



知从木牛 SAFETY FRAME 产品手册

知从®功能安全

知从木牛 SAFETY FRAME

产品手册

1 功能概述

知从木牛（ZC.MuNiu）为汽车电子控制器产品开发，提供完整的基础软件平台解决方案。知从 Safety Frame 是通过知从木牛平台上位机配置工具进行界面化配置的芯片功能安全库软件包，它依据 ISO 26262-10 做独立安全单元（SEooC）研发完成关键器件 Module 基于 AoU 诊断覆盖度需求的内置安全机制设计，针对汽车控制器中 MCU、SBC 汽车控制器中进行功能安全库及软件架构的定制开发。

知从木牛 Safety Frame 产品包含三大组件：

Safety Frame 组件	功能描述	架构角色说明
SF.SBC	配置各半导体厂商 System Basis Chip 驱动包	Monitoring Controller
SF.MCU	配置各半导体厂商 MCU Safety Library 软件包	Function Controller
SF.Architecture	按组件各模块部署 Level 分层调度及管理	参考 EGAS 三层架构

本产品现已适配开发的半导体芯片厂商的系列型号：

Controller	Chip Type	Semiconductor manufacturer	Component
Function	S32K	NXP	SF.MCU
	5748G	NXP	SF.MCU
	5746C	NXP	SF.MCU
	MPC5744P	NXP	SF.MCU
	TC397	Infineon	SF.MCU
	TC275	Infineon	SF.MCU
Monitoring	FS6500	NXP	SF.SBC
	FS4503	NXP	SF.SBC
	TLF35584	Infineon	SF.SBC

2 应用领域

知从木牛 Safety Frame 产品可应用于针对功能安全 ASIL 等级有需求的汽车控制器。

例如：

- 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)
- 电子驻车系统(EPB)
- 电池管理系统(BMS)
- 车身控制器(BCM)
- 发动机管理系统(EMS)
- DC/DC 控制器

本安全手册是为有经验的硬件、基础软件工程师和功能安全工程师编写的，以说明 Safety Frame 功能安全软件库分别将 MCU&SBC 相关安全机制集成到客户应用产品的(子)系统中的产品概况。我们的软件集成工程师可支持和确保该平台产品功能安全库程序的集成服务，并符合适当的应用程序标准，协助客户实现上述汽车控制器达到 ISO26262 ASIL-D 的等级要求。

3 配置环境

i. Safety Frame 产品的 NXP S32K 系列芯片软件配置：

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

ii. Safety Frame 产品的 NXP PowerPC 系列芯片软件配置：

配置环境	
Hardware (Chip)	MPC 5748G / MPC5744P/ MPC5746C
Compilers Supported	WindRiver Diab V5.9.4.0
Evaluation Hardware	SPC5748GSMKU6 1N81M
Debugger	Lauterbach (Trace32 R.2018.02) Isystem (IC5700)
Configuration Tools	Muniu_v5.2.2
Configuration Environment	Win7 64bit

iii. Safety Frame 产品的英飞凌 AURIX 2G TC3xx 软件配置：

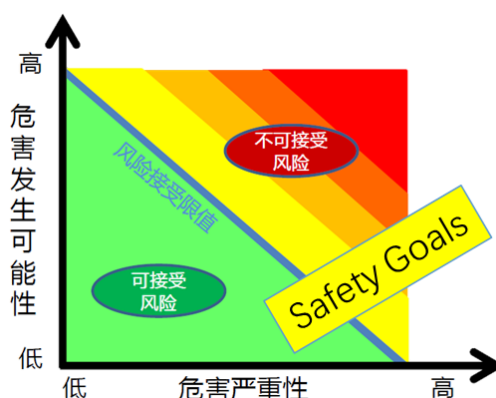
配置环境	
Hardware (Chip)	INFINEON SAK-TC397T-64F300W
Compilers Supported	Tasking TriCore v6.2r2
Evaluation Hardware	TriBoard TC3X7
Debugger	Lauterbach (Trace32 R.2018.02) Isystem (IC5700)
Configuration Tools	Muniu_v5.1.3
Configuration Environment	Win7 64bit

iv. Safety Frame 产品的英飞凌 AURIX 1G TC275 软件配置：

配置环境	
Hardware (Chip)	INFINEON SAK-TC275T-64F200W CA
Compilers Supported	Tasking TriCore v4.2r2/ HighTec 4.6.6.1
Evaluation Hardware	TriBoard TC2X5
Debugger	Lauterbach (Trace32 R.2018.02) Isystem (IC5700)
Configuration Tools	Muniu_v5.1.1
Configuration Environment	Win7 64bit

