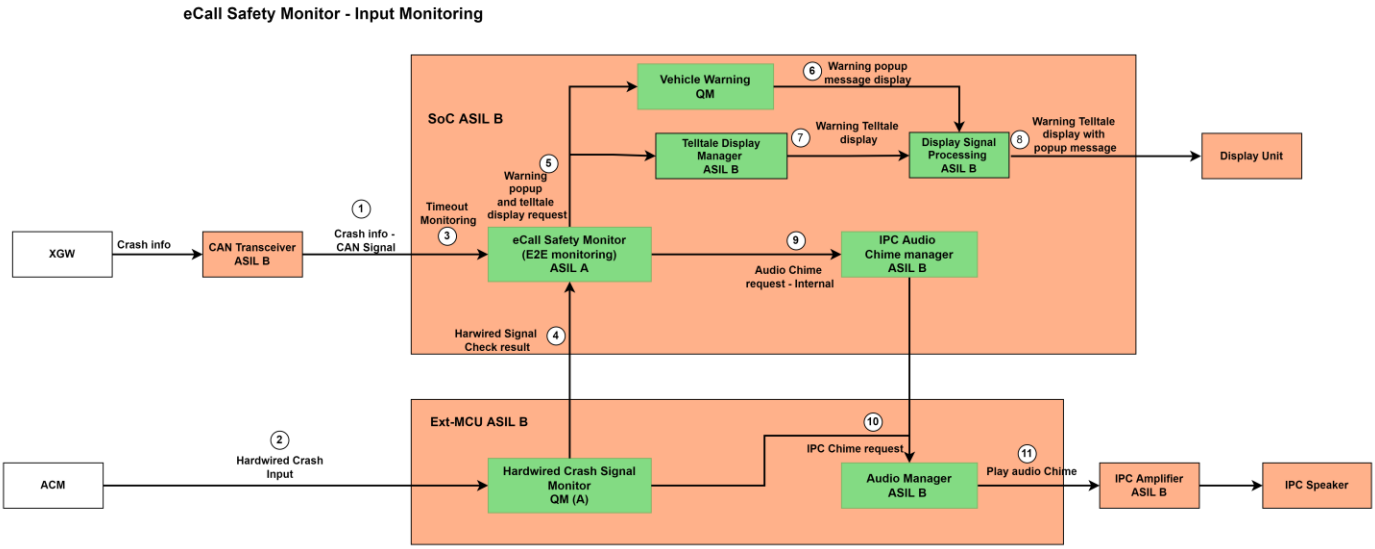


Figure 13 eCall safety monitor – input monitoring

Faults in eCall inputs and its corresponding safety mechanisms are provided in below table:

Sl. No	Fault	SM ID	Safety Mechanism	Traceability	ASIL	Element Allocated
1.	Faults in Receiving Valid CAN messages	SM_01	**E2EP:** Perform timeout, CRC, and Frame counter check for Safety critical CAN messages	eCockpit_TSR006, eCockpit_TSR007, eCockpit_TSR010, eCockpit_TSR012, eCockpit_TSR013, eCockpit_TSR015, eCockpit_TSR016	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
2.	Fault in Hardwired Crash Input	SM_18	**Hardwired crash input Monitoring:** To detect fault in hardwired crash input monitor Hardwired Crash PWM signal.	eCockpit_TSR079	QM(A)	Hardwired crash input signal in [029] BLK PRIMARY CONTROLLER
					B	[029] BLK PRIMARY CONTROLLER
					B	[030] BLK SECONDARY CONTROLLER

(1) SoC receives cyclic CAN messages on crash detection from XGW

(2) SoC receives crash notification from ACM through hardwired input

(3) SoC performs timeout monitoring on the incoming CAN signals on crash detection for every cycle

(4) in parallel, Ext-MCU monitors the Hardwired Crash PWM signal to ensure validity of the input

Either on timeout of the required CAN message(s) or on fault in hardwired crash input, the SoC shall trigger warning popup and warning telltale display request (5) and audio chime request (9)

(6) on receiving warning popup request, the Vehicle Warning block updates the MHU display buffer with the corresponding warning pop-up message as per the received warning request

(7) Telltale Display Manager block updates the Safety data display buffer with corresponding telltale as per the received warning request

(8) Display Signal Processing block further processes the MHU display buffer and Safety data display buffer to obtain the final blended output. The blended display output is sent to display unit to notify the driver.

(10) The audio manager in Ext-MCU would process the audio chime request from SoC and Hardwired Crash Signal monitor block and transmit the processed audio out to IPC amplifier (11) to play continuous audio chime in the IPC Speaker.

Safe State:

1. Acoustic warning through IPC audio chimes – [eCockpit_TSR_SS02]
2. Warning popup message display on MDU –[eCockpit_TSR_SS01]

Note: The SoC would revoke the safe state and transit the system to normal mode if it continues to receive valid CAN signals and hardwired input either for the duration of at least 2 FDTI cycles or transition of IGN from OFF to ON is detected, whichever occurs first. The assumption on number of FDTI cycles for considering fault recovery is provided in assumption

2.5.2 eCall safety monitor – wireless module monitor

2.5.2.1 eCall safety monitor – GNSS and LTE module monitor

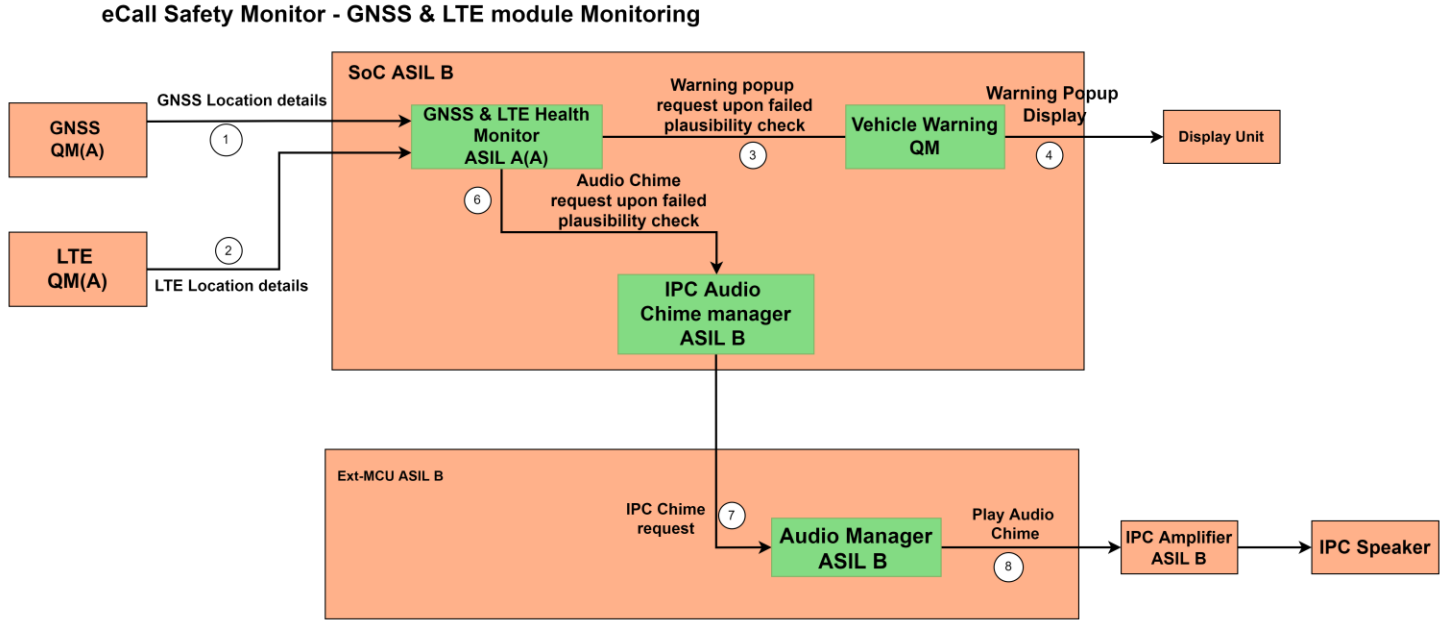


Figure 14 eCall safety monitor – GNSS & LTE module monitor

Faults in GNSS, LTE module and its corresponding safety mechanisms are provided in below table:

Sl. No	Fault	SM ID	Safety Mechanism	Traceability	ASIL	Element Allocated

1.	Fault in GNSS module	SM_19	**Fault in GNSS and LTE module:** Perform plausibility check of the location details obtained from GNSS module and LTE module.	eCockpit_TSR082, eCockpit_TSR083, eCockpit_TSR084, eCockpit_TSR085, eCockpit_TSR086, eCockpit_TSR087, eCockpit_TSR088, eCockpit_TSR112	A(A)	[005] BLK GNSS and [020] BLK_LTE Health Monitor in [029] BLK PRIMARY CONTROLLER
					B	[030] BLK SECONDARY CONTROLLER
					QM(A)	[005] BLK GNSS
2.	Fault in LTE module				QM(A)	[020] BLK_LTE

The health monitor receives the location details from GNSS (1) and location details from LTE module (2) and performs plausibility check of the location coordinates.

Upon detection of any deviation in the plausibility check by health monitor, it requests for safe state of playing audio chime (4) and displaying warning popup (3)

Vehicle Warning receives request for warning popup message and (4) updates the display data with warning popup message and the final blended output will be sent to display unit

IPC Audio Chime manager processes the audio request (4) and sends the IPC chime request (5) to Audio manager.

(5) the audio manager in Ext-MCU would process the audio chime request from SoC (6) and transmit the processed audio out to IPC amplifier to play an audio chime in the IPC Speaker

ASIL Decomposition:

- GNSS Module is rated as QM(A)
- LTE Module is rated as QM(A)
- Plausibility check for monitoring GNSS and LTE module is rated as ASIL A(A)

The SoC shall ensure the freedom of interference between the functions interacting with GNSS and LTE module and functions performing plausibility check

Safe State:

1. Acoustic warning through IPC audio chimes – [eCockpit_TSR_SS02]

2. Warning popup message display on MDU – [eCockpit_TSR_SS01]

2.5.3 eCall Audio Components monitor – Audio Test Play

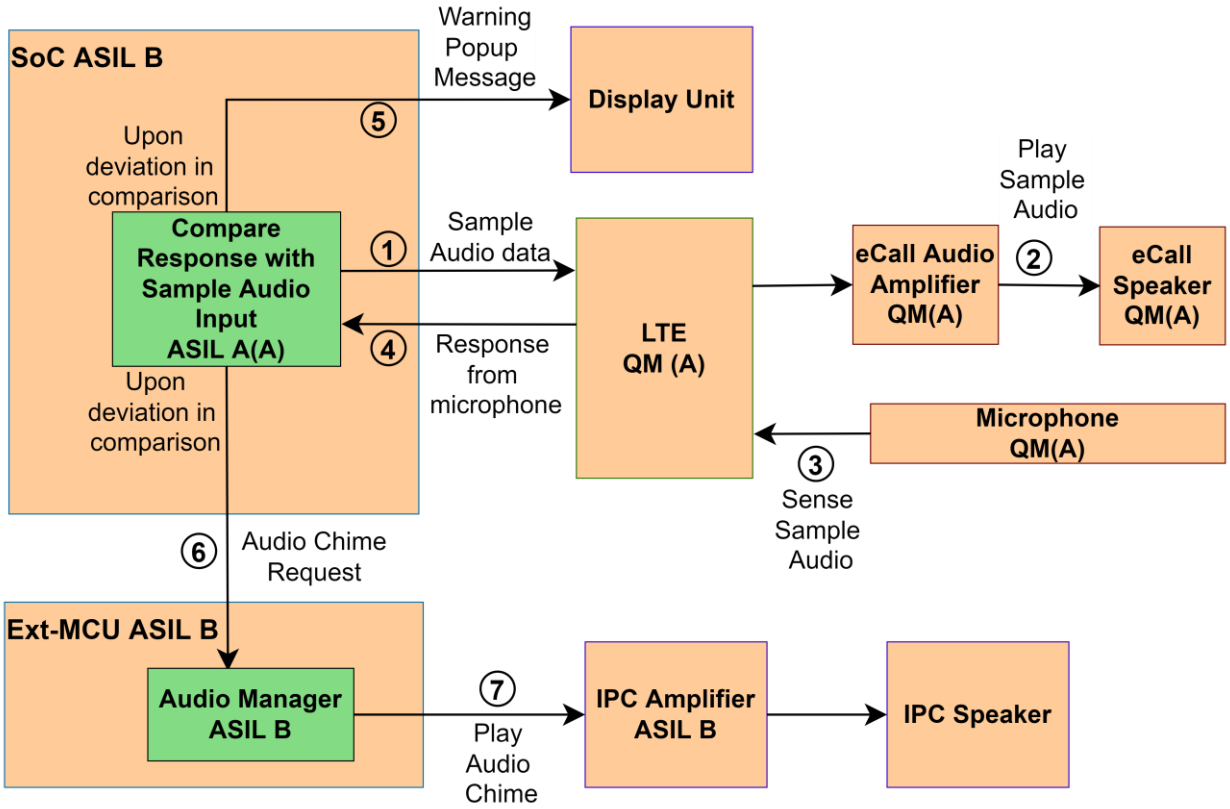


Figure 15 eCall Audio Components - Audio Test Play

Faults in eCall Audio components and its corresponding safety mechanisms are provided in below table:

Sl. No	Fault	SM ID	Safety Mechanism	Traceability	ASIL	Element Allocated
1.	Fault in Audio components	SM_20	**Fault in Audio components:** Perform Audio test play mechanism to detect fault in Microphone, eCall Speaker, eCall Audio Amplifier	eCockpit_TSR112 eCockpit_TSR113 eCockpit_TSR115 eCockpit_TSR116	A(A)	Compare Response with Sample Audio Input block in SoC
					QM(A)	[024] BLK MIC
					QM(A)	[025] BLK ECALL SPK
					QM(A)	[022] `BLK ECALL AUDIO AMPLIFIER
					QM(A)	[020] BLK_LTE
					B	[030] BLK SECONDARY CONTROLLER

(2) The SoC shall request the eCall speaker through LTE module to play the sample audio data

(3) The LTE module shall command the eCall speaker to play the sample audio data through Audio amplifier

(4) The Microphone shall sense the played sample audio data and feed it back to LTE module. The LTE module shall forward the response obtained from microphone (4)

The SoC the perform comparison between the sample audio data and the response received from microphone. Upon detection of deviation in the comparison beyond a certain threshold, the SoC shall transit to safe state by requesting warning popup message display (5) on the display unit. The SoC shall also send the Audio chime request to Audio manager in Ext-MCU (6) to the play the warning audio chime on IPC speakers (7).

Note: The above safety mechanism shall be performed only at every beginning of drive cycle for upto FDTI duration.

ASIL Decomposition:

1. Audio Amplifier is rated as QM(A)
2. eCall Amplifier is rated as QM(A)
3. Microphone is rated as QM(A)
4. Audio Play test comparison block is rated ASIL A(A)

The eCockpit system shall ensure the freedom from interference between the functions handling the audio components and the functions performing safety mechanism for these audio components.

Safe State:

1. Acoustic warning through IPC audio chimes – [eCockpit_TSR_SS02]

2. Warning popup message display on MDU – [eCockpit_TSR_SS01]

2.6 Safety Mechanisms related to Common Cause and Latent Faults

2.6.1 Power monitor

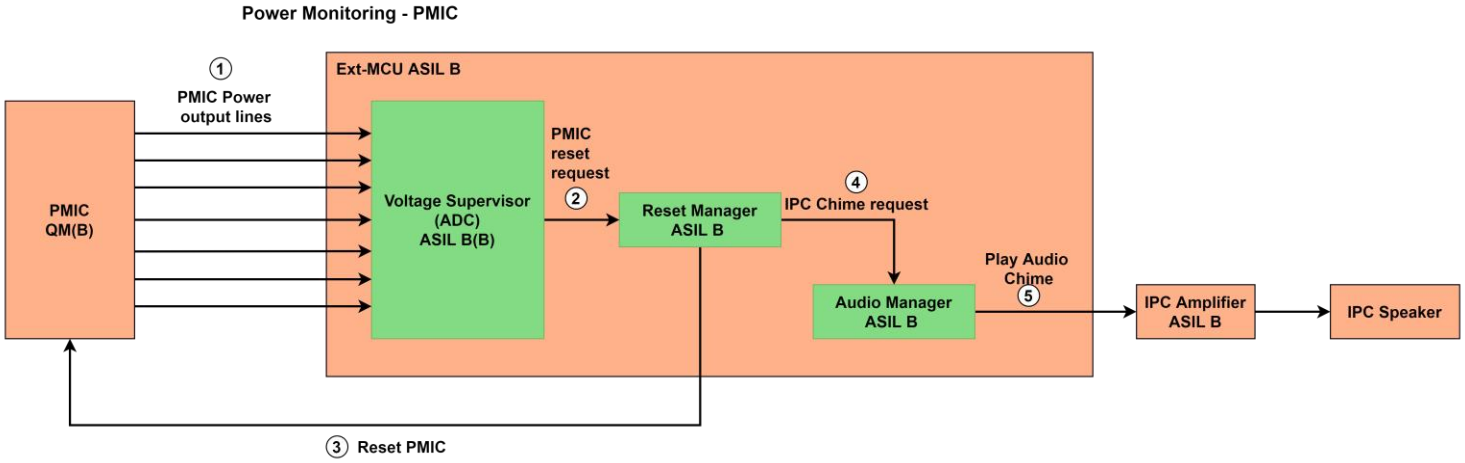


Figure 16 Power monitor

Table related to Safety mechanisms for Power supply Monitoring:

Sl. No	Fault	SM ID	Safety Mechanism	Traceability	ASIL	Element Allocated
1.	Failure modes in PMIC output	SM_21	**PMIC Output Monitor:** To monitor all PMIC power	eCockpit_TSR034, eCockpit_TSR035	B	[030] BLK SECONDARY

			output line to detect over voltage and under voltage conditions			CONTROLLER, [03] PWR SUP PMIC
2.	Failure modes in LV Battery	SM_22	**LV Battery Power Supply Monitor:** To monitor 12V battery supply to detect over voltage and under voltage conditions	eCockpit_TSR091, eCockpit_TSR092	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER, LV Battery Power Supply

Safety Concept for PMIC Output Monitor:

(1) Ext-MCU monitors voltage output routed to critical components of the system such as SoC, DDRAM, Clocks, Oscillators, NVMs (MMC, Hyperflash) from PMIC for valid output

(2) Voltage supervisor request Reset Manager to reset the PMIC

(3) Reset Manager resets PMIC

(4) The Reset manager also requests the Audio manager to play audio chime (5) through the IPC Amplifier

Safe State:

1. Acoustic warning through IPC audio chimes – [eCockpit_TSR_SS02]

2. Resetting of PMIC

2.6.2 Program Flow Monitoring

Faults in SoC and Ext-MCU such as stuck in program execution and related safety mechanisms are provided in below table:

Sl. No	**Fault**	**SM ID**	**Safety Mechanism**	**Traceability**	**ASIL**	**Element Allocated**
1.	Fault in SoC – program execution	SM_23	**Q&A watchdog for SoC:** To monitor SoC through Q&A watchdog using Ext-MCU	eCockpit_TSR049, eCockpit_TSR052, eCockpit_TSR051	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
2.	Fault in Ext-MCU – program execution	SM_25	**Watchdog monitor for Ext-MCU:** To monitor SoC through External watchdog timer	eCockpit_TSR050, eCockpit_TSR051	B	[030] BLK SECONDARY CONTROLLER
		SM_26	**Program Flow Monitoring for Ext-MCU:** To monitor ASIL rated software execution in Ext-MCU through program flow monitoring	eCockpit_TSR117, eCockpit_TSR118, eCockpit_TSR119, eCockpit_TSR120, eCockpit_TSR053	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER

2.6.2.1 External Q&A watchdog monitoring – SoC

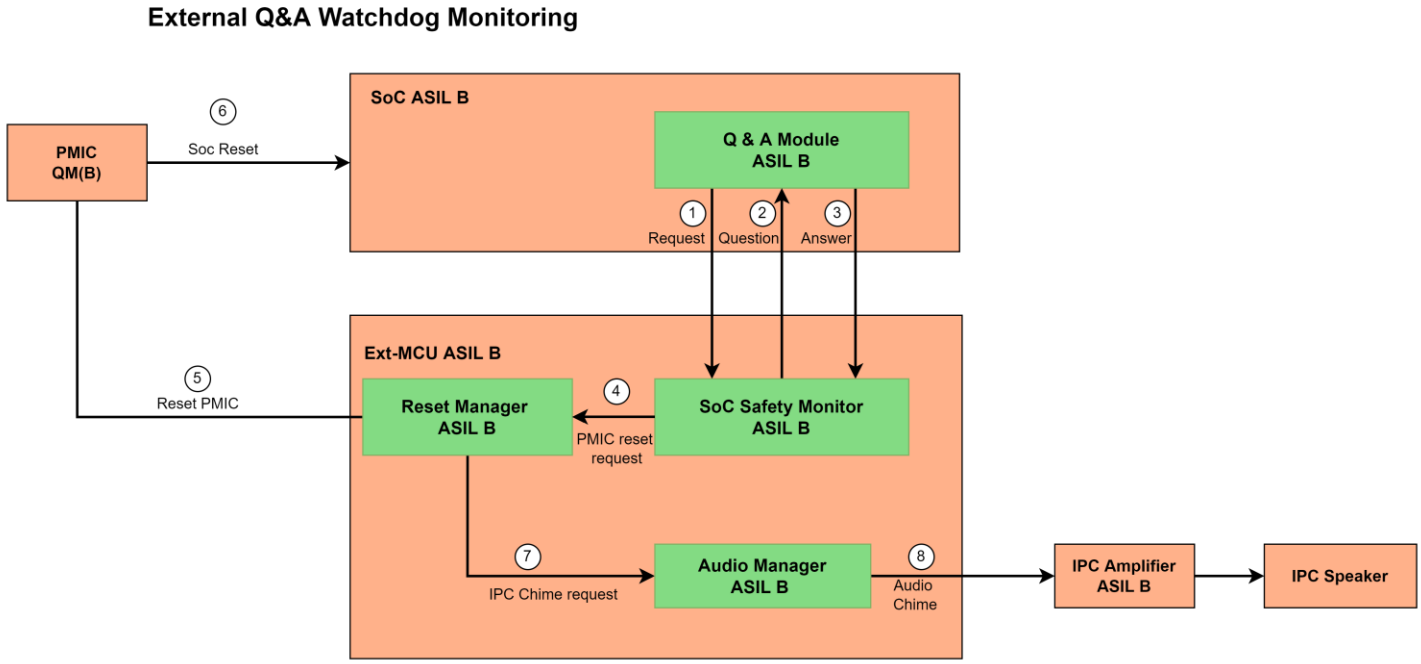


Figure 17 External Q&A watchdog monitoring – SoC

(1) The SoC requests Ext-MCU for Q&A timeout monitoring

(2) The Ext-MCU sends a question to SoC to respond within the predetermined interval

(3) The SoC responds with an answer to the Ext-MCU to verify its functionality

(4) Either on not receiving the request (1) or answer (3) within a predetermined interval, the Ext-MCU shall request the reset manager to reset the SoC

(4) the reset manager block in Ext-MCU change the state of reset pin associated with PMIC (5) to trigger a reset in the SoC (6)

(7) Also, whenever there is a reset operation for SoC, the Ext-MCU triggers an audio warning.

