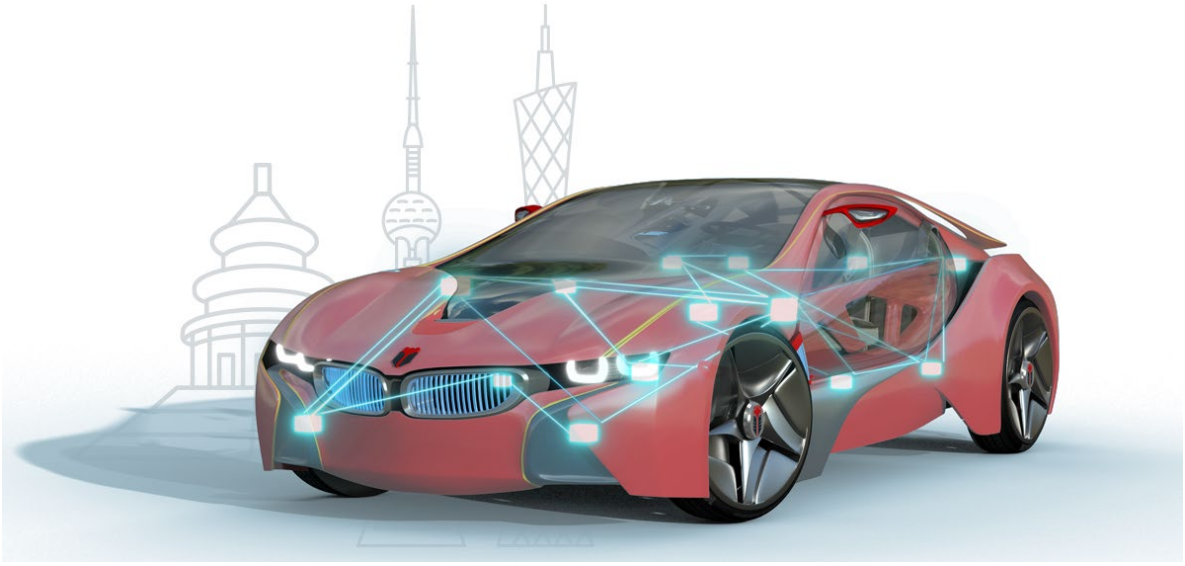
知从木牛 SAFETYLIBRARY 英飞凌 TC2XX 产品手册

ZC.MUNIU SAFETYLIBRARY PRODUCT MANUAL BASED ON INFINEON TC2XX

知从木牛基础软件平台功能安全库

ZC.MuNiu Basic Software Platform Safety Library



知从木牛 SAFETYLIBRARY 英飞凌 TC2XX 产品手册

ZC.MUNIU SAFETYLIBRARY PRODUCT MANUAL BASED ON INFINEON TC2XX

知从木牛基础软件平台功能安全库

ZC.MuNiu Basic Software Platform Safety Library

1 功能概述 FUNCTIONAL OVERVIEW

TC2XX Safety Library 用于帮助客户实现基于 AURIX TC2XX 平台的功能安全要求。Safety Library 具有高扩展性，可以根据不同的客户项目要求进行配置和再开发，最终满足客户的功能安全需求。

The TC2XX Safety Library is designed to assist customers in achieving functional safety requirements based on the AURIX TC2XX platform. The Safety Library is highly scalable and can be configured and redeveloped according to different customer project requirements, ultimately meeting the customers' functional safety requirements.

TC2XX Safety Library 用于实现 TC2XX 系列的软件安全机制，包括 MCU 内部模块的测试和硬件安全机制的驱动。

The TC2XX Safety Library is used to implement the software safety mechanisms of the TC2XX, including the testing of internal MCU modules and the driving of hardware safety mechanisms.