4 开发背景

汽车电控系统的电气化、智能化发展日趋复杂，对于电子电气架构的安全性要求也越来越高。通过对道路车辆应用场景的 HARA 分析，为了使安全目标被降级分解、保持危害发生可能性低于风险的受限值，汽车功能安全越来越受到重视。近年来，在功能安全标准上参考 ISO 26262；在软件架构安全架构上参考 E-GAS 分层。在电子电气系统中，应用 SEooC(safety element out of context)进行设计开发。



ECU 产品的功能安全工程师，根据半导体供应商提供的 Safety Manual 中列出的大量应用安全机制结合自身产品需求来查漏补缺，进一步筛选出需要根据开发的 FMEDA 配置来确定具体需要使用哪些模块的诊断软件开发。一般来说，ASIL 级别越高，需要实现的安全措施就越多，而这需要付出相当大的工作量和落地门槛：

- ✧ 昂贵成本（较多未用模块冗余）、芯片内置安全机制开发对半导体厂商依赖度极高；
- ✧ 软件团队的开发精力集中在 ECU 级而非 MCU 级，多芯片搭配较难落地安全机制。

应对客户上述困扰，知从木牛 Safety Frame 产品不仅适配 MCU 芯片，也为特定 ASIL-x 等级 SBC 的供电系统、时序监控系统，甚至集成外设 SOC 专用芯片驱动，按照 ISO 26262-5(2011) Clause 8 中介绍的 2 个度量：Single-point fault metric(单点故障度量)和 Latent-fault metric(潜伏故障度量)做安全分析，针对不同的 ASIL 等级要求和故障失效分析方法均要求其达到单点故障度量和潜伏故障度量提供基础软件平台功能安全库的保障。

	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 %

知从科技推出 SAFETY FRAME 为各车载控制器客户提供诚挚的 ASIL 等级分解咨询、FMEDA 分析过程支持、芯片级自检安全机制开发、SafetyFrame 配置与软件集成等全流程功能安全服务。

