AN13659

Enabling Automotive Safety Display Based on i.MX RT1170 with Safety MCU S32K

Rev. 0 — 23 June 2022 Application note

Document information

Information	Content
Keywords	AN13659, Functional Safety, Safety Display, i.MX RT1170, S32K
Abstract	The S32K series MCU can work with i.MX RT1170 to implement a safety display and make the system reach ASIL B.

1 Introduction

The i.MX RT1170 is a new processor family featuring NXP's advanced implementation of a high-performance Arm Cortex-M7 Core and a power efficient Arm Cortex-M4 Core. It offers high-performance processing optimized for the low power consumption and real-time response. The i.MX RT1170 has rich video features, including MIPI CSI/DSI, LCD display, graphic accelerator, and camera interface.

The S32K series MCU is AEC-Q100 qualified and combines a scalable family of low-power Arm Cortex-M series-based microcontrollers. It features advanced safety, security, and software support for industrial and automotive ASIL B/D applications in the body, zone control, and electrification. The S32K series MCU can be used to make sure that automotive products work in a safe state when unexpected errors occur.

This document intends to describe how to connect S32K with i.MX RT1170 in an automotive board, including hardware design and software development.

To illustrate this design development process, the following modules of S32K and i.MX RT1170 are involved:

- Controller Area Network (CAN)
- Universal Asynchronous Receiver/Transmitter (UART)
- Serial Peripheral Interface (SPI)
- MIPI DSI Host Controller (MIPI_DSI)
- Display Content Integrity Checker (DCIC)

2 Overview

Automotive Safety Integrity Level (ASIL) is an important concept in automotive functional safety standard ISO 26262. Four ASILs are defined: ASIL A, ASIL B, ASIL C, and ASIL D, where ASIL A is the lowest safety integrity. In addition to these four ASILs, the class QM (quality management) denotes no requirement to comply with ISO 26262, whose safety level is even lower than ASIL A.

The i.MX RT1170's rich multimedia features and high performance make it ideal for multimedia applications in automotive. Under increasingly strict functional safety requirements in the automotive field, the multimedia elements in automotive, such as display and audio, must prompt the driver with critical safety information, which should achieve ASIL B according to ISO 26262.

As QM devices, i.MX RT1170 cannot independently make the whole system reach ASIL B. To achieve this, an external MCU that is an ASIL B device is necessary. According to ISO26262-9:2018, ASIL decomposition is only allowed if the elements implementing the decomposed requirements are sufficiently independent. Figure 1 shows that ASIL decomposition can be applied to make a system consisting of ASIL B components and QM components, ASIL B(B) + QM(B), to reach ASIL B. From the perspective of effectiveness and compatibility, S32 series MCUs are highly recommended as an ASIL B(B) component in such a system.

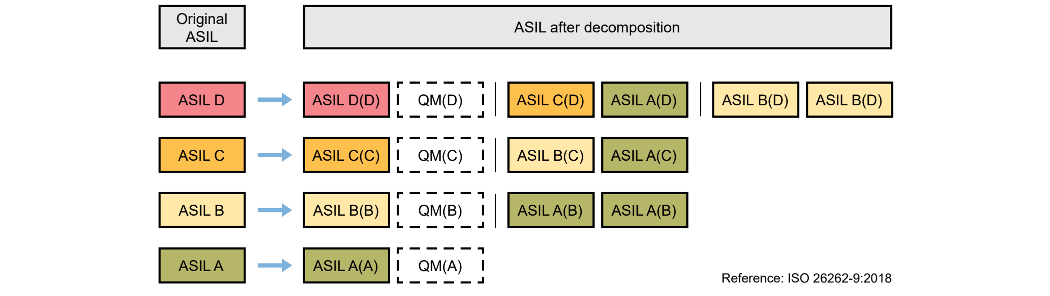


Figure 1. Example of ASIL decomposition

A platform can be designed based on RT1170 and S32K to build safety multimedia concept. The platform can offer a solid foundation to enable HUD, small cluster, HMI, entry-level DMS, and voice command designs. It can integrate rich automotive display/camera interfaces to meet automotive application needs. The added ASIL B MCU S32K and PMIC can help build a functional safety concept and level up its functional safety integrity from system perspective. Safety display is a proper example of automotive multimedia applications with functional safety. S32K118 is for the ASIL B(B) part, which is responsible for processing safety critical information. Whereas i.MX RT1176 is for the QM(B) part, mainly to perform multimedia functions.

For more detailed technical information on S32 and safety-related development, access the links available in Table 1.

Table 1. S32 and safety related links

Reference Link	Description
S32 Automotive Platform	S32 MCUs and MPUs for automotive and industrial applications provide an architecture that balances performance and power efficiency.
S32K Series MCU	It is the homepage of S32K automotive MCUs.
S32K1 Microcontrollers for General Purpose	The S32K1 MCUs of 32-bit AEC-Q100 qualified MCUs combine a scalable family of Arm Cortex-M-based microcontrollers.
S32K1 Software and Tool	It consists of documentation for S32K1.
NXP SafeAssure Product Catalog	The page lists the functional safety automotive applications. The work products (including safety manual, FMEDA, analysis report, assessment/confirmation measurement report, and PPAP) can be provided under NDA.
SafeAssure Community	
Safety Software Framework (SAF)	SAF comprises a set of software components that establish the safety foundations for automotive applications on S32 platform devices with ISO26262 compliance. It provides detection and reaction mechanisms for latent faults and single-point faults.
Safety by Software (SbSW)	Safety by Software (SBSW) is a new way of achieving ASIL D with high-level measures, supported by NXP S32X hardware. The SBSW hardware module and SBSW firmware check the user application flow, compare results of main and redundant algorithms, and detect faulty behavior with high degree of independence.