(8) the audio manager block in the Ext-MCU plays intended audio chime on receiving audio request from the reset manager

Safe State:

1. Acoustic warning through IPC audio chimes [eCockpit_TSR_SS02]
2. Triggering reset of SoC by Ext-MCU [eCockpit_TSR_SS05]

2.6.2.2 External watchdog monitoring – External MCU

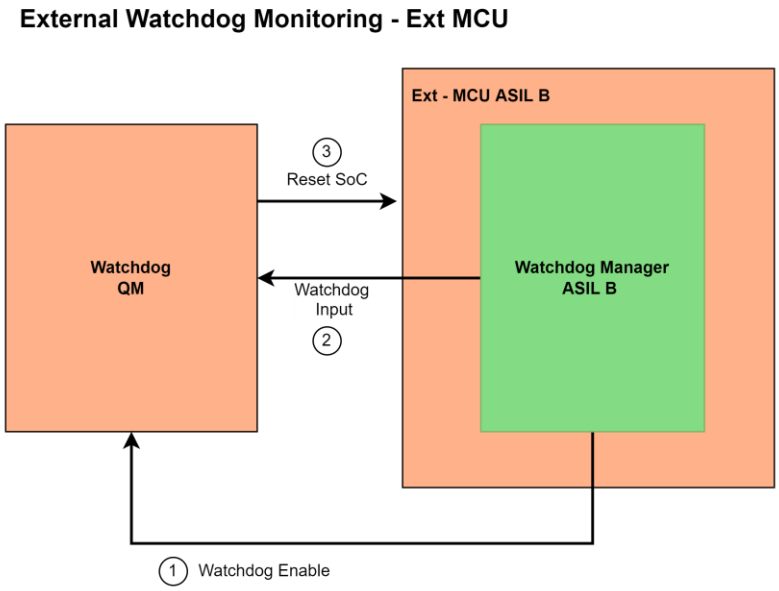


Figure 18 External watchdog monitoring – External MCU

(1) The Ext-MCU enables watchdog during initialization

(3) the watchdog resets the Ext-MCU, on not receiving the WDI input from SoC (2) within the predetermined interval

2.6.2.3 Program flow monitoring – SoC

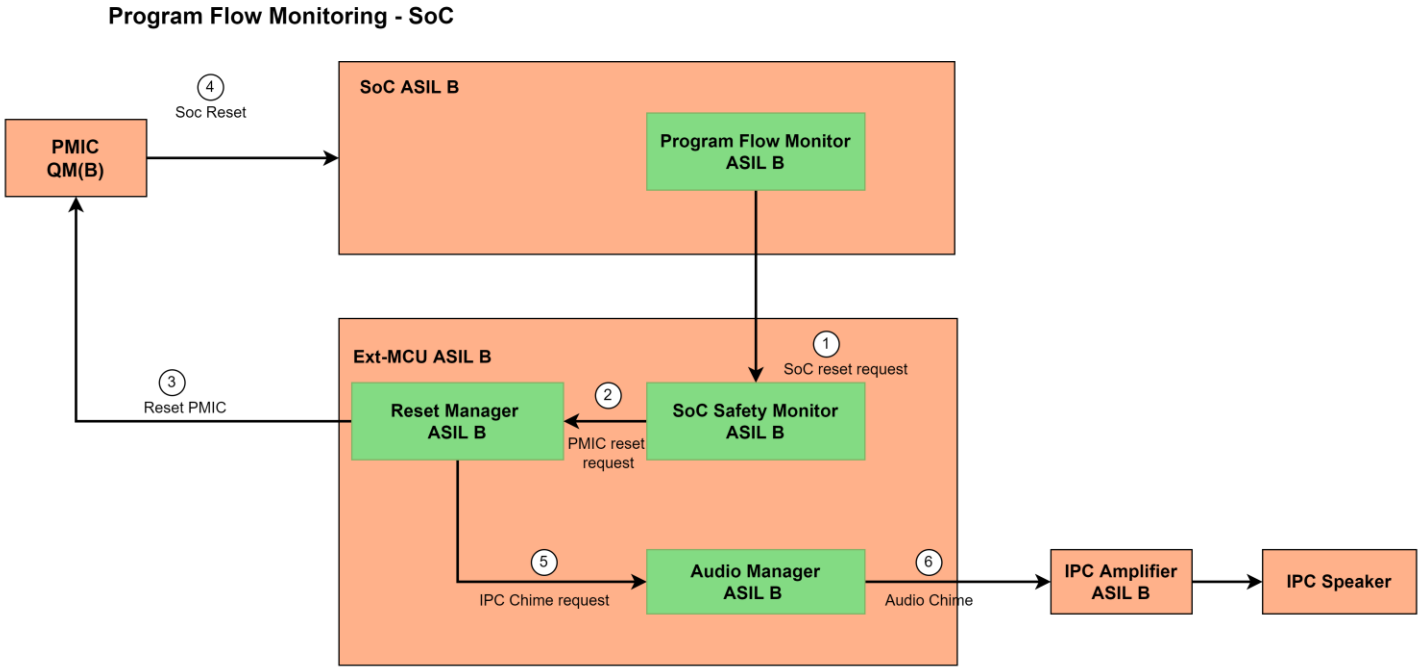


Figure 19 Program flow monitoring – SoC

(1) The SoC perform program flow monitoring on the safety functions executed in the real time core with the help of another ASIL rated processing cores. On detection of fault in program flow, the SoC triggers a reset request to the Ext-MCU through RFSO pin

(2) The SoC safety monitor block in the Ext-MCU monitors the external interrupt from SoC through RFSO pin and triggers a PMIC request to the reset manager block

(3) the reset manager block in Ext-MCU changes the state of reset pin associated with PMIC to trigger a reset for the SoC (4) within FRTI duration

(5) Also, whenever there is a reset operation, the Ext-MCU triggers an audio warning.

(6) the audio manager block in the Ext-MCU plays intended audio chime on receiving audio request from the reset manager within FRTI duration

Safe State:

1. Acoustic warning through IPC audio chimes [eCockpit_TSR_SS02]
2. Triggering reset of SoC by Ext-MCU [eCockpit_TSR_SS05]

2.6.2.4 Program flow monitoring – Ext-MCU

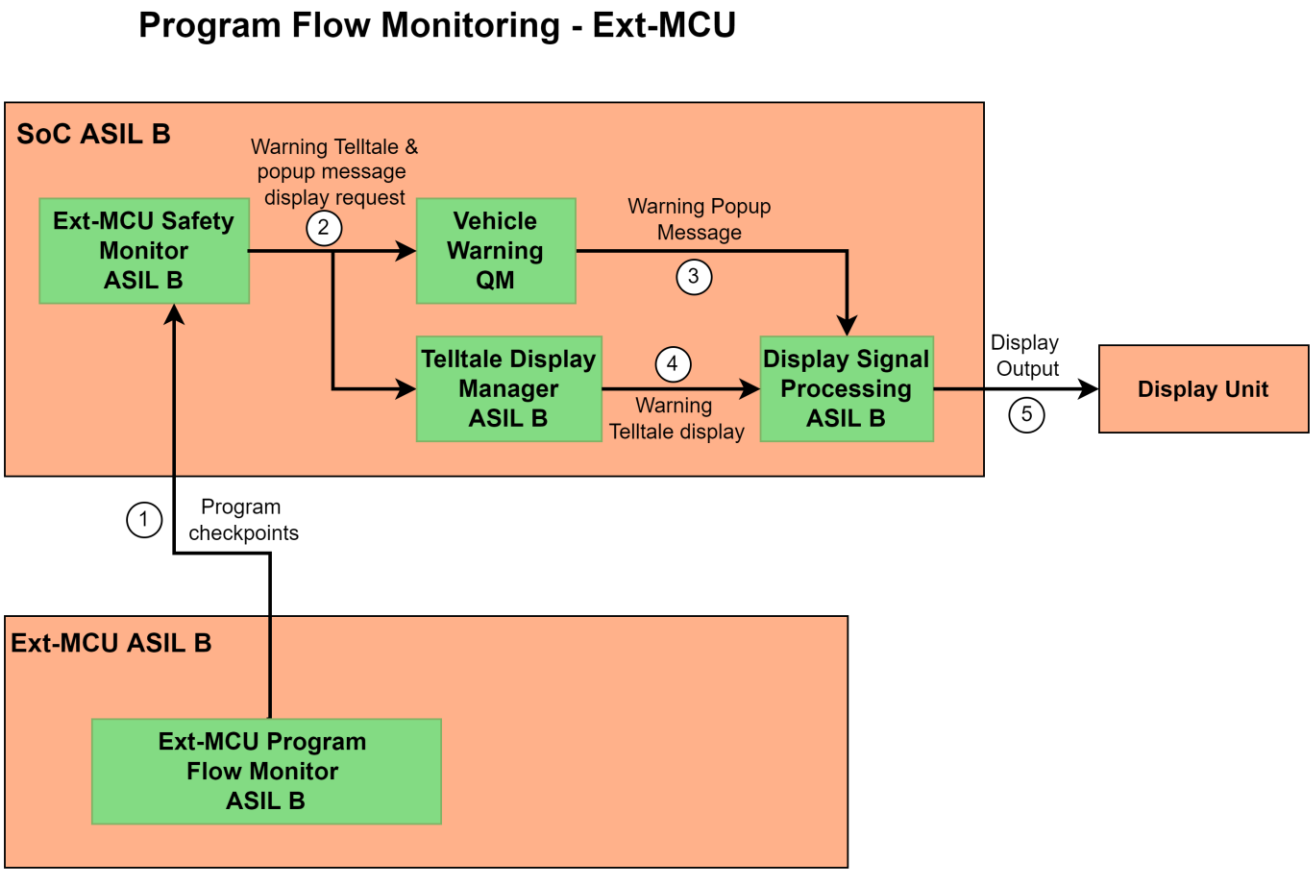


Figure 20 Program Flow Monitoring - Ext-MCU

Safety Concept:

(1) The Ext-MCU shall set several checkpoints through all safety related software functions and pass the checkpoints through communication interface to SoC in predetermined order and interval

The Ext-MCU Safety Manager block in SoC shall monitor the checkpoints to check the correctness of execution time and sequence of safety related functions in Ext-MCU

Upon detection of any deviation while monitoring the checkpoints within FDTI duration, the SoC shall check the reset status of Ext-MCU, to detect if Ext-MCU is being reset.

Note: Ext-MCU can be either reset due to the external reset circuit connected to it or due to self-reset.

(2) Upon failing to detect reset in Ext-MCU, the Ext-MCU Safety Manager block in SoC shall trigger request to display warning telltale and warning popup message within FRTI duration

(3) The Vehicle Warning block updates the MHU display buffer with warning popup message details and stores it in DDRRAM memory

(4) Telltale Display Manager block updates the safety data display buffer with warning telltale and stores it in DDRRAM memory

(5) Display Signal Processing block processes the updated MHU display buffer and safety data display buffer in DDRRAM and provides the blended display output to display unit within FRTI duration.

Safe State description:

1. Warning telltale + warning popup message display on MDU [eCockpit_TSR_SS01]
   Rationale: It is less likely for occurrence of failure in SoC at the same time when fault occurs in Ext-MCU, as multi-point failure is considered less probable
2. Once after the Ext-MCU reset (triggered either by self-reset or external reset circuit), if the fault in Ext-MCU is found recovered, the SoC shall remove the warning telltale and warning popup message display.
3. If the fault in the Ext-MCU is failed to recover and persists even after 2 consecutive drive cycles, on the 3rd drive cycle, the SoC shall transit the eCockpit system to system off state.
   Rationale: Though multi-point failure is considered less probable, if the fault persists for multiple drive cycle, operating SoC in absence of Ext-MCU monitoring for long time is not reliable. Any failure occurring in SoC thereafter becomes a single point fault. Hence when fault in Ext-MCU persists after 2 drive cycles, entering to eCockpit system off state becomes a reliable safe state.

2.6.3 Built-in self-test safety mechanisms

Safety mechanisms related to BIST and runtime tests in SoC and Ext-MCU are provided below:

Sl. No	Fault	SM ID	Safety Mechanism	Traceability	ASIL	Element Allocated
1.	Fault in SoC operation	SM_27	**BIST for SoC:** To perform BIST for SoC	eCockpit_TSR043, eCockpit_TSR045	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
		SM_28	**Runtime Tests for SoC:** To perform Runtime tests for SoC to detect random hardware and transient faults	eCockpit_TSR044, eCockpit_TSR045	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER
2.	Fault in Ext-MCU operation	SM_29	**Runtime Tests for Ext-MCU:** To perform Runtime tests for Ext-MCU to detect random hardware and transient faults	eCockpit_TSR046, eCockpit_TSR047, eCockpit_TSR053	B	[029] BLK PRIMARY CONTROLLER, [030] BLK SECONDARY CONTROLLER

