S32 Safety Software Framework

Product Brief

1.0 Software ProductOverview

The S32 Safety Software Framework (SAF) is a software product containing software components for establishing the safety foundation for customer's safety applications compliant with ISO 26262 functional safety. It allows integration up to ASIL D automotive safety integrity level. It is developed as Safety Element out of Context (SEooC). The S32 Safety Software Framework is designed to be integrable within AUTOSAR® and non - AUTOSAR applications. It is a software product covering all NXP S32 Automotive Platform devices (see Figure 1, S32K in a separate package).

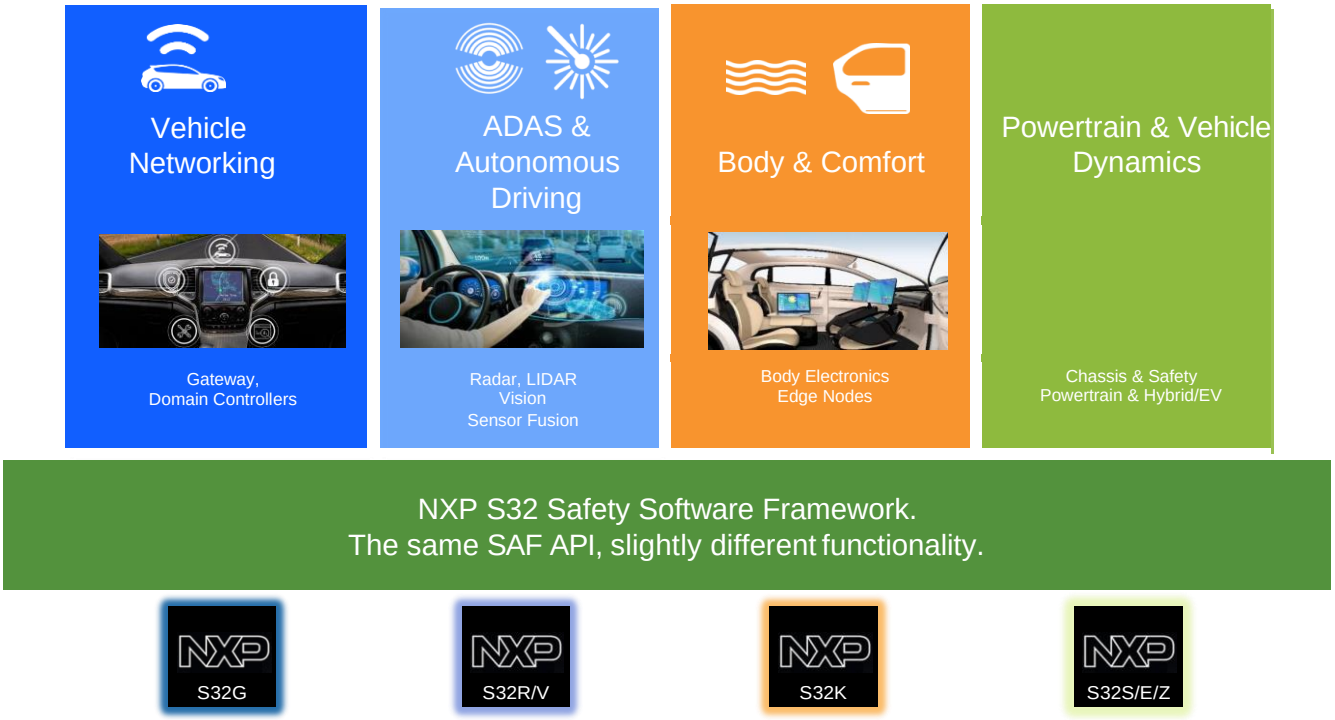
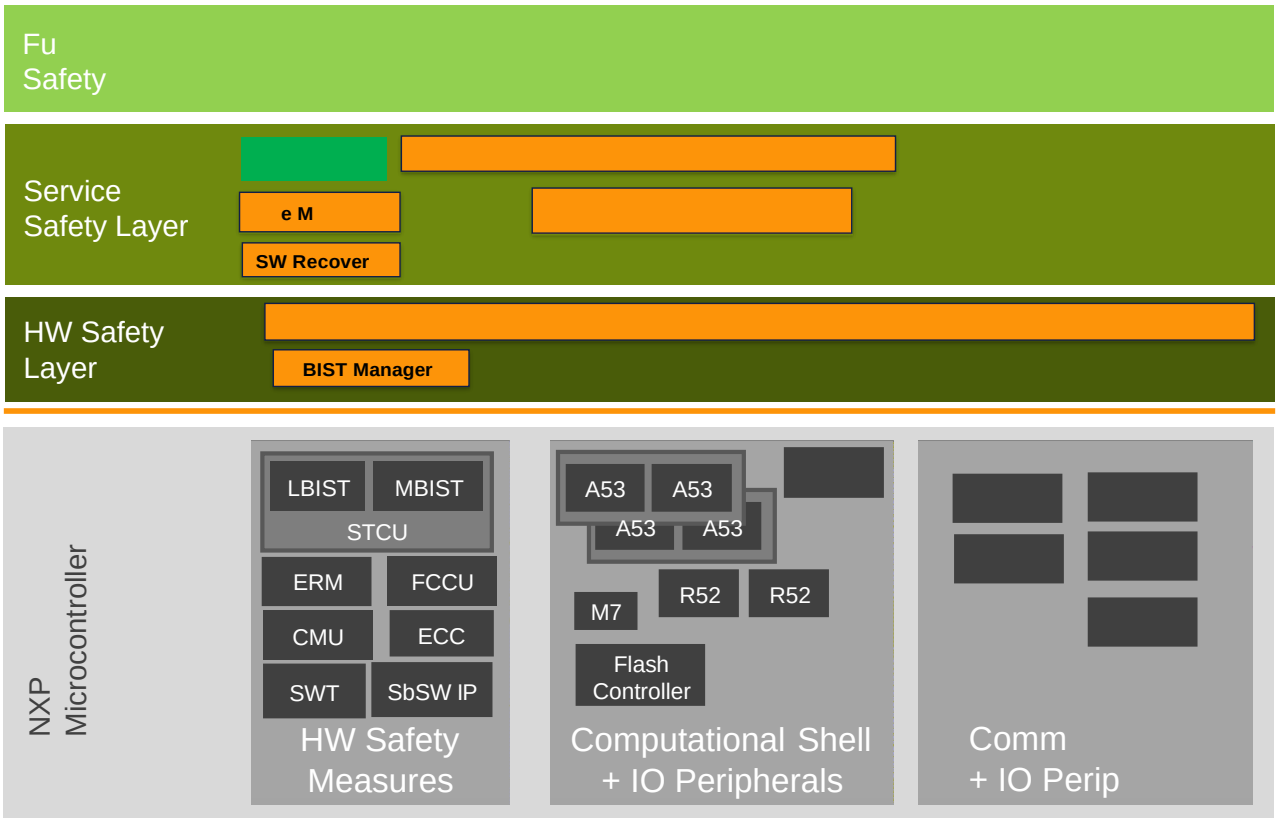