Table 1. S32 and safety related links*...continued*

Reference Link	Description
AUTOSAR	AUTOSAR addresses the challenge of rising code complexity by providing open automotive software architecture. This architecture supports the development of standardized electronic systems that improve quality, performance, safety, and environmental friendliness. It also helps to simplify the process of updating software over the lifetime of a vehicle.
Real-Time Drivers (RTD)	Real-Time Drivers (RTD) are new and innovative drivers set. They support real-time software on AUTOSAR and non-AUTOSAR applications targeting Arm Cortex-M cores and ISO 26262 compliance for all software layers, providing full IP and features.

3 Assumed hazard analysis and safety goal

To illustrate the concept of safety display, take an example of simple safety analysis.

Safety Hazard: The image presented on display may not be aligned with what is expected by S32K. The mismatch of instrument information may cause the driver to make misplaced judgments, resulting in traffic accidents.

Safety Goal: The image presented on display should be aligned with what is expected by S32K.

Safety Mechanism: To make sure that the content on display is aligned with the expected, check the Cyclic Redundancy Check (CRC) value of each frame on display. Figure 2 shows the safety display concept of the platform. The detailed hardware and software design of the platform is introduced in the below sections.

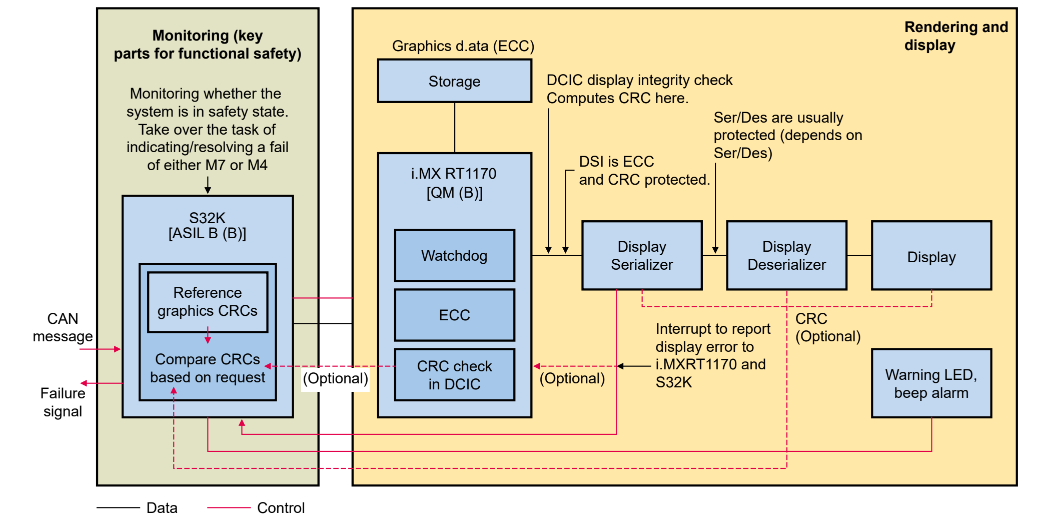


Figure 2. S32K + i.MX RT1170 safety display architecture

The Fault Tolerant Time Interval (FTTI) at vehicle level is a crucial concept and is presented in Figure 3. The integrated functional safety application should be able to bring the system into a safe state before potential hazardous events happen.

To make the system transition to a safe state within the FTTI after a fault occurrence, some operations should be done according to certain use-cases. These operations include resetting related modules in i.MX RT1170 or notifying the driver with a warning LED or beep alarm.

It is assumed that S32K FHTI (FDTI + FRTI) is shorter than the expected FTTI. The FTTI can be set to a fixed value, for example, 350 ms.

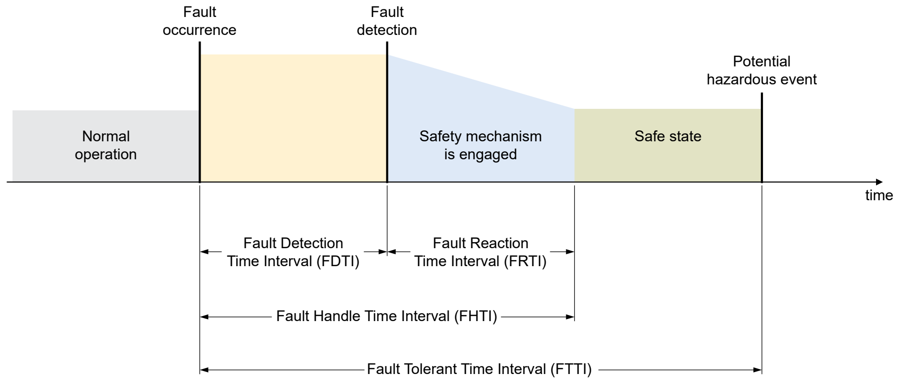


Figure 3. Fault tolerant time interval

4 Hardware design consideration

This chapter discusses hardware design in detail. Based on it, the safety display feature can be enabled.