2.6.3.1 Built-in self-test safety mechanism – SoC

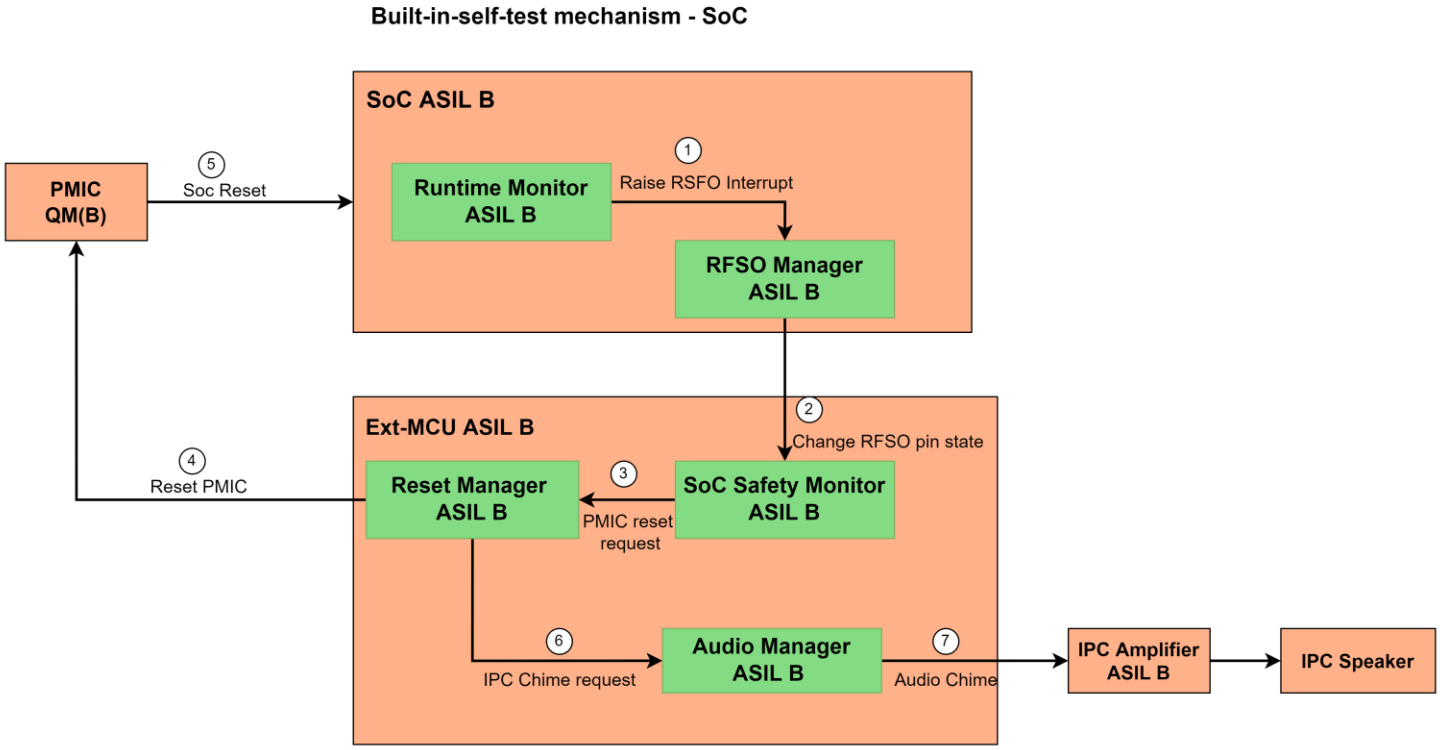


Figure 21 Built-in self-test safety mechanism – SoC

(1) The SoC performs runtime tests on the processing cores and peripheral modules within the SoC and requests RFSO manager block to trigger an RFSO interrupt on detection of a fault

(2) The RFSO manager block in the SoC triggers an external interrupt which is monitored by the Ext-MCU

(3) The SoC safety monitor block in the Ext-MCU monitors the external interrupt from SoC through RFSO pin and triggers a PMIC reset request to the reset manager block

(4) the reset manager block in Ext-MCU changes the state of reset pin associated with PMIC to trigger a reset in the SoC (5)

(6) Also, whenever there is a reset operation, the Ext-MCU triggers an audio warning.

(7) the audio manager block in the Ext-MCU plays intended audio chime on receiving audio request from the reset manager

Safe State:

1. Acoustic warning through IPC audio chimes [eCockpit_TSR_SS02]
2. Triggering reset of SoC by Ext-MCU [eCockpit_TSR_SS05]

2.6.3.2 Built-in self-test safety mechanism – Ext-MCU

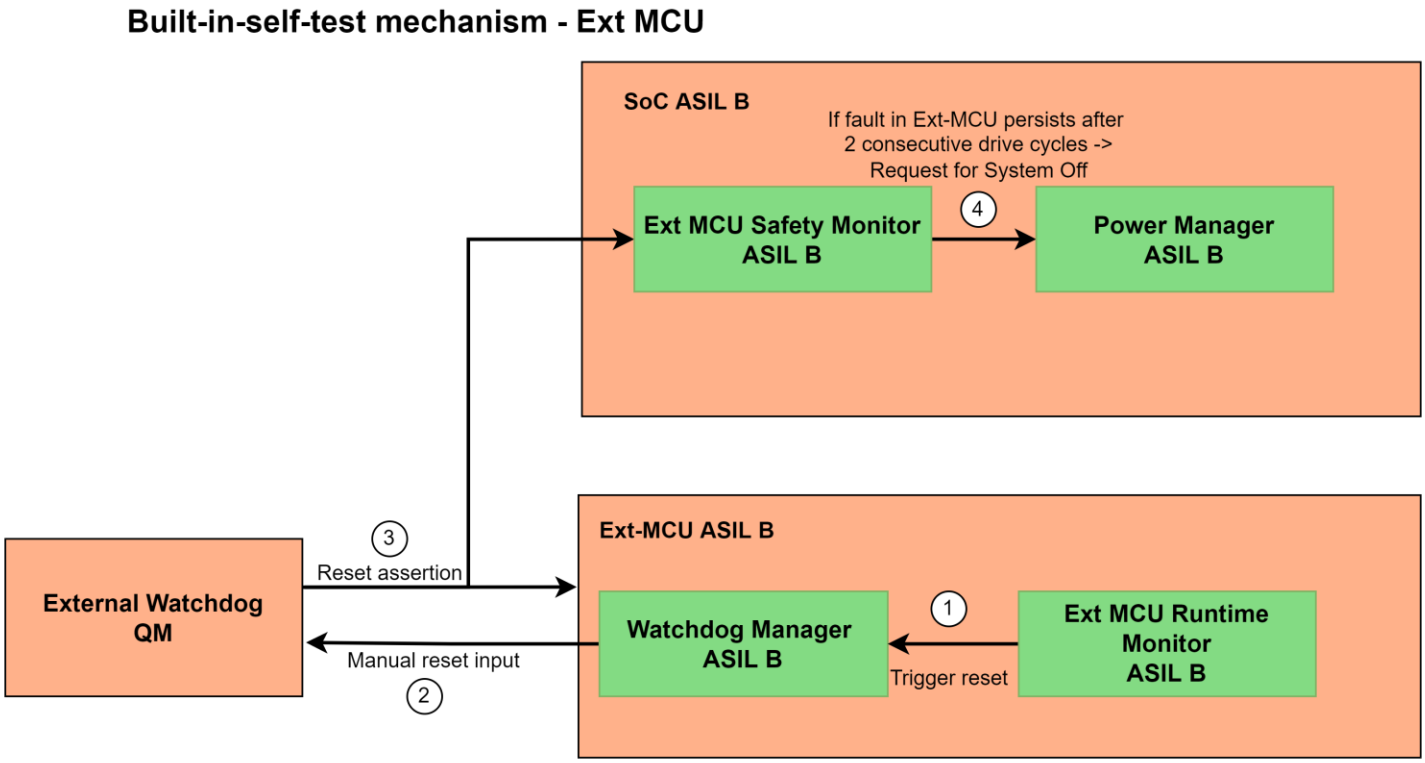


Figure 22 Built-in self-test safety mechanism – Ext-MCU

(1) The Ext-MCU performs runtime test on the internal peripherals of the controller and request a reset to the watchdog manager on detecting a fault

(2) the watchdog manager triggers a manual reset output to assert reset in the Ext-MCU (3)

(4) If the fault in the Ext-MCU is failed to recover and persists even after 2 consecutive drive cycles, on the 3rd drive cycle, the SoC shall transit the eCockpit system to system off state.

Rationale: Though multi-point failure is considered less probable, if the fault persists for multiple drive cycle, operating SoC in absence of Ext-MCU monitoring for long time is not reliable. Any failure occurring in SoC thereafter becomes a single point fault. Hence when fault in Ext-MCU persists after 2 drive cycles, entering to eCockpit system off state becomes a reliable safe state.

2.7 System Safety Architecture Diagram with ASIL allocations

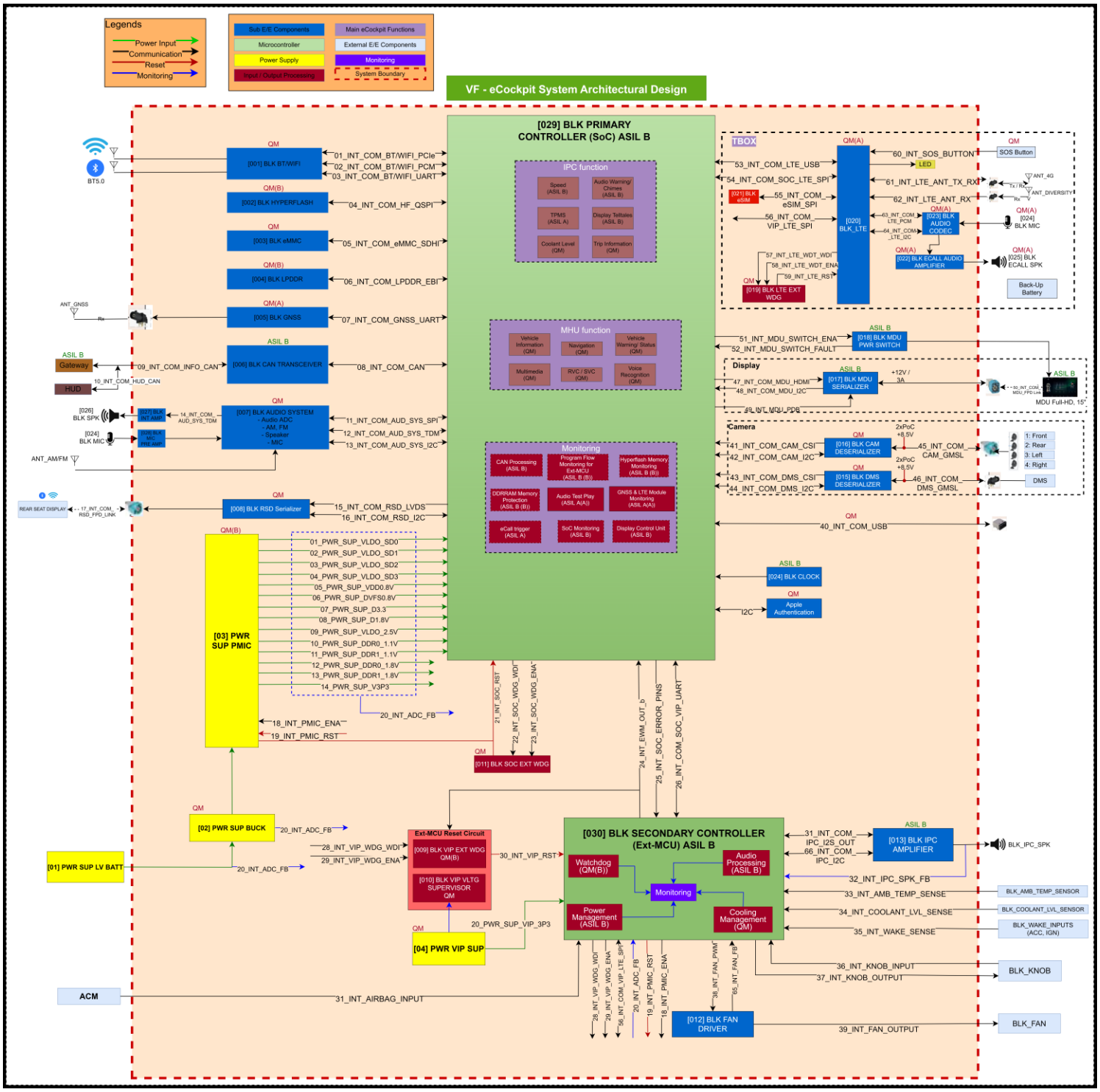


Figure 23 System Safety architecture block diagram with ASIL/ QM rating as per the safety mechanisms considered

2.7.1 Safety System Architecture Description

2.7.1.1 Blocks:

Sl.No	Block Name	Block Description
1.	[001] BLK BT/WIFI	Bluetooth and Wifi Module

2.	[002] BLK HYPERFLASH	HyperFlash Memory block
3.	[003] BLK eMMC	Embedded Multi-Media Card memory block
4.	[004] BLK LPDDR	DDRRAM memory block
5.	[005] BLK GNSS	GNSS module
6.	[006] BLK CAN TRANSCEIVER	CAN Transceiver block
7.	[007] BLK AUDIO SYSTEM	Audio System for AM/FM functionality with speakers and microphones
8.	[008] BLK RSD SERIALIZER	Rear Seat Display block
9.	[009] BLK VIP EXT WDG	External Watchdog timer block for Ext-MCU (VIP)
10.	[010] BLK VLTG SUPERVISOR	Voltage Supervisor for Ext-MCU supply voltage monitoring
11.	[011] BLK SOC EXT WDG	External Watchdog timer block for SoC
12.	[012] BLK FAN DRIVER	Fan Driver block
13.	[013] BLK IPC AMPLIFIER	IPC speaker Amplifier block
14.	[015] BLK DMS DESERIALIZER	Deserializer block for DMS camera
15.	[016] BLK CAM DESERIALIZER	Derializer block for Surround View Monitoring cameras
16.	[017] BLK MDU SERIALIZER	Serializer block for MDU
17.	[018] BLK MDU PWR SWITCH	Power Switch block to control power supply to MDU
18.	[019] BLK LTE EXT WDG	External watchdog timer block for LTE
19.	[020] BLK LTE	LTE block in TBOX module
20.	[021] BLK eSIM	Embedded SIM for LTE
21.	[022] BLK ECALL AUDIO AMPLIFIER	Audio Amplifier for eCall speaker
22.	[023] BLK AUDIO CODEC	Audio Codec block for eCall audio system
23.	[024] BLK MIC	Microphones for eCockpit systems
24.	[025] BLK ECALL SPK	eCall Speaker block in TBOX module
25.	[026] BLK SPK	Speaker block used for eCockpit Audio System
26.	[027] BLK INT AMP	Amplifier for eCockpit Audio System speakers
27.	[028] BLK MIC PRE AMP	Amplifier for Microphones
28.	[029] BLK PRIMARY CONTROLLER	Primary /Main Controller (SoC) of eCockpit System
29.	[030] BLK SECONDARY CONTROLLER	Secondary Controller/ Ext-MCU (VIP) of eCockpit System