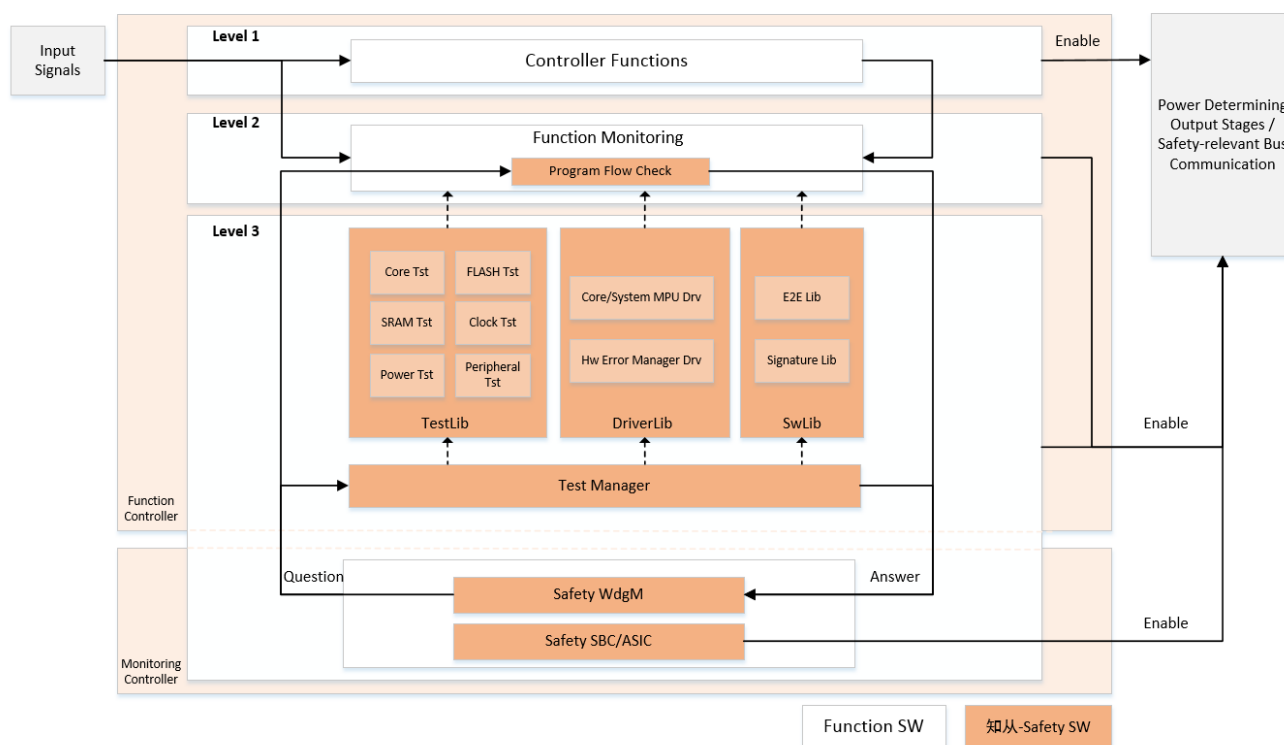
5 功能描述

5.1 产品特点

知从科技推出 SAFETY FRAME 产品的功能和特性如下：

- 知从木牛配置工具支持 AUTOSAR 4.2.2 和 AUTOSAR 4.4 标准；
- Safety Frame 安全等级 ASIL-B，额外安全机制可支持最高 ASIL-D 安全等级应用需求；
- 按照 ASPICE 软件开发流程，实现从客户需求、MCU Safety Manual、安全库代码、测试报告的可追溯性；
- Safety Frame 安全软件架构自主设计中，结合了 EGAS Monitoring Controller 监控机制；
- SwLib 自检库 Safety Mechanism 实现软件程序流监控并包含 E2E 功能，调用接口灵活，分担客户重新开发工作量；
- 该产品做为 AUTOSAR Complex Driver 组件集成，兼容半导体供应商 MCAL 驱动包；
- 管理内部看门狗系统，可选配集成知从 SBC 产品库，实现完整 Safety WdgM 功能；
- Test Manager 集成 MCU 故障收集 Driver（eg.SMU/FCCU）可支持客户产品 Safety Goal 对 FTTI 时间需求的安全关断监控设计；
- 芯片自检库 TestLib 支持各模块按需可裁剪的定制化开发，适应开发周期较短项目，代码精简且缩减软件容量；
- 针对某些客户 ECU 产品的非 AUTOSAR 软件架构，知从 SafetyFrame 具有良好的软件集成兼容性。

5.2 软件架构



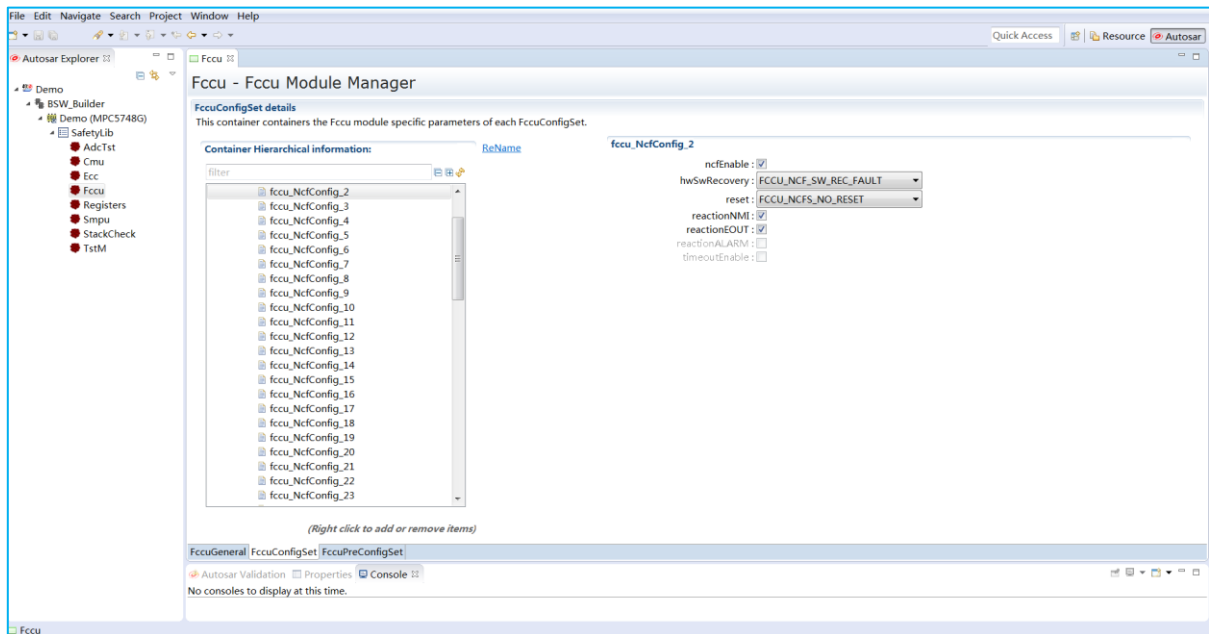
SAFETY FRAME 包括 MCU 内部模块自检测试（即 SF.MCU）和 SBC 硬件安全机制的驱动（即 SF.SBC），SF.Architecture 的核心模块为 Test Manager，用于 MCU&SBC 的 Safety Library 调度管理，包括 Safety Wdgm、Safety SBC/ASIC 驱动模块调度、与应用层 PFC(Program Flow Check)接口等，其包含 3 个库接口模块：