4.1 Functional safety block diagram

Figure 4 shows the functional safety block diagram based on ASIL-B MCU S32K118.

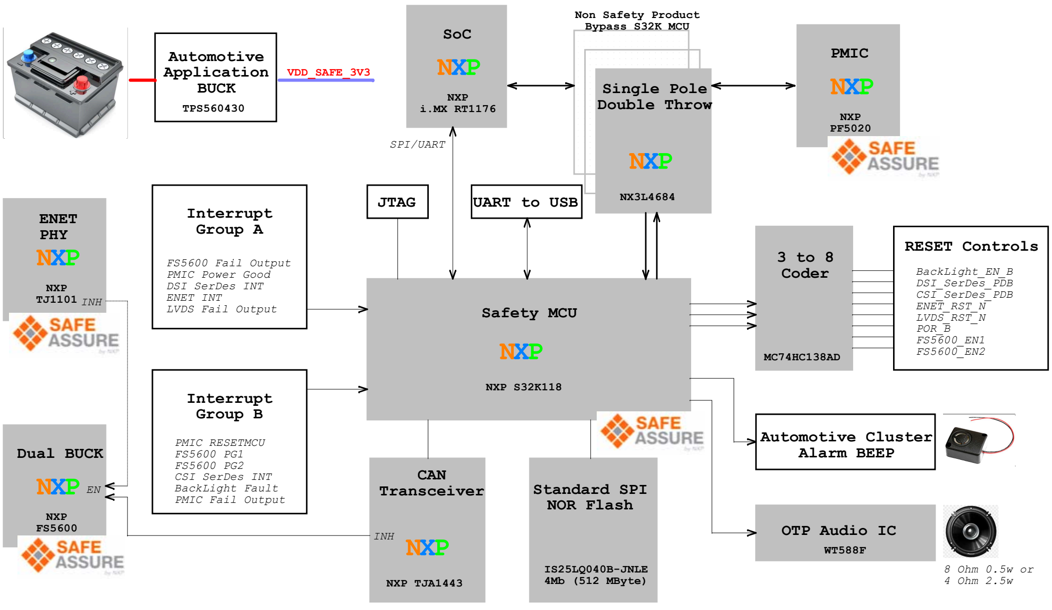


Figure 4. Functional safety block diagram based on ASIL-B MCU S32K118

4.2 Power domain isolation

In a safety MCU domain, a dedicated BUCK converter, for example TPS560430, is used for the core and I/O supply. The power input of the BUCK converter is a 12 V supply so that the safety parts work under an isolated power domain compared with i.MX RT1170 (supplied by the PMIC PF5020).

4.3 Functional safety requirements

Figure 5 shows that safety MCU S32K is used for monitoring different fail/fault outputs from peripherals and interrupt sources.

