AURIX^{TM} Knowledge Lab 2021

SafeTpack for AURIX^{TM} TC3xx

AURIX^{TM} Knowledge Lab 2021

Implementing AURIX^{TM} Safety Measures with SafeTpack

hitex

EMBEDDED TOOLS & SOLUTIONS

Michael Weiß

Senior Account Manager
Embedded Solutions

michael.weiss@hitex.de

Hitex SafeTpack

Safety solution for AURIX™ TC3xx & TC4xx

What ist the Hitex SafeTpack?

- SafeTpack is the safety solution for the AURIX TC3xx microcontroller family
- SafeTpack is designed to cover the most common AURIX^{TM} safety manual requirements for a lot of applications in automotive and industry

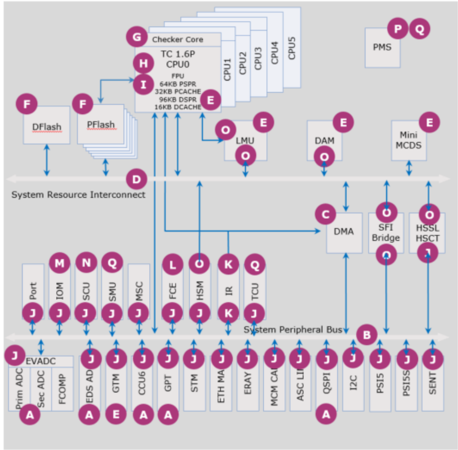
Copyright: Infineon

This seems to be…

… a lot of effort to implement all necessary internal and external safety mechanisms!

AURIX™ HW measures supporting safety

infineon



- A Redundant, spatial separated peripherals
- B Safe SPB
- C Safe DMA
- D Safe SRI
- E SRAM ECC (SECDED with enhancements to detect multi bit failures)
- F Flash ECC (PFLASH with DECTED, DFLASH with TECQED)
- G Lockstep core
- H CPU self tests (90% Latent Fault Metric)
- I Memory protection core
- J Memory protection peripherals
- K Safe Interrupt Processing
- L Flexible CRC Engine (FCE)
- M IO Monitor
- N Clock Monitoring
- O E2E protection
- P Power Supply Monitoring
- Q Self Test

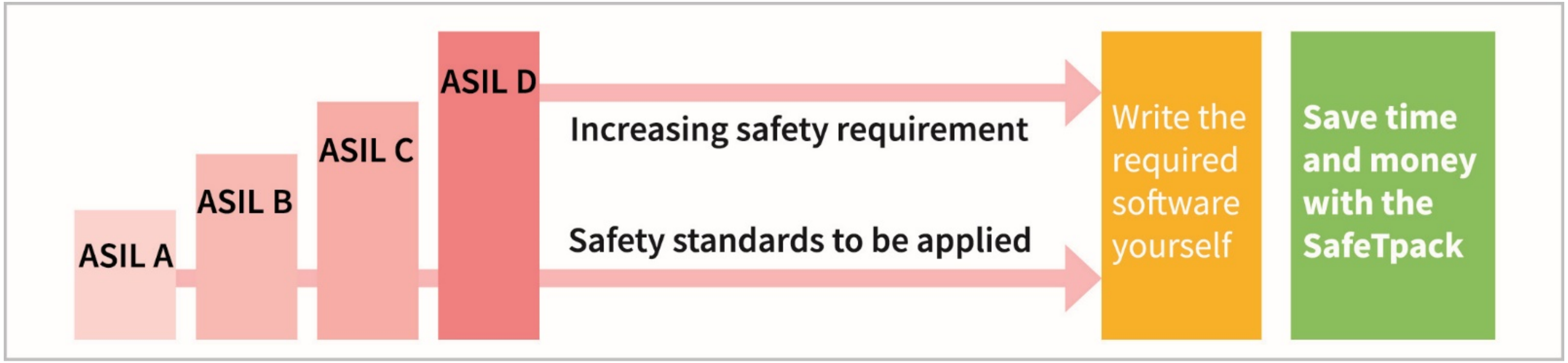
Copyright © Infineon Technologies AG 2021.

+ 1000+ pages of documentation = Hitex SafeTpack

Safety solution for AURIX™ TC3xx & TC4xx

Reduce complexity with SafeTpack
→ Save time and money

Why do you need a SafeTpack ?


ASIL A
ASIL B
ASIL C
ASIL D
Increasing safety requirement
Safety standards to be applied
Write the required software yourself
Save time and money with the SafeTpack

- Concentrate on your application knowhow
- „Reinventing the wheel" costs time and money …

  with SafeTpack, we cover a lot of AURIX^{TM} knowhow for you
- SafeTpack is PRO-SIL^{TM} ready and provides a rapid way to achieve your ASIL goals
- SafeTpack saves time, money and your nerves

At a glance: what does the SafeTpack offer ?

