S32 Safety Software Framework (SAF)


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 Software Framework (SAF) and Safety Peripheral Driver (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

Safety Software Framework Block Diagram Block Diagram

- Standby/Off mode entry
  - FDCU
    - Error Out Un-related
  - SquareCheck
    - phil-dma
  - ModeSelector
    - Status Check results and statistical buffer data to NVM

- Boot to Safety
  - eXeCue
    - Safety Context Start
    - Execute SquareCheck Start
      - App
      - Safety Analysis
      - SquareCheck
      - BIST

- Normal Operation
  - SW Fault
    - Application SW
    - SquareCheck
    - $CST^*$
    - HW Emits
    - Low Recovery
    - HW Recovery
      - FDCU
        - MCU HW safe-stated
      - Error Out Un-related

- Degraded Operation
  - No Fault in Degraded CIP
    - Degraded App SW
    - SquareCheck
    - $CST^*$
    - HW Emits
    - Temp Recovery

- Global Recovery
  - HW Recovery (entry if NVM)
    - Read fault information
    - Runtime recovery through functional reset

Legend:
- SW Operation
- HW Operation
- S32K3 SAF Component
- ← SW Transition
- → HW Transition

* Structural Core Test (SCT) provided via separate installation packages
* Degraded mode available in software
View additional information for S32 Safety Software Framework (SAF).

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