知从.木牛

ZC.MuNiu

# 知从木牛 SAFETYLIBRARY 英飞凌 TC397 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 TC397 产品手册

## 知从®木牛基础软件平台功能安全库

## 1 功能概述

TC397 Safety Library 用于帮助客户实现基于 AURIX TC397 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。

TC397 Safety Library 用于实现 TC397 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

TC397 Safety Library 可应用于有功能安全等级需求的控制器。

例如：

- 电池管理系统(BMS)
- 智能驾驶控制器(ADAS)
- 智能网关控制器(Gateway)
- 智能刹车系统(iBooster)
- 车身稳定控制(ESC/Onebox)
- 电动助力转向(EPS)
- 车身控制器(BCM)
- 发动机管理系统(EMS)
- 底盘域线控系统应用

通过将 Safety Library 集成到基于 TC397 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-TC397T-64F300W |
| **Compilers Supported** | Tasking TriCore v6.2r2 |
| **Evaluation Hardware** | TriBoard TC3X7 |
| **Debugger** | Lauterbach (Trace32 R.2018.02)<br>Isystem (IC5700) |
| **Configuration Tools** | Muniu_v5.1.3 |
| **Configuration Environment** | Win7 64bit |

| 编译器选项 | |
|---|---|
| **Tasking 编译选项** | --cpu=tc39x --iso=99 --keep-temporary-files --integer-enumeration -Wa--emit-locals=+equ,+symbols -Wa--section-info=+list,-console -Wa--optimize=+generics,+instr-size -Wa--debug-info=+asm,+hll,+local,+smart -Wc--debug-info=default -Wc--align=4 -Wc--default-a0-size=0 -Wc--default-a1-size=0 -Wc--default-near-size=0 -Wc--optimize=aceFgIklMnopRsUvwy,+predict -Wc--tradeoff=2 -Wc--language=-gcc,+volatile,-strings,-comments |
| **Tasking 链接选项** | --cpu=tc39x -Wl--output=TC397_ADAS.hex:IHEX -Wl--optimize=1 --output=TC397_ADAS.elf --lsl-file=TC397_ADAS.lsl -Wl--map-file -Wl--map-file-format=2 |

# 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。

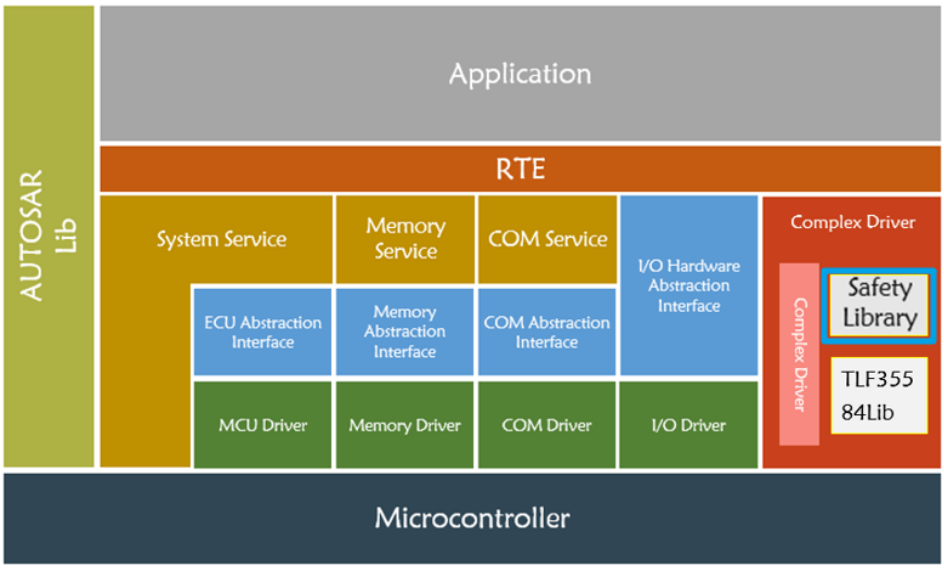
对于微控制器(MCU，以下简称 MCU)，在电子电气系统中，作为 SEooC(safety element out of context)进行设计开发。MCU 为了满足以上提到的 2 个度量要求，需要实现相应的安全机制。而安全机制可以分配到硬件和软件模块中。MCU 的 Safety Library 安全库就是实现分配到软件上的安全机制。

