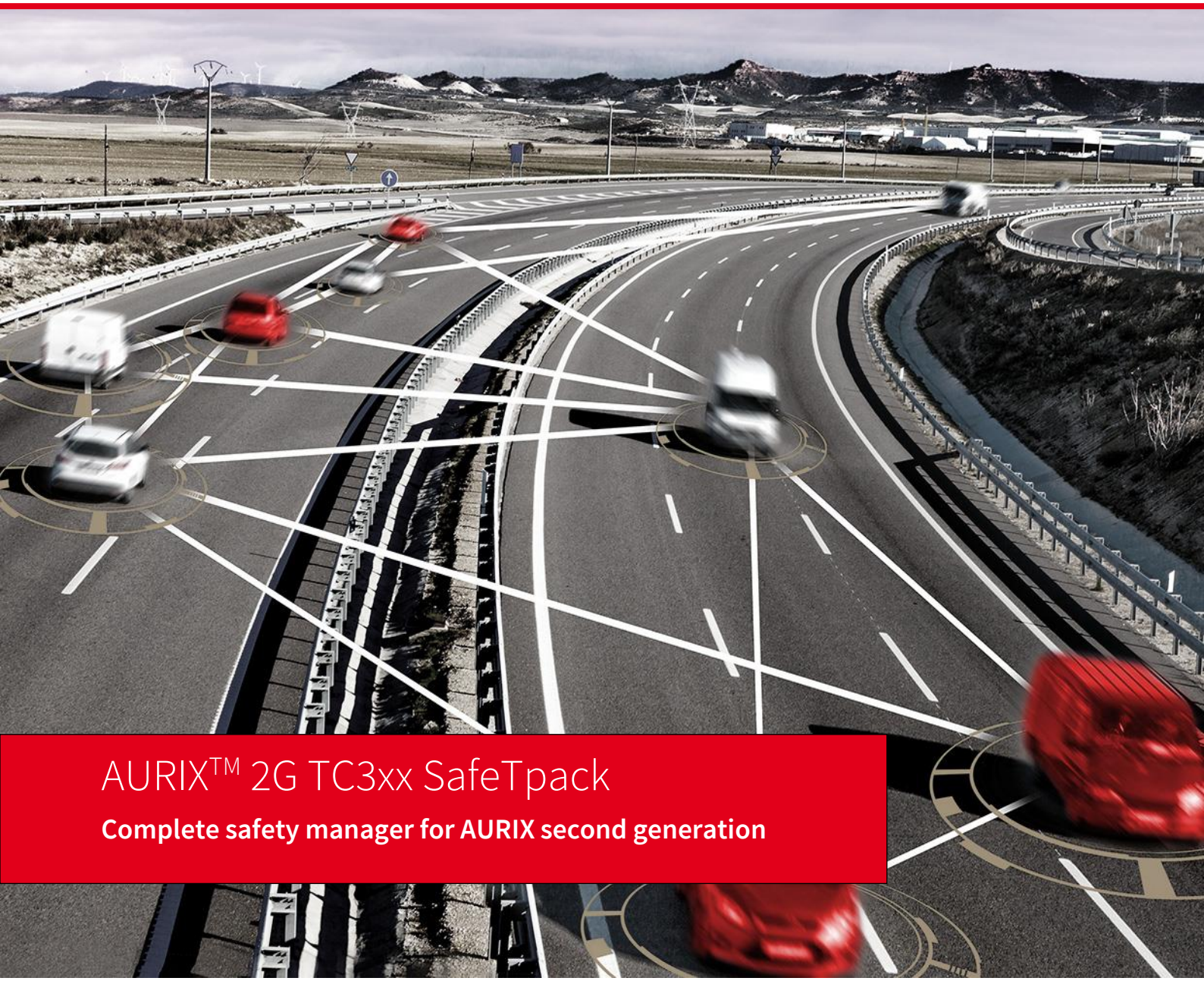
hitex
EMBEDDED TOOLS & SOLUTIONS

Building a safe and secure embedded world



AURIX™ 2G TC3xx SafeTpack

Complete safety manager for AURIX second generation

> Product Brief

Contents

1. Overview

AURIX SafeTpack safety manager for AURIX 2nd generation TC3xx

PRO-SIL™ SafeTpack is a complete safety manager for the AURIX second generation 32-bit safety microcontrollers that provides a shortcut to implementing the safety manual requirements. Like the PRO-SIL™ SafeTlib for AURIX TC2xx first generation, it provides a rapid and straightforward way to achieve ISO 26262 or IEC 61508 certification for safety applications using TC3xx second generation devices.

