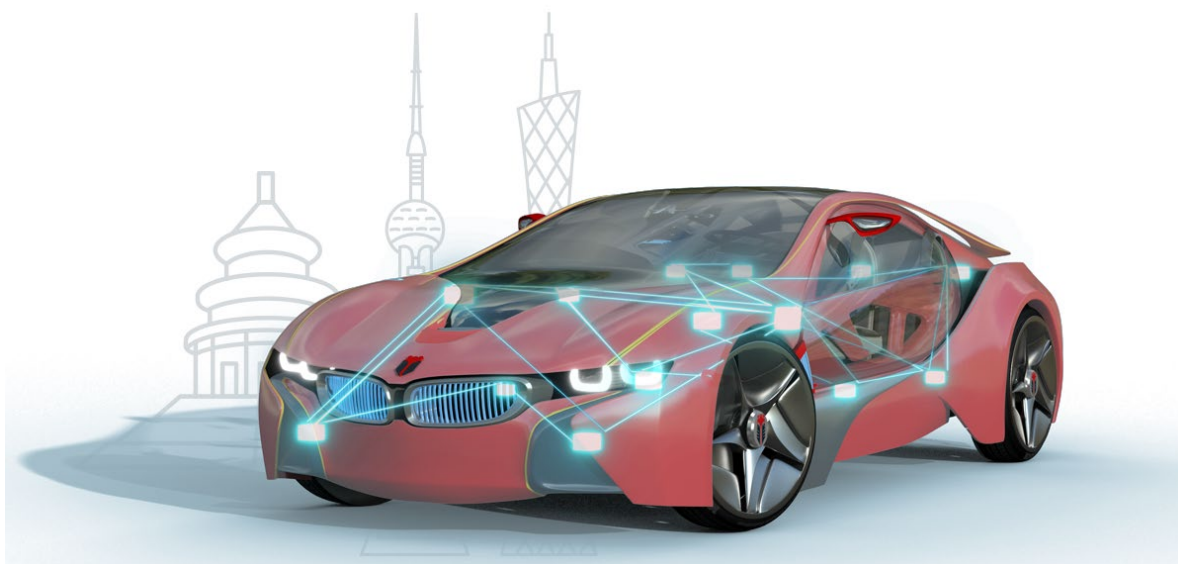




# 知从木牛 SAFETYFRAME 旗芯微 FC7240 产品手册

知从®木牛基础软件平台功能安全库



# 知从木牛 SAFETYFRAME 旗 芯微 FC7240 产品手册

知从®木牛基础软件平台功能安全库

## 1 功能概述

FC240 Safety Frame 用于帮助客户实现基于 FlagChip FC7240 平台的功能安全要求。Safety Frame 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。

FC7240 Safety Frame 用于实现 FC7240 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

FC7240 Safety Frame 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)
- 车身稳定控制(ESC/Onebox)
- 电动助力转向(EPS)
- 底盘域线控系统应用
- 防抱死制动系统(ABS)
- 主动悬架控制系统

通过将 Safety Frame 集成到基于 FC7240 的控制器中，可达到 ISO26262 ASIL-D 的等级要求。

### 3 配置环境

配置环境	
<b>Hardware (Chip)</b>	FLAGCHIP FC7240F2MDS
<b>Compilers Supported</b>	IAR v8.32
<b>Evaluation Hardware</b>	FC7240 Demoboard
<b>Debugger</b>	Lauterbach (Trace32 R.2018.02) Isystem (IC5700)
<b>Configuration Tools</b>	ZCMuNiu v4.4.0
<b>Configuration Environment</b>	Win10 64bit