| | 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 % |

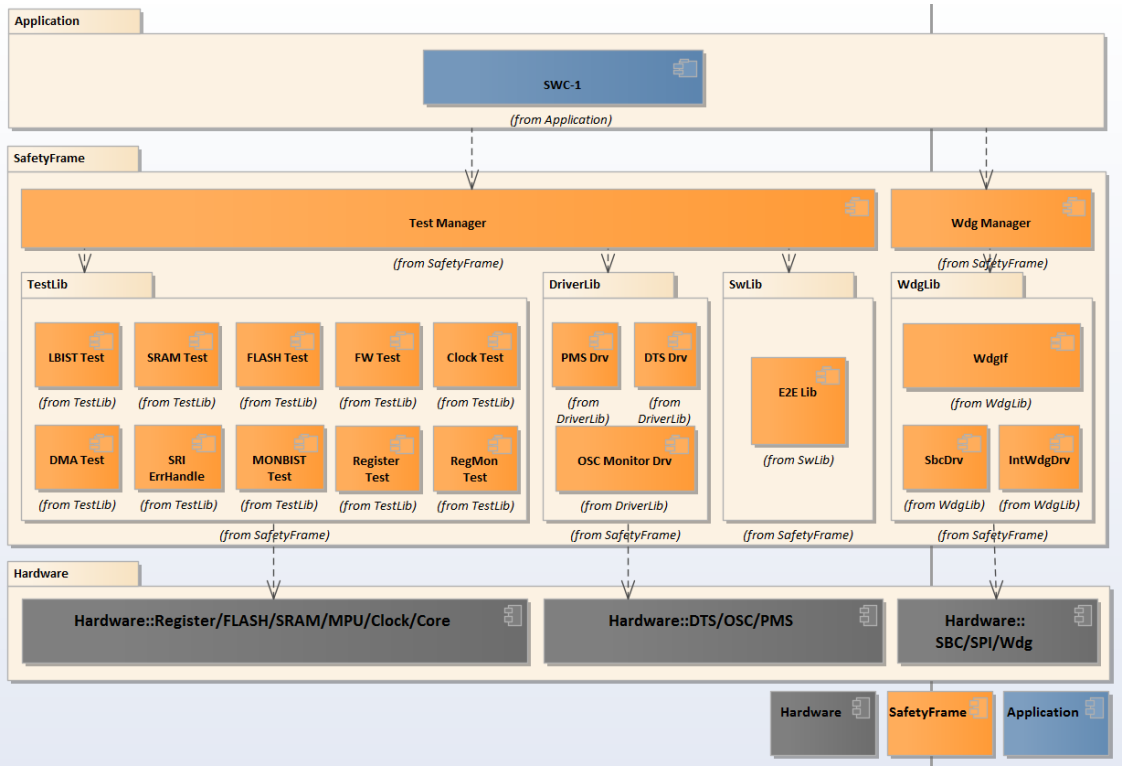
# 5 功能描述

## 5.1 产品特点




- 可作为复杂驱动集成到 AUTOSAR 中
- 可集成到非 AUTOSAR 软件架构中，灵活适配
- 支持多核测试及应用
- Safety Library 具有内部程序流监控
- 高安全性：支持多核自检测试，搭配知从科技 TLF35584Lib 可实现高达 ASIL-D 需求
- 高扩展性：各模块可配置满足不同客户的应用需求

## 5.2 软件架构




软件架构

实现的功能模块：

| 模块 | 子模块 | 描述 |
|---|---|---|
| **测试库** | LBIST Test | Logic BIST配置和结果检测 |
| | SRAM Test | MBIST SRAM 数据检测 |
| | FLASH Test | FLASH数据检测 |
| | FW Test | MCU Firmware启动检测 |
| | Clock Test | 时钟合理性模块检测 |
| | Register Test | 寄存器检测 |
| | DMA Test | DMA传输过程检测 |
| | SRI ErrHandle | SRI错误处理 |
| | MONBIST | Power BIST配置和结果检测 |
| | RegMon Test | 寄存器监控检测 |
| **驱动库** | PMS Driver | PMS监控配置驱动 |
| | DTS Driver | 温度监控配置和检测驱动 |
| | OSC Monitor Drv | OSC监控配置驱动 |
| **SwLib** | E2E Lib | E2E保护协议库 |
| **Wdg 驱动库** | WdgIf | 看门狗驱动接口 |
| | SbcDrv | SBC芯片驱动 |