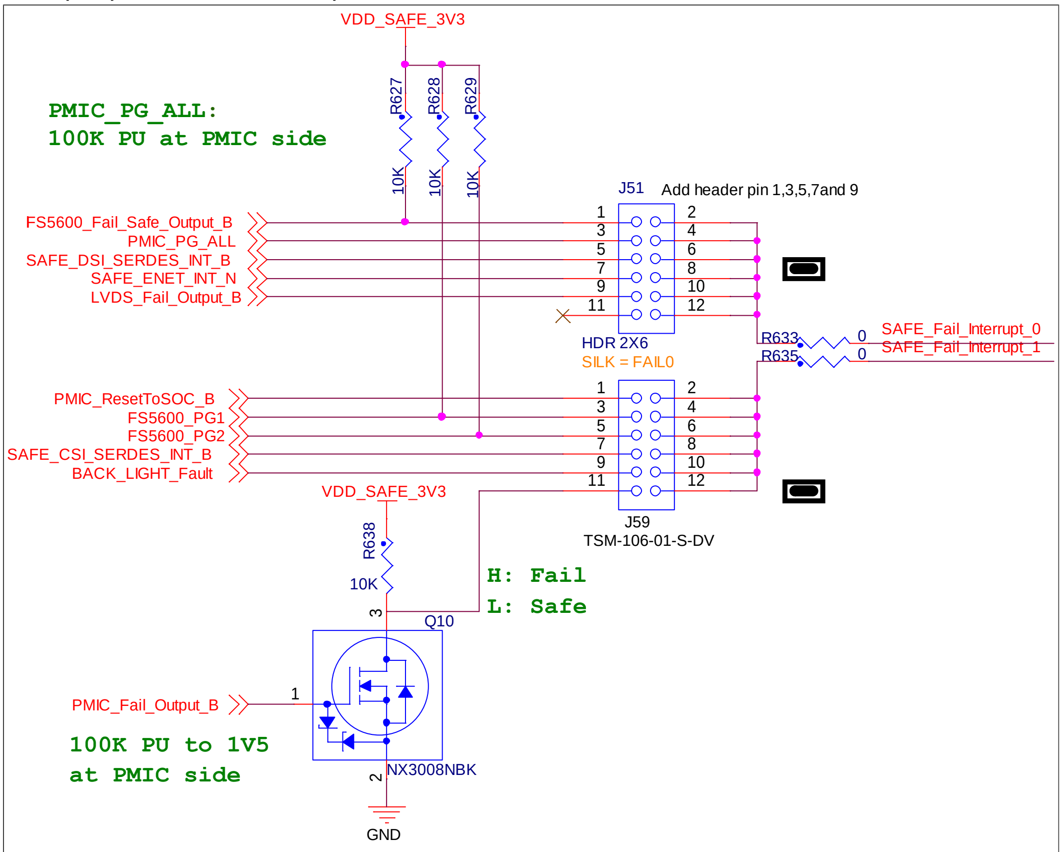


Figure 5. Fail and fault interrupts to MCU

Figure 6 shows that S32K is used for receiving different information of vehicle ECUs or sensors through CAN bus.

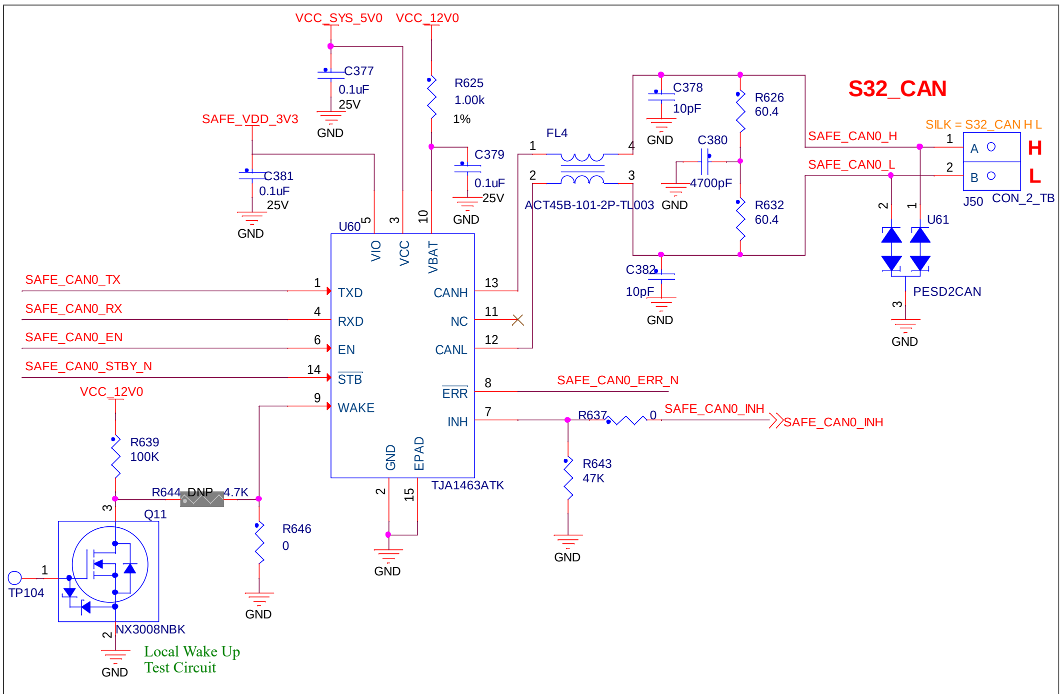


Figure 6. Dedicated CAN transceiver in MCU domain

Figure 7 shows that S32K drives the redundant alarm and warning LED after receiving fail/fault interrupt signals.

In addition, UART or SPI should be connected between S32K and i.MX RT1170.