- **TestLib**--实现 MCU 芯片模块的检测。
- **DriverLib**--实现 MCU 芯片模块的驱动。
- **SwLib**--用户常用的数字签名库、端到端保护库等接口。

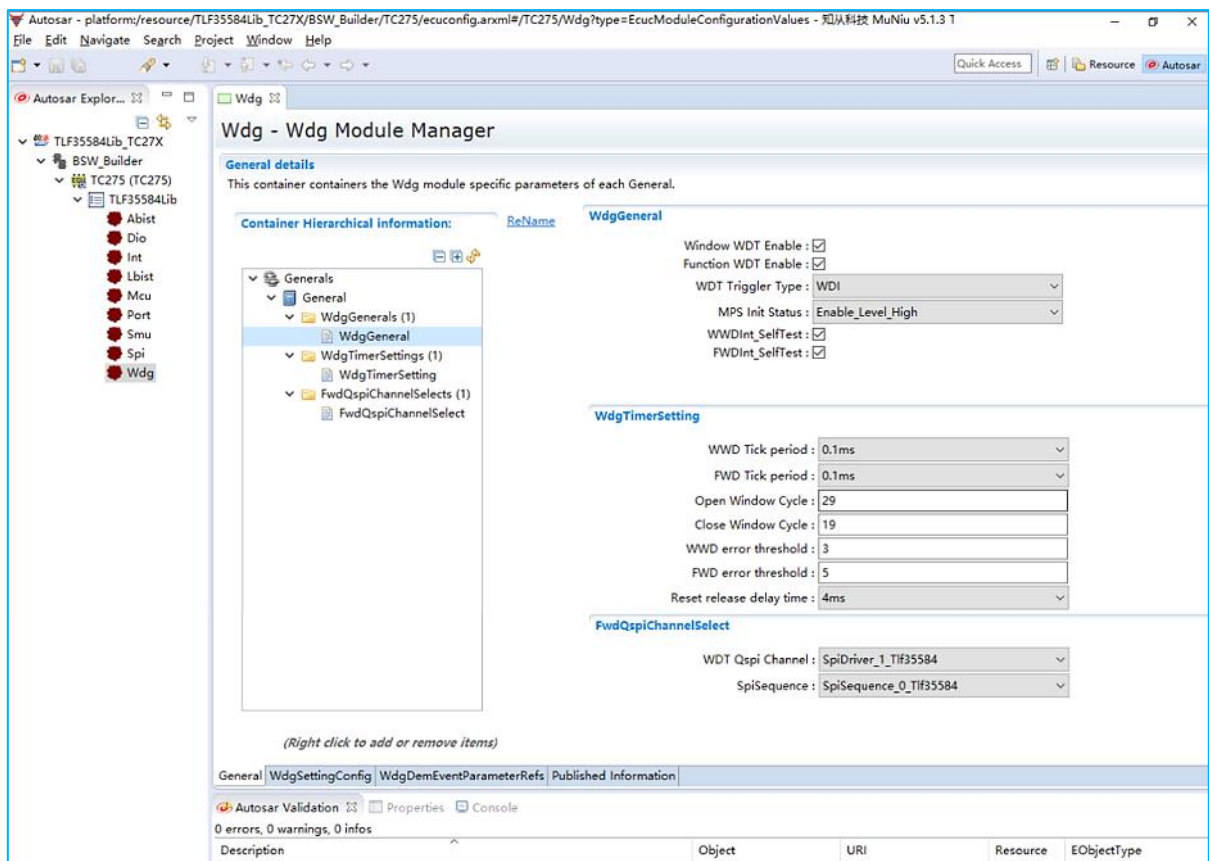
SAFETY FRAME 在软件模块化分层原则上，将 Function Controller 和 Monitoring Controller 分别由 SF.MCU 和 SF.SBC 实现，并部署在 EGAS Level2 和 Level3 层级，充分考虑了程序流监控和关断路径设计的应用需求。

