知从.木牛

ZC.MuNiu

知从木牛 SAFETYLIBRARY 英飞凌 TC275 产品手册

知从®木牛基础软件平台功能安全库

知从木牛 SAFETYLIBRARY 英飞凌 TC275 产品手册

知从®木牛基础软件平台功能安全库

1 功能概述

TC275 Safety Library 用于帮助客户实现基于 AURIX TC275 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。

TC275 Safety Library 用于实现 TC275 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。

2 应用领域

TC275 Safety Library 可应用于有功能安全等级需求的控制器。

例如：

- 电机控制器
- 电池管理系统(BMS)
- 底盘系统应用
- 电气稳定控制(ESC)
- 电动助力转向(EPS)

通过将 Safety Library 集成到基于 TC275 的控制中，可达到 ISO26262 ASIL-D 的等级要求。

3 配置环境

配置环境	
Hardware (Chip)	INFINEON SAK-TC275T-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	
编译选项	-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	-nostartfiles -T"..\SafetyLibrary.ld" @iROM.objectlist -mcpu=tc27xx -Wl,--mem-holes -Wl,--warn-orphan

Taskingv4.2r2 编译器选项	
编译选项	-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	-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

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(2011) 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。

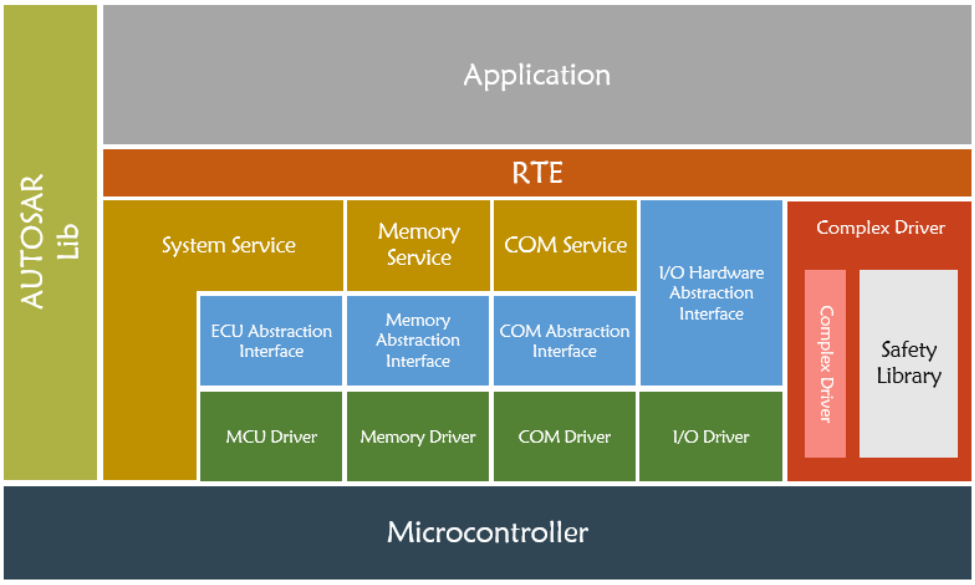
对于微控制器(MCU，以下简称 MCU)，在电子电气系统中，作为 SEooC(safety element out of context)进行设计开发。MCU 为了满足以上提到的 2 个度量要求，需要实现相应的安全机制。而安全机制可以分配到硬件和软件模块中。MCU 的 Safety Library 安全库就是实现分配到软件上的安全机制。