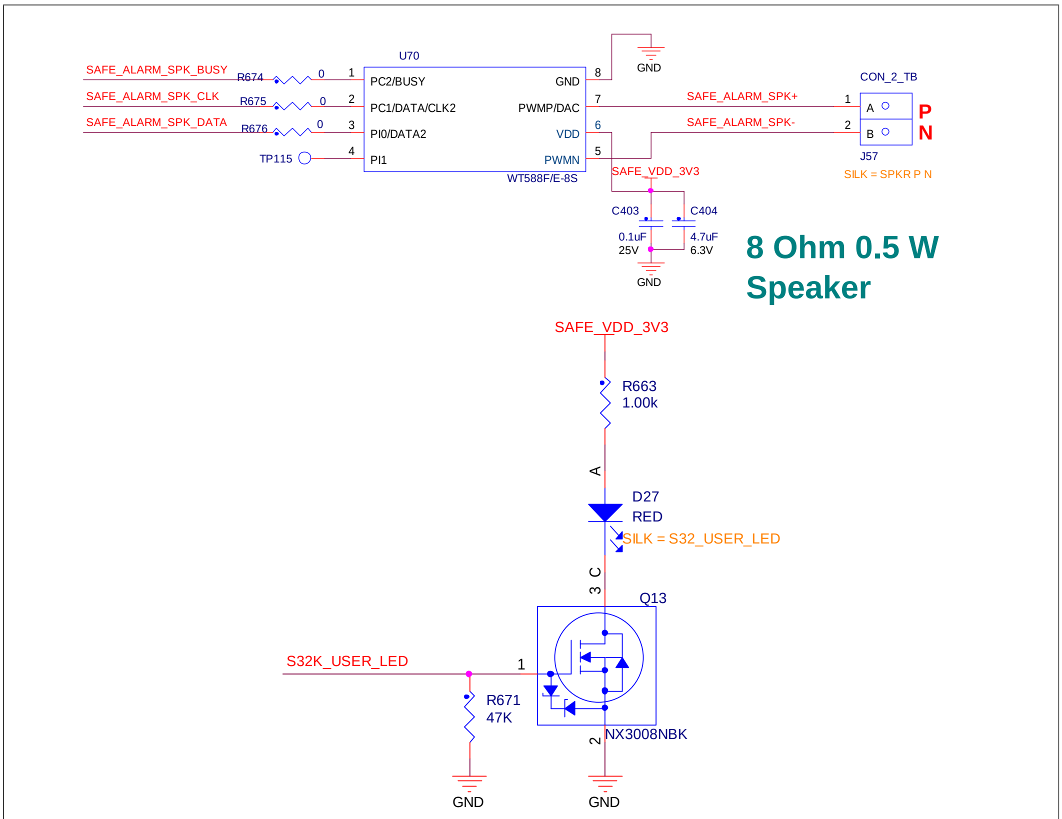
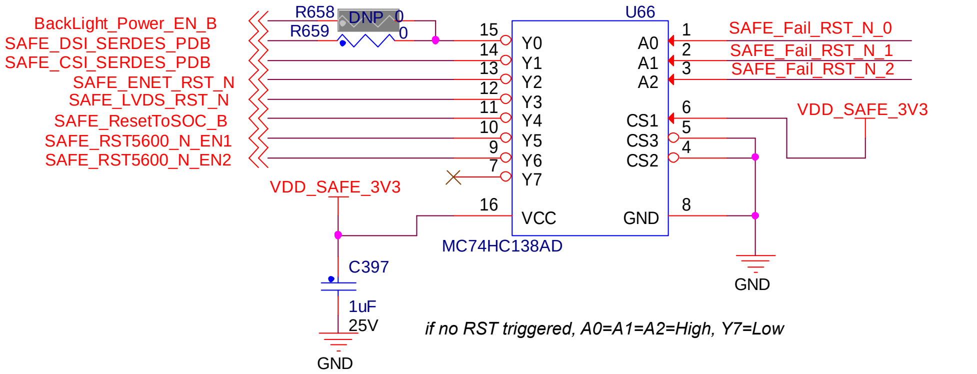


Figure 7. Redundant alarm speaker

Figure 8 shows the design of reset signal pins (reset pins of different modules, for example, backlight, DSI SerDes, and LVDS). Here, S32K is in charge of the failed peripheral's reset controls, such as displays, system power, and so on.

Figure 8. Reset signals from MCU to failed peripherals

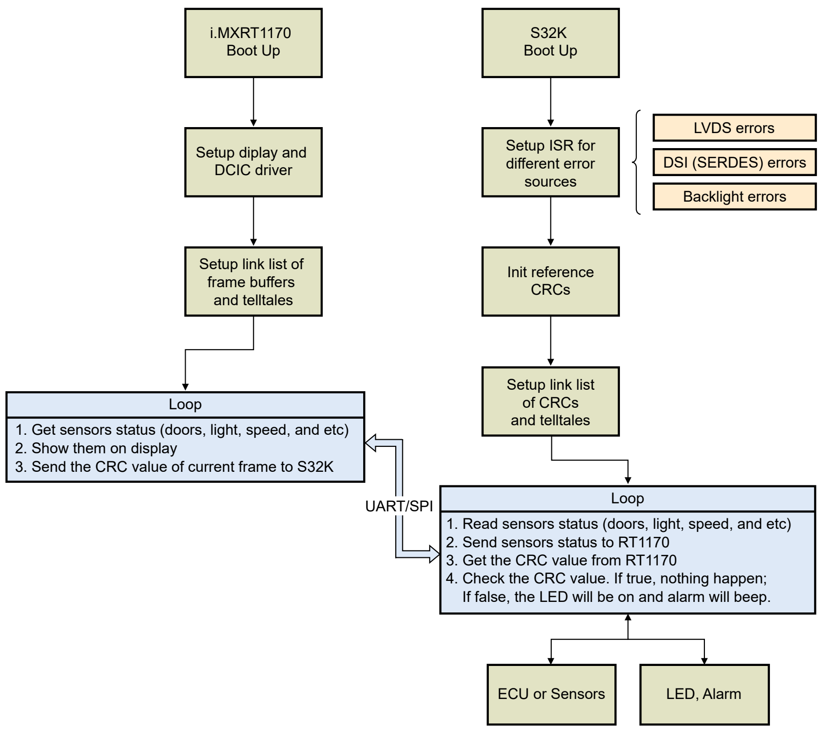


5 Software enablement

This chapter discusses communication as a key step in enabling safety display.