2.7.1.2 Power Supply:

Sl.No	Power Supply Name	Description
1.	[01] PWR SUP LV BATT	12V Low Voltage Battery Power Supply module
2.	[02] PWR SUP BUCK	5V Power Supply Buck Converter module
3.	[03] PWR SUP PMIC	Power Supply module for SoC
4.	[04] PWR VIP SUP	Power Supply module for Ext-MCU (VIP)
5.	01_PWR_SUP_VLDO_SD0	3.3V PMIC output
6.	02_PWR_SUP_VLDO_SD1	1.8V PMIC output
7.	03_PWR_SUP_VLDO_SD2	1.8V PMIC output
8.	04_PWR_SUP_VLDO_SD3	1.8V PMIC output
9.	05_PWR_SUP_VDD0.8V	0.8V PMIC output
10.	06_PWR_SUP_DS0.8V	0.8V PMIC output
11.	07_PWR_SUP_D3.3	3.3V PMIC output
12.	08_PWR_SUP_D1.8V	1.8V PMIC output
13.	09_PWR_SUP_VLDO_2.5V	2.5V PMIC output
14.	10_PWR_SUP_DDR0_1.1V	1.1V PMIC output
15.	11_PWR_SUP_DDR1_1.1V	1.1V PMIC output
16.	12_PWR_SUP_DDR0_1.8V	1.8V PMIC output
17.	13_PWR_SUP_DDR1_1.8V	1.8V PMIC output
18.	14_PWR_SUP_V3P3	3.3V PMIC input
19.	20_PWR_SUP_VIP_3P3	3.3V Supply for Ext-MCU

2.7.1.3 Interfaces:

Sl.No	Interface Name	Interface Description
1.	01_INT_COM_BT/WIFI_PCIe	PCIe communication between SoC and BT/WiFi module
2.	02_INT_COM_BT/WIFI_PCM	PCM communication between SoC and BT/WiFi module
3.	03_INT_COM_BT/WIFI_UART	UART communication between SoC and BT/WiFi module
4.	04_INT_COM_HF_QSPI	SPI communication between SoC and HyperFlash memory
5.	05_INT_COM_eMMC_SDHI	SD card Host Interface between SoC and eMMC memory
6.	06_INT_COM_LPDDR_EBI	Extended Bus Interface between SoC and LPDDR (DDRRAM) memory
7.	07_INT_COM_GNSS_UART	UART communication between SOC and GNSS
8.	08_INT_COM_CAN	CAN Tx, Rx communication between SOC and CAN Transceiver
9.	09_INT_COM_INFO_CAN	INFO CAN communication between SoC and Gateway
10.	10_INT_COM_HUD_CAN	CAN Bus communication SoC and HUD
11.	11_INT_COM_AUD_SYS_SPI	SPI communication between SoC and Audio System
12.	12_INT_COM_AUD_SYS_TDM	TDM interface between SoC and Audio System
13.	13_INT_COM_AUD_SYS_I2C	I2C communication between SOC and Audio System
14.	14_INT_COM_AUD_SYS_TDM	TDM communication between SoC and Audio System
15.	15_INT_COM_RSD_LVDS	LVDS communication between SoC and Rear Seat Display Serializer
16.	16_INT_COM_RSD_I2C	I2C communication between SoC and Rear Seat Display Serializer
17.	17_INT_COM_RSD_FPD_LINK	Flat Panel Display Link communication between Rear Seat Display Serializer and RSD Display Unit
18.	18_INT_PMIC_ENA	Interface to enable the PMIC power supply output
19.	19_INT_PMIC_RST	Interface to reset the PMIC power supply output
20.	20_INT_ADC_FB	ADC feedback of power supply output from LV Battery, PMIC, voltage regulators etc
21.	21_INT_SOC_RST	Interface to trigger Reset for SoC
22.	22_INT_SOC_WDG_WDI	Watchdog Input interface of external watchdog for SoC
23.	23_INT_SOC_WDG_ENA	Watchdog Enable interface of external watchdog for SoC
24.	24_INT_EWM_OUT_b	External Watchdog Monitor reset out signal from Ext-MCU
25.	25_INT_SOC_ERROR_PINS	SoC Error reporting pins like FSCLKST, RFSO pins
26.	26_INT_COM_SOC_VIP_UART	UART communication between SoC and Ext-MCU
27.	28_INT_VIP_WDG_WDI	Watchdog Input interface of external watchdog for Ext-MCU (VIP)
28.	29_INT_VIP_WDG_ENA	Watchdog Enable interface of external watchdog for Ext-MCU (VIP)
29.	30_INT_VIP_RST	Interface to trigger Reset for Ext-MCU (VIP)
30.	31_INT_COM_IPC_I2S_OUT	I2S communication between Ext-MCU and IPC Amplifier
31.	32_INT_IPC_SPK_FB	Voltage and Current feedback of IPC Amplifier output
32.	33_INT_AMB_TEMP_SENSE	Interface to obtain Ambient Temperature
33.	34_INT_COOLANT_LVL_SENSE	Interface to obtain Coolant level
34.	35_INT_WAKE_SENSE	Interfaces to obtain wake-up inputs for eCockpit System like Accessory, Ignition etc
35.	36_INT_KNOB_INPUT	Interface to obtain Knob press input
36.	37_INT_KNOB_OUTPUT	Interface to provide output to Knob
37.	38_INT_FAN_PWM	Interface to provide PWM input to Fan driver
38.	39_INT_FAN_OUTPUT	Interface to obtain feedback from Fan driver
39.	40_INT_COM_USB	USB connection for eCockpit
40.	41_INT_COM_CAM_CSI	Camera Serial Interface for SVM Cameras deserializer
41.	42_INT_COM_CAM_I2C	I2C communication between SVM Cameras deserializer and SoC
42.	43_INT_COM_DMS_CSI	Camera Serial Interface for DMS Camera deserializer
43.	44_INT_COM_DMS_I2C	I2C Communication between DMS Camera deserializer
44.	45_INT_COM_CAM_GMSL	Gigabit Multimedia Serial Link (GMSL) interface between SVM cameras and deserializer
45.	46_INT_COM_DMS_GMSL	Gigabit Multimedia Serial Link (GMSL) interface between DMS camera and deserializer
46.	47_INT_COM_MDU_HDMI	HDMI communication between SoC and MDU serializer
47.	48_INT_COM_MDU_I2C	I2C communication between SoC and MDU serializer
48.	49_INT_MDU_PDB	Power Down Mode pin to reset MDU serializer

49.	50_INT_COM_MDU_FPD Link	FPD link between MDU serializer and MDU
50.	51_INT_MDU_SWITCH_ENA	Enable/Disable input for MDU Power switch
51.	52_INT_MDU_SWITCH_FAULT	Fault diagnostic output from MDU Power switch to SoC
52.	53_INT_COM_LTE_USB	USB communication between SoC and LTE
53.	54_INT_COM_SOC_LTE_SPI	SPI communication between SoC and LTE
54.	55_INT_COM_eSIM_SPI	SPI communication between LTE and eSIM
55.	56_INT_COM_VIP_LTE_SPI	SPI communication between Ext-MCU (VIP) and LTE
56.	57_INT_LTE_WDT_WDI	Watchdog Input interface of external watchdog for LTE
57.	58_INT_LTE_WDT_ENA	Watchdog Enable interface of external watchdog for LTE
58.	59_INT_LTE_RST	Reset input interface for LTE
59.	60_INT_SOS_BUTTON	Manual input to trigger eCall
60.	61_INT_LTE_ANT_TX_RX	LTE Main Antenna interface
61.	62_INT_LTE_ANT_RX	LTE Diversity Antenna interface
62.	63_INT_COM_LTE_PCM	PCM communication between LTE and Audio codec
63.	64_INT_COM_LTE_I2C	I2C communication between LTE and Audio codec

Following are the design constraints in the eCockpit resulting from the hardware and software elements:

Design Constraints in MDU:

The MDU does not have the capability to validate the data it displays. Hence the SOC cannot guarantee that the safety data is displayed correctly on MDU.

3 Technical Safety Concept

3.1 Criteria for coexistence of elements and FFI – SoC

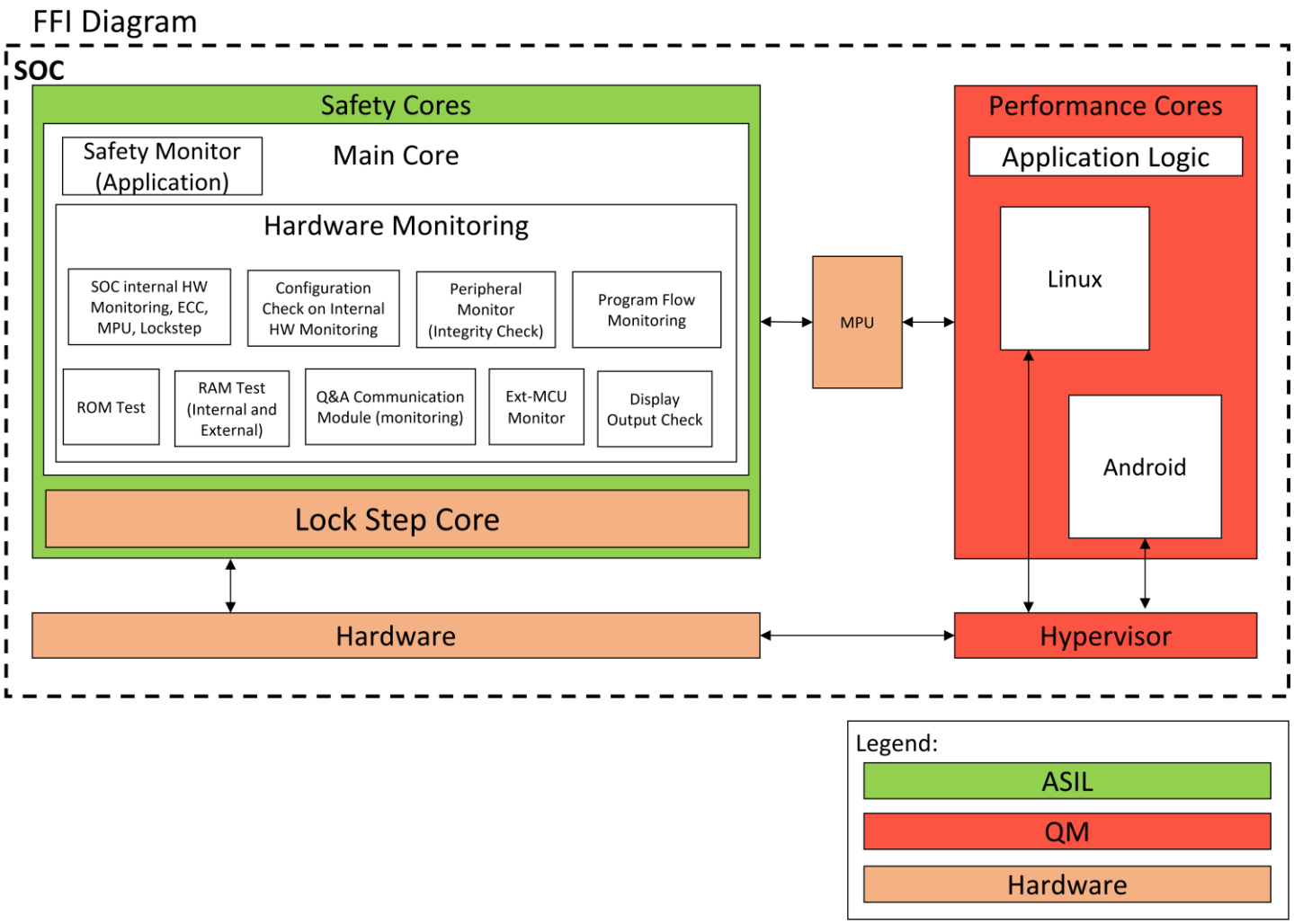


Figure 24 Freedom of Interference – SOC

The SoC used has 9 cores and uses 3 OS:

1. AUTOSAR – ASIL B Compliant – run on ARM real-time core
2. XEN Hypervisor – runs on A53 and A57 cores
    a. Linux for IPC domain – QM rated
    b. Android for MHU domain – QM rated

Argument(s) to provide evidence on achieving freedom from interference for memory:

- All safety related components are placed under the memory partition used by the AUTOSAR OS
- CPU is controlled by highest ASIL software components (ASIL B).
- Hardware redundancy of the main safety core is provided by using lock step core CPU
- There is no separate partition for execution of ASIL A rated functions. Both ASIL A and ASIL B rated functions are executed in the ASIL B partition. The difference would be on the diagnostic coverage, where ASIL B rated functions have more coverage compared to ASIL A rated functions.

