恩智浦半导体
产品简介

文档编号：1
第 1 版，2021 年 9 月

S32K3xx 安全软件框架——产品简介

目录

1. 软件产品概述

S32 安全软件框架（SAF）包含不同软件组件，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，作为不受条件限制的独立安全元件（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）。

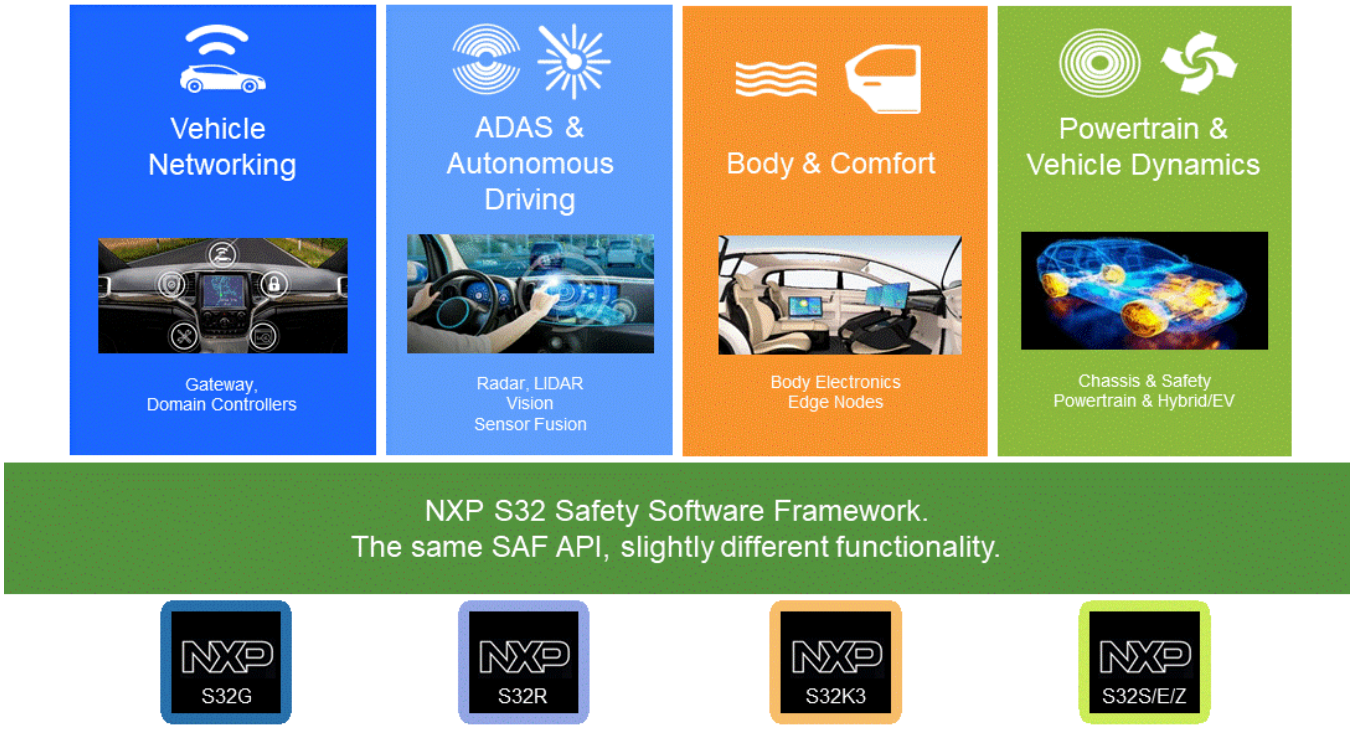


图 1. 恩智浦的 S32 安全软件框架支持所有恩智浦 S32 芯片

S32 安全软件框架提供了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**——扩展型微控制器错误管理器（Microcontroller Error Manager）
- **Mode Selector**——模式选择器
- **sBoot**——安全启动（Safety Boot）
- **SquareCheck**——Square Check（查看检验器（Checker））
- **SW Recovery**——软件恢复