	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 %

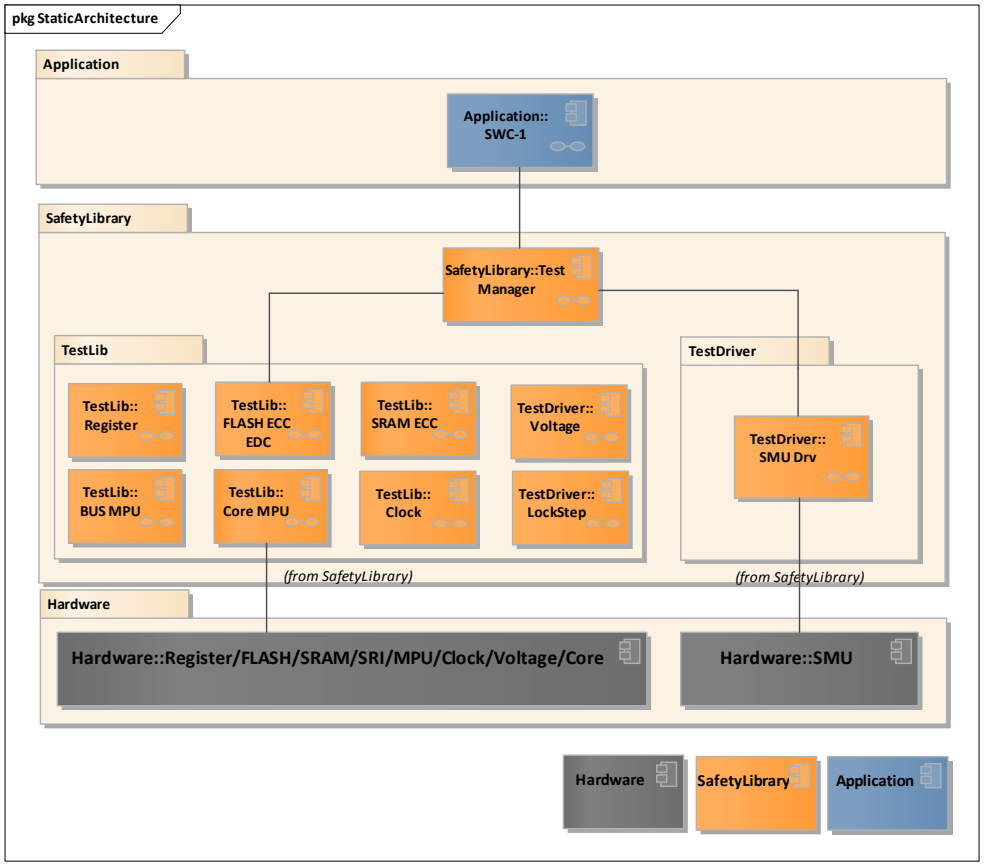
5 功能描述

5.1 产品特点



- 可作为复杂驱动集成到 AUTOSAR 中
- 满足控制器 ASIL-D 需求
- 可集成到非 AUTOSAR 软件架构中
- 高扩展性：每个模块实现可配置性，满足不同的客户需求
- 支持多核测试
- Safety Library 内部程序流监控

5.2 软件架构



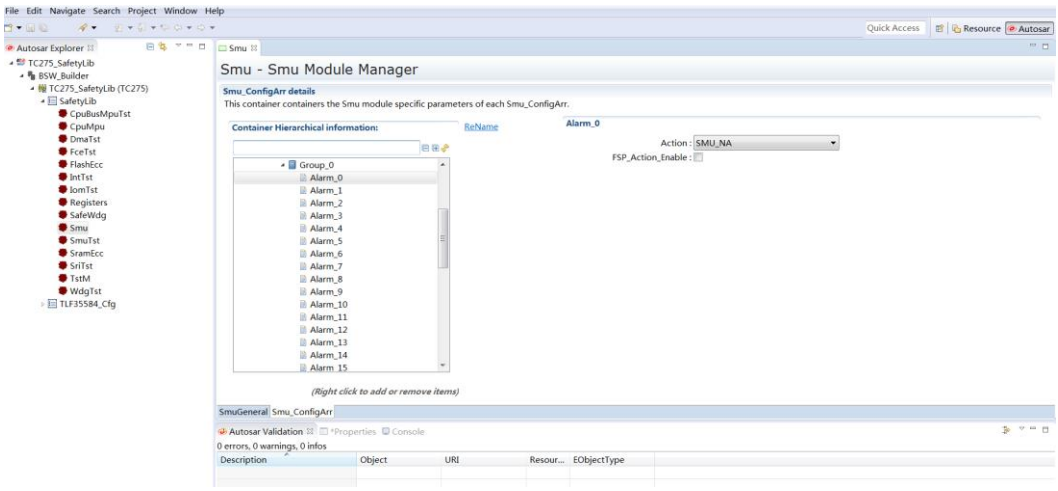
知从模板 TC275 SafetyLibrary 功能列表：

模块	子模块	描述
测试库	Lockstep CPU Comparator Alarm Test	检测 Lockstep 逻辑是否正常
	CPU Trap Test	检测 Trap 功能，检测是否进入相应的 Trap
	Voltage Monitors Test	检测 MCU 内部供电过压和欠压监控功能是否正常
	Clock Monitor Test	检测时钟监控功能是否正常
	SRAM ECC Test	检测 SRAM ECC 和 EDC 逻辑是否正常
	LMU ECC Monitor Test	检测 LMU ECC 和 EDC 逻辑是否正常
	SRAM Address Monitor Test	检测 SRAM 的错误地址监控功能是否正常
	SRAM Error Tracking Test	检测 SRAM 错误追踪功能是否正常
	PFLASH ECC Test	检测 PFLASH ECC 和 EDC 逻辑是否正常

