NXP MCU S32K14X SAFETY LIBRARY

产品手册

知从®木牛基础软件平台功能安全库

NXP MCU S32K14X SAFETY LIBRARY

产品手册

知从®木牛基础软件平台功能安全库

SAFETLIB FUNCTIONS OVERVIEW

Implementation of S32K14x platform software safety mechanisms, including MCU internal module test and hardware safety mechanism driver.

1 功能概述

S32K14x Safety Library 用于帮助客户实现基于 S32K14x 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。

S32K14x Safety Library 用于实现 S32K14x 平台的软件安全机制，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

S32K14x Safety Library 可应用于有功能安全等级需求的控制器。

例如：

- 车身控制器
- 电池管理系统(BMS)
- 网关控制器
- 车载娱乐模块
- 胎压监控系统
- 门控单元
- 车灯控制单元
- 电子驻车制动系统

通过将 Safety Library 集成到基于 S32K14x 平台的控制器中，可达到 ISO26262 ASIL-B 的等级要求。

APPLICATION AREA

- BCM
- Battery Management System
- Gateway
- Infotainment Connection Module
- TPMS
- Door Control Unit
- Lighting
- Electronic Park Brake

3 配置环境

配置环境	
Hardware (Chip)	S32K144/S32K146/S32K148
Compilers Supported	S32 Design Studio for ARM(2018.R1)
Evaluation Hardware	S32K144 EVB
Debugger	Lauterbach (Trace32 R.2018.02) Isystem (IC5700)
Configuration Tools	Muniu_v5.0.5
Configuration Environment	Win7 64bit

编译器选项	
S32 Design Studio for ARM 编译选项	-mcpu=cortex-m4 -c –Os -ggdb3 -mcpu=cortex-m4 -mthumb -mlittle-endian -fomit-frame-pointer -msoft-float -fno-common -Wall -Wextra -Wstrict-prototypes -Wno-sign-compare -fstack-usage -fdump-ipa-all -std=c99
S32 Design Studio for ARM 链接选项	-mcpu=cortex-m4 -msoft-float -mthumb -e _start -nostartfiles -static -lc -lm -lgcc -lnosys

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。

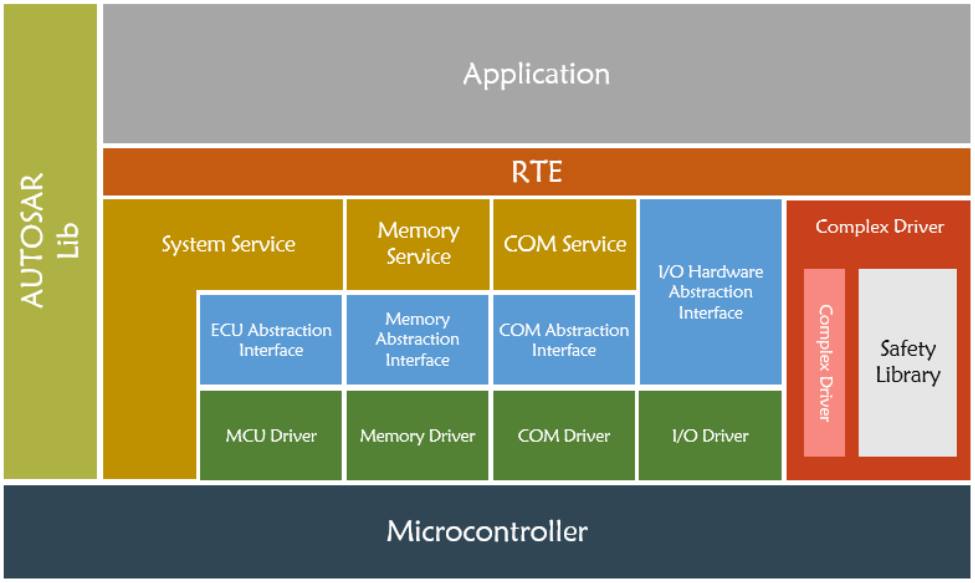
对于微控制器(MCU，以下简称 MCU)，在电子电气系统中，作为 SEooC(safety element out of context)进行设计开发。MCU 为了满足以上提到的 2 个度量要求，需要实现相应的安全机制。而安全机制可以分配到硬件和软件模块中。MCU 的 Safety Library 安全库就是实现分配到软件上的安全机制。