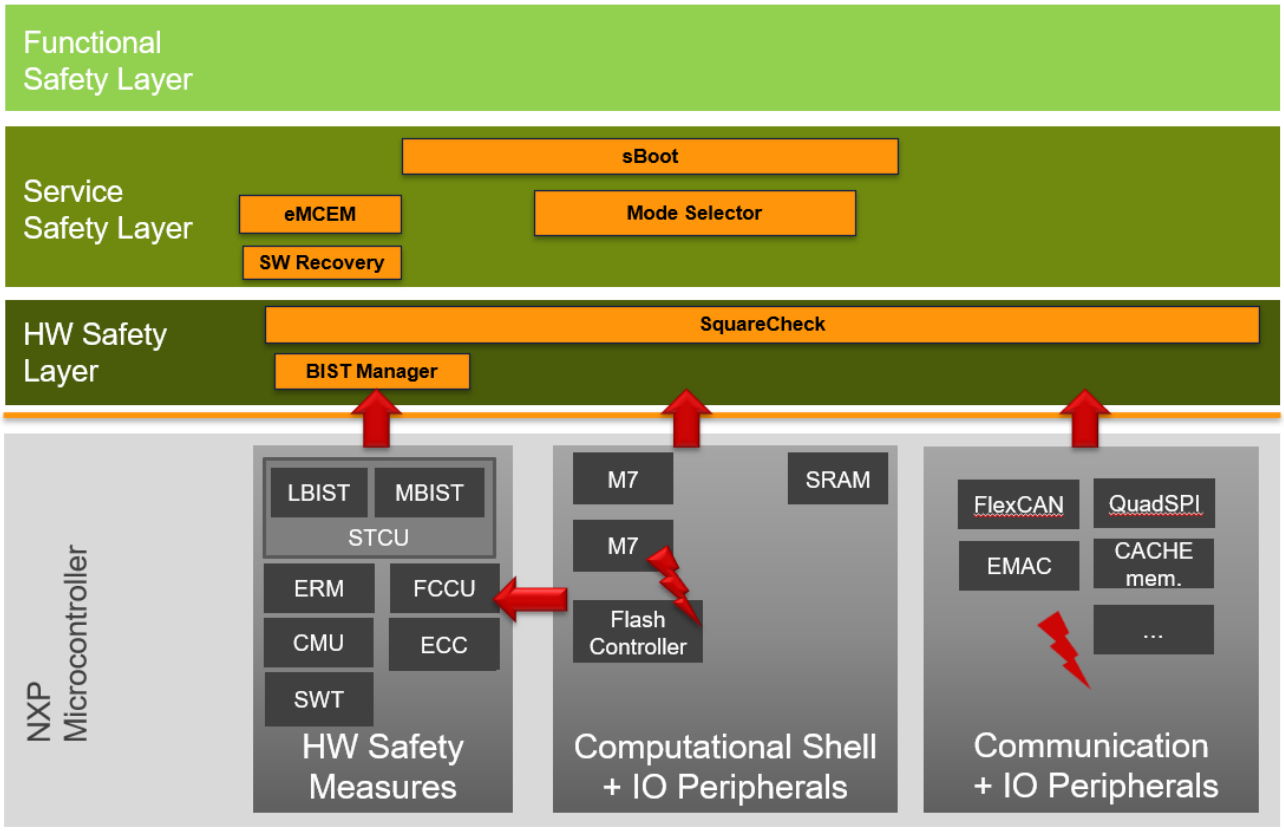


图 2. 恩智浦安全软件框架内容

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。

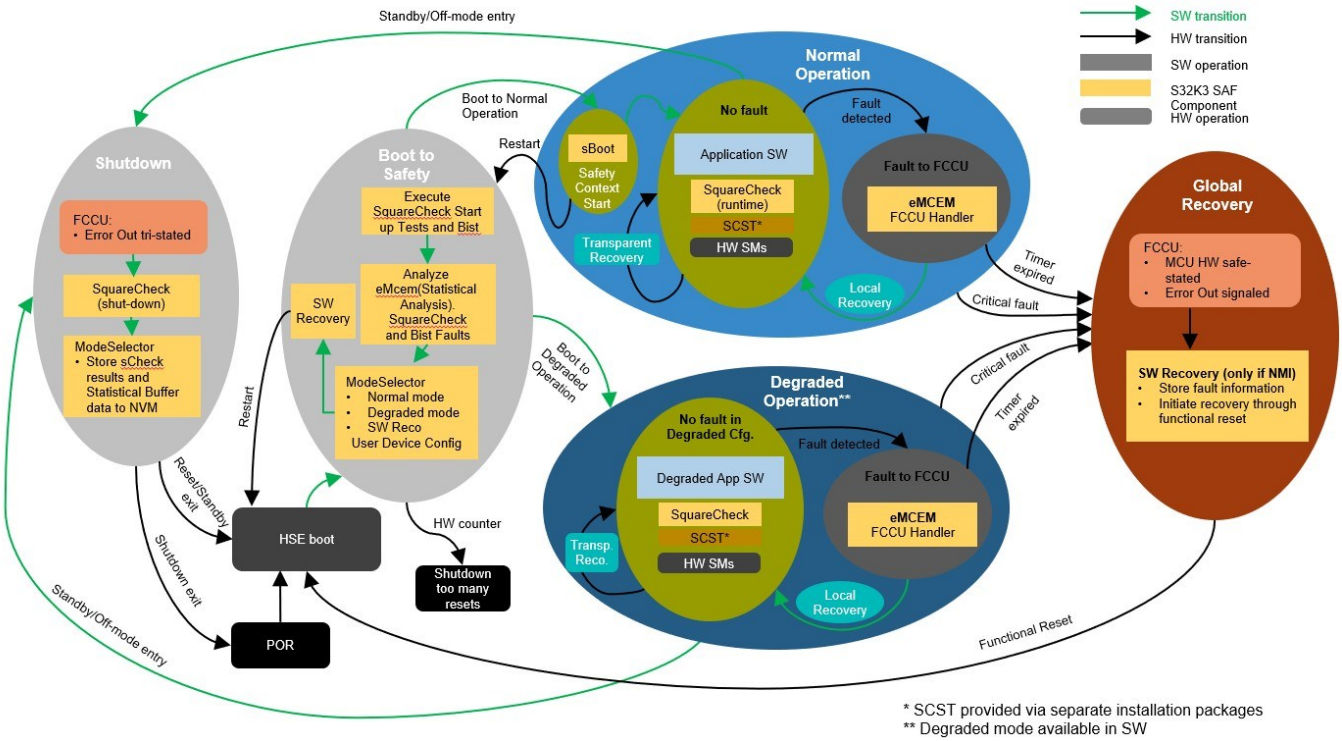


图 3. S32 安全软件框架操作图

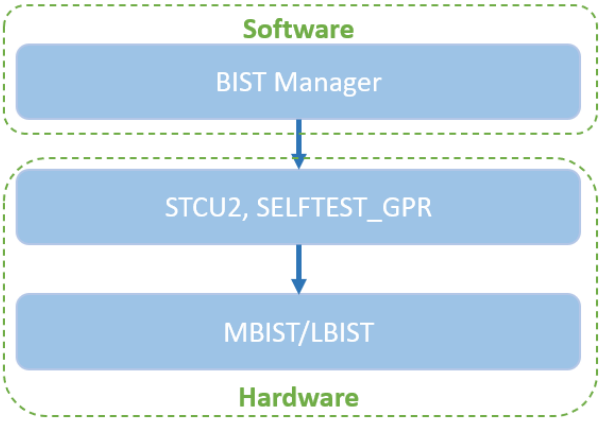
2. 软件内容

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，例如潜在故障检测
- 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策略
- 符合 ISO 26262 标准