5.1 Workflow

Figure 9. Software flowchart of safety display



The above flowchart in Figure 9 describes the behavior of i.MX RT1170 and S32K after power-on. In addition to the initialization and configuration process, its main modules are two loop bodies. The two loop bodies are the key processing procedures of safety display. S32K informs i.MX RT1170 to display the desired content, which is related to the status information of the ECUs or sensors received by the CAN. i.MX RT1170 parses and displays the content. At the same time, DCIC completes the calculation of the CRC value of the current frame. No faults are detected when the CRC values received by the S32K match the references, while a fault is detected when the CRC values do not match. The S32K then initiates the transition to a safe state.

5.2 S32K118

Before completing the safety display function, S32K must create a list of different CRC values corresponding to different display contents. Table 2 shows a list of such CRC items.

Table 2. Example of CRC items

Index	Icon	Status	CRC32
0	Left turn light	ON	
1	Left turn light	OFF	
2	Right turn light	ON	
3	Right turn light	OFF	
4	High beam	ON	
5	High beam	OFF	
6	Seat belt	Fastened	
7	Seat belt	Not Fastened	
……	……	……	……
20	Speed	0 km/h	
21	Speed	1 km/h	
22	Speed	2 km/h	
23	Speed	3 km/h	
……	……	……	……
219	Speed	200 km/h	
……	……	……	……

S32K obtains the status of sensors and ECUs through CAN bus, then converts this information into multiple bytes and sends it to i.MX RT1170 through SPI or UART. Then i.MX RT1170 decodes the content and displays them as expected. For the two communication methods here, the corresponding diagnostic mechanism should be added to ensure the safety of the system. For example, for CAN communication, alive counters or CRC8 can be applied to ensure the correctness of data. The communication timeout should be considered for both CAN and SPI/UART because the system should not apply the last valid data to the real-time systems. When discussing timeout, it can be set to frame refresh interval. According to ISO26262-5: Annex D.6, frame counter and timeout monitoring can be taken as a safety mechanism or measure of communication bus timeout. Refer Table 3 for more information.

Table 3. Communication bus (serial, parallel)

Safety mechanism/ measure	See overview of techniques (See the following section in ISO 26262-5-2018)	Typical diagnostic coverage considered achievable	Notes
One-bit hardware redundancy	D.2.5.1	Low	
Multi-bit hardware redundancy	D.2.5.2	Medium	

Table 3. Communication bus (serial, parallel)*...continued*

Safety mechanism/ measure	See overview of techniques (See the following section in ISO 26262-5-2018)	Typical diagnostic coverage considered achievable	Notes
Read back of sent message	D.2.5.9	Medium	
Complete hardware redundancy	D.2.5.3	High	Common mode failures can reduce diagnostic coverage
Inspection using test patterns	D.2.5.4	High	
Transmission redundancy	D.2.5.5	Medium	Depends on type of redundancy. Effective only against transient faults
Information redundancy	D.2.5.6	Medium	Depends on type of redundancy
Frame counter	D.2.5.7	Medium	
Timeout monitoring	D.2.5.8	Medium	
Combination of information redundancy, frame counter, and timeout monitoring	D.2.5.6, D.2.5.7 and D.2.5.8	High	For systems without hardware redundancy or test patterns, high coverage can be claimed for the combination of these safety mechanisms

Note: *i.MX RT1170 only supports CRC32 calculation of 16 Regions. So the number of elements that DCIC must monitor should not exceed 16.*

Table 4 shows an example of different tell-tales that is displayed.

Table 4. Example of display content control

Name	Field	Description
......	......	......
Power	18:11	Remaining mileage
Speed	10:4	Current Speed (km/h)
Seat belt	3	1 - Not Fastened 0 - Fastened
High beam	2	1 - ON 0 - OFF
Right turn light	1	1 - ON 0 - OFF
Left turn light	0	1 - ON 0 - OFF

In addition to the safety display, the S32K also reserves several pins for detecting other peripheral interrupts to respond accordingly. For example, Table 5 lists two sets of interrupt definitions for a reference platform and reset control module described in the hardware design consideration chapter. They can be used for implementing safety mechanisms.

Table 5. Peripheral interrupts to S32K

Group A (PTB3_GPIO: SAFE_Fail_Interrupt_0)	Group B (PTB3_GPIO: SAFE_Fail_Interrupt_1)
FS5600_FAIL_SAFE_OUTPUT_B	PF5020_PMIC_RESET_SOC_B
PF5020_PMIC_PG_ALL	FS5600_PG1
SAFE_DSI_SERDES_INT_B	FS5600_PG2
SAFE_ENET_INT_N	SAFE_CSI_SERDES_INT_B
LVDS_FAIL_OUTPUT_B	BACK_LIGHT_FAULT
	PF5020_PMIC_FAIL_OUTPUT_B

5.3 i.MX RT1170

Interrupts such as LVDS fault, DSI serializer fault, DSI de-serializer fault, and backlight errors are directly generated from the peripheral. Therefore less work should be done on i.MX RT1170 side. This chapter focuses on the display modules of i.MX RT1170.