2 应用领域 APPLICATION FIELD

TC2XX Safety Library 可应用于有功能安全等级需求的控制器。例如：

The TC2XX Safety Library can be applied to controllers that require functional safety levels. For example:

- 电机控制器
  Motor Controller
- 电池管理系统(BMS)
  Battery Management System
- 底盘系统应用
  Chassis System Applications
- 电气稳定控制(ESC)
  Electronic Stability Control
- 电动助力转向(EPS)
  Electric Power Steering

通过将 Safety Library 集成到基于 TC2XX 的控制器中，可达到 ISO26262 ASIL-D 的等级要求。

By integrating the Safety Library into the control based on TC2XX, it is possible to meet the ISO 26262 ASIL-D level requirements.

配置环境 Configuration Environment	
Hardware (Chip)	INFINEON SAK-TC2XXT-64F200W CA
Compilers Supported	HighTec 4.6.6.1/Tasking v4.2r2
Evaluation Hardware	TriBoard TC2X5
Debugger	Lauterbach (Trace32 R.2018.02) Isystem (IC5700)
Configuration Tools	Muniu_v5.1.3
Configuration Environment	Win7 64bit

Hightec 4.6.6.1 编译器选项 Hightec 4.6.6.1 Compiler Options	
编译选项 Complier options	-fno-common -fno-short-enums -Os -g2 -W -Wall -Wextra -Wdiv-by-zero -Warray-bounds -Wcast-align -Wignored-qualifiers -Wformat -Wformat-security -save-temps=obj -DBRS_DERIVATIVE_TC27X -fno-builtin -iquote -Wl,--gc-sections -Wl,--mem-holes -Wl,--no-warn-flags -Wl,--cref -fshort-double -mcpu=tc27xx -mversion-info -std=c99 -maligned-data-sections
链接选项 Linker Options	-nostartfiles -T"..\SafetyLibrary.ld" @iROM.objectlist -mcpu=tc27xx -Wl,--mem-holes -Wl,--warn-orphan

Taskingv4.2r2 编译器选项 Taskingv4.2r2 Compiler Options	
编译选项 Complier options	-Ctc27x --lsl-core=vtc --iso=99 --language=-gcc,-volatile,+strings --switch=auto --align=4 --no-clear --default-near-size=0 --default-a0-size=0 --default-a1-size=0 -O2 --tradeoff=4 --compact-max-size=200 -g --source
链接选项 Linker Options	-Ctc27x --lsl-core=vtc -l"D:\Git\xxx" -Wl-o"${PROJ}.hex":IHEX:4 -Wl-o"${PROJ}.sre":SREC:4 --hex-format=s -Wl-DMCU_SMALL_ENDIAN=1 "../xxx_SW.lsl" -Wl-OtxyCL -Wl--map-file="${PROJ}.mapxml":XML -Wl-mcrfiklsmnoduq -Wl--error-limit=42 -g

4 开发背景 DEVELOPMENT BACKGROUND

目前，汽车上的电子电气架构越来越复杂，对汽车电子的安全性要求也越来越高，为了满足汽车的安全性需求，汽车功能安全越来越受到重视。提到功能安全，大家首先想到的是功能安全的标准 ISO26262。其中，ISO 26262-5(2018) Clause 8 中介绍了 2 个度量：Single-point fault metric(单点故障度量)和 Latent-fault metric(潜伏故障度量)。根据不同的 ASIL 等级要求，单点故障度量和潜伏故障度量需要达到相应的等级。

Currently, the electronic and electrical architecture of automobiles is becoming increasingly complex, and the safety requirements for automotive electronics are also rising. To meet the safety requirements of automobiles, functional safety is gaining more attention. When it comes to functional safety, the first thing that comes to mind is the functional safety standard ISO 26262. In particular, ISO 26262-5(2018) Clause 8 introduces two metrics: Single-point fault metric (single-point fault metric) and Latent-fault metric (latent fault metric). Depending on the required ASIL level, the single-point fault metric and latent fault metric must meet the corresponding levels.

