知从木牛 SAFETYLIBRARY 恩智浦

MPC5746C 产品手册

知从®木牛基础软件平台功能安全库

知从木牛 SAFETYLIBRARY

恩智浦 MPC5746C 产品手册

知从®木牛基础软件平台功能安全库

1 功能概述

MPC5746C Safety Library 用于帮助客户实现基于 MPC5746C 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。

MPC5746C Safety Library 用于实现 MPC5746C 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

MPC5746C Safety Library 可应用于有功能安全等级需求的控制器。

例如：

- 车门控制模块
- 座椅模块
- 车身控制器
- 高端网关控制器

通过将 Safety Library 集成到基于 MPC5746C 的控制中，并通过系统设计，可达到 ISO26262 ASIL-D 的等级要求。

3 配置环境

配置环境	
Hardware (Chip)	MPC 5746C
Compilers Supported	WindRiver Diab V5.9.4.0
Debugger	Lauterbach (Trace32 R.2018.02) Isystem (IC5700)
Configuration Tools	Muniu_v5.2.2
Configuration Environment	Win7 64bit

编译器选项	
WindRiver Diab 编译选项	-tPPCE200Z4204N3VEG:simple -DMPC5746C -g3 -Wa,-Xisa-vle -DDERIVATIVE_5746C -DDIAB -DMCAL_ENABLE_SUPERVISOR_MODE -DAUTOSAR_OS_NOT_USED -DEU_DISABLE_ANSILIB_CALLS -Xdialect-ansi -XO -Xsize-opt -Xsmall-data=0 -Xsmall-const=0 -Xno-common -Xdebug-dwarf2 -Xdebug-local-all -Xdebug-local-cie -Xdebug-struct-all -Xforce-declarations -Xmacro-undefined-warn -ee1481 -Xnested-interrupts -Xaddr-sconst=0x11 -Xaddr-sdata=0x11 -Xlink-time-lint -W:as:,
WindRiver Diab 链接选项	tPPCE200Z4204N3VEG:simple -Xelf -m6 -Xlink-time-lint -lc -YP,C:/WindRiver/diab/5.9.4.0/PPCVLEEN/simple:C:/WindRiver/diab/5.9.4.0/PPCVLEEN:C:/WindRiver/diab/5.9.4.0/PPCVLEE/simple:C:/WindRiver/diab/5.9.4.0/PPCVLEE ./flash.dld

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。

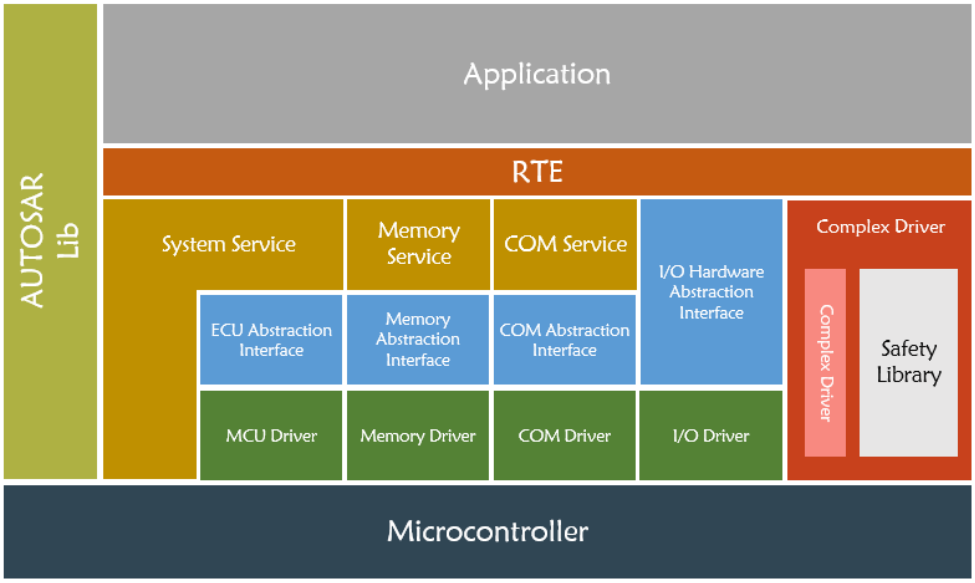
对于微控制器(MCU，以下简称 MCU)，在电子电气系统中，作为 SEooC(safety element out of context)进行设计开发。MCU 为了满足以上提到的 2 个度量要求，需要实现相应的安全机制。而安全机制可以分配到硬件和软件模块中。MCU 的 Safety Library 安全库就是实现分配到软件上的安全机制。