Figure 10. High-level integration block diagram of display and camera

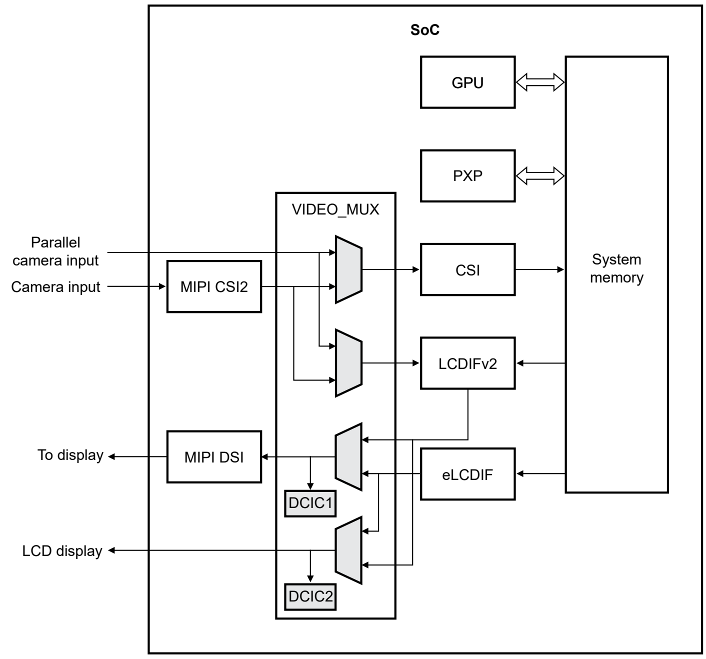


Figure 10 shows that i.MX RT1170 implements a Display Content Integrity Checker (DCIC), which can be a part of the safety mechanism. The DCIC verifies whether safety-critical information sent to a display has been corrupted. This type of verification is required in some safety-sensitive systems, like the warning icons in a vehicle cluster, and includes compliance with the ASIL B specification.

There are two DCICs in i.MX RT1170. DCIC1 is for MIPI_DSI and DCIC2 is for parallel display output. The DCIC1 processes the signals from internal DSI bus. While DCIC2 processes the signals from pads of SoC, the input and output path of display pins should be enabled when DCIC2 is enabled.

Each DCIC can check up to 16 regions with static content. The expected data signatures of these regions must be calculated with CRC32 polynomial and written to DCIC_DCICRRS. When the check flow runs, the module compares DCIC_DCICRCS and DCIC_DCICRRS. If they are different, the error interrupt status is set.

The DCIC provides an additional mismatch indication for the external controller besides the interrupts to the SoC core. The EXT_DCIC signal, if enabled DCIC_DCICIC[EXT_SIG_EN], continuously oscillates at a rate that is an integer division of the main clock (hsp_clk). For more information about DCIC, refer to *i.MX RT1170 Processor Reference Manual* (IMXRT1170RM).

Our safety display hardware and software architecture are expected to use the calculated CRC value, shown in Table 6, rather than error interrupt or oscillated clock because i.MX RT1170 is a QM device.

Table 6. DCICx_DCICRCSn field descriptions

Field	Description
CALCULATED_SIGNATURE	32-bit actual signature (CRC calculation result) for the ROI during the last frame. Updated automatically at the beginning of a next frame.

Take the seat belt icon as an example here. Figure 11 shows an image that displays when the seat belt is not fastened without DCIC CRC errors.

Figure 11. Seat belt is not fastened without DCIC CRC errors

Figure 12 shows an image that displays if the belt is fastened without DCIC CRC errors.

Figure 12. Seat belt is fastened without DCIC CRC errors

Figure 13 shows an image that displays an abnormal icon when the seat belt is fastened.

Figure 13. Seat belt is fastened but an abnormal icon is displayed

6 i.MX RT1170 + S32K Demo

The i.MX RT1170 and S32K demos may be developed in different IDEs. For example, the i.MX RT1170 demo may use IAR Embedded Workbench (IAR EW) for Arm, while the S32K demo may use S32 Design Studio for Arm.

6.1 Run seat belt functional safety demo

Here is a reference platform based on i.MX RT1170 + S32K. After downloading the images into the platform, safety display demo simulates three different cases, as shown in Table 7.

Table 7. Example of different cases of safety display for safety belt

Different scenarios	Safety belt status	Safety belt icon	DCIC CRC check	LED (S32K)	Alarm (S32K)
Case 1	Not fastened	On	Correct	Off	Off

Table 7. Example of different cases of safety display for safety belt...*continued*

Different scenarios	Safety belt status	Safety belt icon	DCIC CRC check	LED (S32K)	Alarm (S32K)
Case 2	Fastened	Off	Correct	Off	Off
Case 3	Fastened	Abnormal	Wrong	On	On

Figure 14, Figure 15, and Figure 16 show different cases of safety displays for the safety belt.

