SCST Library Product Brief

1.0 Software Product Overview

The SCST (Structural Core Self Test) Library is the software product used for the runtime detection of permanent HW faults in processor cores. It contains test codes (atomic tests) that stimulates processor core submodules with the predefined test vectors and observes and evaluates the core logic response. It typically achieves 90% DC (Diagnostic Coverage). It targets various processor core submodules, like:

- Data Path units (ALU, Multiplier),
- Divider, if available,
- Load/Store unit,
- Instruction decoder,
- Forwarding logic, if available,
- Coprocessors e.g. FPU, if available.

The details can be found in the Diagnostic Coverage Estimation document, which is a part of the delivery of each individual SCST product. Faults that are considered as safe (e.g. faults in the debuging logic) are not tested and are excluded from the DC calculation, see Figure 1: SCST Library content.

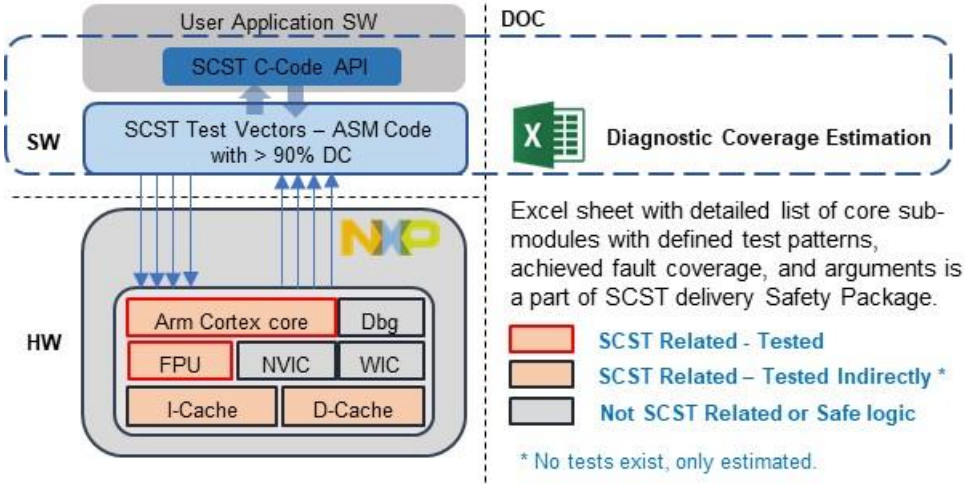

Figure 1: SCST Library content example

The SCST Library can be used to detect single-point faults or latent faults, see [1] for the fault differentiation. In both cases, SCST detects permanent faults only and it is primarily intended for processor cores which do not use HW techniques supporting safety in terms of permanent fault detection, e.g. delayed-lockstep. If SCST is used to detect latent faults, then it is sufficient to run it only during start-up or shut-down. To detect single-point faults, SCST needs to be executed periodically in runtime.

SCST Diagnostic Coverage is estimated analytically. The RTL-code of the core submodules together with Arm Architecture Manual is examined in detail by the developer. An expert individually analyses the core submodules, defines the test patterns, and analytically estimates DC.

SCST is developed as Safety Element out of Context [1]. The highest ASIL assigned to the SCST safety requirements is ASIL-B(D) supporting the achievement of safety goals up to ASIL-D, however in the case when SCST is used to detect single-point faults, SCST diagnostic coverage is

sufficient only for ASIL-B. Hence, SCST can be used to support ASIL-B(D) requirements and other run-time measures shall be in place to detect the remaining single-point faults to achieve ASIL-C and ASIL-D metrics.

2.0 Software Content

The SCST Library is essential in supporting applications to achieve safety. The main components of the SCST Libray are as follows:

- SCST Library source code:
  - Is written in Assembly language.
  - Is divided into dedicated atomic tests targeting specific parts of the core.
  - Provides reaction to a detected fault (destroys test signature).
- Simple API written in C:
  - Provides flexible atomic tests execution.
  - Signals first detected fault to the user application.
  - Provides support for atomic test fault injection by destroying test signature to allow to the user application testing it's own fault reaction mechanisms.
  - Conforms with MISRA C standard.
- Fault Coverage Estimation document which:
  - Contains detailed argumentation for the claimed DC estimation.

3.0 Supported Targets

The SCST Library described in this product is available for NXP S32G2 devices' Arm® Cortex-A53 core.

4.0 Quality, Standards Compliance and Testing Approach

The SCST Library software products were developed according to the NXP Software Development Processes that is ISO 26262, Automotive-SPICE, IATF16949 and ISO 9001 compliant.

5.0 References

1. ISO 26262-1:2018**.** *Road vehicles - Functional safety - Part 1:Vocabulary*, 2018, {ISO 26262-1:2018(E)}.