S32 Safety Software Framework (SAF) and Safety Peripheral Drivers (SPD)

SAF

Last Updated: Jun 7, 2024

The S32 Safety Software Framework (SAF) contains software components to establish the foundation for customer’s safety applications in compliance with ISO 26262 functional safety standard. Safety Peripheral Drivers (SPD) is part of the standard software bundle.

SAF provides complete software safety mechanisms coverage of S32 processors hardware safety mechanisms. SAF is developed as Safety Element out of Context (SEooC) and allows the integration up to ASIL D. SAF can also be used within AUTOSAR™ and non-AUTOSAR applications.

Safety packages contain software components safety analysis and safety manual which are available in the SafeAssure NDA Community.
S32 Safety Software Framework (SAF) and Safety Peripheral Drivers (SPD) Block Diagram

**SAF**
- SquareCheck
- sBoot
- SW Recovery
- ModeSelector
- BIST Manager
- eMCEM
  - SW API
- HW IP
  - FCCU
  - ERM
  - EIM

**SAF_EVAL**
- Reduced SquareCheck
- Reduced sBoot
- Reduced SW Recovery
- Reduced ModeSelector
- BIST Manager
- eMCEM
  - SW API
- HW IP
  - FCCU
  - ERM
  - EIM

**SPD**
- BIST Manager
- eMCEM
  - SW API
- HW IP
  - FCCU
  - ERM
  - EIM

---

S32 Safety Software Framework Block Diagram Block Diagram

- **Shutdown**
  - FCU
  - Error Out tri-stated
  - SquareCheck
  - (shut-down)
  - ModeSelector
  - Stores Check results and Statistical Buffer data to NVM

- **Boot to Safety**
  - Execute SquareCheck Start up Tests and Bist
  - Analyze eMCEM (Statistical Analysis): SquareCheck and Bist Faults
  - ModeSelector
  - + Normal mode
  - + Degraded mode
  - + SW Reco
  - User Device Config

- **Normal Operation**
  - No Fault
  - Application SW
  - SquareCheck (runtime)
  - eMCEM
  - FCCU Handler
  - HW SMs

- **Degraded Operation**
  - No Fault in Degraded Cfg.
  - Degraded App SW
  - SquareCheck
  - eMCEM
  - FCCU Handler
  - HW SMs

- **Local Recovery**
  - Transparent Recovery
  - Fault to FCCU
  - SW Recovery (only if NMI)
  - • Store fault information
  - • Initiate recovery through functional reset

- **Degraded Recovery**
  - FCU
  - MCU HW safe-stated
  - Error Out signaled

- **Standby/Off-mode entry**
  - Transient
  - Recovery
  - Boot to Normal Operation

- **Standby/Off-mode exit**
  - Exit
  - POR
  - HSE Boot
  - Standby Off-mode

- **Transmit**
  - HW Counter

- **Functional Reset**
  - Restart
  - Reset/Standby exit
  - Exit

- **SW Operation**
  - **HW Operation**
  - S32K3 SAF Component

---

* Structural Core Self-Test (SCST) provided via separate installation packages
** Degraded mode available in software
View additional information for **S32 Safety Software Framework (SAF) and Safety Peripheral Drivers (SPD)**.

**Note:** The information on this document is subject to change without notice.