

# S32安全软件框架产品简介

## 目录

1. 软件产品概述.....	1
2. 软件内容.....	5
3. 支持的目标.....	9
4. 质量、符合的标准和测试方法.....	10
5. 文档信息.....	11

## 1. 软件产品概述

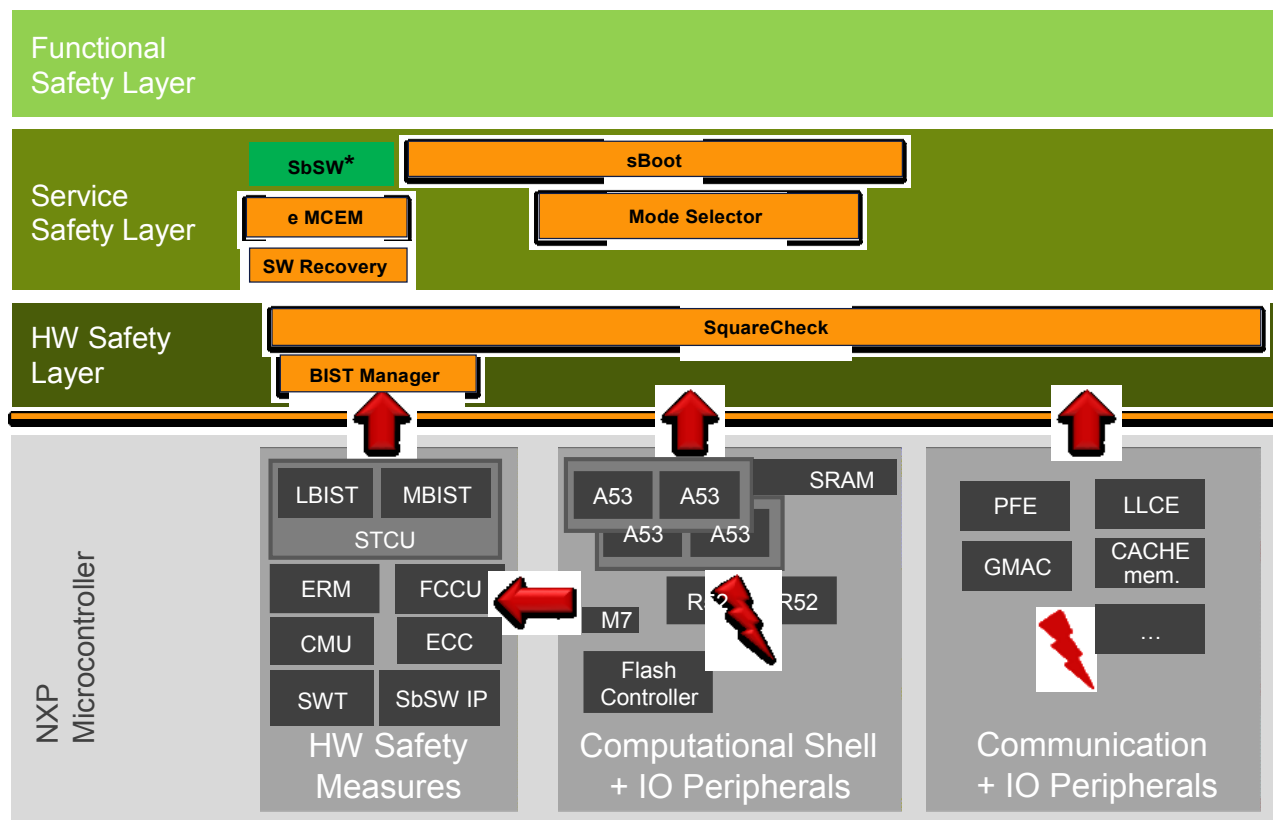
S32安全软件框架（SAF）包含软件组件，为符合ISO 26262功能安全标准的客户安全应用创建安全基础。它能够达到ASIL D汽车安全完整性级别，作为脱离上下文的安全元件（SEooC）开发。S32安全软件框架可集成到AUTOSAR®和非AUTOSAR应用中，该软件产品适用于所有恩智浦S32汽车平台器件（参见图1）。