✓ Provides interfaces to execute and evaluate the startup tests

✓ Supports the necessary Safety Mechanisms (SM), External Safety Mechanisms (ESM) and Safety Mechanism Configurations (SMC)

✓ Provides cyclic tests that ensure the correct operation of the AURIX^{TM} TC3xx CPU and internal busses through a mixture of hardware and software modules

✓ Manages the watchdog system and an optional combined watchdog and power controller (eg. TLF35584 or TLF35585)

Definition of Safety Mechanism

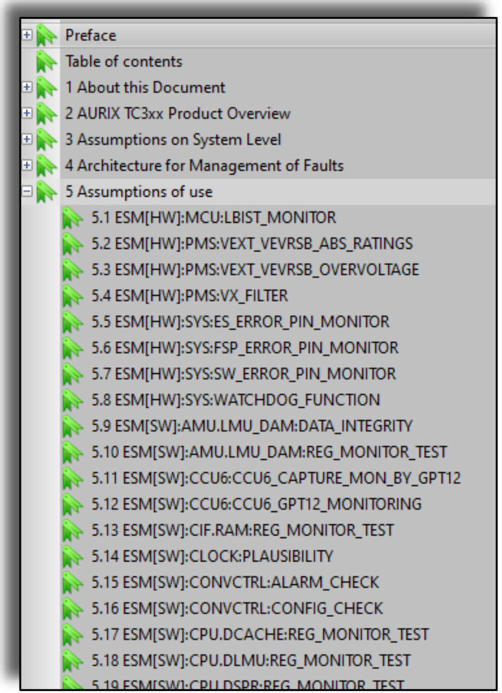
Safety Mechanisms Identifiers as per TC3xx Safety Manual:

- **Safety Mechanism (SM)**: technical solution internal to the MCU by HW or SW
- **External Safety Mechanism (ESM)**: technical solution either in HW or SW, implemented at System level by the system integrator

Additionally the following term is used in the manual for describing the required actions for correctly configuring a safety mechanism:

- **Safety Mechanism Configuration (SMC)**: Initialization or configuration that the Application SW shall perform for enabling a safety mechanism used in the application

→ TC3xx Safety Manual: More than **120** Assumptions of Use (ESM & SMC)



Preface
Table of contents
1 About this Document
2 AURIX TC3xx Product Overview
3 Assumptions on System Level
4 Architecture for Management of Faults
5 Assumptions of use
5.1 ESM[HW]:MCU:LBIST_MONITOR
5.2 ESM[HW]:PMS:VEXT_VEVRSB_ABS_RATINGS
5.3 ESM[HW]:PMS:VEXT_VEVRSB_OVERVOLTAGE
5.4 ESM[HW]:PMS:VX_FILTER
5.5 ESM[HW]:SYS:ES_ERROR_PIN_MONITOR
5.6 ESM[HW]:SYS:FSP_ERROR_PIN_MONITOR
5.7 ESM[HW]:SYS:SW_ERROR_PIN_MONITOR
5.8 ESM[HW]:SYS:WATCHDOG_FUNCTION
5.9 ESM[SW]:AMU.LMU_DAM:DATA_INTEGRITY
5.10 ESM[SW]:AMU.LMU_DAM:REG_MONITOR_TEST
5.11 ESM[SW]:CCU6:CCU6_CAPTURE_MON_BY_GPT12
5.12 ESM[SW]:CCU6:CCU6_GPT12_MONITORING
5.13 ESM[SW]:CIF.RAM:REG_MONITOR_TEST
5.14 ESM[SW]:CLOCK:PLAUSIBILITY
5.15 ESM[SW]:CONVCTRL:ALARM_CHECK
5.16 ESM[SW]:CONVCTRL:CONFIG_CHECK
5.17 ESM[SW]:CPU.DCACHE:REG_MONITOR_TEST
5.18 ESM[SW]:CPU.DLMU:REG_MONITOR_TEST
5.19 ESM[SW]:CPU.DSPR:REG_MONITOR_TEST

How to implement these TC3xx Safety Mechanisms ?

hitex
EMBEDDED TOOLS & SOLUTIONS

✓ Yes, several safety features and test capabilities are realized in hardware.

✓ Yes, some tests (e.g., PBIST, LBIST) are implemented in hardware.

⚠ **But still a lot Assumptions of Use (ESM/SMC) needs to be implemented!**

- You have to implement, configure, trigger and to evaluate startup tests.
- You have to implement, configure, execute and evaluate runtime tests (SFR & Die Temperature Sensor tests etc.).
- You have to implement, configure and handle functional and window watchdog like external TLF35584 and the AURIX$^{\text{TM}}$ internal Safety Watchdog.
- You have to follow the development process given by your Safety Standard.
- … and much more

✓ And that’s what the SafeTpack is designed for …

Overview TC3xx Startup Safety Mechanisms

APPLICATION SW STARTUP:

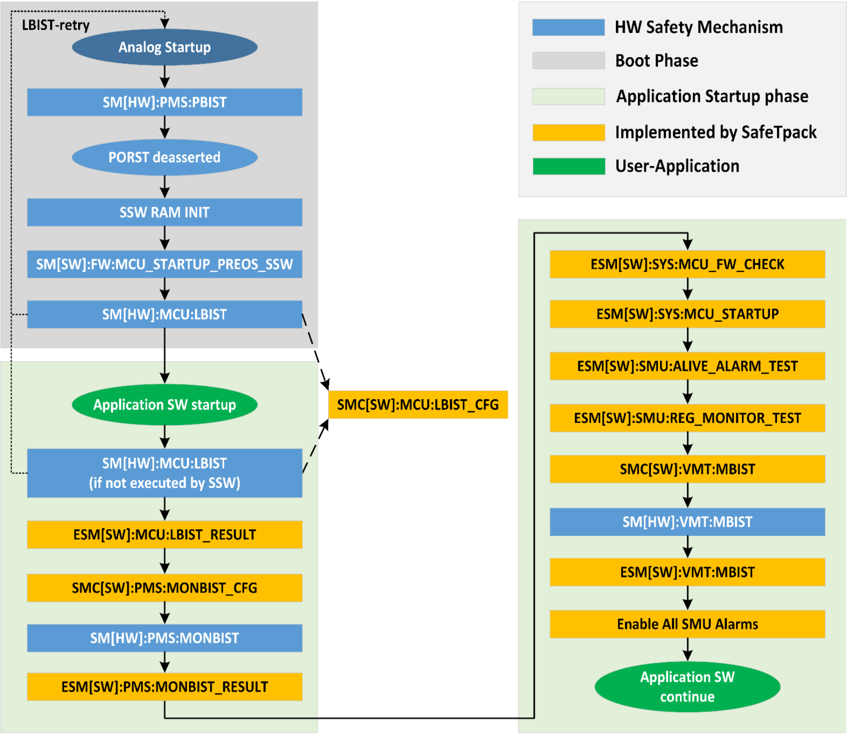
During Application SW startup, the **user is responsible** for executing a number of operations for ensuring the absence of latent faults and correctly initialize the MCU before starting the runtime execution.

Application SW startup

could contain a bootloader / boot-manager.

Application SW continue

could contain the customer application startup with driver initialization and so on.



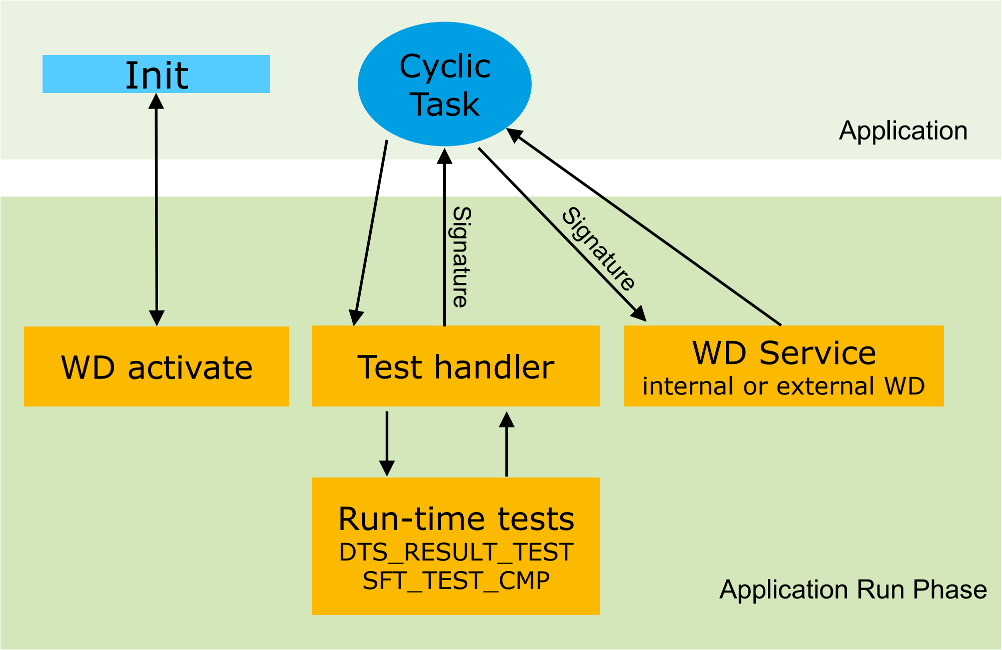
🟦 HW Safety Mechanism
⬜ Boot Phase
🟩 Application Startup phase
🟨 Implemented by SafeTpack
🟩 User-Application

LBIST-retry
Analog Startup
SM[HW]:PMS:PBIST
PORST deasserted
SSW RAM INIT
SM[SW]:FW:MCU_STARTUP_PREOS_SSW
SM[HW]:MCU:LBIST
Application SW startup
SM[HW]:MCU:LBIST (if not executed by SSW)
SMC[SW]:MCU:LBIST_CFG
ESM[SW]:MCU:LBIST_RESULT
SMC[SW]:PMS:MONBIST_CFG
SM[HW]:PMS:MONBIST
ESM[SW]:PMS:MONBIST_RESULT
ESM[SW]:SYS:MCU_FW_CHECK
ESM[SW]:SYS:MCU_STARTUP
ESM[SW]:SMU:ALIVE_ALARM_TEST
ESM[SW]:SMU:REG_MONITOR_TEST
SMC[SW]:VMT:MBIST
SM[HW]:VMT:MBIST
ESM[SW]:VMT:MBIST
Enable All SMU Alarms
Application SW continue