	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 %

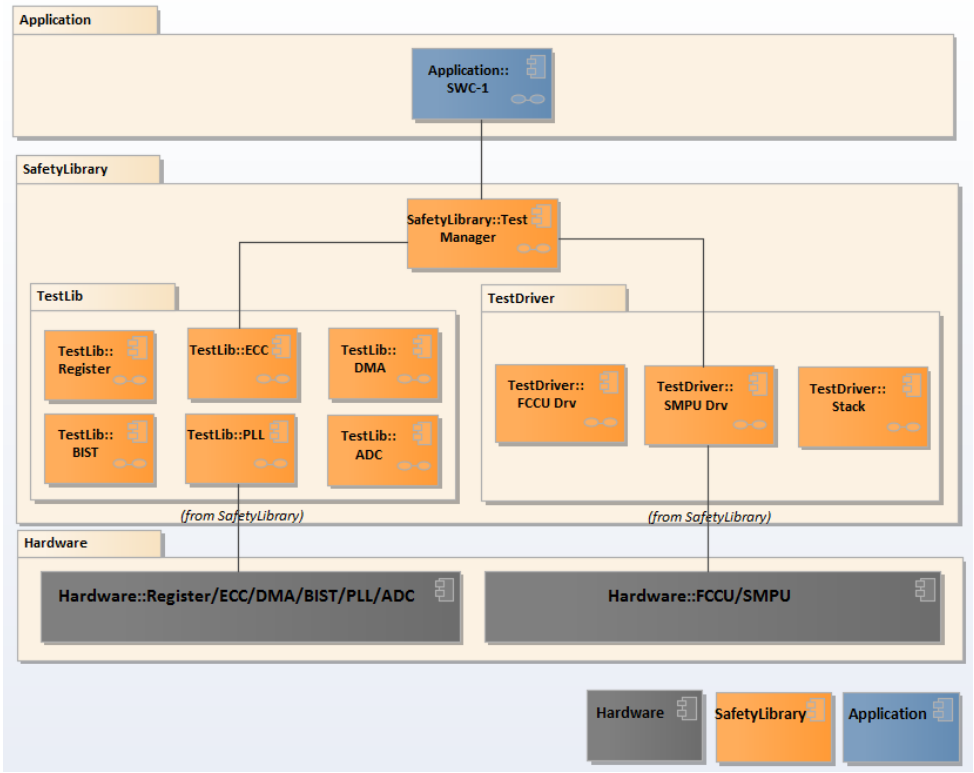
5 功能描述

5.1 产品特点



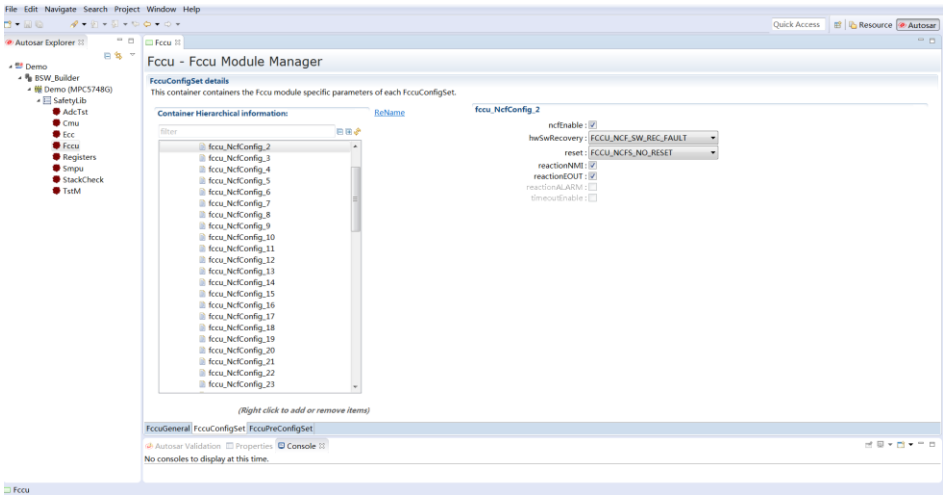
- 可作为复杂驱动集成到 AUTOSAR 中
- 满足控制器不同的安全等级需求
- 可集成到非 AUTOSAR 软件架构中
- 高扩展性：每个模块实现可配置性，满足不同的客户需求
- Safety Library 内部程序流监控

5.2 软件架构



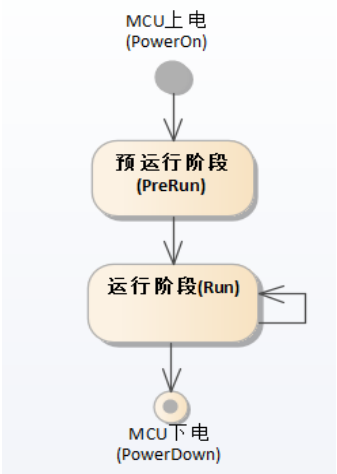
模块	子模块	描述
管理模块	Test Manager	Safety Library 的管理
测试库	BIST Test	BIST检测模块
	Dma Monitor	DMA检测模块
	ECC Test	ECC检测模块
	CMU Test	CMU时钟检测模块
	ADC Test	ADC检测模块
	Register Test	寄存器检测模块
驱动库	System MPU Driver	SMPU驱动
	Stack Monitor	堆栈监控模块
	FCCU Driver	FCCU驱动
通用模块	Common	通用类型定义、MemMap定义等

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，MPC5746C 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，此阶段下 FCCU 为 Normal 状态，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，此阶段下 FCCU 为 Normal 状态，在 OS 运行时进行。

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	FCCU 详细设计说明书
	FCCU 错误处理列表
	FCCU 模块评审记录
	BIST 详细设计说明书
	Register 详细设计说明书
	register 评审记录
	SMPU 详细设计说明书
	SMPU 评审记录
	Stack 详细设计说明书
	ECC 详细设计说明书
	ECC 模块评审记录
	DMA 详细设计说明书
	PLL 模块详细设计说明书
	PLL 模块评审记录
	ADC 模块详细设计说明书
	TestManger 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	第二次测试的 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

开发流程	文档描述
软件认可测试	BIST 软件测试报告
	FCCU 软件测试报告
	Register 软件测试报告
	SMPU 软件测试报告
	Stack 软件测试报告
	ECC 软件测试报告
	DMA 软件测试报告
	PLL 软件测试报告
	ADC 软件测试报告
	TestManger 软件测试报告
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　月二十五日

木牛软件产品登记证书