## 4 开发背景

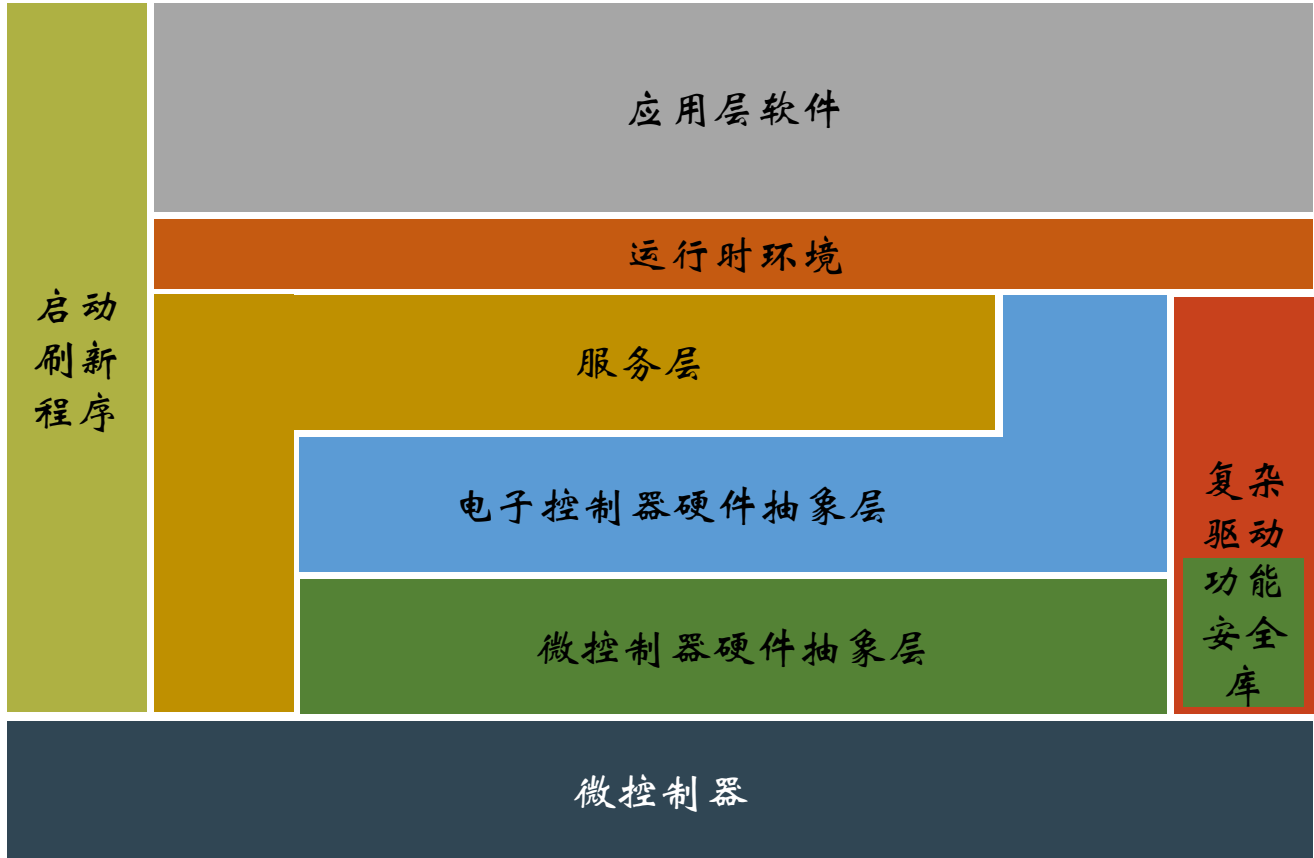
目前，汽车上的电子电气架构越来越复杂，对汽车电子的安全性要求也越来越高，为了满足汽车的安全性需求，汽车功能安全越来越受到重视。提到功能安全，大家首先想到的是功能安全标准 ISO26262。其中，ISO 26262-5(2018) Clause 8 中介绍了 2 个度量：Single-point fault metric(单点故障度量)和 Latent-fault metric(潜伏故障度量)。根据不同的 ASIL 等级要求，单点故障度量和潜伏故障度量需要达到相应的等级。