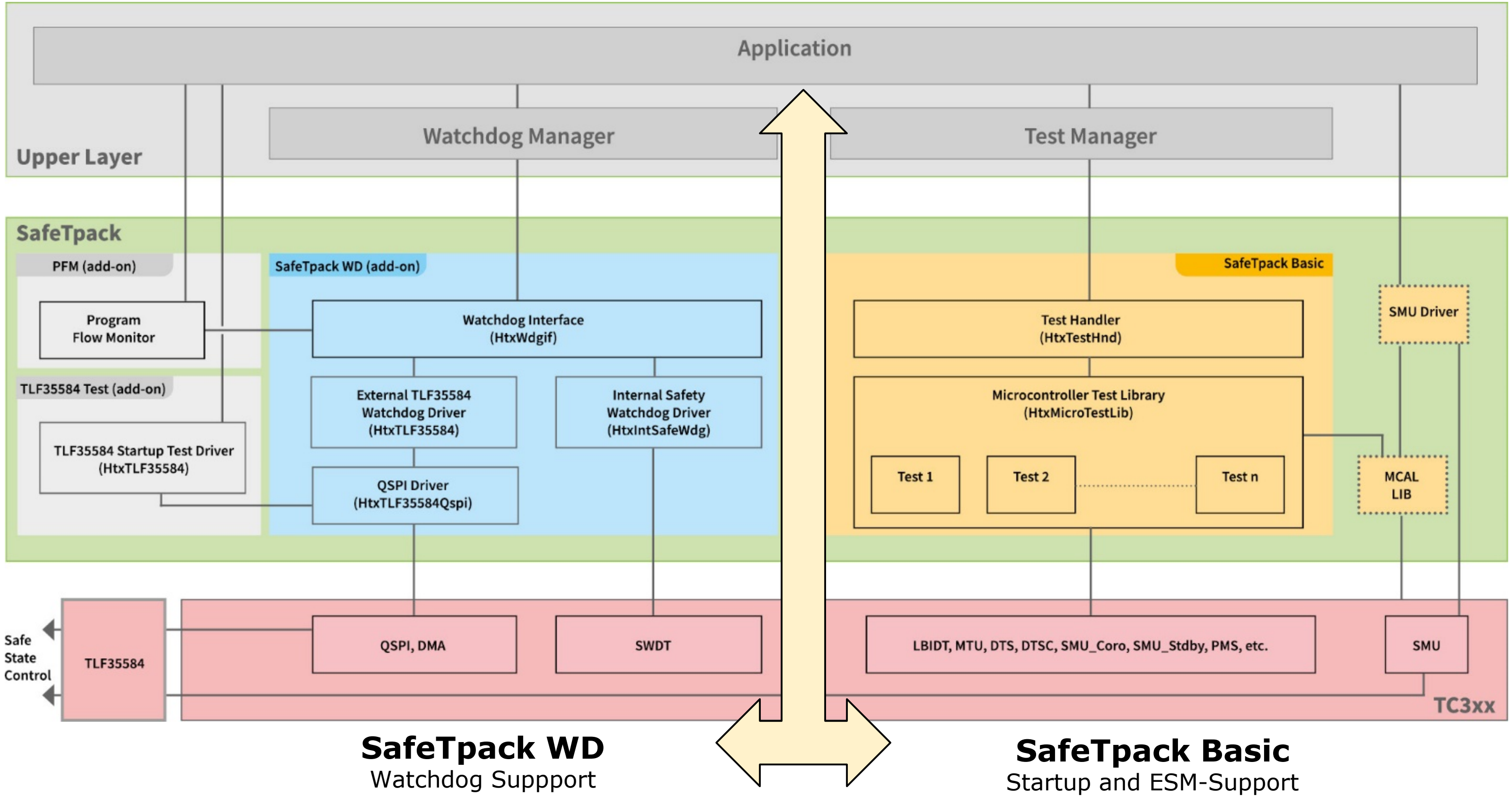
[Derived from TC3xx Safety Manual v1.10 Figure 7]

Overview TC3xx Watchdog Safety Mechanisms

- SafeTpack provides services for internal and external Watchdog
- Support of Saftey Mechanisms (SM) at runtime like
  - die temperature sensor (DTS) or
  - special function registers (SFR)