5.3 配置工具

i. 知从木牛工具实现对 Safety Frame 产品的 MCU 芯片配置：

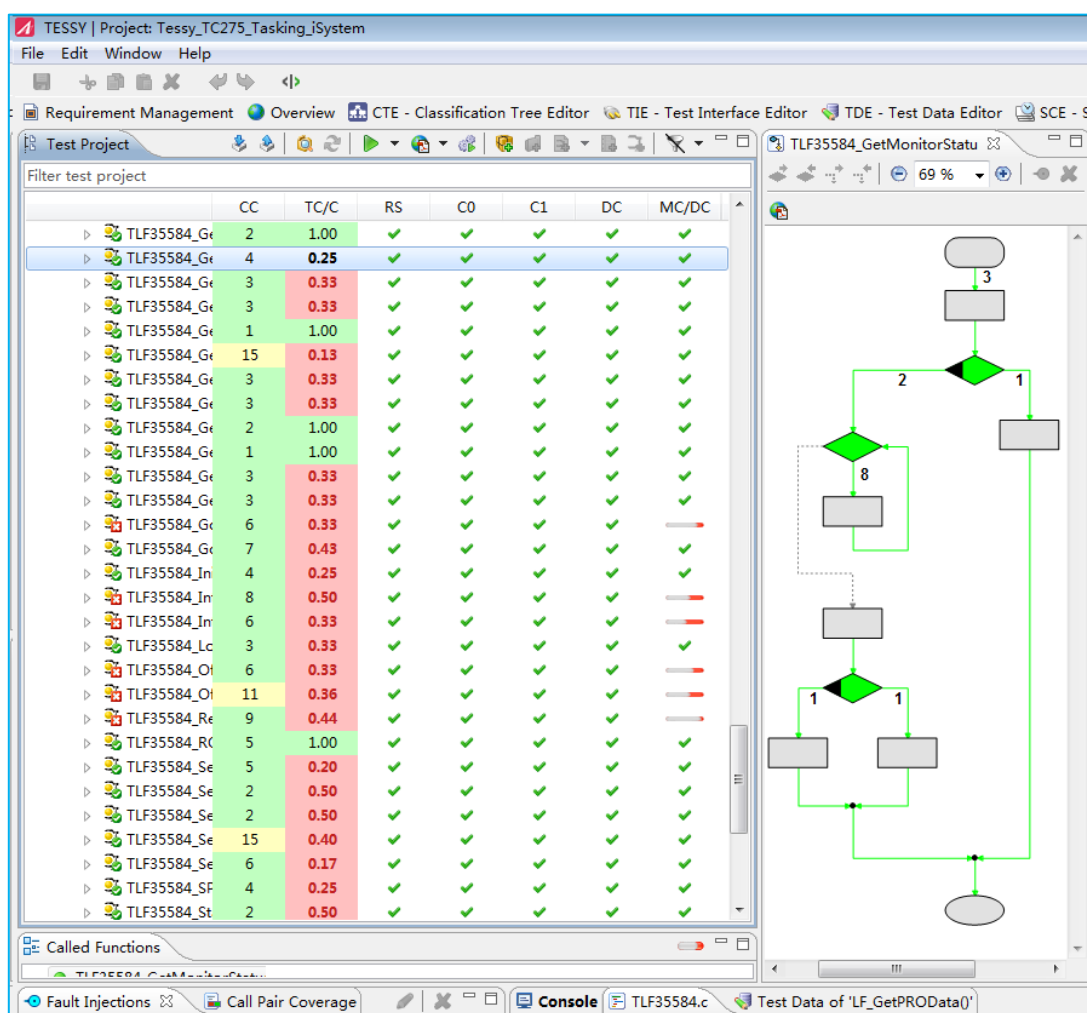


ii. 知从木牛工具实现对 Safety Frame 产品的 SBC 芯片配置：



5.4 软件测试

测试环境	
静态代码 QAC	7.2 R MISRA-C: 2004
动态 Tessa	4.2.8
Evaluation Hardware	Evaluation Board
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	SAFETY FRAME 详细设计说明书
	Muniu 配置工具设计
	软件详细设计追踪表
	SAFETY FRAME 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	SAFETY FRAME 软件测试报告
	SAFETY FRAME 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

申请评估中。

7.2 功能安全证书

申请认证中。

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6128984号	
软件名称：	知从木牛安全架构软件 [简称：知从木牛SafetyFrame] V1.0
著作权人：	上海知从科技有限公司
开发完成日期：	2020年06月30日
首次发表日期：	2020年07月03日
权利取得方式：	原始取得
权利范围：	全部权利
登记号：	2020SR1250288
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。	
	
	2020年11月04日
No. 06664531	

木牛软件著作权登记证书



知从木牛 SAFETYFRAME 产品证书