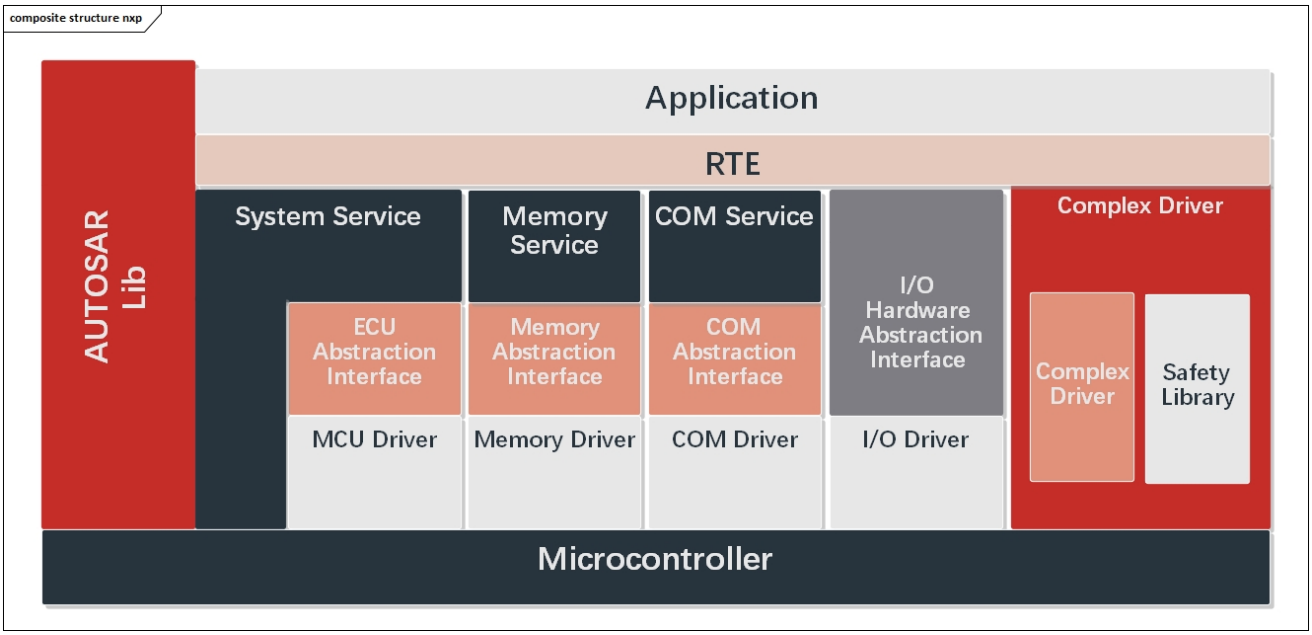
对于微控制器(MCU，以下简称 MCU)，在电子电气系统中，作为 SEooC(safety element out of context)进行设计开发。MCU 为了满足以上提到的 2 个度量要求，需要实现相应的安全机制。而安全机制可以分配到硬件和软件模块中。MCU 的 Safety Frame 安全库就是实现分配到软件上的安全机制。

For microcontrollers (MCU, referred to as MCU below), within the electronic and electrical system, they are designed and developed as SEooC (safety element out of context). To meet the aforementioned metric requirements, MCUs need to implement corresponding safety mechanisms. These safety mechanisms can be allocated to both hardware and software modules. The Safety Frame safety library for MCUs is the implementation of safety mechanisms allocated to software.

	ASIL B	ASIL C	ASIL D
Single-point fault metric	≥90 %	≥97 %	≥99 %

	ASIL B	ASIL C	ASIL D
Latent-fault metric	≥60 %	≥80 %	≥90 %

5.1 产品特点 Product Feature



- 可作为复杂驱动集成到 AUTOSAR 中

  Can be integrated as a complex driver into AUTOSAR .

- 满足控制器 ASIL-D 需求

  Meet the ASIL-D requirements of the controller.

- 可集成到非 AUTOSAR 软件架构中

  Can be integrated into non-AUTOSAR software architecture.

- 高扩展性：每个模块实现可配置性，满足不同的客户需求

  High scalability: Each module is configurable to meet different customer requirements.