图1. 恩智浦的S32安全软件框架支持所有恩智浦S32芯片

S32安全软件框架提供硬件和服务安全层的软件模块，如图2所示。提供的软件模块如下所示：

- **BIST Manager**——内置自检管理器，涵盖Logic BIST (LBIST) 和Memory BIST (MBIST)
- **eMCEM**——扩展微控制器错误管理器 (Microcontroller Error Manager)
- **Mode Selector**——模式选择器 (包括安全配置 (Safety Config))
- **sBoot**——安全启动 (Safety Boot)
- **SquareCheck**——Square Check (查看检验器 (Checker))
- **SW Recovery**——软件恢复



\*SbSW——软件安全

图2. 恩智浦安全软件框架内容

备注：如用户想开发自己的安全解决方案，可使用包含BIST Manager和eMCEM的S32安全外设驱动程序（SPD）产品。它补充了S32实时驱动产品，为片上外设模块提供软件支持。

S32安全软件框架组件在启动、运行时和故障恢复期间都会涉及。组件参与情况如图3所示。这些组件交换数据，在给定的应用状态下执行正确的测量和响应。

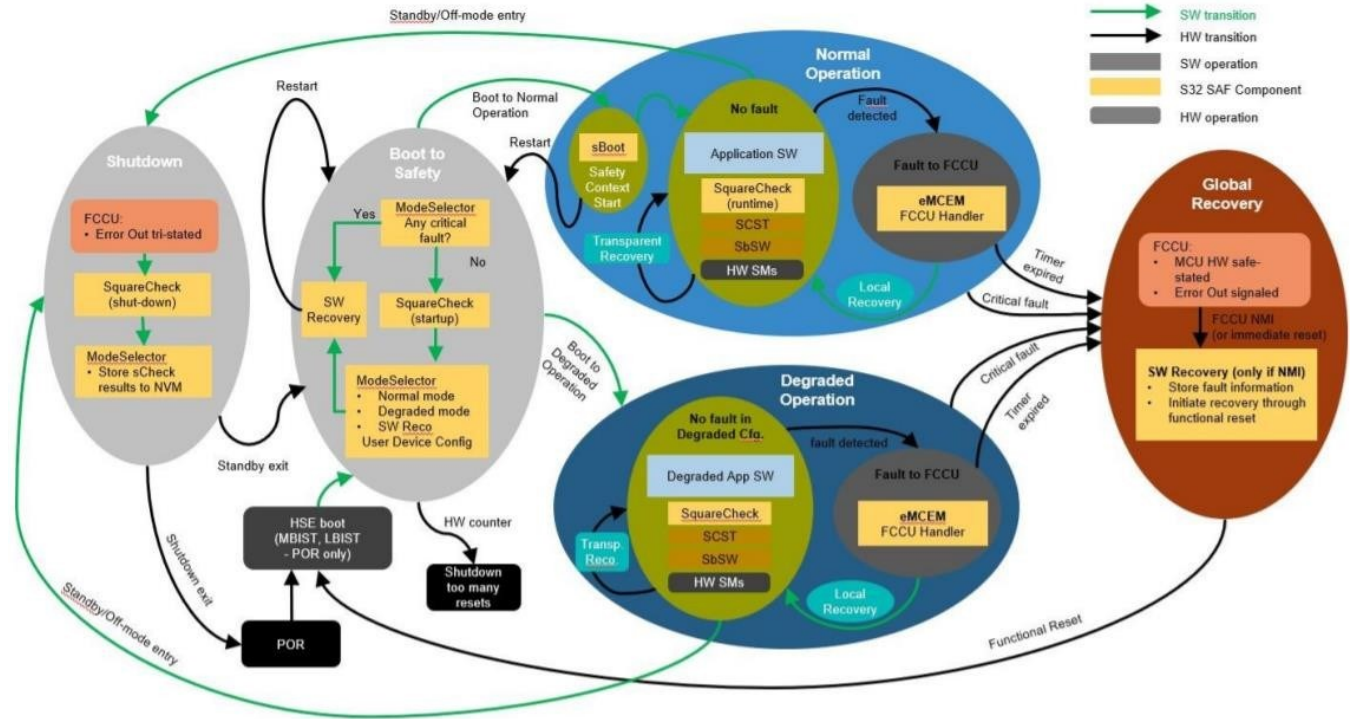