Figure 14. Case 1 - Safety belt is not fastened and the safety belt icon is on

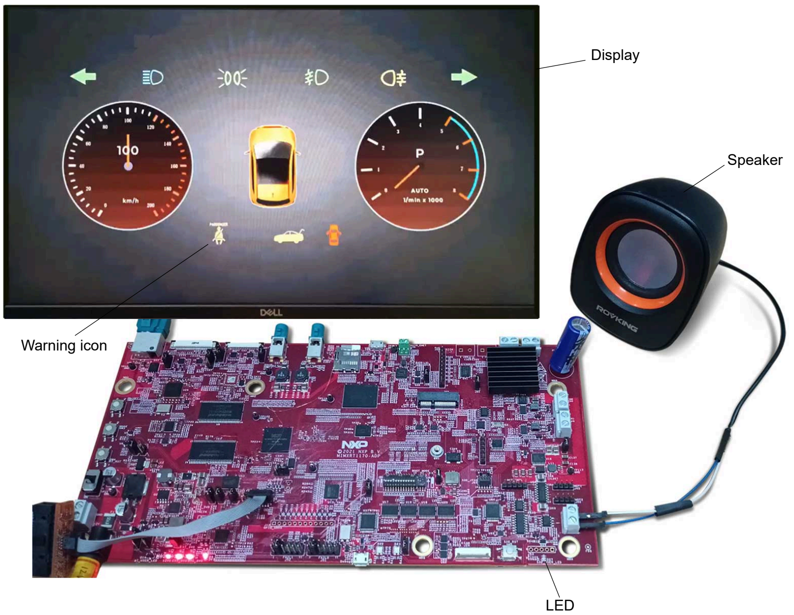


Figure 15. Case 2 - Safety belt is fastened and the safety belt icon is off

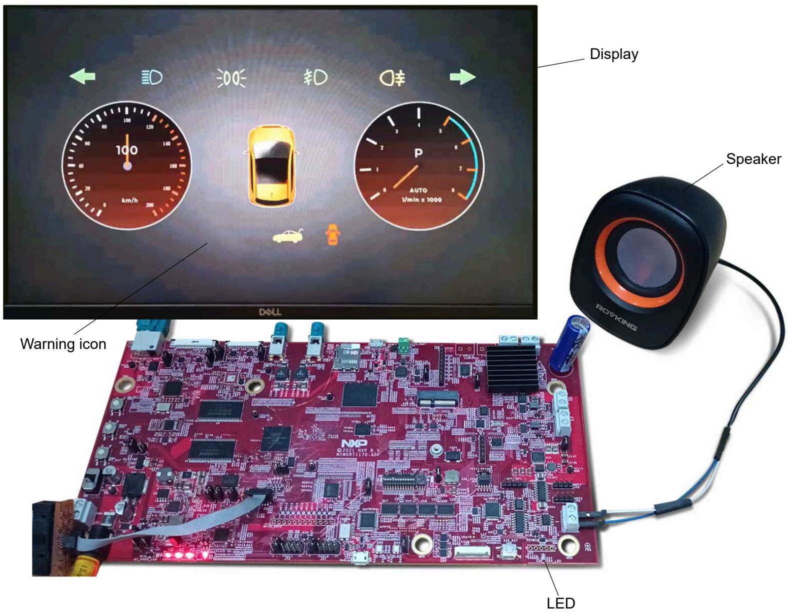
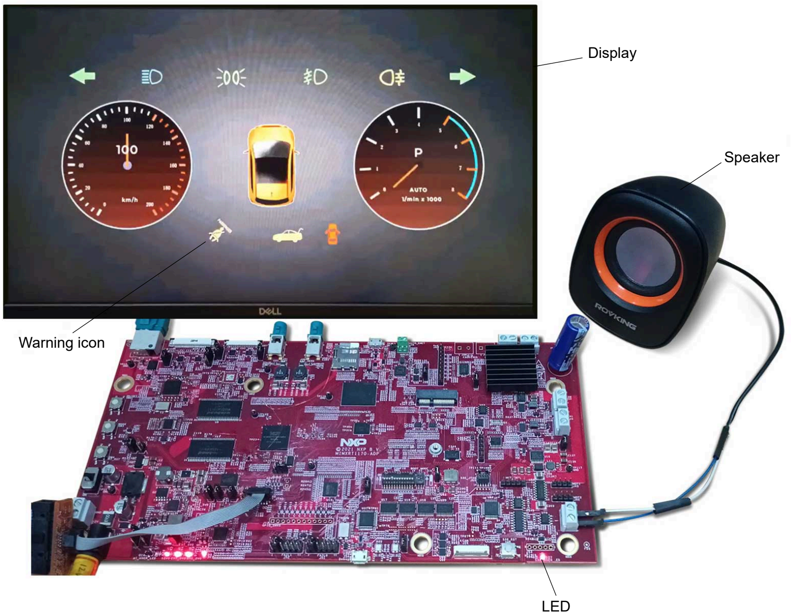


Figure 16. Case 3 - Safety belt is fastened and the safety belt icon is abnormally displayed



7 References

- *i.MX RT1170 Processor Reference Manual* (document IMXRT1170RM)
- *S32K1xx Series Reference Manual* (document S32K-RM)

8 Revision history

Revision history

Revision number	Date	Substantive changes
0	23 June 2022	Initial release

9 Legal information

9.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

9.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

9.3 Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Contents

Date of release: 23 June 2022
Document identifier: AN13659