测试库	PFLASH Address Error Detection Test	检测 PFLASH 地址的 ECC 和 EDC 逻辑是否正常
	PFLASH ECC Error Detection Logic Comparator Test	检测 PFLASH 的 EDC 比较逻辑是否正常
	PFLASH Error Tracking Test	检测 PFLASH 错误追踪功能是否正常
	SRI Error Detection Test	检测 SRI 总线传输数据的 EDC 错误
	SRI Error Handle Test	检测 SRI 总线传输协议错误
	SPB Error Handle Test	检测 SPB 错误捕获功能是否正常
	SPB Timeout Test	检测 SPB 总线超时未响应错误功能是否正常
	Register Monitor Test	检测静态配置寄存器是否被篡改
	Register Access Protection Test	检测 SRI 和外设寄存器访问保护功能是否正常
	CPU Memory Protection Test	检测 CPU MPU 功能是否正常
	CPU Bus MPU Test	检测 CPU BUS MPU 功能是否正常
	CPU Register Access Protection Test	检测 CPU 寄存器访问保护功能是否正常
	AURIX Watchdogs test	检测 AURIX 内部看门狗功能是否正常
	Reset Stable State Check	MCU 复位后，检测 MCU 是否达到稳定状态
	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，
	SMU Fault Signaling Protocol Test	检测 Fault Signaling Protocol 的功能是否正常
	SMU Initialization Check	检测 SMU 初始化配置是否正常
	SMU Configuration Lock Test	检测 SMU 配置锁功能是否正常
	SMU Alarms Test	检测 SMU 的相应 Alarm 触发是否正常
	SMU Test	检测 SMU 的相应 Action 触发是否正常
	SMU Recovery Timer Test	检测 SMU 的 Recovery 定时器功能是否正常
	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

测试库	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
	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
	Watchdog Timer Initialization Check	检测 Watchdog 定时器的配置是否正确
	Interrupt Router Error Detection Code Test	检测中断 SRC 寄存器 ECC 功能是否正常
	Flexible CRC Engine (FCE) Test	检测 FCE 功能是否正常
	DMA Cyclic Redundancy Check Test	检测 DMA 传输数据的 CRC 功能是否正常
	LMU Bus MPU Test	检测 LMU BUS MPU 功能是否正常
	LMU Register Access Protection Test	检测 LMU 寄存器访问保护功能是否正常
	IOM test	检测输入输出监控功能是否正常
	Peripheral SRAM ECC Test	检测 SRAM ECC 逻辑是否正常
	SRAM Address Monitor Test	检测外设 SRAM 的错误地址监控功能是否正常
	Peripheral SRAM Error Tracking Test	检测外设 SRAM 错误追踪功能是否正常
	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
	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
	QSPI Protection	QSPI 通信协议实现 End-to-End 通信保护功能
	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
驱动库	SMU Driver	实现 SMU 的初始化配置、故障处理、FSP 配置、配置锁检测
Test Manager	测试管理模块	管理 Safety Library 测试库和驱动库

5.3 配置工具



为了满足客户的不同项目需求，提高 Safety Library 的扩展性，TC275 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。

5.4 软件测试

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

6 过程文档

开发流程	文档描述
需求收集	客户需求文档
软件需求分析	需求分析
	需求分析规格书
	软件需求追踪表
	客户问题沟通表
软件架构设计	软件架构说明书
	软件架构的追踪表
软件详细设计和单元设计	SafetyLibrary 详细设计说明书
	Muniu 配置工具设计
	软件详细设计追踪表
	SafetyLibrary 详细设计评审
软件单元测试	QAC 分析报告
	Tessy 测试报告
	软件单元验证策略
软件集成和集成测试	集成策略
	集成手册
	集成测试策略
	集成测试报告
	资源分析报告
软件认可测试	SafetyLibrary 软件测试报告
	SafetyLibrary 软件测试报告评审
发布	发布文档

7 功能安全

7.1 功能安全评估报告

7.2 功能安全证书

To be continued.

8 证书

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

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