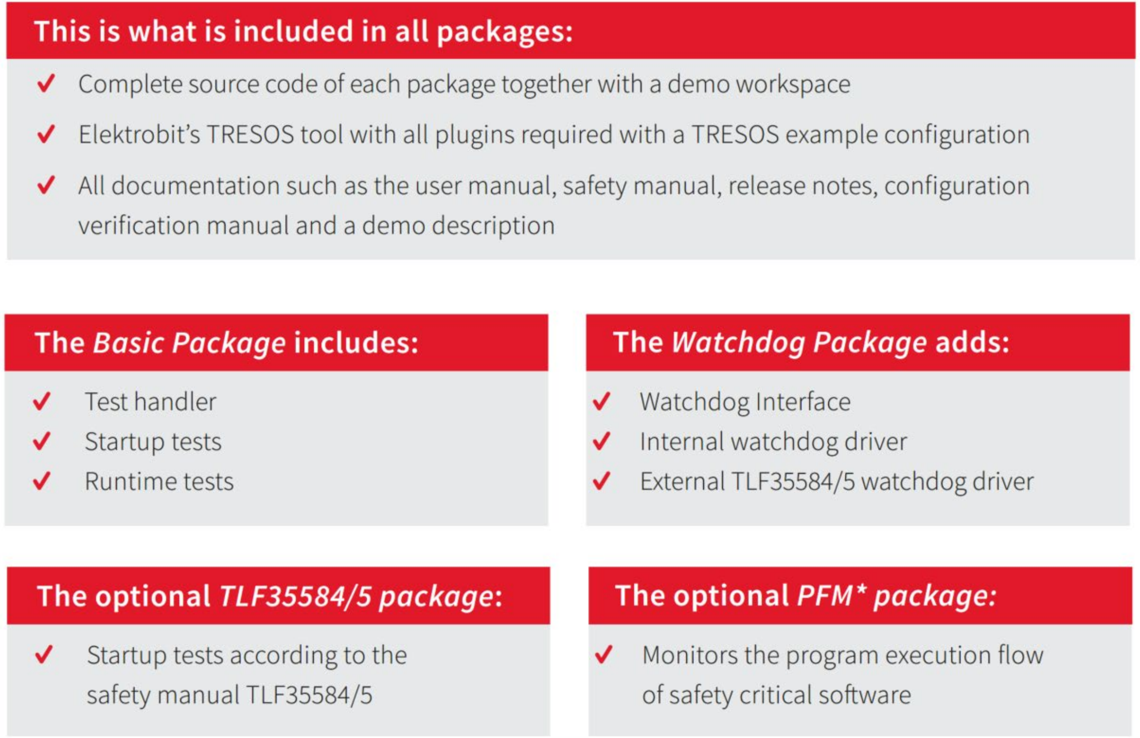
SafeTpack Architecture / Two Main Packages


Application
Upper Layer
Watchdog Manager
Test Manager
SafeTpack
PFM (add-on)
Program Flow Monitor
TLF35584 Test (add-on)
TLF35584 Startup Test Driver (HtxTLF35584)
SafeTpack WD (add-on)
Watchdog Interface (HtxWdgif)
External TLF35584 Watchdog Driver (HtxTLF35584)
Internal Safety Watchdog Driver (HtxIntSafeWdg)
QSPI Driver (HtxTLF35584Qspi)
SafeTpack Basic
Test Handler (HtxTestHnd)
Microcontroller Test Library (HtxMicroTestLib)
Test 1
Test 2
Test n
SMU Driver
MCAL LIB
Safe State Control
TLF35584
QSPI, DMA
SWDT
LBIDT, MTU, DTS, DTSC, SMU_Coro, SMU_Stdby, PMS, etc.
SMU
TC3xx

SafeTpack WD
Watchdog Suppport

SafeTpack Basic
Startup and ESM-Support

Modules Overview



This is what is included in all packages:

- ✓ Complete source code of each package together with a demo workspace
- ✓ Elektrobit's TRESOS tool with all plugins required with a TRESOS example configuration
- ✓ All documentation such as the user manual, safety manual, release notes, configuration verification manual and a demo description

The *Basic Package* includes:

- ✓ Test handler
- ✓ Startup tests
- ✓ Runtime tests

The *Watchdog Package* adds:

- ✓ Watchdog Interface
- ✓ Internal watchdog driver
- ✓ External TLF35584/5 watchdog driver

The optional *TLF35584/5 package*:

- ✓ Startup tests according to the safety manual TLF35584/5

The optional *PFM* package*:

- ✓ Monitors the program execution flow of safety critical software

- SafeTpack`s modular system makes it easy to customize and supplement individual functions

- Depending on your precise requirements, different SafeTpack packages can be selected