	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

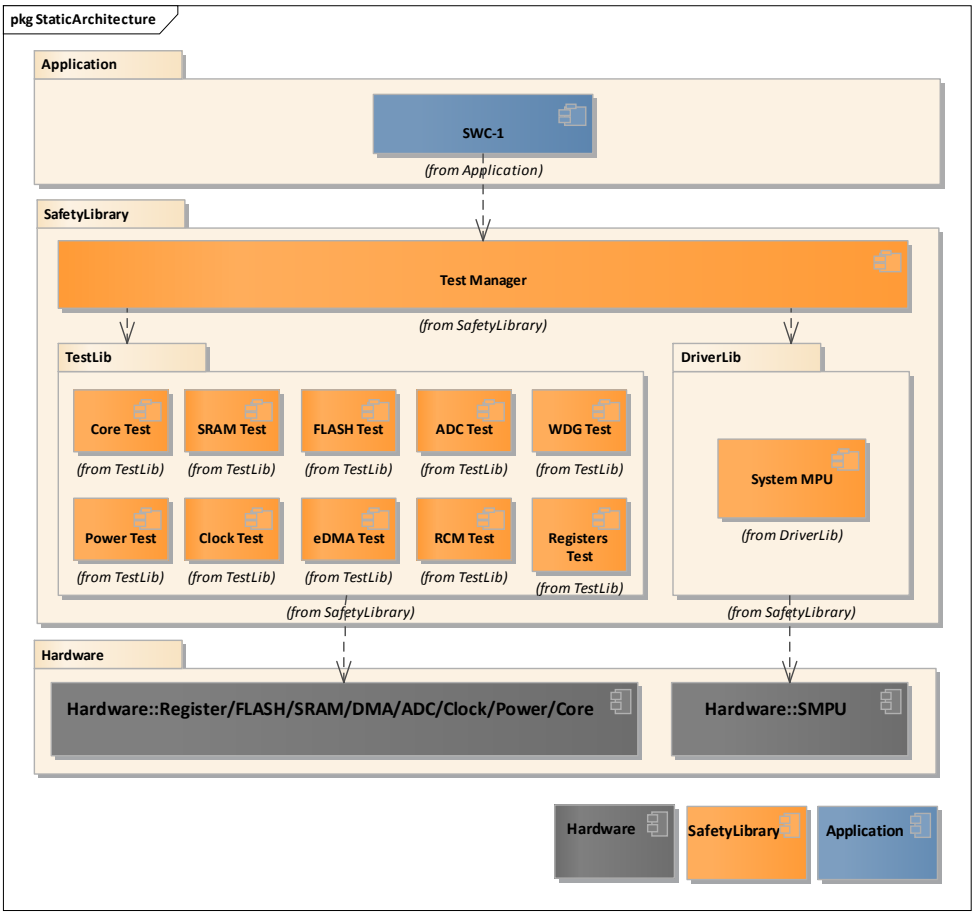


- 可作为复杂驱动集成到 AUTOSAR 中
- 满足控制器 ASIL-B 需求
- 可集成到非 AUTOSAR 软件架构中
- 高扩展性：每个模块实现可配置性，满足不同的客户需求
- Safety Library 内部程序流监控

CHARACTERISTIC

- SafeTlib within AUTOSAR
- ASIL-B
- AUTOSAR & non-AUTOSAR environment
- High Scalability
- Internal Flow Monitor