- The ASIL rated components are protected from QM component interaction through memory and access protection mechanisms
- Memory partition for ASIL and QM components are created

Argument(s) to provide evidence on achieving freedom from interference for timing:

- The SoC has external watchdog monitoring mechanism to detect any execution delay in ASIL rated components
- The Q&A watchdog monitoring of SoC with suitable checkpoints in association with Ext-MCU provides logical monitoring of the timely execution of various software components in correct sequence

Argument(s) to provide evidence on achieving freedom from interference for communication:

- The Safety core of SoC receives the input messages over CAN and performs E2E checks such as CRC, timeout monitoring etc., to detect faults in communication of data from other ECUs

The details on memory partition will be provided in system and software architecture document. Further details on the software processes that argues on freedom from interference will be provided during software phase in the software architectural design document.

3.2 Criteria for coexistence of elements and FFI – Ext-MCU

The Ext-MCU runs in a single partition with its compliance being ASIL B. The Ext-MCU is primarily a monitoring device for the SoC and provide other functions like power monitoring and audio warning.
As the Ext-MCU is a monitoring device which mainly monitors the SoC, power lines etc, the following points can be the argument(s) to provide evidence on achieving freedom from interference:

- For Memory:
    - No sharing of memories of Ext-MCU and SoC are independent
- For Timing:
    - No common clock source for operation of Ext-MCU and SoC. Ext-MCU uses its own clock source for controller operation
- Power Supply:
    - The Ext-MCU is powered with an independent power supply different from the power supply source of SoC

Further details on the software processes that argues on freedom from interference will be provided during software phase in the software architectural design document.

3.3 Fault Tolerance Time Interval (FTTI)

The FTTI, FDTI and FRTI durations for eCockpit system are obtained from the functional safety concept [Ref 02]. Following are the details regarding consideration of FTTI, FDTI and FRTI values:

1. FDTI: 3000ms
2. FRTI: 1000ms
3. FTTI: 5000ms

Where, FTTI > FDTI + FRTI

4 System Safety Analysis

For the eCockpit system, both the FTA analysis and FMEA analysis is performed as part of the system safety analysis. The FMEA details can be obtained from [Ref 05]

Below are the excerpts of FTA analysis performed for the system in the Medini Analyzer tool. The technical safety requirements are derived for each low-level event that would act as a single point fault to violate the safety goal. The traceability of TSR and FTA events are shown in the TSR specification document and in the Medini tool.

4.1 FTA tree diagram – -eCockpit-CSG01

The analysis for CSG01 is combined with CSG02 as both are similar in function while considering the technical aspect of the function with respect to eCockpit system.