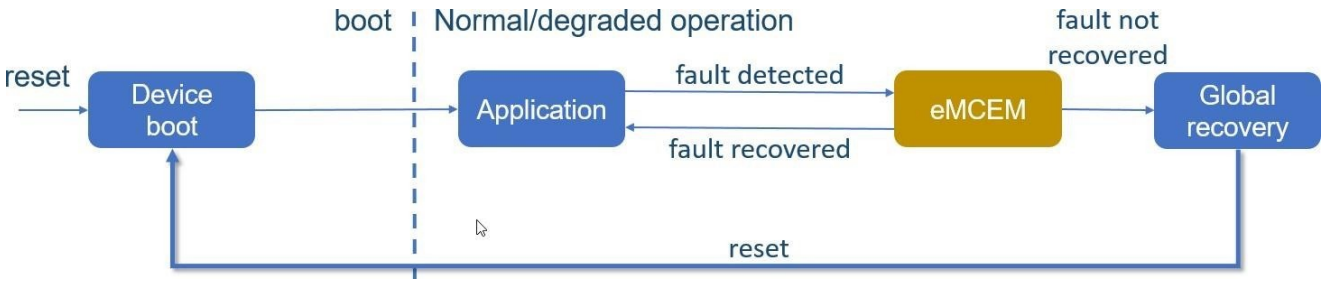
BIST Manager（内置自检管理器）

- MBIST 和 LBIST 硬件模块的驱动程序
- 启动执行 LBIST 和 MBIST 硬件模块并分析结果



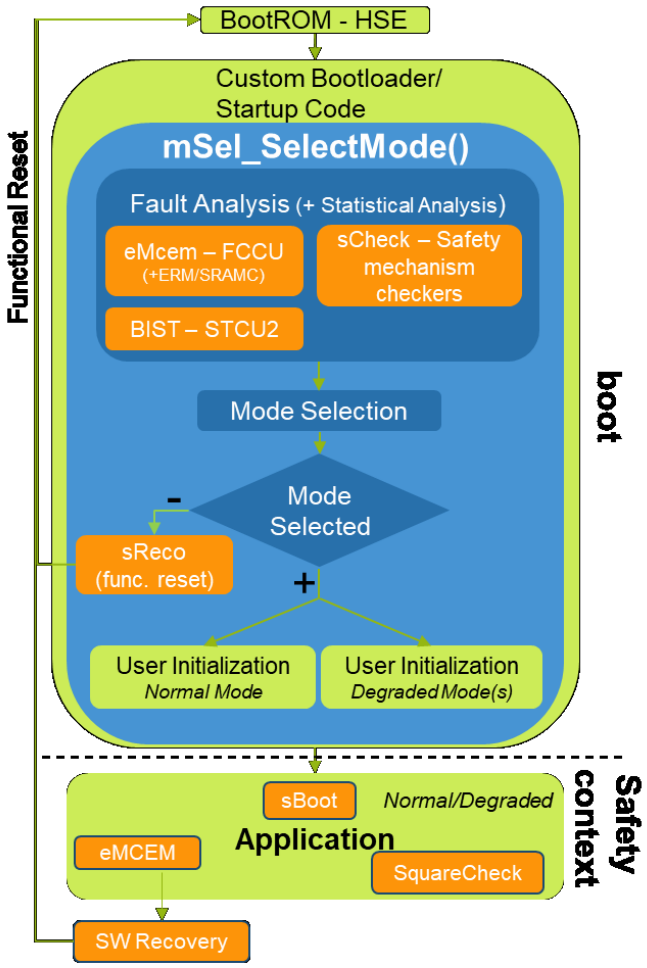
eMCEM（扩展微控制器错误管理器）

- 微控制器的故障管理（FCCU HW IP）
- 故障响应配置（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
- 如果在 SquareCheck 测试各自的安全机制过程中，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



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

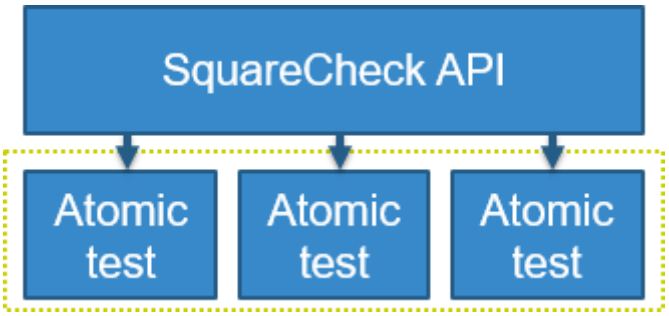


sBoot（安全启动）

- 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

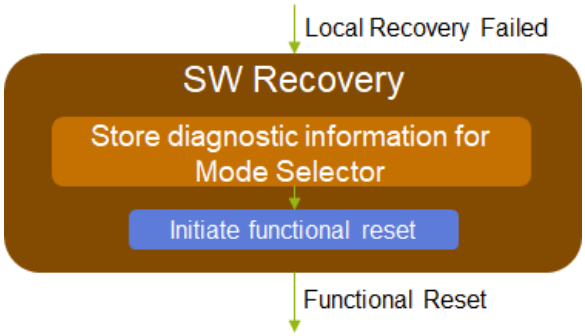
SquareCheck

- 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



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



3. 支持的目标

本产品简介中描述的 S32 安全软件框架旨在与恩智浦半导体 S32K3xx 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. 修订记录

版本号	日期	实质性变更
1	2021 年 9 月	初版发布

How to Reach Us:

Home Page:
nxp.com

Web Support:
nxp.com/support

Document Number: 1
Rev. 1
09/2021