SafeTpack with and without AUTOSAR

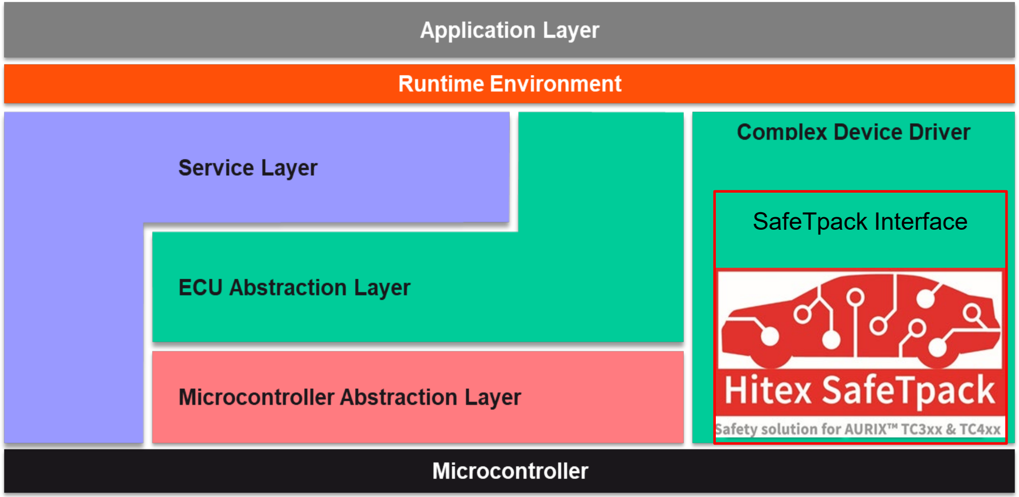
- A2G SafeTpack can be used in AUTOSAR environments

  → SafeTpack acts as an AUTOSAR complex device driver

- SafeTpack is 100% compatible with the Infineon MCAL

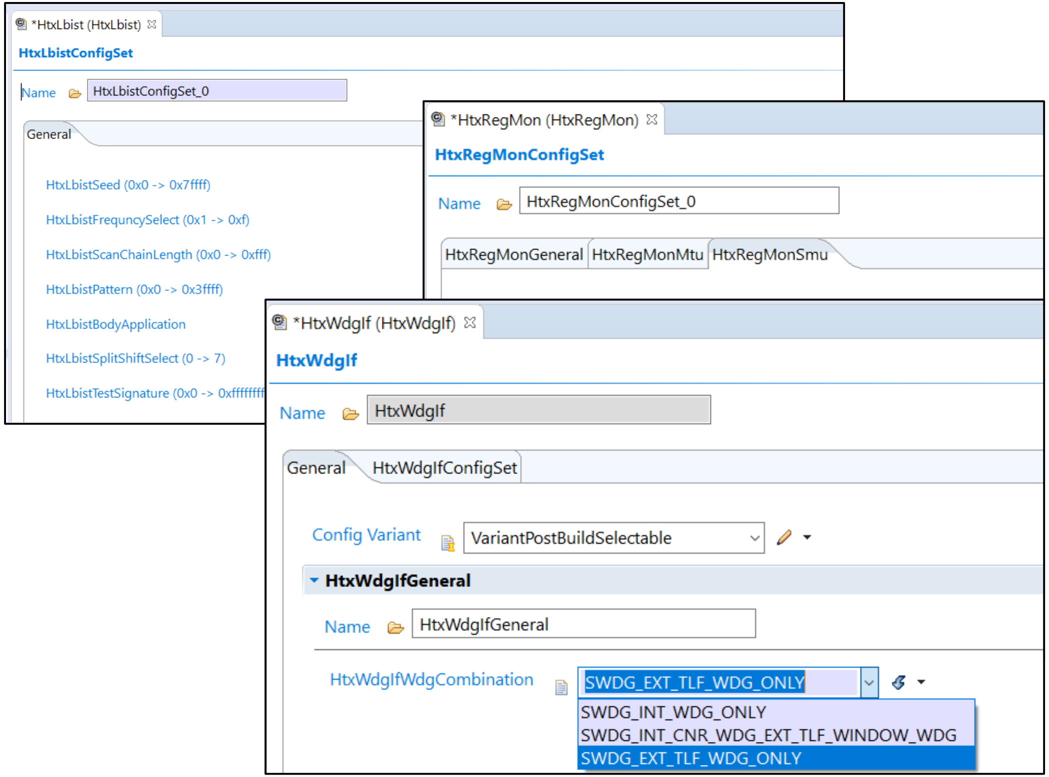
- In Non-AUTOSAR environments SafeTpack can still be used independently

  → For PXROS HR environments SafeTpack implementations are available.



Fully configurable with Tresos Studio (included)

- SafeTpack is fully configurable with Elektrobit Tresos Studio
- That`s the same configuration Tool as for MCAL drivers
- Individual tests and the test sequences are configurable using EB Tresos tool
- EB Tresos Studio is part of the delivery package



*HtxLbist (HtxLbist)

HtxLbistConfigSet

Name: HtxLbistConfigSet_0

General

HtxLbistSeed (0x0 -> 0x7ffff)

HtxLbistFrequncySelect (0x1 -> 0xf)

HtxLbistScanChainLength (0x0 -> 0xfff)

HtxLbistPattern (0x0 -> 0x3ffff)

HtxLbistBodyApplication

HtxLbistSplitShiftSelect (0 -> 7)

HtxLbistTestSignature (0x0 -> 0xffffffff

*HtxRegMon (HtxRegMon)