SafeTlib vs. SafeTpack

The AURIX second generation contains a Logic Built-In Self-Test (LBIST) which replaces the MicroTestLib in the SafeTlib. These both perform Latent Fault Metric tests on the AURIX silicon. However the SafeTlib provides numerous other safety-related functions which can have a huge effect on the overall Single Point Fault Metric, Latent Fault Metric and FIT rate of the system. These functions are still needed on the AURIX second generation and are included in the SafeTpack safety management system.

Easy SafeTlib to SafeTpack migration

SafeTpack coordinates the execution of startup and cyclic tests that ensure the correct operation of the AURIX CPU and internal busses through a mixture of hardware and software modules. It also manages the watchdog system and the optional TLF35584 combined watchdog and power regulator. By retaining the existing PRO-SIL™ SafeTlib overall structure and API, migration of existing TC2xx safety applications to TC3xx is made much simpler.

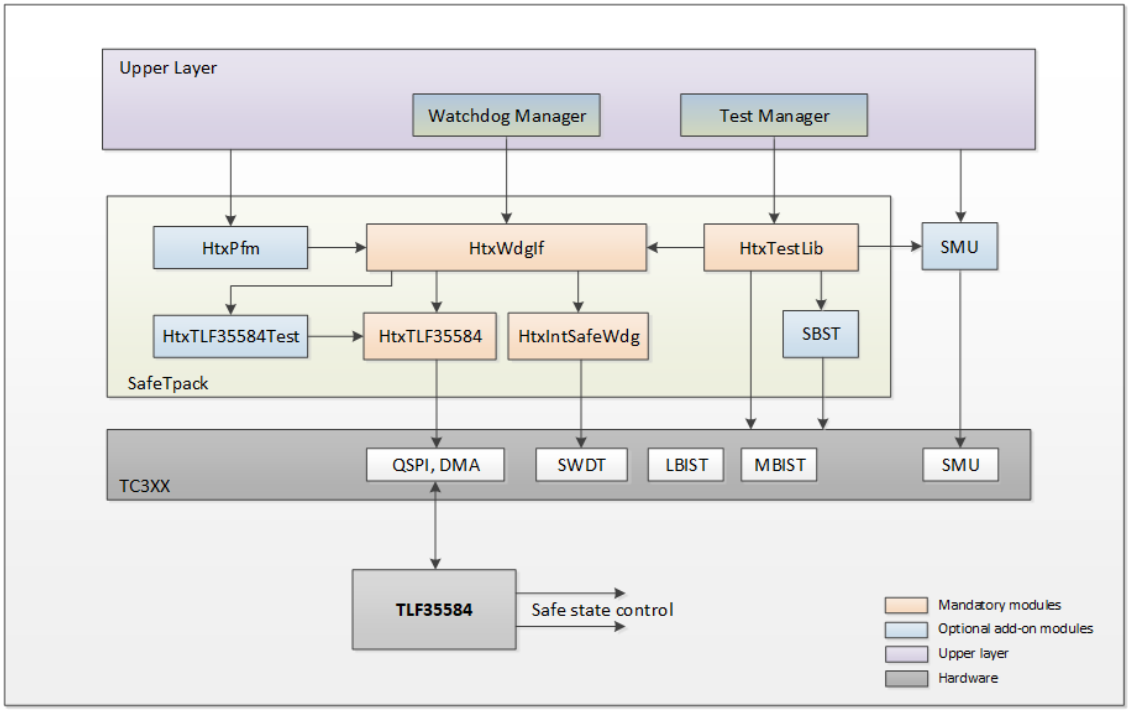
AUTOSAR complex driver

SafeTpack can be used either with or without AUTOSAR, where it constitutes a complex driver. Moreover the SafeTpack is 100% compatible with the Infineon MCAL but can still be used independently.

Inside the SafeTpack

SafeTpack has four main sections:

1. Test library/test manager
2. Internal/external safety watchdog interface and drivers
3. Signature monitor/error reporting system
4. Safety Management Unit (SMU) driver



2. Test library and test manager

The Test Library includes a Test Manager that launches the TC3xx built-in test functions such as the LBIST, PBIST, MONBIST and MBIST as well as the optional SBST for the non-lockstep mode of the Signal Processing Units (ASIL-C) and non-lockstep AURIX CPU cores (ASIL-B). Support for redundant Sfr configuration checking for ASIL-D is also included. The Test Manager reports any errors via an application call-back and a predefined 32-bit test result signature value, which is passed to the Signature Monitor. Tests are activated and configured using the Tresos Studio environment.