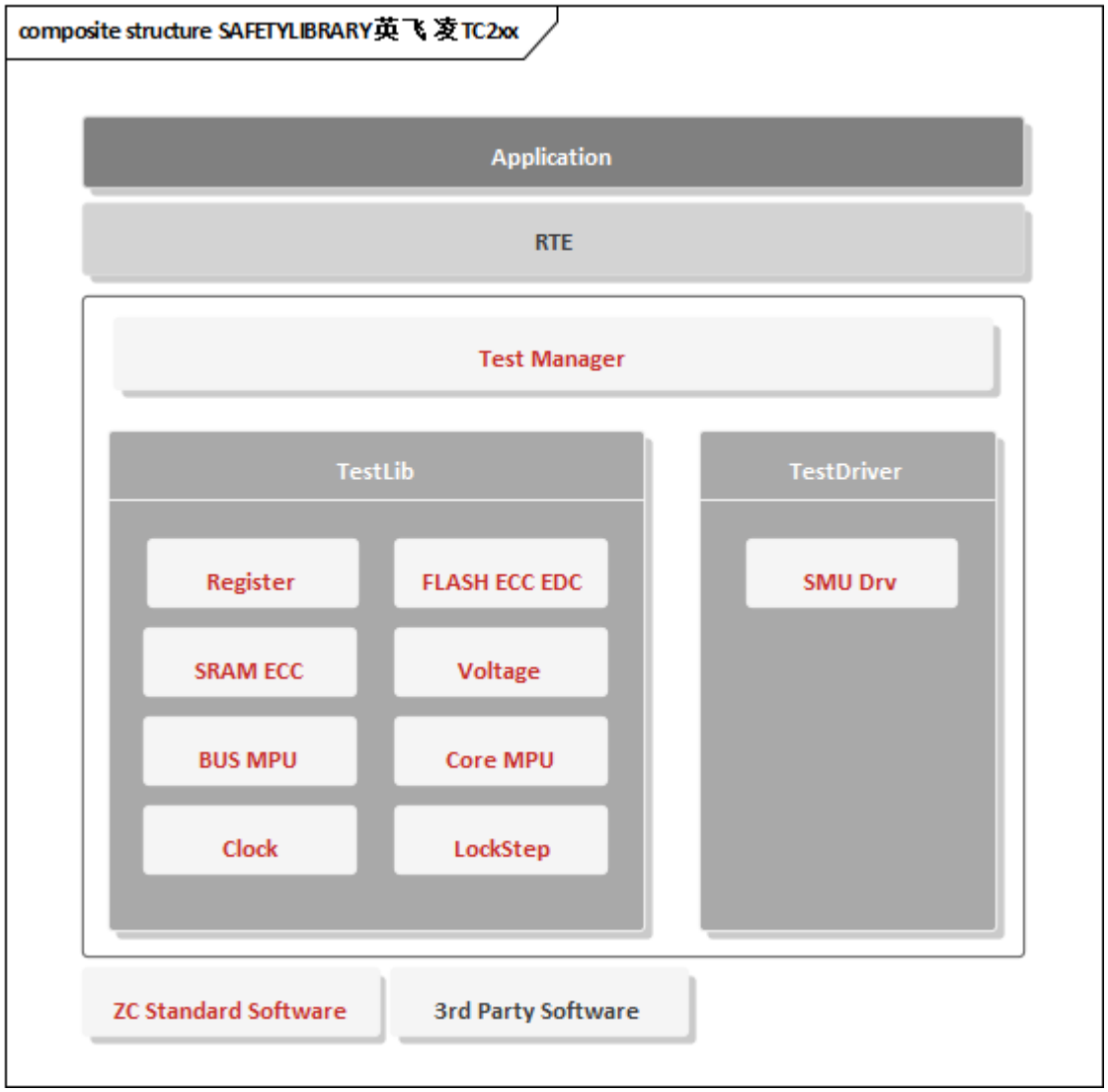
- 支持多核测试

  Support multi-core testing

- Safety Library 内部程序流监控

  Internal Program Flow Monitoring of the Safety Library.

5.2 软件架构 Software Architecture



知从模板 TC2XX SafetyLibrary 功能列表：

TC2XX SafetyLibrary Feature List:

模块 Module	子模块 Sub-module	描述 Description
	Lockstep CPU Comparator Alarm Test	检测 Lockstep 逻辑是否正常 Check if the Lockstep logic is functioning correctly.
	CPU Trap Test	检测 Trap 功能，检测是否进入相应的 Trap. Test the Trap function to see if it enters the appropriate Trap state.

