

# SafeTkit TC1767/1782

## First steps to IEC 61508/ISO 26262: making your application safe

### At a glance

#### Complete evaluation of the PRO-SIL™ SafeTcore library:

- Shows the safety features with the included application
- Lets you modify and reload the application
- Allows to make your application safe by including the SafeT library

The Hitex 32-bit SafeTkit provides a great introduction to the Infineon safety system for the TriCore microcontroller family by providing the heart of an ASIL-D/SIL3 capable platform in an easy-to-configure and easy-to-use format.

All the major PRO-SIL™ SafeTcore features are available and can be reconfigured to assess their effect on system behaviour and gain an understanding of the concepts



underlying them. The kit contains all the elements required to produce a working application that has the potential for ASIL-D or SIL3 certification\*.

*\*The kit allows the techniques and concepts required for eventual ASIL-D/SIL3 certification*

#### PRO-SIL™

All PRO-SIL™ labeled parts are designed to meet the needs of ISO 26262 and IEC 61508 on the TriCore dual CPU architecture. By using the SafeTcore set of powerful self-test routines that run on the PCP both at startup and cyclically from within an application, the correct operation of the user's software and the TriCore CPU itself can be verified.

In the event of a random hardware failure or software upset, an orderly shutdown is possible. To satisfy the requirement for no common cause failures between the PCP and TriCore, the operation of the entire safety system is verified externally by the independently-powered CIC61508 safety monitor via a high speed SPI link.

and other critical analog voltages elsewhere in the system.

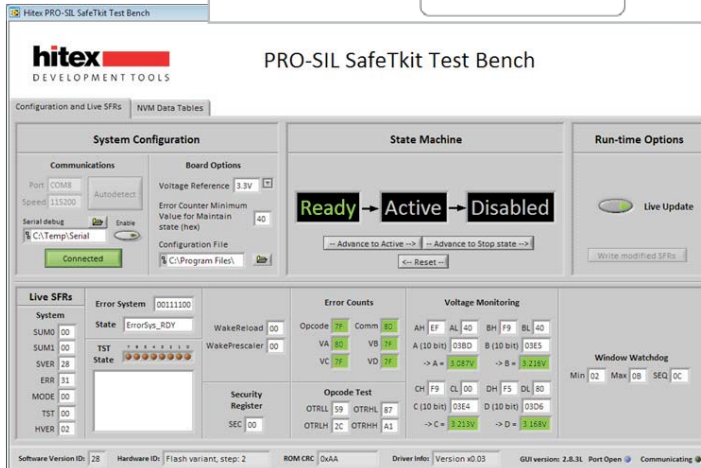
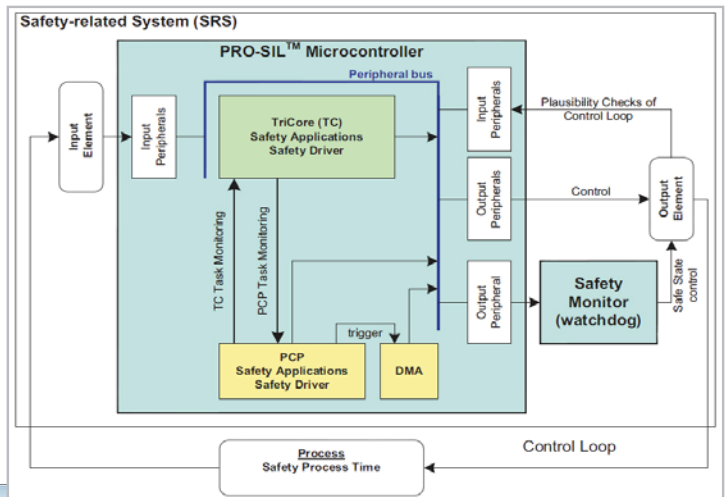
In the event of a failed TriCore test or supply voltage drop, the CIC61508 can provide up to three user-defined pin state sequences for managing a safe shutdown of critical hardware.