Figure 1. NXP's S32 Safety Software Framework supporting all NXP S32 devices

The S32 Safety Software Framework provides the software modules from Hardware and Service safety layers as shown in Figure 2. The Software modules provided are:

- **BIST Manager** - Built in Self-Test Manager covering both LBIST (Logic BIST) and MBIST (Memory BIST)
- **eMCEM** – extended Microcontroller Error Manager
- **Mode Selector** – Mode Selector (including Safety Config)
- **sBoot** – Safety Boot
- **SquareCheck** – Square Check (Check the Checkers)
- **SW Recovery** – Software Recovery



*** SbSW – Safety by SW**

Figure 2. NXP's S32 Safety Software Framework content

Note: The users who will develop their own safety solution can use the S32 Safety Peripheral Drivers (SPD) product containing the BIST Manager and eMCEM. It complements the S32 Real Time Drivers product to provide software support for the on-chip peripheral modules.

The S32 Safety Software Framework components are involved during boot, runtime, and fault recovery. The components involvement is depicted in Figure 3. The components exchange data to execute the right measures and responses at the given application state.

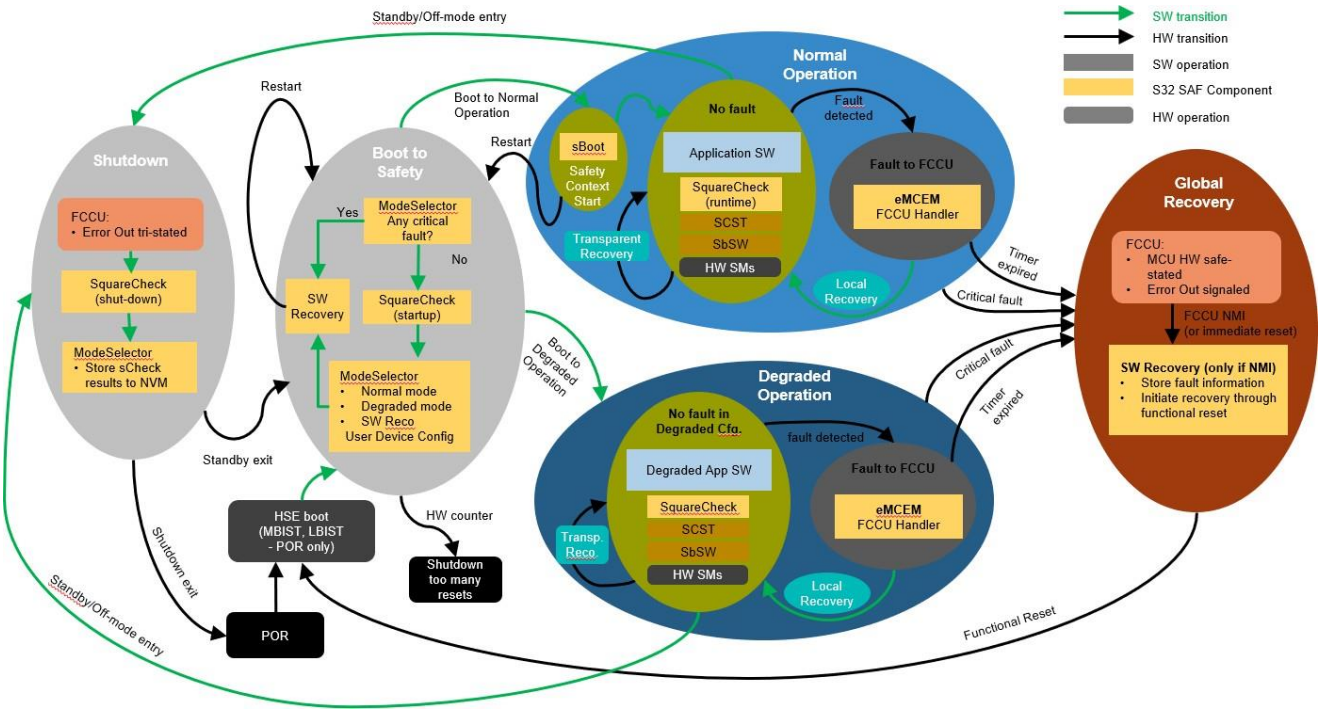


Figure 3. S32 Safety Software Framework operation diagram

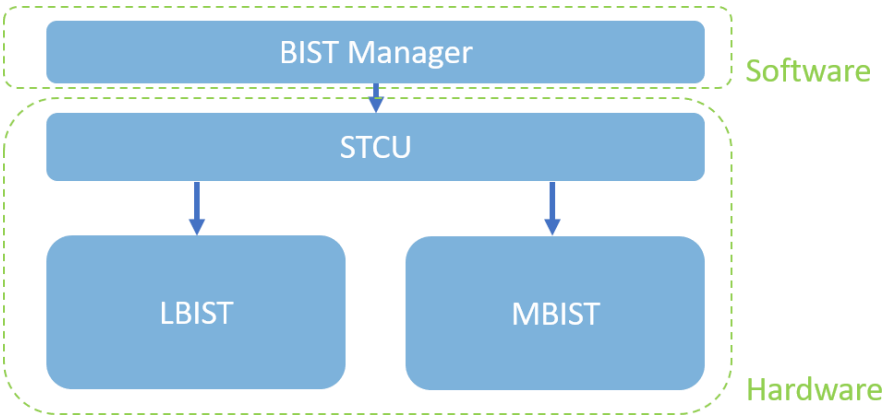
2.0 Software Content

The S32 Safety Software Framework is essential in supporting applications on S32 Automotive Platform devices to achieve safety. The main features of the S32 Safety Software Framework are as follows:

- Checking the hardware safety mechanisms, i.e., latent fault detection
- BIST management and deployment to provide high availability
- Enabling booting into either normal or degraded modes
- Ensuring the device is correctly setup to be able to start safety function
- Handling and reaction to detected faults
- Support for local and global recovery strategies
- Compliance with ISO 26262

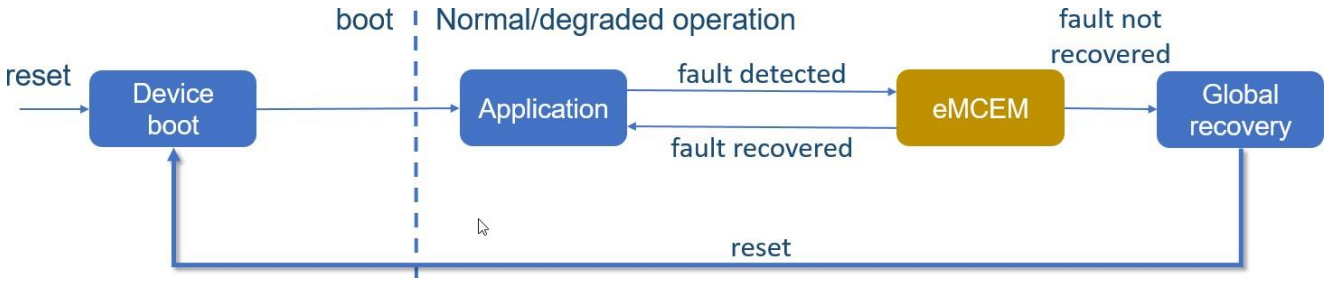
BIST Manager (Built in Self Test Manager)

- A driver for MBIST and LBIST HW modules
- Analyzes the results provided by LBIST and MBIST HW and initiates their execution



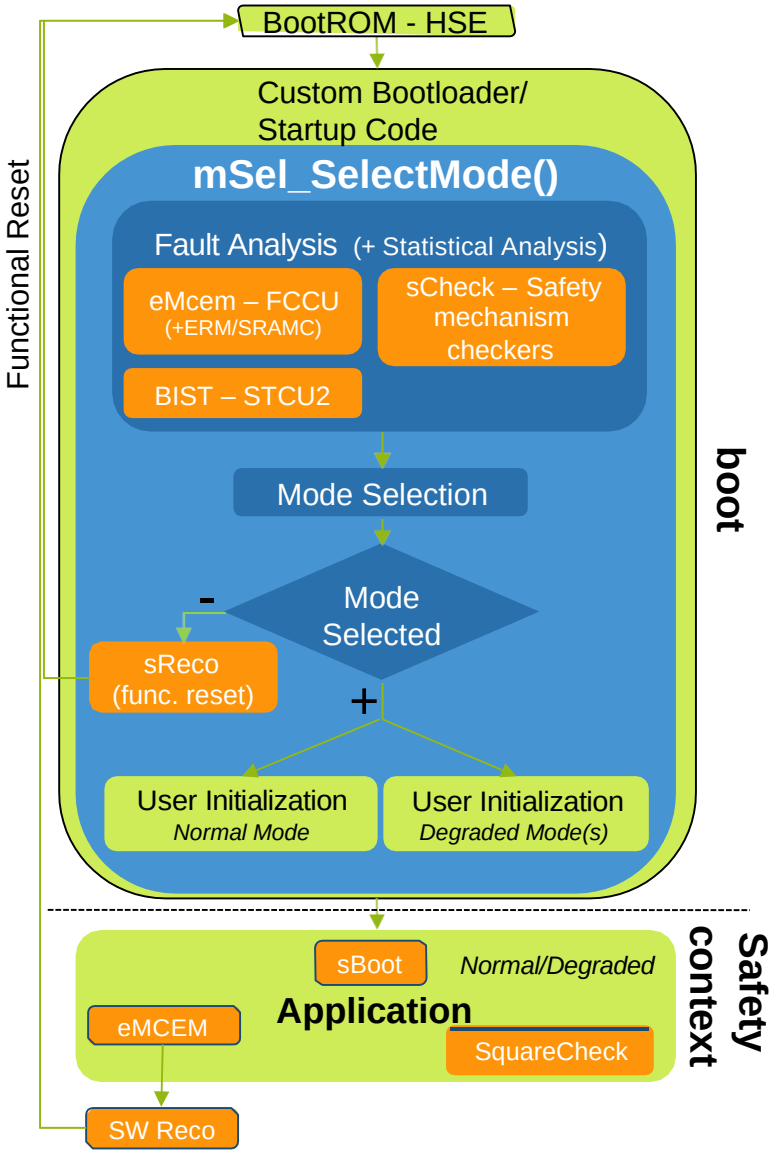
eMCEM (Extended Microcontroller Error Manager)