图3. S32安全软件框架操作图

## 2. 软件内容

S32安全软件框架对于保障S32汽车平台器件上的应用安全至关重要，其主要特性如下所示：

- 检查硬件安全机制，即潜在故障检测
- BIST管理和部署，以保证高可用性
- 支持引导至正常或降级模式
- 确保器件正确设置，能够启动安全功能
- 对检测到的故障进行处理和应对
- 支持本地和全局恢复战略
- 符合ISO 26262标准

### BIST Manager ( 内置自检管理器 )

- MBIST和LBIST硬件模块的驱动程序
- 分析LBIST和MBIST硬件提供的结果并启动执行

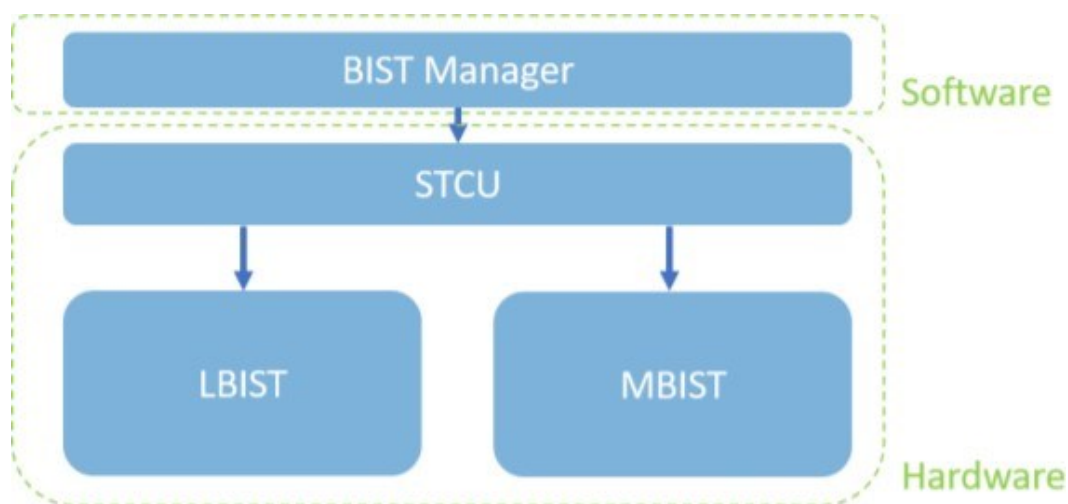


图4. BIST Manager ( 内置自检管理器 )

## eMCEM (扩展微控制器错误管理器)

- 微控制器的故障管理
- 故障反应配置 (复位、告警IRQ、NMI、无反应)
- 高超的错误处理机制
- 允许为每个FCCU故障注册单独的告警处理程序
- 如果SquareCheck测试了各自的安全机制, 则对故障反应进行重定向
- 故障状态报告和故障清除
- 错误注入
- 内存错误报告

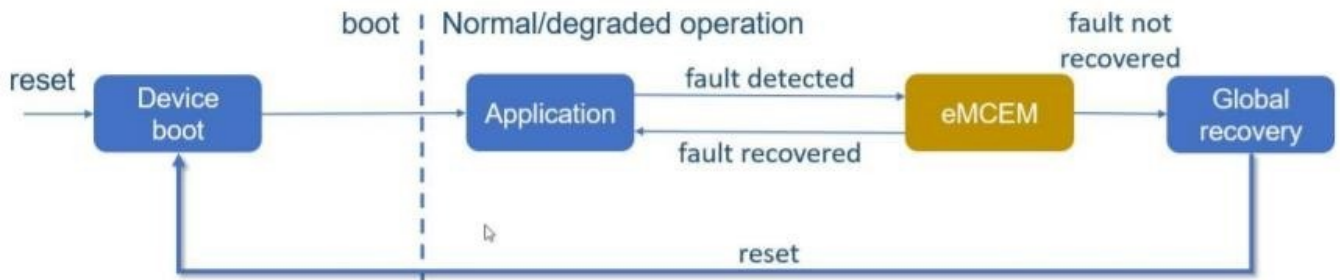


图5. eMCEM (扩展微控制器错误管理器)