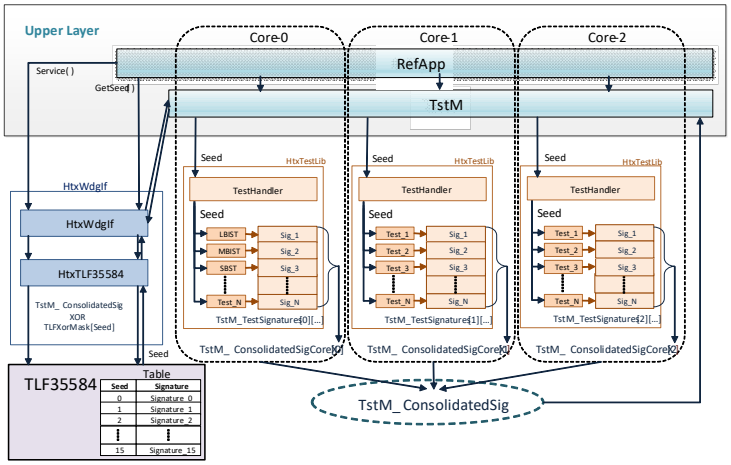
3. Safety watchdog interface & signature monitor

The Safety Watchdog Interface can work with either the on-chip internal watchdog (QM, ASIL-A, ASIL-B*) or the external TLF35584 combined power supply and safety monitor (ASIL-B/C/D). In the latter case, the interface provides an optimized, low-overhead, DMA-based QSPI driver.

The supported watchdog configurations are:

Configuration	Comment	Functional Watchdog Provider	Time Window Watchdog Provider
1	QM, ASIL-A	Internal Safety Watchdog	None
2	ASIL-B, ASIL-C	Internal Safety Watchdog	TLF35584
3	QM, ASIL-A, ASIL-B	TLF35584	None
4	ASIL-B, ASIL-C, ASIL-D	TLF35584	TLF35584
5	User Defined	User Defined	User Defined

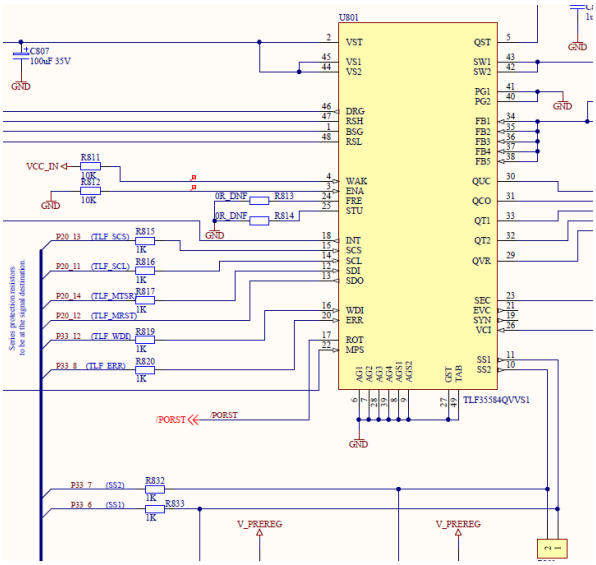
The signatures from the test library are fed via the Signature Monitor to refresh the watchdog, with an incorrect signature causing the safe state to be entered. The Safety Watchdog Interface can be extended to collect signatures from optional Assumption of Use (AoU) modules such as the Hitex Program Flow Monitor (HtxPfm), ADC self-test, redundantly implemented Sfr checks, Die Temperature Sensor Monitor, DMA monitor etc..



The Safety Watchdog Interface and Signature Monitor are intended to be used both for the AURIX 2G self-test phase and thereafter in the user's application, as in the AURIX TC2xx SafeTlib. This relieves the user from having to create his own TLF35584 servicing system.

3.1. Extended TLF35584 support

The optional HtxTLF35584Test module provides the AoU TLF35584 startup tests such as the Window Watchdog Test, Functional Watchdog Test, Error Pin Monitor Test and Analog built-in Self-Test (ABIST) etc., as per the TLF35584 safety Manual.