测试库 Test Library	Voltage Monitors Test	检测 MCU 内部供电过压和欠压监控功能是否正常 Verify the over-voltage and under-voltage monitoring functions of the MCU's internal power supply are operating normally.
	Clock Monitor Test	检测时钟监控功能是否正常 Check if the clock monitoring function is working properly.
	SRAM ECC Test	检测 SRAM ECC 和 EDC 逻辑是否正常 Test the SRAM ECC (Error-Correcting Code) and EDC (Error Detection Code) logic for correctness.
	LMU ECC Monitor Test	检测 LMU ECC 和 EDC 逻辑是否正常 Verify the LMU (Local Memory Unit) ECC and EDC logic for correctness.
	SRAM Address Monitor Test	检测 SRAM 的错误地址监控功能是否正常 Check if the SRAM's erroneous address monitoring function is operating correctly.
	SRAM Error Tracking Test	检测 SRAM 错误追踪功能是否正常 Test the SRAM error tracking function for proper operation.
	PFLASH ECC Test	检测 PFLASH ECC 和 EDC 逻辑是否正常 Verify the PFLASH ECC and EDC logic for correctness.
测试库 Test Library	PFLASH Address Error Detection Test	检测 PFLASH 地址的 ECC 和 EDC 逻辑是否正常 Check the ECC and EDC logic of the PFLASH address for normal operation.
	PFLASH ECC Error Detection Logic Comparator Test	检测 PFLASH 的 EDC 比较逻辑是否正常 Test the EDC comparison logic of the PFLASH for normal operation.
	PFLASH Error Tracking Test	检测 PFLASH 错误追踪功能是否正常

测试库 Test Library		Verify the PFLASH error tracking function for proper operation.
	SRI Error Detection Test	检测 SRI 总线传输数据的 EDC 错误 Detect EDC errors in SRI (Serial Communication Interface) bus data transmission.
	SRI Error Handle Test	检测 SRI 总线传输协议错误 Detect protocol errors in SRI bus transmission.
	SPB Error Handle Test	检测 SPB 错误捕获功能是否正常 Check if the SPB (Standard Programmable Bus) error capture function is operating normally.
	SPB Timeout Test	检测 SPB 总线超时未响应错误功能是否正常 Verify the SPB bus timeout and non-response error function is working correctly.
	Register Monitor Test	检测静态配置寄存器是否被篡改 Detect if the static configuration registers have been tampered with.
	Register Access Protection Test	检测 SRI 和外设寄存器访问保护功能是否正常 Verify the access protection function of SRI and peripheral registers is working properly.
	CPU Memory Protection Test	检测 CPU MPU 功能是否正常 Check if the CPU Memory Protection Unit (MPU) function is operating normally.
	CPU Bus MPU Test	检测 CPU BUS MPU 功能是否正常 Verify the CPU BUS MPU function is working correctly.
	CPU Register Access Protection Test	检测 CPU 寄存器访问保护功能是否正常 Test the CPU register access protection function for proper operation.
	AURIX Watchdogs test	检测 AURIX 内部看门狗功能是否正常