## ModeSelector (模式选择器)

- 用于选择应用程序正常模式或降级模式的软件组件
- 降级模式通过允许在出现非关键永久性故障的情况下使用器件来提高器件可用性
- 选择基于FCCU结果、SquareCheck结果、可选的MBIST/LBIST结果以及SW Recovery存储的诊断信息。
- 在无法选择操作模式的情况下, 也可以调用SW Recovery, 然后进行功能复位 (Functional Reset)
- 当系统处于安全状态时, 在引导 (启动) 阶段执行
- 硬件资源区域的配置以及与可选模式所需故障源的关联

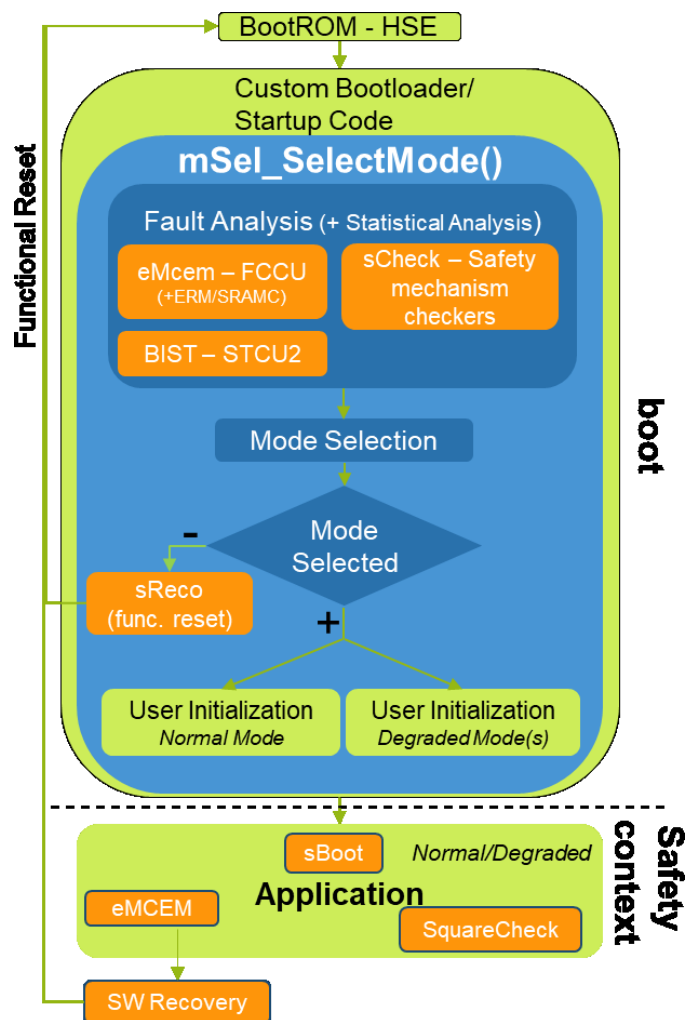


图6. ModeSelector

### sBoot（安全启动）

- 用于检查器件是否启动到安全配置的软件组件
- 在建立安全上下文之前，在应用程序执行开始时执行
- 验证器件配置满足硬件安全手册（SM）的假设

## SquareCheck

- 用于潜在故障检测的软件组件
- 检测硬件安全机制中的故障
- 提供启动、运行时和关闭API
- 根据ISO 26262提供所需的诊断覆盖率，最高可达ASIL D级