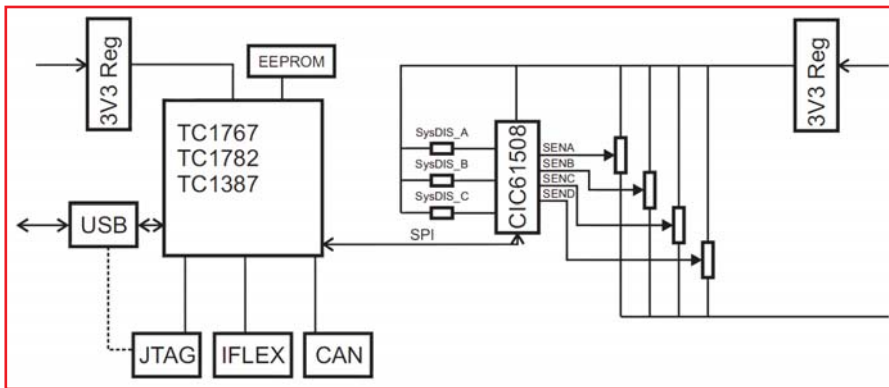
#### PRO-SIL™ SafeTcore Features

- Satisfies the requirements of ISO 26262 ASIL-D by decomposition
- Suitable for IEC 61508 SIL3
- Removes the need for independent hardware safety measures..
- Created using an ISO 26262 development process
- Externally certifiable

#### CIC61508

The CIC61508 safety monitor provides the verification of periodic TriCore CPU tests using a windowed watchdog approach. It also is able to monitor the TriCore CPU power supply





If the potentiometer voltages go outside preset ranges or the TriCore self-tests fail, the CIC61508 will move to the DISABLE sequence and its three System Disable pins will assume a state determined by the user's own configuration of the calibration data area. The reason for the failure can then be investigated via source level debugging of the application using HiTOP54-TC debugger or any changes to the system configuration made either through the compiler IDE or the PRO-SIL SafeTkit Test Bench. For demonstration purposes, faults can be injected to allow the system's response to them to be assessed.

## Using The PRO-SIL™ SafeTkit

A demonstration application is supplied which contains a typical SafeTcore configuration. At power-up, the SafeTcore initialises and performs a complete TriCore and CIC61508 self-test. If the voltage monitors are enabled and the potentiometers on the SafeTkit board are in the correct ranges (or the monitors are all disabled), SafeTcore

requests the CIC61508 to enter ACTIVE mode where it begins to continuously monitor the four voltages and the TriCore's internal cyclic selftest results.



## SafeTkit Features

- Real time viewing of voltage monitor inputs
- ErrSYS, error counters
- Force from ACTIVE to DISABLED mode (RA\_Stop()).
- Program DFLASH with new voltage thresholds
- Reset of CIC61508 and SafeTcore from SafeTkit test board
- Change voltage thresholds, inc and dec sizes, opcode test table
- Change failure reaction times (inc and dec values)
- Vary CIC61508 trip timeouts
- Enable/disable voltage monitors
- Change safety path pin patterns
- Calibration data import/export.
- Read CIC SVER, HVER and CRC
- CIC61508 DFLASH programming

## SafeTkit Contents

- TC1767/1782 Triboard with SAK-CIC61508
- Tasking VX Toolset v3.5r1 evaluation version
- HiTOP54-TC debugger and flash programmer (256K code size limited)
- SafeTcore libraries (limited to included boards)
- Demonstration application
- TestBench driver supplied as a library
- User manual and quick start guide
- USB cable



Visit us on the internet! [www.hitex.com](http://www.hitex.com)

### Main Office Germany

Greschbachstraße 12 Tel. +49-721-9628-0  
D-76229 Karlsruhe Fax +49-721-9628-149  
E-mail sales@hitex.de

### Hitex USA

2070 Business Center Tel. 800-45-HITEX  
Drive, Suite 280 Tel. +1-949-863-0320  
Irvine, CA 92612 Fax +1-949-863-0331  
E-mail info@hitex.com

### Hitex UK

Warwick University Tel. +44-(0)24-7669-2066  
Science Park Fax +44-(0)24-7669-2131  
GB-Coventry CV4 7EZ E-mail info@hitex.co.uk

This brochure is intended to give overview information only. Since our policy is one of continuing development, changes and technical enhancements are possible. Trademarks of other companies used in the text refer exclusively to the products of these companies. Hitex, HISIM, HITOP, DProbe, JProbe, USB Agent, Tanto and Tantino are trademarks of Hitex Development Tools GmbH. Copyright ©2007.