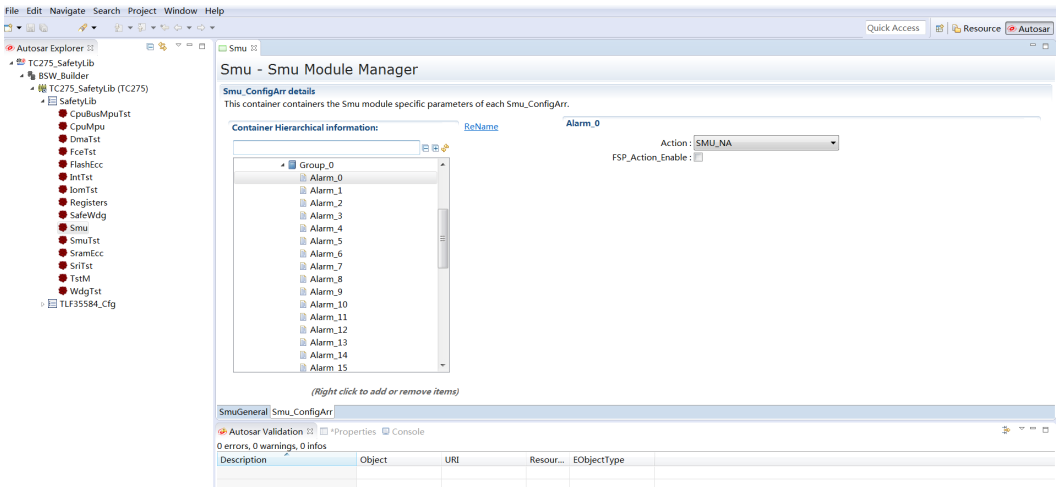
		Verify the internal watchdog function of AURIX is functioning correctly.
	Reset Stable State Check	MCU 复位后，检测 MCU 是否达到稳定状态 After MCU reset, check if the MCU has reached a stable state.
	SBCU Configuration Check	在复位或软件初始化后，软件需要检查总线控制单元的配置是否正确 After reset or software initialization, the software needs to check if the configuration of the bus control unit is correct.
	SMU Fault Signaling Protocol Test	检测 Fault Signaling Protocol 的功能是否正常 Test the functionality of the Fault Signaling Protocol.
	SMU Initialization Check	检测 SMU 初始化配置是否正常 Verify the initialization configuration of the SMU is correct.
	SMU Configuration Lock Test	检测 SMU 配置锁功能是否正常 Check if the SMU configuration lock function is operating normally.
	SMU Alarms Test	检测 SMU 的相应 Alarm 触发是否正常 Verify if the SMU's corresponding Alarm triggers are operating correctly.
	SMU Test	检测 SMU 的相应 Action 触发是否正常 Test if the SMU's corresponding Action triggers are functioning properly.
	SMU Recovery Timer Test	检测 SMU 的 Recovery 定时器功能是否正常 Check if the SMU's Recovery timer function is working correctly.
	Non-Lockstep CPU MPU Initialization Check	对于非锁步的内核使用 CPU MPU，检测 MPU 的配置在初始化时或者每次 CPU MPU 更改之后的配置是否正确

		For non-lockstep cores using the CPU MPU, verify the MPU configuration is correct during initialization or after any change to the CPU MPU.
	Non-Lockstep CPU BUS MPU Initialization Check	对于非锁步的内核使用 BUS MPU，检测 MPU 的配置在初始化时或者每次 BUS MPU 更改之后的配置是否正确 For non-lockstep cores using the BUS MPU, verify the MPU configuration is correct during initialization or after any change to the BUS MPU.
	LMU BUS MPU Initialization Check	对于非锁步的内核使用 LMU BUS MPU，检测 MPU 的配置在初始化时或者每次 LMU BUS MPU 更改之后的配置是否正确 For non-lockstep cores using the LMU BUS MPU, verify the MPU configuration is correct during initialization or after any change to the LMU BUS MPU.
	Watchdog Timer Initialization Check	检测 Watchdog 定时器的配置是否正确 Check if the Watchdog timer configuration is correct.
	Interrupt Router Error Detection Code Test	检测中断 SRC 寄存器 ECC 功能是否正常 Verify the ECC function of the interrupt SRC (Source) register is operating normally.
	Flexible CRC Engine (FCE) Test	检测 FCE 功能是否正常 Test the FCE (Flash Correction Engine) function for proper operation.
	DMA Cyclic Redundancy Check Test	检测 DMA 传输数据的 CRC 功能是否正常 Verify the CRC (Cyclic Redundancy Check) function for DMA (Direct Memory Access) data transfer is working correctly.
	LMU Bus MPU Test	检测 LMU BUS MPU 功能是否正常 Check if the LMU BUS MPU function is operating normally.