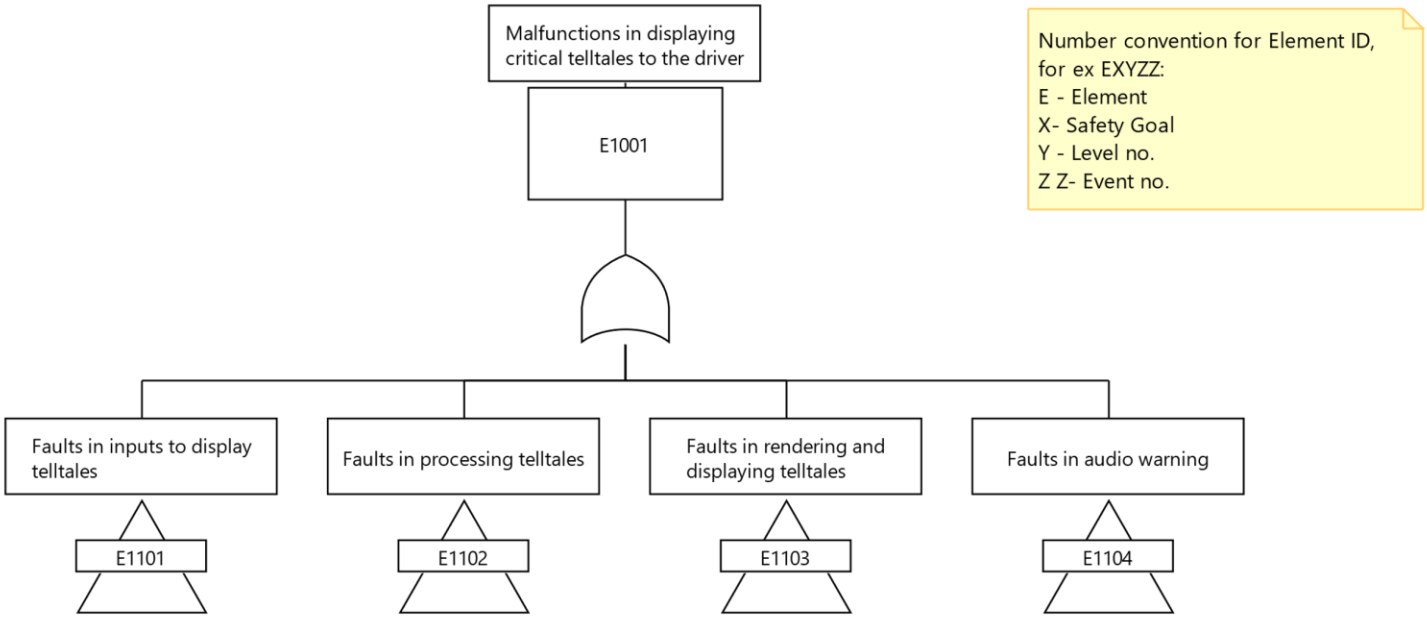


Figure 25 FTA tree diagram – -eCockpit-CSG01

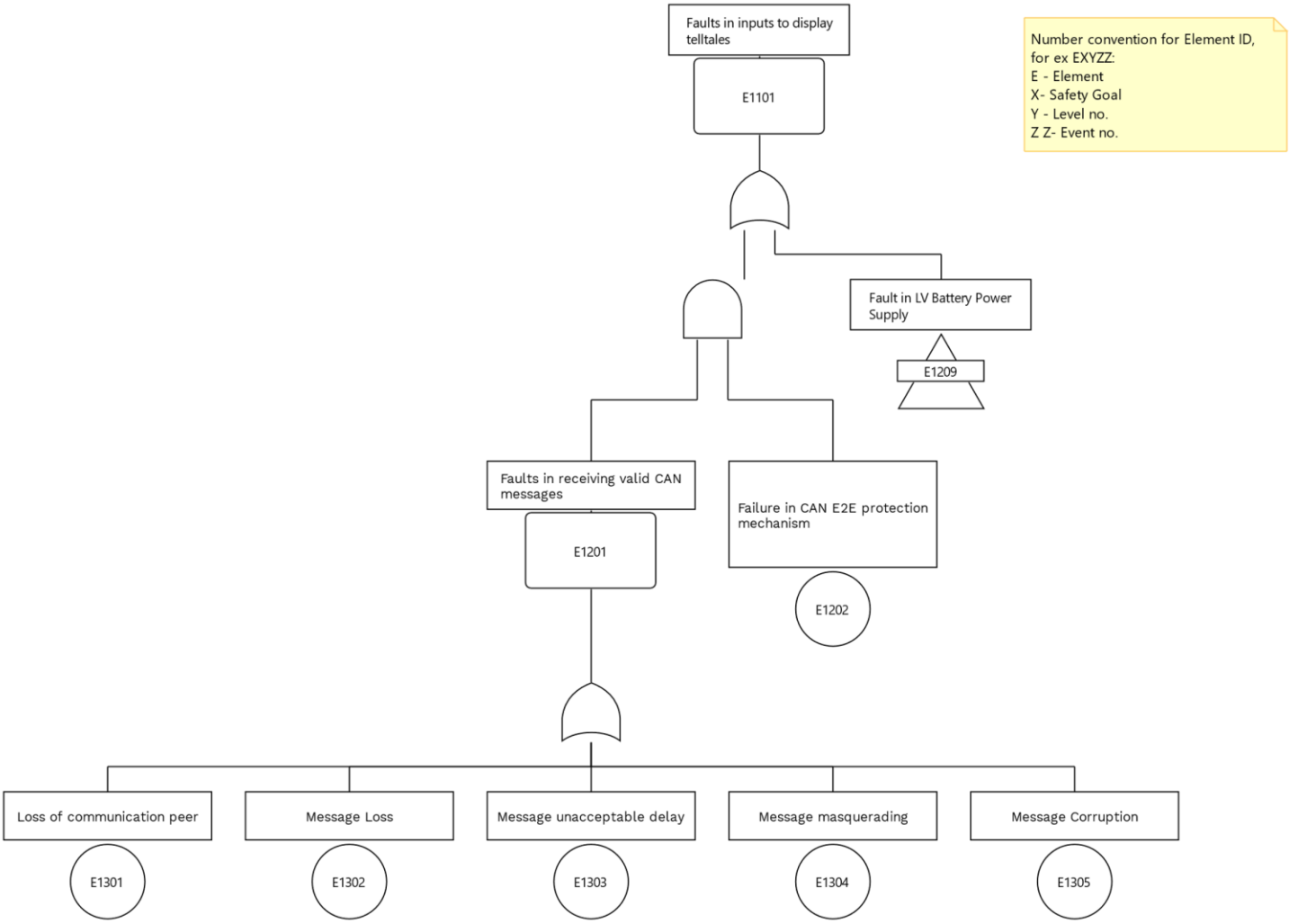


Figure 26 FTA for -eCockpit-CSG01 - Fault in Inputs

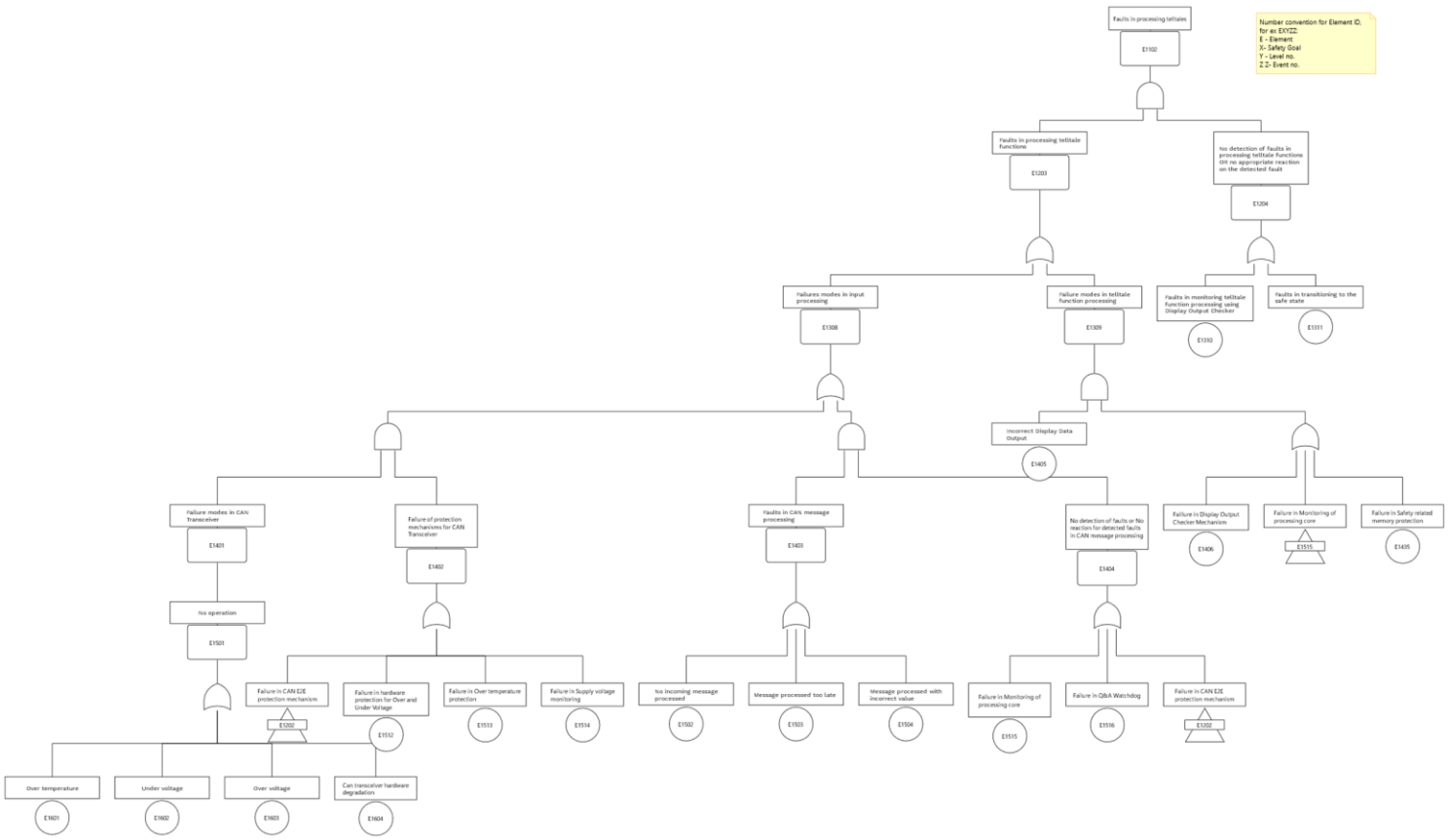


Figure 27 FTA for -eCockpit-CSG01 - Faults in Processing

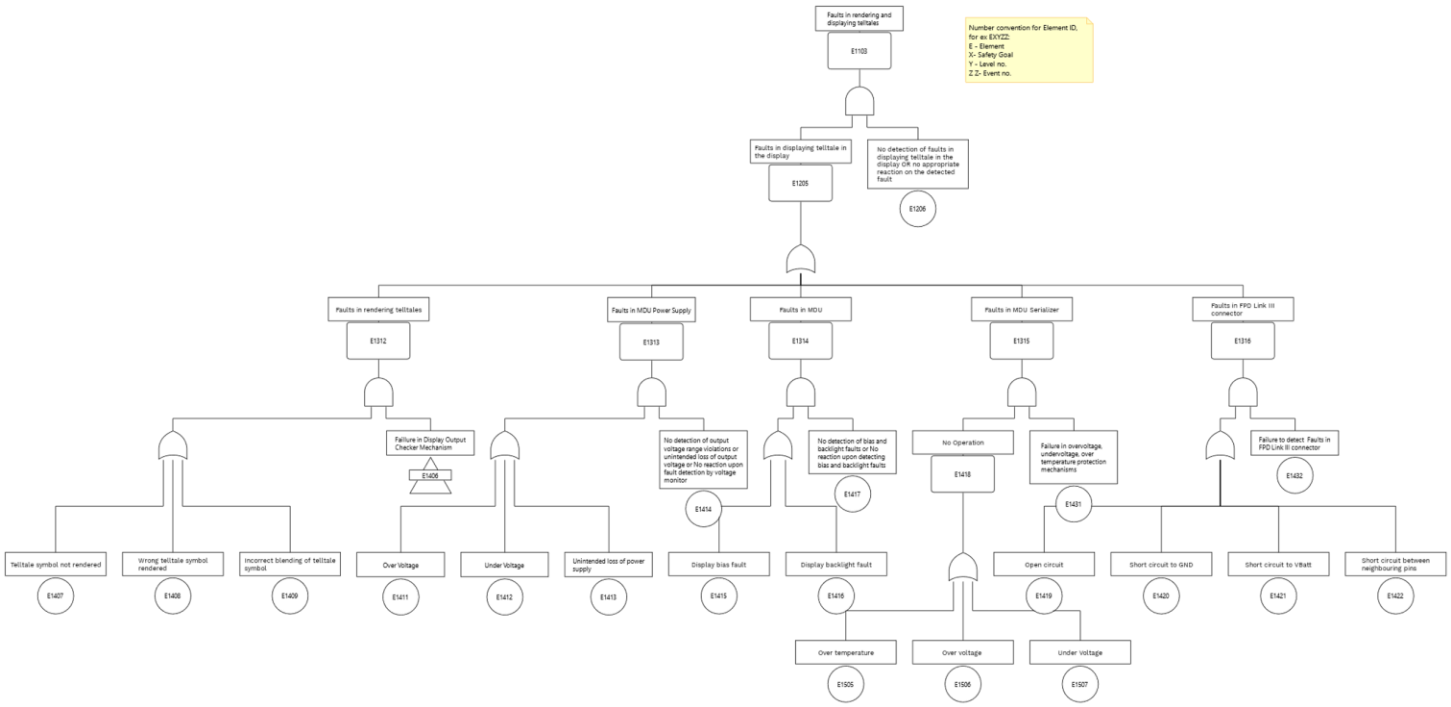


Figure 28 FTA for -eCockpit-CSG01 - Faults in Telltale Display

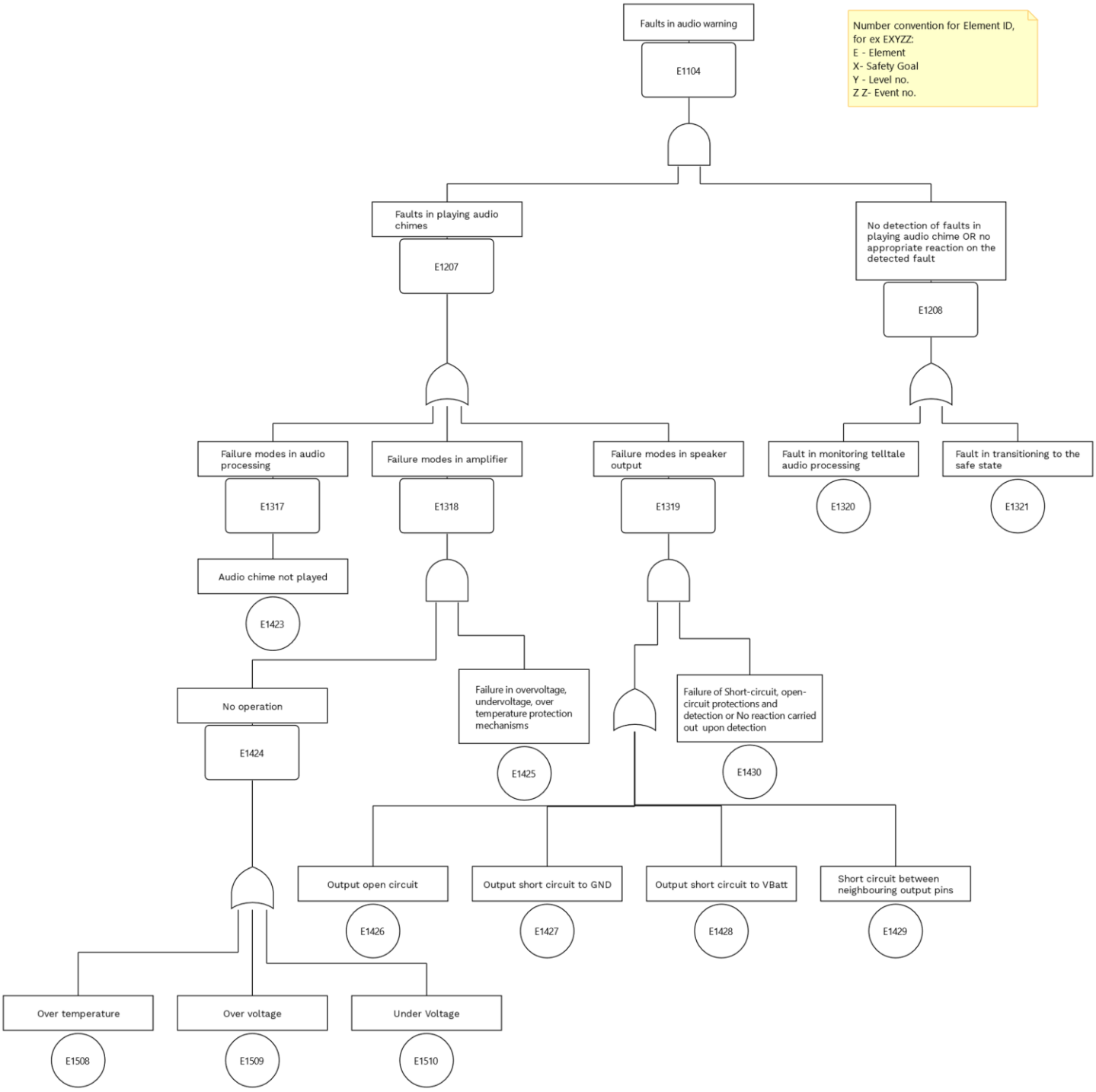


Figure 29 FTA for -eCockpit-CSG01 - Faults in Audio Warning

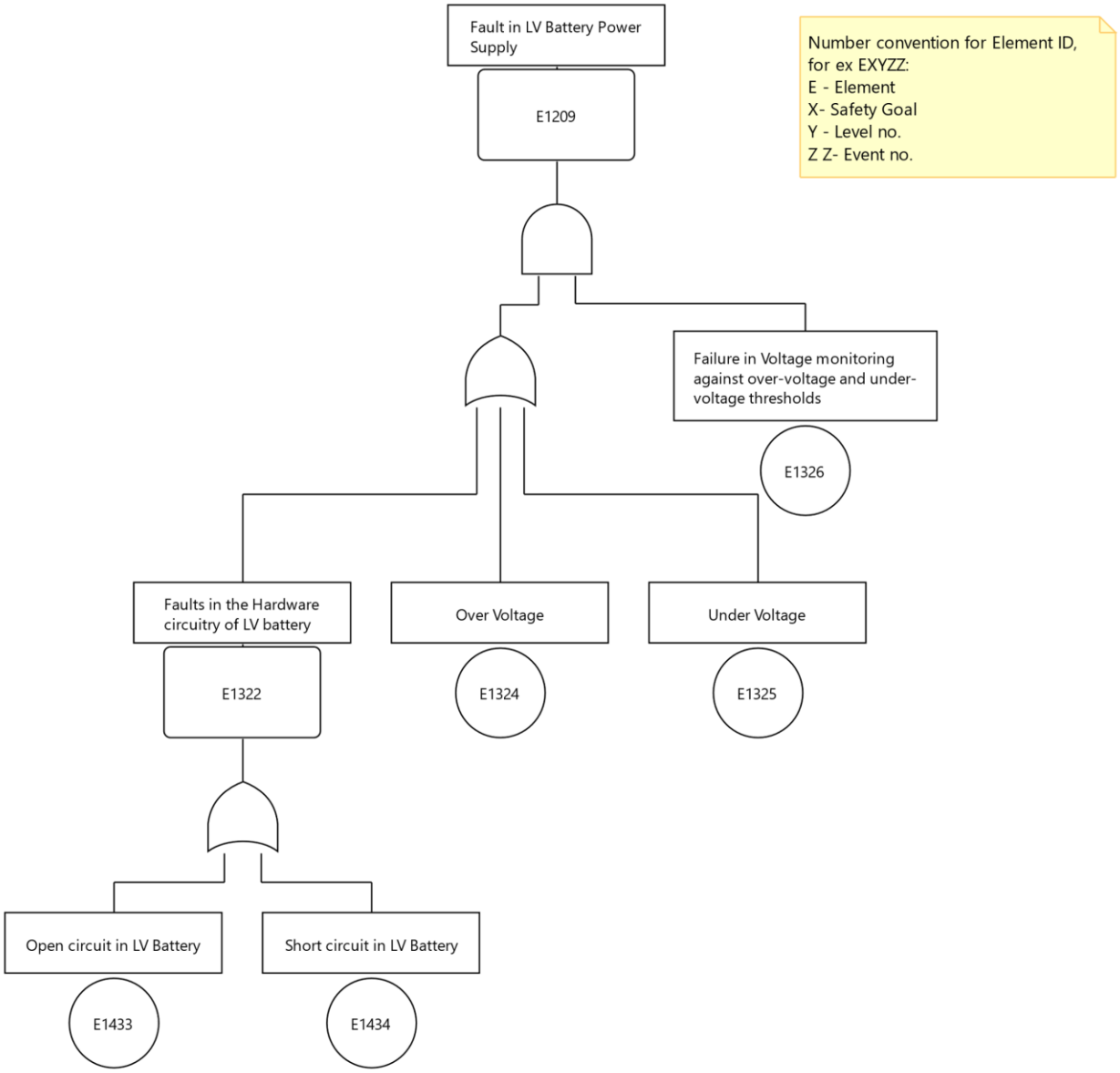


Figure 30 FTA for -eCockpit-CSG01 - Faults in Power Supply

4.2 FTA tree diagram – -eCockpit-CSG02

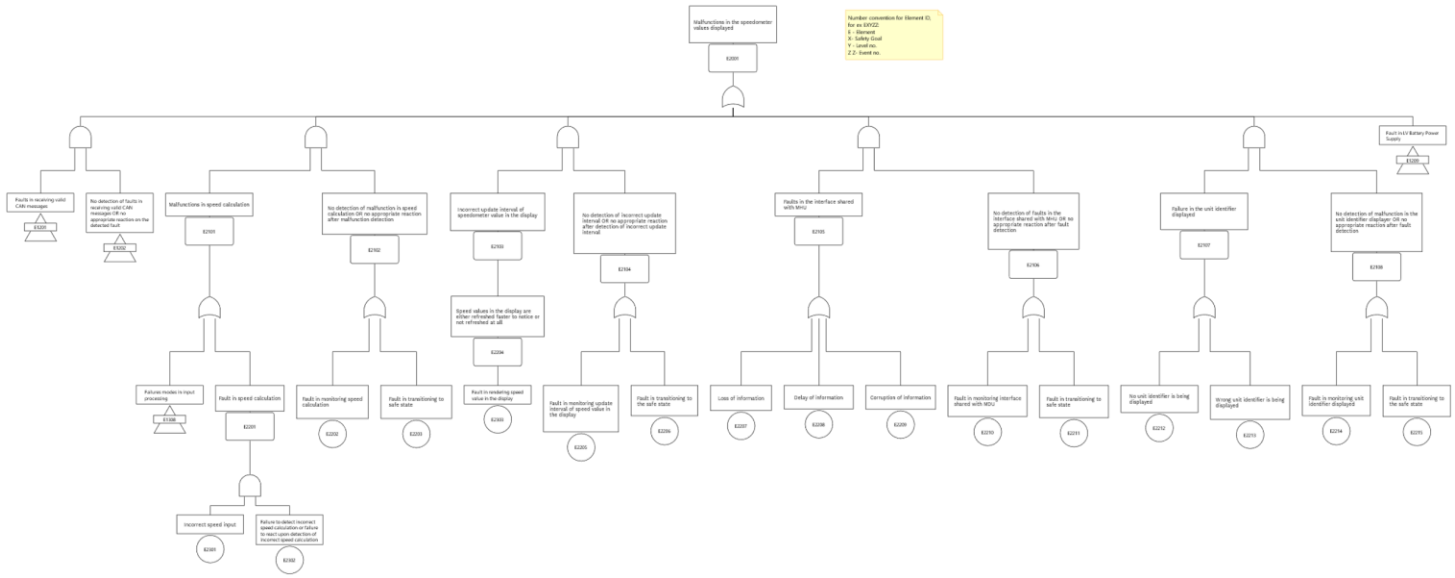


Figure 31 FTA tree diagram – -eCockpit-CSG02

4.3 FTA tree diagram – -eCockpit-CSG03

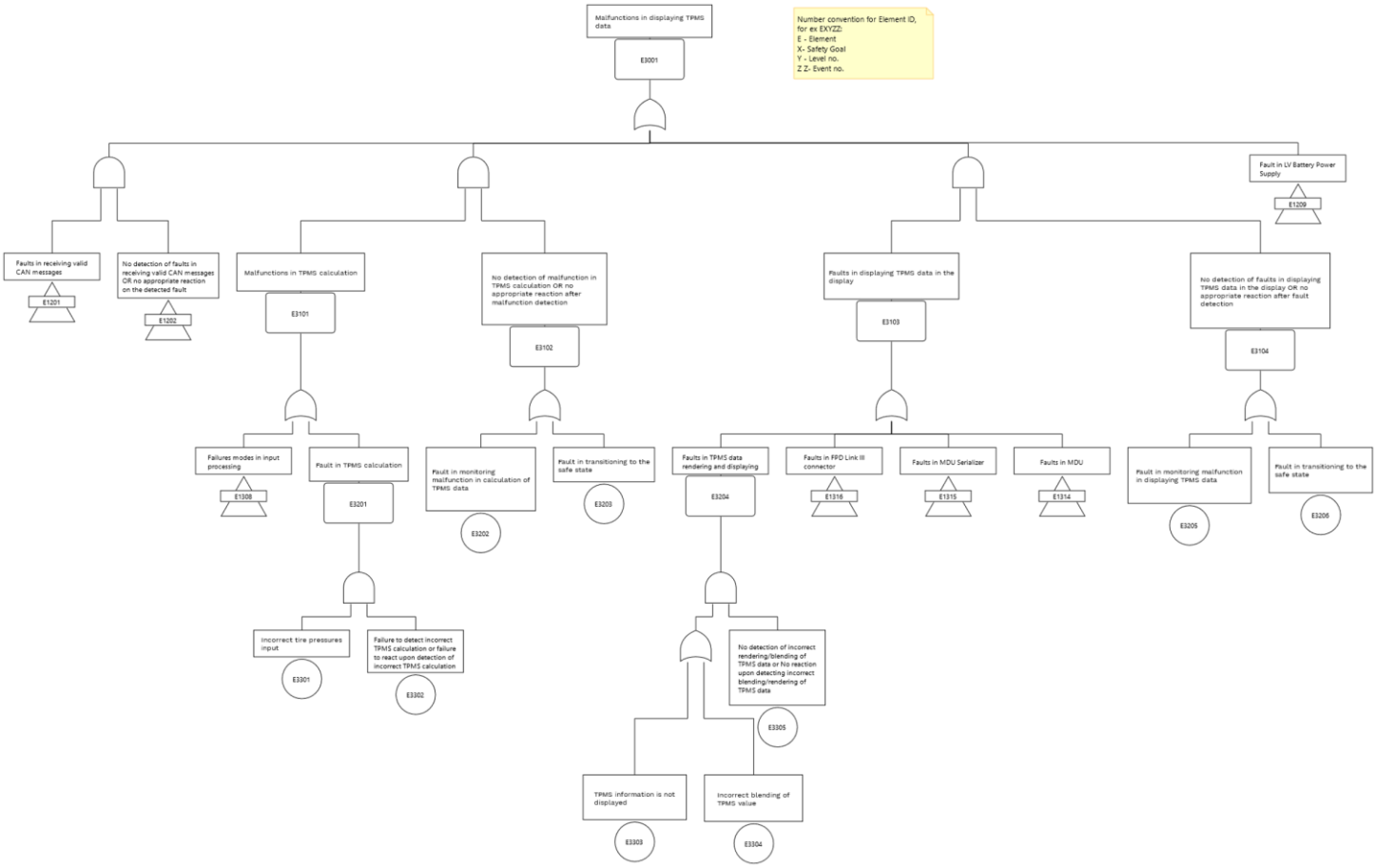


Figure 32 FTA tree diagram – -eCockpit-CSG03

4.4 FTA tree diagram – -eCockpit-CSG04

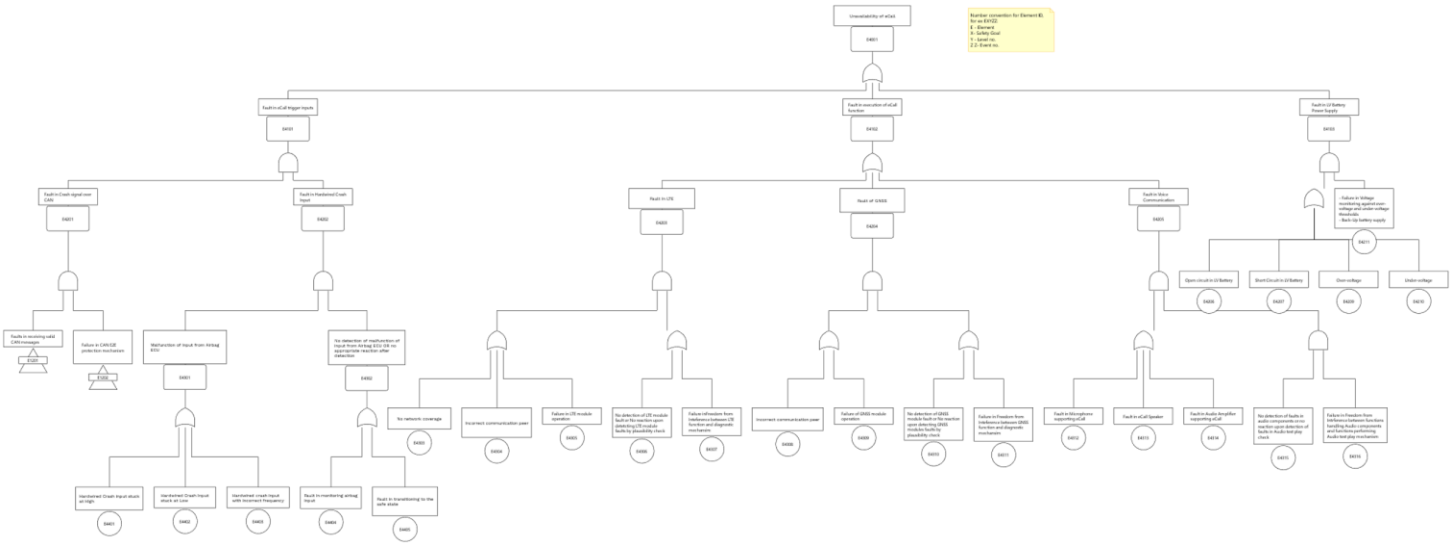


Figure 33 FTA tree diagram – -eCockpit-CSG04

5 Technical Safety Requirements

Technical Safety Requirements are derived and archived in SharePoint.

Document Name and Version: [Ref 04]

6 Assumptions

The identifier for assumptions under technical safety concept and requirements are captured in the below table with suffix ASM_TSC followed by three-digit numbers.

ID	Assumption	Status	Remarks
ASM_TSC_001	The selected primary and secondary controller is assumed to be ASIL B certified and complies to recommendations of ISO 26262:2018 for ASIL B systems.	Valid	
ASM_TSC_002	Memory (HyperFlash/eMMc, DDRAM), MDU power switch, external watchdog, and Voltage supervisor are assumed to be QM as they merely act as passive devices, and no data computation is expected out of those components.	Valid	
ASM_TSC_003	MDU Serializer is assumed to be ASIL B certified and complies to recommendations of ISO 26262:2018 for ASIL B systems	TBC	To be validated in HW phase
ASM_TSC_004	Requirements related to environmental conditions and installation space are already considered by system teams on SYS2 and SYS3 phase of ASPICE methodologies.	TBC	To be validated by systems team