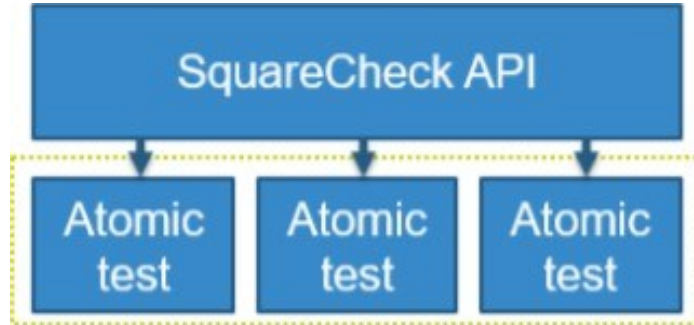


图7. SquareCheck

## SW Recovery ( 软件恢复 )

- 用于全局恢复的软件组件
- 如果MCU需要从本地恢复无法处理的故障中恢复，或者Mode Selector无法选择任何操作模式，则调用该组件
- 存储Mode Selector的诊断信息
- 当MCU处于安全状态时执行



图8. SW Recovery



### 3. 支持的目标

本产品简介中介绍的S32安全软件框架旨在与恩智浦半导体S32G2器件一起使用。

## 4.质量、符合的标准和测试方法

S32安全软件框架软件产品是根据符合ISO 26262、Automotive SPICE、IATF 16949和ISO 9001标准的恩智浦软件开发流程开发的。

## 5. 文档信息

表1. 测试样本修订记录

版本号	日期	实质性变更
1	2021年10月	初版发布

**How to Reach Us:**

**Home Page:**  
[nxp.com](http://nxp.com)

**Web Support:**  
[nxp.com/support](http://nxp.com/support)

Information in this document is provided solely to enable system and software implementers to use NXP products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document. NXP reserves the right to make changes without further notice to any products herein.

NXP makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does NXP assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. "Typical" parameters that may be provided in NXP data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including "typicals," must be validated for each customer application by customer's technical experts. NXP does not convey any license under its patent rights nor the rights of others. NXP sells products pursuant to standard terms and conditions of sale, which can be found at the following address: [nxp.com/SalesTermsandConditions](http://nxp.com/SalesTermsandConditions).

NXP, the NXP logo, NXP SECURE CONNECTIONS FOR A SMARTER WORLD, COOLFLUX, EMBRACE, GREENCHIP, HITAG, I2C BUS, ICODE, JCOP, LIFE VIBES, MIFARE, MIFARE CLASSIC, MIFARE DESFire, MIFARE PLUS, MIFARE FLEX, MANTIS, MIFARE ULTRALIGHT, MIFARE4MOBILE, MIGLO, NTAG, ROADLINK, SMARTLX, SMARTMX, STARPLUG, TOPFET, TRENCHMOS, UCODE, Freescale, the Freescale logo, AltiVec, C 5, CodeTEST, CodeWarrior, ColdFire, ColdFire+, C Ware, the Energy Efficient Solutions logo, Kinetis, Layerscape, MagniV, mobileGT, PEG, PowerQUICC, Processor Expert, QoriQ, QoriQ Converge, Ready Play, SafeAssure, the SafeAssure logo, StarCore, Symphony, VortiQa, Vybrid, Airfast, BeeKit, BeeStack, CoreNet, Flexis, MXC, Platform in a Package, QUICC Engine, SMARTMOS, Tower, TurboLink, and UMEMS are trademarks of NXP B.V. All other product or service names are the property of their respective owners. ARM, AMBA, ARM Powered, Artisan, Cortex, Jazelle, Keil, SecurCore, Thumb, TrustZone, and  $\mu$ Vision are registered trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. ARM7, ARM9, ARM11, big.LITTLE, CoreLink, CoreSight, DesignStart, Mali, mbed, NEON, POP, Sensinode, Socrates, ULINK and Versatile are trademarks of ARM Limited (or its subsidiaries) in the EU and/or elsewhere. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. The Power Architecture and Power.org word marks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.

© 2021 NXP B.V.

Document Number: 2.4  
Rev. 2.4  
01/2022