3.2. Optional TLF3068x support

For 3V3 and ADAS systems, the TLF30684 will be supported in the same way as the TLF35584.

3.3. Management unit (SMU) driver & configurator

This allows the user to configure the SMU for the purposes of startup safety testing by the SafeTpack and if the application is not based on MCAL, it can also be used to configure the SMU for the user's own application.

4. SafeTpack usage (ISO26262) and availability

As SafeTpack is a software component of a larger user-defined system, in the ASIL-B form, it is supplied as source code with the ISO26262-style Safety Manual and Safety Case Report. Hitex can provide assistance with the user's certification procedure by special arrangement. SafeTpack may be used at up to ASIL-D, subject to special measures being taken by the user.

SafeTpack is available in two forms and safety levels.

4.1. Trial version

Fully functional, partial source code/object library with a Getting Started guide, limited configurator and basic documentation, supplied with simple reference application showing SafeTpack usage. For evaluation purposes only on Infineon and Hitex evaluation boards. It will allow the correct servicing of the internal or TLF35584 safety watchdogs. It is included with Infineon and Hitex AURIX second generation evaluation boards. Free of charge.

4.2. ASIL-B Production Version

Fully functional source code with configurator, simple reference application showing SafeTpack usage, ISO 26262 Safety Manual and Safety Case Report.

4.3. Optional modules

4.3.1. SBST for non-lockstep CPUs

This optional add-on module contains the Infineon SBST for non-locked step CPUs that are to be used for ASIL-B. It manages the SBST slices and reports the output status through the signature management system.

4.3.2. SBST for signal processing unit

This optional add-on module contains the Infineon SBST for the non-locked step SPU that is to be used for ASIL-B. It manages the SBST slices and reports the output status through the signature management system.

4.3.3. Program flow monitor

The HtxPFM add-on is able to verify that tasks and functions are called in the expected order. It is able to run on all cores and the status is reported via the signature manager to the internal or external functional watchdog.

4.3.4. TLF35584 ABIST (**A**nalog **B**uilt-**I**n **S**elf **T**ests)

Tests the comparator and evaluation logic related to the monitoring functions contributing to the activation of Secondary Safety Shutdown path and Interrupt generation. It also includes the TLF35584 Window Watchdog Test, the TLF35584 Functional Watchdog Test and the TLF35584 Error Pin Monitor Test.

4.3.5. DMA monitor

DMA Monitor verifies the integrity of the data transferred by DMA. It uses the Data CRC, Address CRC and TimeStamp hardware safety features of the DMA to verify the integrity of the data transfer.

4.3.6. EVADC VADC monitor

The EVADC Monitor performs the Broken Wire Detection test, Out Of Bounds test, Internal Multiplexer Diagnostics test, Converter Diagnostics test and Voltage Reference Monitor test.

4.3.7. Die temperature (DTS) test

Provides functions to initialise, configure and perform Die Temperature measurements and tests the Die Temperature upper limit and lower limit SMU alarms.

Further add-on modules are in preparation.

5. Getting started and working with SafeTpack

It is highly recommended to integrate SafeTpack with your application at the earliest possible stage. The Trial Version package is recommended for this. It is completely representative of the ASIL-B version and can act as a functional placeholder during early product development on standard Infineon and Hitex boards. It will ensure that the TLF35584 is correctly serviced and that the basic testing and error reporting system is in place from the start of the project.

When transferring to custom hardware, the SafeTpack ASIL-B version is required to allow full configuration, continued development and final release.

Ask for a free trial version: sales@hitex.de.

AURIX toolchain support:

- Tasking v6.2r1p3/6.2r2
- Hightec GCC v4.9.2
- Planned: GHS, Windriver/Diab.

Silicon support

- TC399, TC398 B-step (Q4 2018)
- TC397 (Q1 2019)

hitex
EMBEDDED TOOLS & SOLUTIONS

Hitex Head Office, Germany

Hitex GmbH
Greschbachstr. 12
76227 Karlsruhe
Germany

Phone: +49-721-9628-0
Fax: +49-721-9628-149
Email: info@hitex.de

Hitex UK

Hitex (UK) Ltd
Millburn Hill Road
University of Warwick Science Park
Coventry CV4 7HS
United Kingdom

Phone: +44 (0)2476 69 2066
Fax: +44 (0)2476 69 2131
Email: sales@hitex.co.uk