ASM_TSC_005	Testing related to environmental conditions and installation space are assumed to taken into considered in System Testing.	TBC	To be validated by systems team
ASM_TSC_006	The system implements Q&A monitoring algorithm in both primary and secondary controllers to ensure the feasibility of safety mechanism provided in section 2.6.2.1	TBC	To be confirmed by system implementation team
ASM_TSC_007	The secondary controller is capable of	Obsolete	Not mandatory to be implemented

	monitoring audio activity on the speaker out lines (SPK+, SPK-) from IPC audio amplifier through a dedicated feedback mechanism. The monitoring activity is not intended to verify the correctness of the audio played but to detect the audio activity (chimes) triggered by the IPC audio amplifier.		
ASM_TSC_008	Level translators, voltage regulators and passive components used within the system is assumed to be developed in accordance with recommendations of ISO 26262:2018 for ASIL B systems and will meet with the target hardware metrics of a ASIL B system.	Valid	
ASM_TSC_009	It is assumed that safety measures at vehicle level are derived to handle situation or malfunctions that arise out of common cause failure e.g., KL30, KL15 failure in the system.	Valid	
ASM_TSC_010	Requirements on production, operation, service and decommissioning, and Hardware-Software Interface (HSI) specification will be updated and refined by team. Safety Validation will be conducted by appropriate stakeholders identified by and the Safety Validation report will be verified for its conformance to ISO 26262:2018.	Valid	
ASM_TSC_011	The block represented in the safety mechanism section are abstract blocks and does not represent the actual SW modules in the software architectural design. It is assumed that the software architecture team develop in line with system architecture design using tools like Enterprise Architect and allocate the safety mechanisms to the corresponding SW modules as per the software architectural design	Valid	Confirmed based on the discussion with
ASM_TSC_012	For fault recovery, minimum time the fault should have recovered to avoid being intermittent and exit the safe state is assumed to be 2 FDTI duration.	TBC	To be validated by systems team