	LMU Register Access Protection Test	检测 LMU 寄存器访问保护功能是否正常 Verify the access protection function of the LMU registers is working properly.
	IOM test	检测输入输出监控功能是否正常 Test the input/output monitoring function for proper operation.
	Peripheral SRAM ECC Test	检测 SRAM ECC 逻辑是否正常 Verify the SRAM ECC logic is functioning correctly.
	SRAM Address Monitor Test	检测外设 SRAM 的错误地址监控功能是否正常 Check if the erroneous address monitoring function of the peripheral SRAM is operating correctly.
	Peripheral SRAM Error Tracking Test	检测外设 SRAM 错误追踪功能是否正常 Test the error tracking function of the peripheral SRAM for proper operation.
	EVR Configuration Check	检测 EVR 的硬件状态配置寄存器的值是否和实际硬件配置一致 Verify that the values of the EVR (Electrical Voltage Regulator) hardware status configuration registers match the actual hardware configuration.
	End-to-End Communication Protection	CAN/Eth/ERAY/HSSL 等通信协议实现 End-to-End 通信保护功能 Implement End-to-End communication protection for communication protocols such as CAN, Ethernet, ERAY, and HSSL.
	QSPI Protection	QSPI 通信协议实现 End-to-End 通信保护功能 Implement End-to-End communication protection for the QSPI communication protocol.
	LMU SRAM Data Path Test	检测 LMU SRAM 数据访问路径是否正常，Run 阶段周期检测

		Check if the LMU SRAM data access path is normal, with periodic detection during the Run phase.
驱动库 Driver Library	SMU Driver	实现 SMU 的初始化配置、故障处理、FSP 配置、配置锁检测 Implement the initialization configuration of SMU, fault handling, FSP configuration, and configuration lock detection.
测试管理 Test Manager	测试管理模块	管理 Safety Library 测试库和驱动库 Manage the Safety Library test library and driver library.

5.3 配置工具 Configuration Tool



为了满足客户的不同项目需求，提高 Safety Library 的扩展性，TC2XX Safety Library 实现了各个模块可配置性，并且实现了 Safety Library 的配置工具。客户可根据不同需求，在配置工具上完成 Safety Library 各个模块的配置工作，可生成配置代码文件，将生成的配置文件集成到工程中即可。

To meet the diverse project requirements of customers and enhance the scalability of the Safety Library, the TC2XX Safety Library has implemented the configurability of each module and has developed a configuration tool for the Safety Library. Customers can complete the configuration of various modules of the Safety Library using the configuration tool according to different requirements. They can generate configuration code files, and integrate the generated configuration files into the project.

5.4 软件测试 Software Testing

测试环境 Test Environment	
静态代码 QAC **Static Code QAC**	7.2 R MISRA-C：2004
动态 Tessy **Dynamic Tessy**	4.2.8
Evaluation Hardware	TriBoard TC2x5 V2.0
Configuration Environment	Win7 64bit

6 过程文档 PROCESS DOCEMENTATION

开发流程 Development Process	文档描述 Document Description
需求收集 Requirement Collection	客户的需求文档 Customer Requirements Document
软件需求分析 Software Requirement Analysis	软件的需求分析 Software Requirements Analysis
	需求分析规格书 Requirements Analysis Specification
	软件需求追踪表 Software Requirements Traceability Matrix
	客户的问题沟通表 Customer Issue Communication Form
软件架构设计 Software Architecture Design	软件架构说明书 Software Architecture Specification
	软件架构的追踪表 Software Architecture Traceability Matrix
软件详细设计和单元设计 Detailed Software Design and Unit Design	SafetyLibrary 详细设计说明书 SafetyLibrary Detailed Design Specification
	Muniu 配置工具设计 Muniu Configuration Tool Design
	软件详细设计追踪表 Software Detailed Design Traceability Matrix
	SafetyLibrary 详细设计评审 SafetyLibrary Detailed Design Review
软件单元测试 Software Unit Testing	QAC 分析报告 QAC Analysis Report
	Tessy 测试报告 Tessy Test Report
	软件单元验证策略 Software Unit Verification Strategy
软件集成和集成测试	集成策略 Integration Strategy
	集成手册 pdf Integration Manual (PDF)