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。

ASIL	SPFM	LFM	PMHF
A	Not Relevant	Not Relevant	Not Relevant
B	$\geq 90\%$	$\geq 60\%$	$<10^{-7}/\text{hour}$
C	$\geq 97\%$	$\geq 80\%$	$<10^{-7}/\text{hour}$
D	$\geq 99\%$	$\geq 90\%$	$<10^{-8}/\text{hour}$

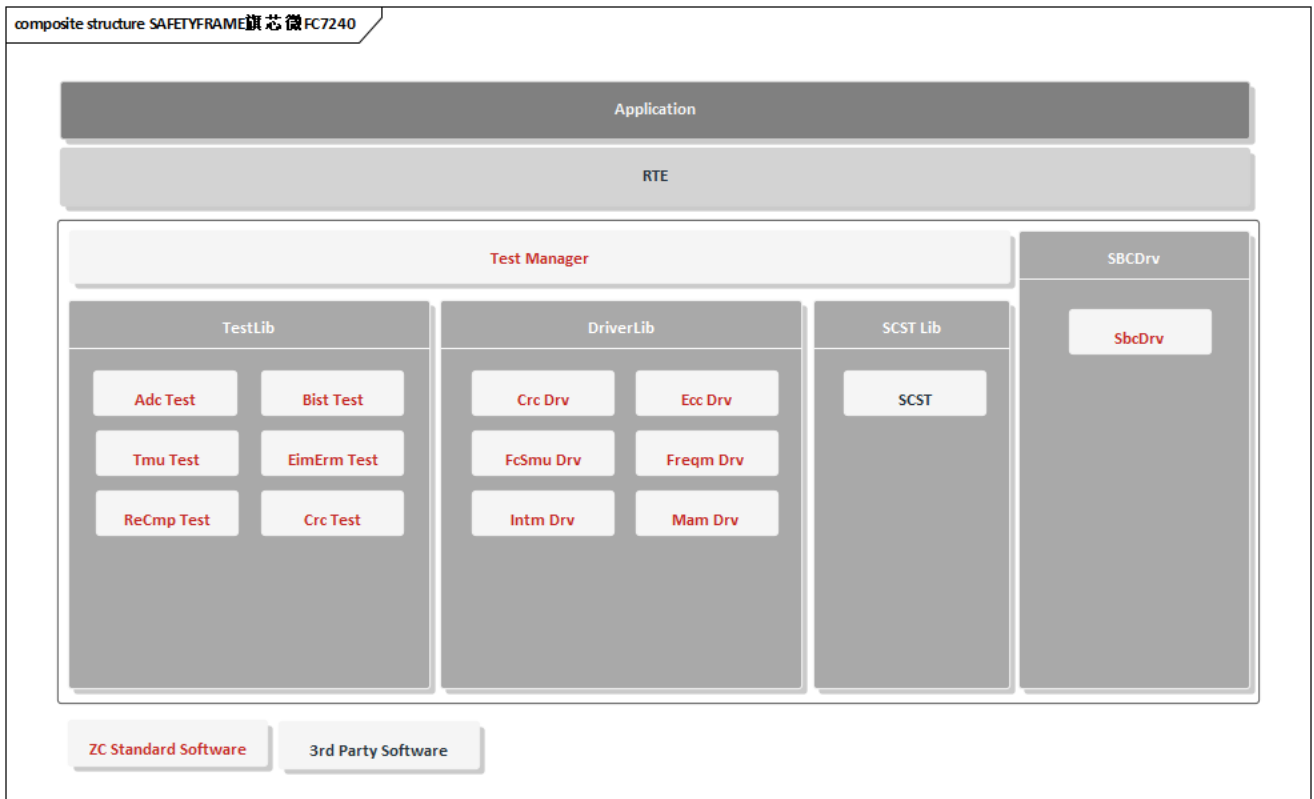
## 5 功能描述

### 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 Frame 具有内部程序流监控
- 高安全性：支持多核自检测，搭配知从科技 FS26 SBCDrv 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	Adc Test	PMC电压监控功能