HtxRegMonConfigSet

Name: HtxRegMonConfigSet_0

HtxRegMonGeneral | HtxRegMonMtu | HtxRegMonSmu

*HtxWdgIf (HtxWdgIf)

HtxWdgIf

Name: HtxWdgIf

General | HtxWdgIfConfigSet

Config Variant: VariantPostBuildSelectable

HtxWdgIfGeneral

Name: HtxWdgIfGeneral

HtxWdgIfWdgCombination: SWDG_EXT_TLF_WDG_ONLY

SWDG_INT_WDG_ONLY
SWDG_INT_CNR_WDG_EXT_TLF_WINDOW_WDG
SWDG_EXT_TLF_WDG_ONLY

SafeTpack - Documents & Resources

Confidential

Hitex SafeTpack

Safety solution for AURIX™ TC3xx & TC4xx

SafeTpack

AURIX_TC3XX

User Manual

Hitex (UK) Ltd Engineering Services

Manual

Hitex UK Engineering Services

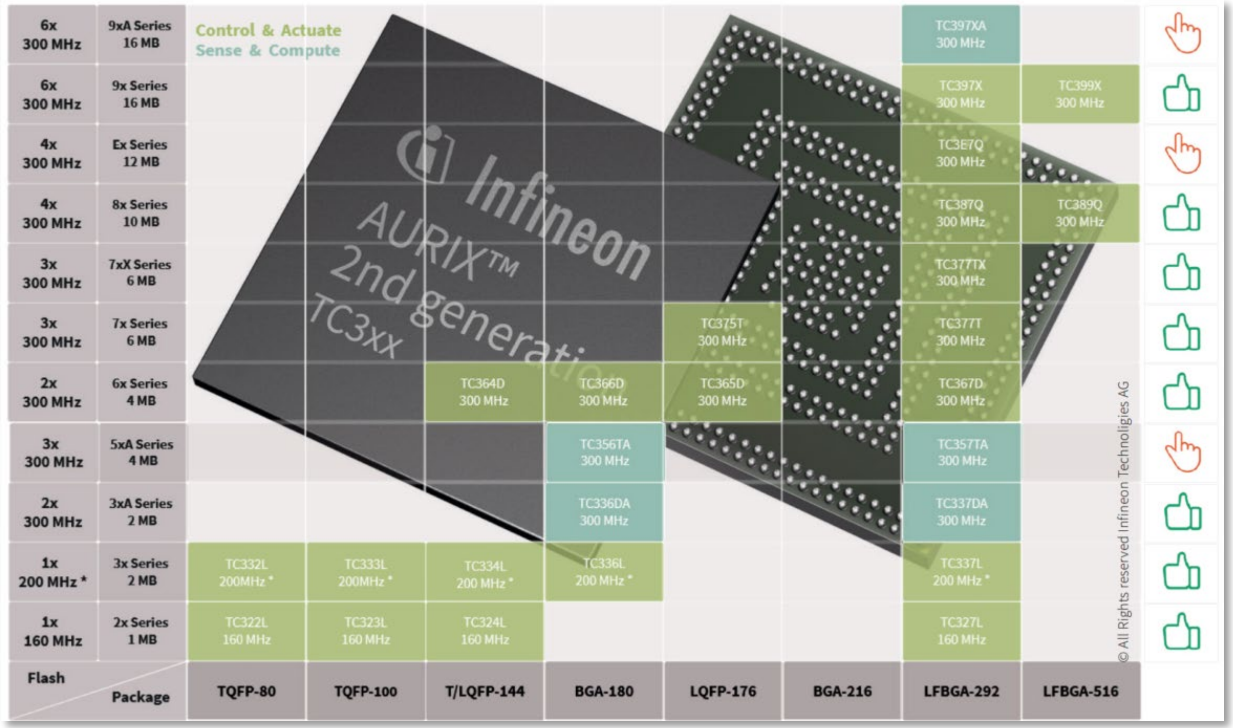
Hitex UK Engineering Services

Hitex UK Engineering Services

All documents are inside

- Package delivery
  - □ Source Code of SafeTpack
  - □ Demo Workspace
  - □ EB Tresos & plug-ins
  - □ Example Tresos configuration
  - □ Democode
- Documents for SafeTpack
  - □ User Manual
  - □ Release Notes
  - □ Configuration Verification Manual
  - □ Demo Description
  - □ SafeTpack Validation Report (on request)
  - □ Safety Case Report (on request)

Most of AURIX^{TM} TC3xx devices and derivatives are supported


Control & Actuate
Sense & Compute
Infineon
AURIX™
2nd generation
TC3xx
© All Rights reserved Infineon Technoligies AG

