Cortex M4
Structural Core Self Test Library

Safety Manual

Rev. 2.0
14 January 2020

Content

1 Introduction

This document contains a list of recommendations originated from Safety Analysis [1] which should be fulfilled / verified by a user for a proper use of the Structural Core Self Test (SCST) Library for Cortex-M4 core.

SCST Library was developed for detecting HW permanent faults in a core by means of executing core instructions with pre-defined operands and comparing their execution results. This library is considered as Safety Element out of Context and was developed according to ASIL B. Safety Analysis (limited to Software FMEA) has been conducted for it and necessary safety measures were identified, see [1].

One part of safety measures has been implemented within the SCST Library itself. Another part (listed in the form of safety requirements and recommendations in this document) has to be addressed within the customer application. These are listed in the corresponding section of this document.

Only when all of the requirements, listed in this document, are addressed within the customer application and assumptions are verified, the SCST Library and its usage can be considered as functionally safe.

2 Functional Safety Recommendations for Application Originated from Safety Analysis Performed for SCST Library for Cortex M4 Core

2.1 Recommendation ID: REQ_M4_SCST_37

Application should use aggregated test result for making test completion and test passed/test failed decision. Safety measure is expected to be implemented on application side.

2.2 Recommendation ID: REQ_M4_SCST_38

If application requests multiple tests for execution, the tests should be grouped in the way that aggregated result for each group of tests is unique. Safety measure is expected to be implemented on application side.

2.3 Recommendation ID: REQ_M4_SCST_39

Use watchdog timer or any other timing facilities for detecting longer execution of the SCST library. Safety measure is expected to be implemented on application side.

Rationale: The SCST Library may exceed expected execution time due to HW fault

2.4 Recommendation ID: REQ_M4_SCST_40

Use of control flow monitoring or other measures for detecting incorrect return from the SCST library. Safety measure is expected to be implemented on application side.

Rationale: The SCST Library may erroneously return control to the wrong location of the application code due to HW fault.

2.5 Recommendation ID: REQ_M4_SCST_41

Check application context (local variables) and stack pointer after invocation of the SCST library. Safety measure is expected to be implemented on application side.

Rationale: The SCST Library may corrupt application context due to HW fault.

2.6 Recommendation ID: REQ_M4_SCST_42

The memory sections of the SCST Library shall be placed in ECC-protected memory or other memory corruption detection mechanism shall be used. Safety measure is expected to be implemented on application side.

Rationale: The SCST Library shall not be executed from corrupted memory.

2.7 Recommendation ID: REQ_M4_SCST_43

Use of application data protection or corruption detection mechanism after invocation of the SCST library. Safety measure is expected to be implemented on application side.

Rationale: The SCST Library may erroneously corrupt application data due to HW fault.

2.8 Recommendation ID: REQ_M4_SCST_44

Use of special purpose and device configuration register protection or corruption detection mechanism after invocation of the SCST library. Safety measure is expected to be implemented on application side.

Rationale: The SCST Library may erroneously corrupt special purpose or device configuration registers.

2.9 Recommendation ID: REQ_M4_SCST_45

Check Interrupt Controller configuration and core interrupt mask and priority registers or use other mechanism for detecting missing interrupts. Safety measure is expected to be implemented on application side.

Rationale: The SCST Library may erroneously disable interrupts or erroneously enable disabled interrupts.

2.10 Recommendation ID: REQ_M4_SCST_46

Check VTOR register value after invocation of the SCST library or use other mechanism for detecting incorrectly serviced interrupts or too long interrupts. Safety measure is expected to be implemented on application side.

Rationale: The SCST Library may erroneously restore user application ISR vector table.

2.11 Recommendation ID: REQ_M4_SCST_47

User application shall decide whether interrupt is expected or not. The application is responsible to provide an appropriate response for exceptions. Safety measure is expected to be implemented on application side.

Rationale: The SCST Library may erroneously generate interrupt/exception due to HW fault.

- End of list of requirements -

3 References

Reference ID	Description	Document revision / Release date
[1]	M4 SCST Safety Analysis	2.0, 14 January 2020

How to Reach Us:

Home Page:
www.nxp.com

Web Support:
www.nxp.com/support