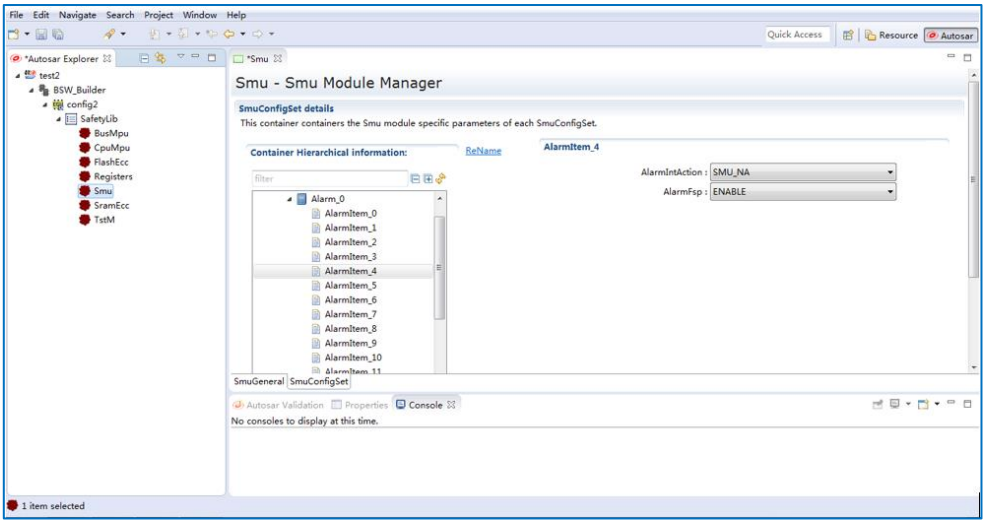
| | | |
|---|---|---|
| | IntWdg Drv | 内部看门狗驱动 |
| **Wdg Manager** | Wdg Manager | 看门狗管理模块 |
| **Test Manager** | Test Manager | 测试管理模块 |

满足的 TC397 Safety Manual 中的 ESM：

| |
|---|
| SMC[SW]:MCU:LBIST_CFG |
| ESM[SW]:MCU:LBIST_RESULT |
| ESM[SW]:DMA:ADDRESS_CRC |
| ESM[SW]:DMA:DATA_CRC |
| ESM[SW]:DMA:ERROR_HANDLING |
| ESM[SW]:DMA:SUPERVISION |
| ESM[SW]:DMA:TIMESTAMP |
| ESM[SW]:PMS:MONBIST_RESULT |
| SMC[SW]:PMS:MONBIST_CFG |
| SMC[SW]:PMS:MON_REDUNDANCY_CFG |
| SMC[SW]:PMS:VX_MONITOR_CFG |
| SMC[SW]:DTS:DTS_CFG |
| ESM[SW]:DTS:DTS_RESULT |
| SMC[SW]:CLOCK:OSC_MONITOR |
| ESM[SW]:CLOCK:PLAUSIBILITY |
| ESM[SW]:SYS:MCU_FW_CHECK |
| ESM[SW]:SRI:ERROR_HANDLING |
| ESM[SW]:NVM.PFLASH:WL_FAIL_DETECT |
| ESM[SW]:VMT:MBIST |
| SMC[SW]:VMT:MBIST |
| AMU.LMU_DAM:REG_MONITOR_TEST |
| CIF.RAM:REG_MONITOR_TEST |
| CPU.DCACHE:REG_MONITOR_TEST |
| CPU.DLMU:REG_MONITOR_TEST |
| CPU.DSPR:REG_MONITOR_TEST |
| CPU.DTAG:REG_MONITOR_TEST |
| CPU.PCACHE:REG_MONITOR_TEST |
| CPU.PSPR:REG_MONITOR_TEST |
| CPU.PTAG:REG_MONITOR_TEST |
| DMA.RAM:REG_MONITOR_TEST |
| EMEM.RAM:REG_MONITOR_TEST |
| ERAY.RAM:REG_MONITOR_TEST |
| GETH.RAM:REG_MONITOR_TEST |
| GTM.RAM:REG_MONITOR_TEST |
| HSPDM.RAM:REG_MONITOR_TEST |
| LMU.RAM:REG_MONITOR_TEST |
| MCMCAN.RAM:REG_MONITOR_TEST |
| PSI5.RAM:REG_MONITOR_TEST |
| SCR.RAM:REG_MONITOR_TEST |
| SDMMC.RAM:REG_MONITOR_TEST |
| SPU.BUFFER:REG_MONITOR_TEST |
| SPU.CONFIG:REG_MONITOR_TEST |

| |
|---|
| SPU.FFT:REG_MONITOR_TEST |
| TRACE.TRAM:REG_MONITOR_TEST |

## 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，TC397 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。

# 6 过程文档

| 开发流程 | 文档描述 |
| --- | --- |
| **需求收集** | 客户的需求文档 |
| **软件需求分析** | ZC 对软件的需求分析 |
| | 需求分析规格书 |
| | 软件需求追踪表 |
| | 客户的问题沟通表 |
| **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** | 软件模块详细设计说明书 |
| | 配置工具设计 |
| | 软件详细设计追踪表 |
| | SafetyLib 工程评审 |
| **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 pdf |
| | 集成测试策略 |
| | 集成测试报告 |
| | 资源分析报告 |
| | 木牛.SafetyLibrary 配置工具使用指导书 |
| | 木牛.SafetyLibrary 配置工具软件配置管理文档 |
| **软件认可测试** | 软件测试报告 |
| | 软件测试策略 |
| **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