5.2 软件架构

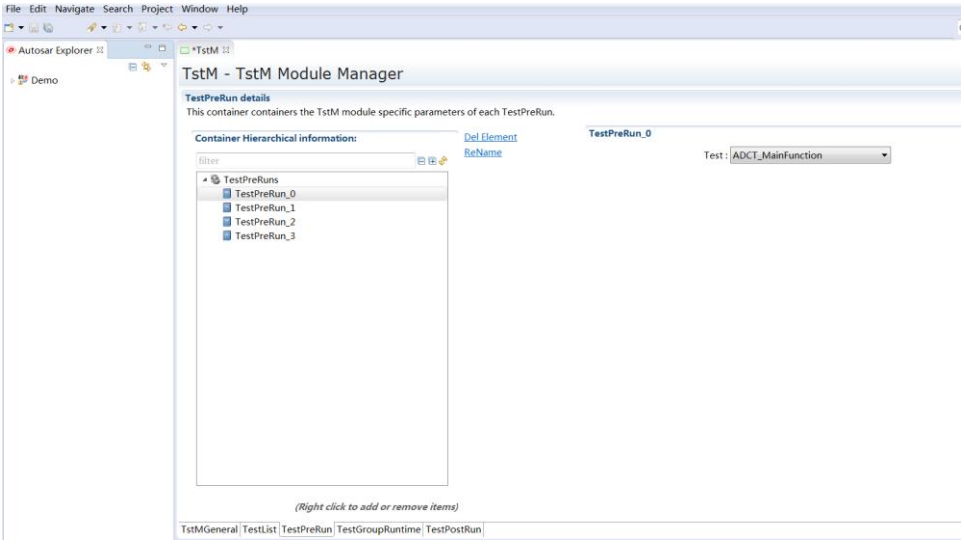


模块	子模块	描述
管理模块	Test Manager	Safety Library 的管理模块
测试库	Core Test	Core检测模块
	eDMA Monitor	DMA检测模块
	SRAM Test	SRAM检测模块
	FLASH Test	FLASH检测模块
	Power Test	供电检测模块
	Clock Test	时钟检测模块
	WDG Test	WDG检测模块
	ADC Test	ADC检测模块
	RCM Test	复位检测模块
	Register Test	寄存器检测模块
驱动库	System MPU Driver	SMPU驱动
通用模块	Common	通用类型定义、MemMap定义等

SAFETYLIB ARCHITECTURE

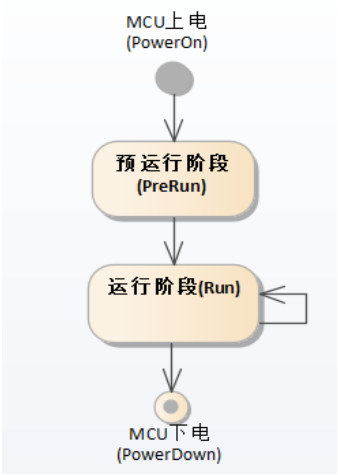
- Core Test
- SRAM Test
- FLASH Test
- Register Test
- WDG Test
- ADC Test
- Power Test
- CLock Driver
- DMA Test
- RCM Test
- SMPU Driver

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，S32K14X 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 运行阶段



- 预运行阶段
  此阶段是对 MCU 的安全机制进行测试，一般此阶段在 OS 启动之前进行。
- 运行阶段
  此阶段是在任务运行时进行，在 OS 运行时进行。

SAFETLIB CONFIGURATION TOOL

Configuration tool is used to satisfy different customer requirements.

SAFETLIB RUN PHASE

- Pre-run
- Run

6 过程文档

开发流程	文档描述
需求收集	顾客的需求文档
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
	配置工具评审
	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

DOCUMENTATION DURING DEVELOPMENT

Provide documentation according to customer requirements.

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。

FUNCTION SAFETY

Provide the report of the assessment according to customer requirement.