开发流程 Development Process	文档描述 Document Description
Software Integration and Integration Testing	集成测试策略 Integration Test Strategy
	集成测试报告 Integration Test Report
	资源分析报告 Resource Analysis Report
软件认可测试 Software Qualification Testing	SafetyLibrary 软件测试报告 SafetyLibrary Software Test Report
	SafetyLibrary 软件测试报告评审 SafetyLibrary Software Test Report Review
发布 Release	发布文档 Release documentation

7 功能安全 FUNCTIONAL SAFETY

7.1 功能安全评估报告 Functional Safety Assessment Report

7.2 功能安全证书 Functional Safety Certificate

SGS

SGS TÜV SAAR

CERTIFICATE NO FS/71/220/23/1031
ZERTIFIKAT NR.:

PAGE 1/1
SEITE(N)

LICENCE HOLDER & MANUFACTURER
GENEHMIGUNGSINHABER & HERSTELLER

Shanghai ZC Technology Co., Ltd.
Building C, 888 Huanhu West 2nd Road,
Pudong New Area,
Shanghai,
P.R. China

PROJECT NO/-ID *PROJEKT-NR/-ID*	LICENSED TEST MARK *GENEHMIGTES PRÜFZEICHEN*	CERT. REPORT NO. *ZERTIFIKATSBERICHT NR.*
T4A8-AU01	SGS TÜV SAAR ASIL D COMPLIANT Functional Safety ISO 26262 www.sgs-tuv-saar.com	T4A80002 is an integral part of this certificate. *ist ein integraler Bestandteil dieses Zertifikats.*

Certified product(s)
Zertifizierte(s) Produkt(e)
SafetyFrame
Version 2.1.0

Tested according to
Geprüft nach
ISO 26262-2:2018
ISO 26262-6:2018
ISO 26262-8:2018
ISO 26262-9:2018

Technical Data and Parameter
Technische Daten und Parameter
The judgement of the achieved functional safety for the above-mentioned SafetyFrame Software is "accepted" according to above mentioned standards ASIL D requirements.

The SafetyFrame Software is suitable for integration into systems up to ASIL D.

The certificate is based on voluntary tests. The compliance of the certified product against the requirements of above listed functional safety standards was evaluated. Any changes to the design, components or processing may require repetition of some parts of the certification to retain the certification. All applicable requirements of the testing and certification regulations of SGS-TÜV Saar GmbH have to be complied, see www.sgs-tuv-saar.com/tcr-muc and www.sgs-tuv-saar.com/gtc-muc

Certification Body for Functional Safety & Cyber Security SGS-TÜV Saar GmbH
Zertifizierungsstelle für Funktionale Sicherheit & Cyber Sicherheit

Reference to SGS Certification Database

Munich, Feb 22, 2023
Gudrun Neumann

SGS-TÜV Saar GmbH, Hofmannstr. 50, 81379 München, *Deutschland* / Germany
Website: www.sgs-tuv-saar.com
E-Mail: ts@t-gs.com

8 证书 CERTIFICATE

中华人民共和国国家版权局

计算机软件著作权登记证书

证书号：软著登字第4226054号

软件名称：知从安全库软件
[简称：知从SafetyLib]
V1.0

著作权人：上海知从科技有限公司

开发完成日期：2019年05月31日

首次发表日期：未发表

权利取得方式：原始取得

权利范围：全部权利

登记号：2019SR0805297

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。

中华人民共和国国家版权局
计算机软件著作权
登记专用章
2019年08月02日

No. 04322276

木牛软件著作权登记证书
ZC.MUNIU SOFTWARE COPYRIGHT REGISTRATION CERTIFICATE

上海市软件行业协会

软件产品证书

经评估,知从安全库软件V1.0　　符合《进一步鼓励软件产业和集成电路产业发展的若干政策》和《软件产品评估规范》的有关规定，评估为软件产品，特发此证。

申请企业:上海知从科技有限公司
软件类别:应用软件
证书编号:沪ZC-2019-0123
有 效 期：五年

上海市计算机软件评测重点实验室
（上海计算机软件技术开发中心）
二〇一九年 五月二十五日

木牛软件产品登记证书
ZC. MUNIU SOFTWARE PRODUCT REGISTRATION CERTIFICATE