# 结构核自检库

## 目录



## 1. 软件产品概述

SCST（结构核自检）库是一款用于运行时检测处理器核永久性硬件故障的软件产品。它包含测试代码（原子测试），由此用预定义的测试向量激发处理器核的子模块，并观察和评估核的逻辑响应。它通常能达到90%的DC（诊断覆盖率）。它针对各种处理器内核的子模块，如：

- 数据路径单元（ALU、乘法器、除法器）
- 加载/存储单元
- 指令解码器
- 转发逻辑
- FPU & NEON

详细情况可以在诊断覆盖率估算文件中找到，该文件是每个单独的SCST产品交付的一部分。

被认为是安全的故障（如调试逻辑中的故障）不会被测试，并被排除在DC计算之外，见图1：恩智浦的SCST库内容。

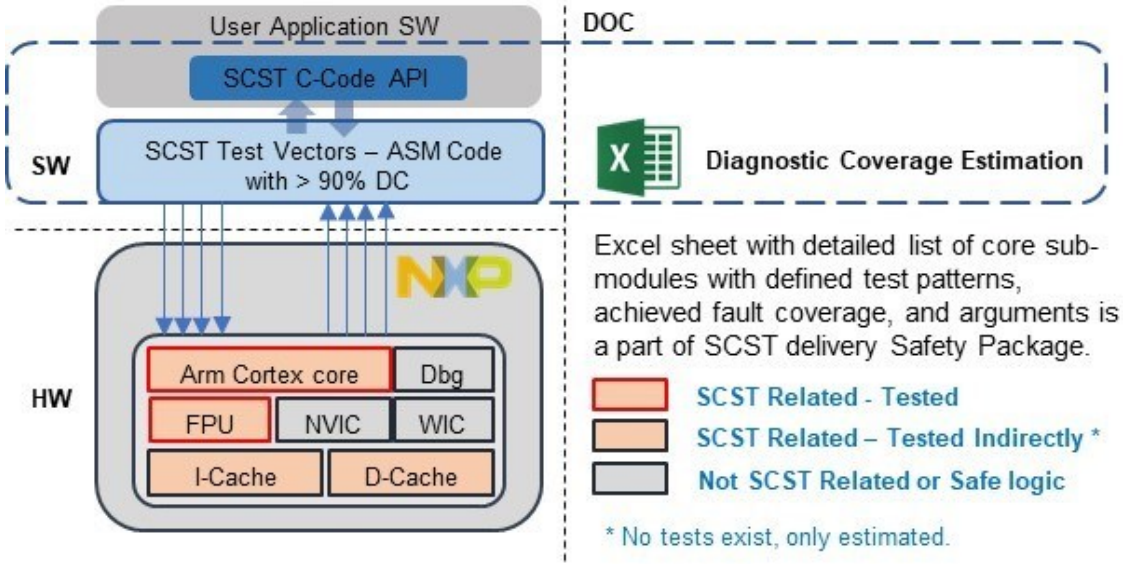


**图1. 恩智浦的SCST库内容示例**

SCST库可用于检测单点故障或潜在故障，故障的区分请见[1]。在这两种情况下，SCST只检测永久性故障，它主要用于某些处理器核，而这些处理器核不使用支持永久性故障检测安全的硬件（HW）技术，例如延迟锁步。如果使用SCST来检测潜在的故障，那么只需在启动或关闭时运行即可。为了检测单点故障，需要在运行时周期性执行SCST。

SCST是作为脱离上下文的安全元素（SEooC）而开发的[1]。分配给SCST安全要求的最高ASIL是ASIL-B(D)，支持实现高达ASIL-D的安全目标。然而，在SCST用于检测单点故障的情况下，SCST的诊断覆盖率仅对ASIL-B是足够的。因此，SCST可用于支持ASIL-B(D)要求，并应采用其他运行时措施来检测剩余的单点故障，以实现ASIL-C和ASIL-D指标。

# 2. 软件内容

SCST库在支持应用程序实现安全方面至关重要。SCST库的主要组成部分如下。

- SCST库的源代码：
  - 是用汇编语言编写的。
  - 针对核的特定部分，划分为专门的原子测试。
  - 对检测到的故障做出反应（破坏测试签名）。
- 用C语言编写的简单API：
  - 提供灵活的原子测试执行。
  - 向用户应用程序发送首次检测到的故障信号。
  - 通过破坏测试签名来支持原子测试故障注入，允许用户应用程序测试它自己的故障反应机制。
  - 符合MISRA C标准。
- 故障覆盖率估算文件，其中：
  - 包含对所声称的DC估算的详细论证。

# 3. 支持的目标

本产品简介中描述的SCST库可用于恩智浦S32G器件的Arm® Cortex-A53核。

# 4. 质量、符合的标准和测试方法

A53 SCST库软件产品是根据“恩智浦软件开发流程”开发的，符合ISO 26262、Automotive-SPICE、IATF16949和ISO9001标准。

# 5. 参考资料

1. ISO 26262-1：2018。道路车辆——功能安全——第1部分：词汇表，2018，{ISO 26262-1:2018（E）}。

# 6. 文档信息

**表1. 修订记录**

| 版本号 | 日期 | 实质性变更 |
|---|---|---|
| 1 | 2022年3月 | 初版发布 |
| 2 | 2022年4月 | 固定内核和平台描述 |

***How to Reach Us:***

**Home Page:**
nxp.com

**Web Support:**
nxp.com/support



Document Number: 1
Rev. 2
04/2022