- Fault management of the microcontroller
- Configuration of fault reactions (reset, alarm IRQ, NMI, no reaction)
- Sophisticated error handling mechanism
- Allows to register an individual alarm handler for each FCCU fault
- Redirection of fault reaction if the respective safety mechanism is tested by SquareCheck
- Fault status reporting and fault clearing
- Error injection
- Memory error reporting



ModeSelector (Mode Selector)

- A SW component used for selecting the application normal mode or degraded mode
- Degraded modes increase device availability by enabling a usage of the device under the presence of non-critical permanent faults
- The selection is based on FCCU results, SquareCheck results, optionally MBIST/LBIST results, and diagnostic information stored by SW Recovery.
- There is also a possibility to call SW Recovery followed by Functional Reset in the cases of no operating mode can be selected
- Executed during the boot (startup) phase when the system is in a safe state
- Configuration of HW resource regions and association to the fault sources needed for the selectable modes

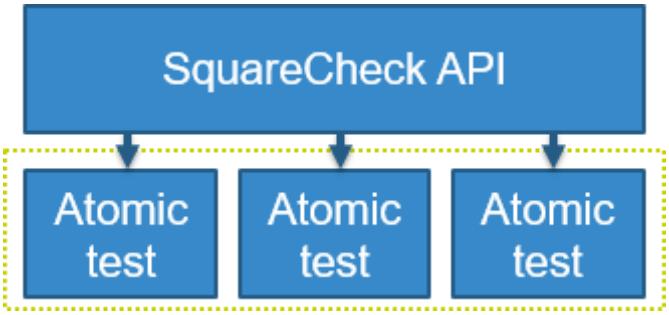


sBoot (safe Boot)

- A SW component checking whether the device booted to a safe configuration
- Executed at the beginning of the application execution before the safety context is established
- Verifies that the device configuration meets the hardware safety manual (SM) assumptions

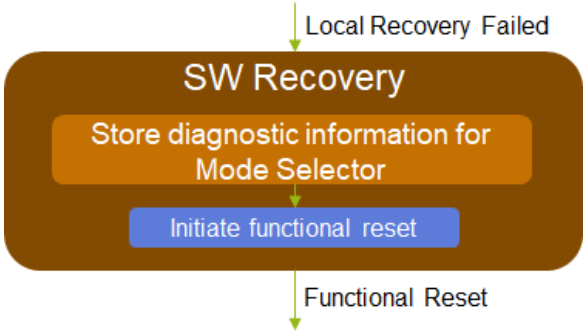
SquareCheck

- A SW component used for latent fault detection
  - Detects faults in the hardware safety mechanisms
- Provides start-up, runtime and shut-down APIs
- Provides required Diagnostic Coverage as per ISO 26262 up to ASIL D



SW Recovery (Software Recovery)

- A SW component used for global recovery
- Called either in the case the MCU needs to recover from a fault that could not be handled by a local recovery or in the case Mode Selector can't select any operational mode
- Store diagnostic information for Mode Selector
- Executed when MCU is in a safe state



3.0 Supported Targets

The S32 Safety Software Framework described in this product brief is intended to be used with NXP Semiconductors S32G2 devices.

4.0 Quality, Standards Compliance and Testing Approach

The S32 Safety Software Framework software product is developed according to NXP Software Development Processes that is ISO 26262, Automotive-SPICE, IATF 16949 and ISO 9001 compliant.