	Bist Test	Logic & Memory BIST配置和结果检测
	Crc Test	CRC Checker数据检测
	Ecc Test	ECC Checker数据检测
	EimErm Test	故障注入及故障状态检测
	RegCmp Test	寄存器周期检测
	Tmu Test	ADC采样值监控检测
驱动库	Crc Driver	CRC Checker数据检测配置驱动
	FcSmu Driver	故障状态检测配置驱动
	Freqm Driver	时钟监控功能配置驱动
	Intm Driver	中断监控配置驱动
	Mam Driver	MAN端口访问监控配置驱动
SCST Lib	SCST	CM7内核自检
Wdg 驱动库	SBCDrv	SBC芯片驱动
Test Manager	Test Manager	测试管理模块

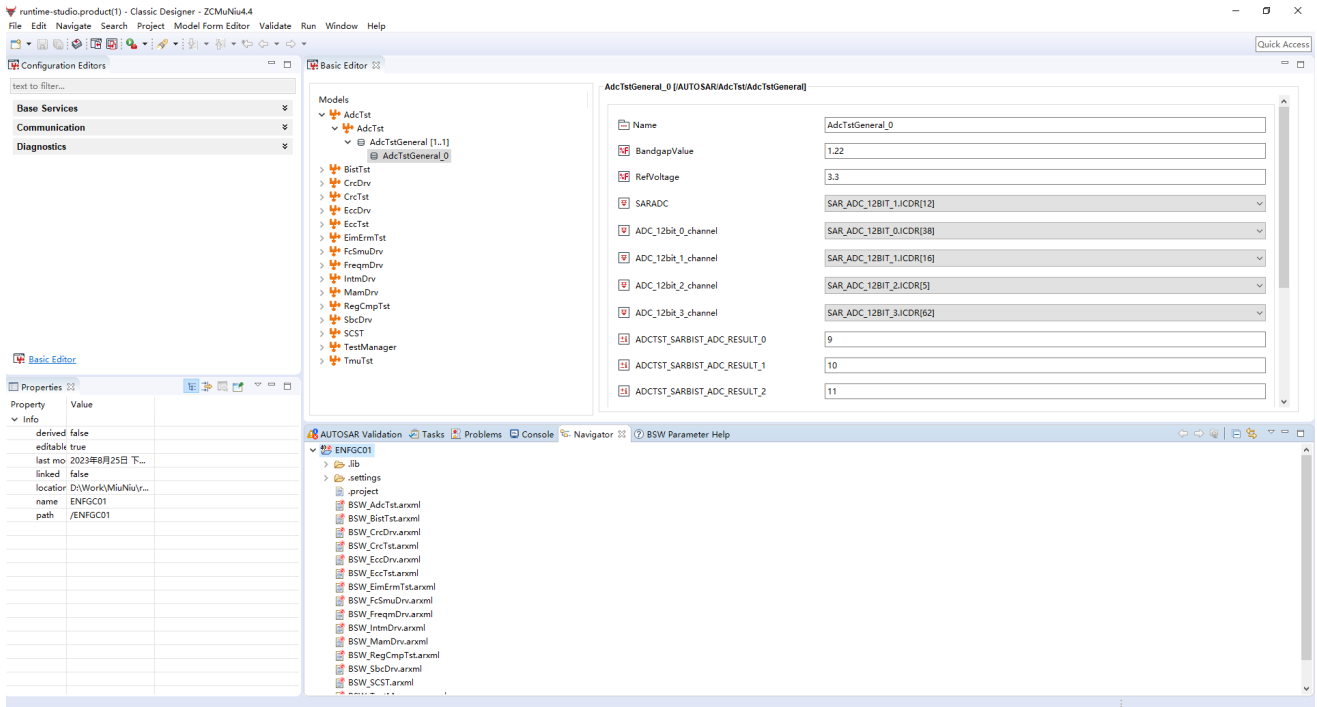
满足的 FC7240 Safety Manual 中的 ESM:

SM1. ADC. PWR_CHK
SM3. SBC
SM1. PMC_MON
SM1. SCG. CRC
SM3. CLOCK_JITTER
SM1. FC. ECC
SM1. FC. ECC_MON
SM1. EIM. Flash
SM1. ERM. Flash
SM1. FC. PGMON
SM1. Flash_IFR. RDT
SM1. ROM. ECC
SM1. EIM. ROM
SM1. ERM. ROM
SM1. EIM. SYSRAM
SM1. ERM. SYSRAM
SM1. CM7. LOCKSTEP_MON_RDT
SM1. EIM. LOCKSTEP
SM1. ITCM. ECC
SM1. EIM. ITCM
SM1. ERM. ITCM
SM1. DTCM. ECC
SM1. EIM. DTCM
SM1. ERM. DTCM
SM1. CM7. CACHE_ECC
SM1. EIM. CACHE
SM1. ERM. CACHE
SM2. CM7. SELFTTEST
SM1. MAM. EDC
SM1. MAM. RDT
SM1. EIM. MAM
SM1. MAM. WDOG
SM1. MAM. MPU
SM1. FMC. EDC
SM1. EIM. FMC
SM4. CPM. SWCHK
SM4. MB. SWCHK
SM1. INTM
SM1. TMU. ADC
SM1. TMU. CMP
SM1. SCM. CRC
SM1. ISM
SM3. EXT_WDOG
SM1. FCSMU
SM1. FCSMU. MON
SM1. FCSMU. CRC



SM3. FCSMU_MON
SM1. STCU
SM1. STCU. WDOG
SM1. DMA_CFG. ECC
SM1. EIM. DMA
SM1. ERM. DMA
SM1. DMA. MON
SM1. FCSPI. MON
SM1. FCUART. MON
SM1. FlexCAN. ECC
SM1. EIM. FlexCAN
SM1. ERM. FlexCAN
SM1. ERM. ENET
SM1. ADC_SelfTest
SM1. FREQM
SM4. PMC. SWCHECK
SM4. SCG. SWCHECK
SM4. CMU. SWCHECK
SM4. PCC. SWCHECK
SM4. MAM. SWCHECK
SM4. CM7. MPU_SWCHECK
SM1. FMC. ENC
SM1. ERM. FMC
SM4. FMC. SWCHECK
SM4. WDG. SWCHECK
SM4. INTM. SWCHECK
SM4. ISM. SWCHECK
SM4. RGM. SWCHECK
SM4. DMA. SWCHECK
SM4. FCPI.T. SWCHECK
SM4. ADC. SWCHECK
SM4. COMM_SAFEPROT
SM1. ERM. ENET
SM1. ADC_SelfTest
SM1. FREQM
SM4. PMC. SWCHECK
SM4. SCG. SWCHECK
SM4. CMU. SWCHECK
SM4. PCC. SWCHECK
SM4. MAM. SWCHECK
SM4. CM7. MPU_SWCHECK
SM1. FMC. ENC
SM1. ERM. FMC
SM4. FMC. SWCHECK
SM4. CRC_SWCHECK

## 5.3 配置工具



为了满足客户的不同项目需求，提高 Safety Frame 的扩展性，FC7240 Safety Frame 实现了各个模块可配置性，并且实现了 Safety Frame 的配置工具。客户可根据不同需求，在配置工具上完成 Safety Frame 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
	Safety Frame 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.Safety Frame 配置工具使用指导书
	木牛.Safety Frame 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。



No. 04322276

  
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

木牛软件著作权登记证书



木牛软件产品登记证书



公众号



业务联系

成为全球领先的**汽车基础软件**公司

To Be the Global Leading **Automotive Basic Software** Company