	Flash / Package	TQFP-80	TQFP-100	T/LQFP-144	BGA-180	LQFP-176	BGA-216	LFBGA-292	LFBGA-516	
6x 300 MHz	9xA Series 16 MB							TC397XA 300 MHz		☝
6x 300 MHz	9x Series 16 MB							TC397X 300 MHz	TC399X 300 MHz	👍
4x 300 MHz	Ex Series 12 MB							TC3E7Q 300 MHz		☝
4x 300 MHz	8x Series 10 MB							TC387Q 300 MHz	TC389Q 300 MHz	👍
3x 300 MHz	7xX Series 6 MB							TC377TX 300 MHz		👍
3x 300 MHz	7x Series 6 MB					TC375T 300 MHz		TC377T 300 MHz		👍
2x 300 MHz	6x Series 4 MB			TC364D 300 MHz	TC366D 300 MHz	TC365D 300 MHz		TC367D 300 MHz		👍
3x 300 MHz	5xA Series 4 MB				TC356TA 300 MHz			TC357TA 300 MHz		☝
2x 300 MHz	3xA Series 2 MB				TC336DA 300 MHz			TC337DA 300 MHz		👍
1x 200 MHz *	3x Series 2 MB	TC332L 200MHz *	TC333L 200MHz *	TC334L 200 MHz *	TC336L 200 MHz *			TC337L 200 MHz *		👍
1x 160 MHz	2x Series 1 MB	TC322L 160 MHz	TC323L 160 MHz	TC324L 160 MHz				TC327L 160 MHz		👍

👍 supported devices

☝ Not supported yet
please contact us

SafeTpack: future ready – what`s coming

- Maintenance Release
  - Compatibility to MCAL 2.0.0, Tasking 6.3r1.p2, HighTec GNU 4.9.4.1, TRESOS V26.2
  - Support for all devices in one installation package
  - Consideration of customer issues occurred in first releases

- Implementation of new watchdog drivers e.g. TLF35585 or others

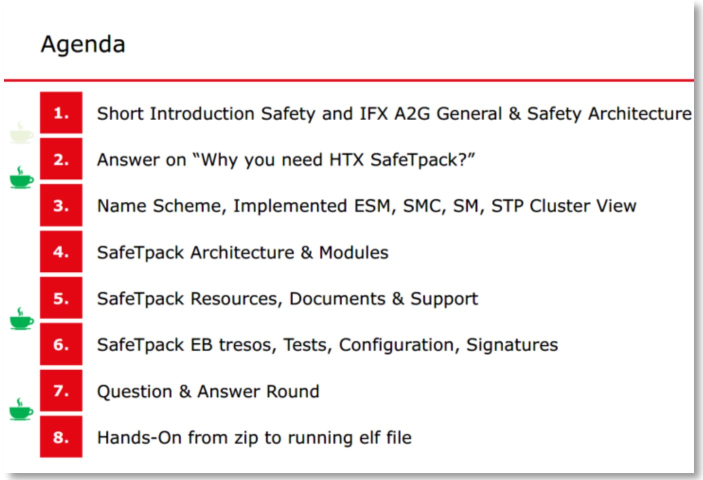
- Implementation of further ESMs & SMCs! Missing ESMs ? Just, tell us!

- AURIX^{TM} TC4xx support on our roadmap

Our services around SafeTpack and Functional Safety

- Web based training for SafeTpack integrators:
  - first-hand information and valuable hints on safe and reliable integration
  - Highly recommended for fast implementation

- Project-related consulting
  - AURIX^{TM} related
  - Functional Safety & Security



Agenda

1. Short Introduction Safety and IFX A2G General & Safety Architecture
2. Answer on "Why you need HTX SafeTpack?"
3. Name Scheme, Implemented ESM, SMC, SM, STP Cluster View
4. SafeTpack Architecture & Modules
5. SafeTpack Resources, Documents & Support
6. SafeTpack EB tresos, Tests, Configuration, Signatures
7. Question & Answer Round
8. Hands-On from zip to running elf file

- SafeTpack integration into your application as a full service
- SafeTpack customizing
- Hard- and software development in the context of AURIX^{TM} and functional safety
- Embedded Testing & Verification

Summary: Main advantages of SafeTpack

- ✓ Developed according to ISO 26262-2018
- ✓ Similar to the AURIX^{TM} TC2xx SafeTLib: Easy handling, no changeover
- ✓ Modular: Only pay what is used
- ✓ Comes with a demo application
- ✓ Included configuration tool, to set up all parameters individually
- ✓ Can be used either with or without AUTOSAR
- ✓ 100% compatible with the Infineon MCAL but can still be used independently
- ✓ Includes Elektrobit’s Tresos tool to configure SafeTpack
- ✓ Provides drivers and watchdog interface for Infineon TLF35584/85 and AURIX^{TM} Internal Safety Watchdog including signature handling
- ✓ SafeTpack saves time, money and nerves

AURIX^{TM} Knowledge Lab 2021

Any questions?

EBVElektronik | An Avnet Company |

escrypt SECURITY. TRUST. SUCCESS.

hitex EMBEDDED TOOLS & SOLUTIONS

infineon

TASKING

Thank you for your attention! Please contact me …

Michael Weiß
Senior Account Manager
Embedded Solutions

ichael.weiss@hitex.de