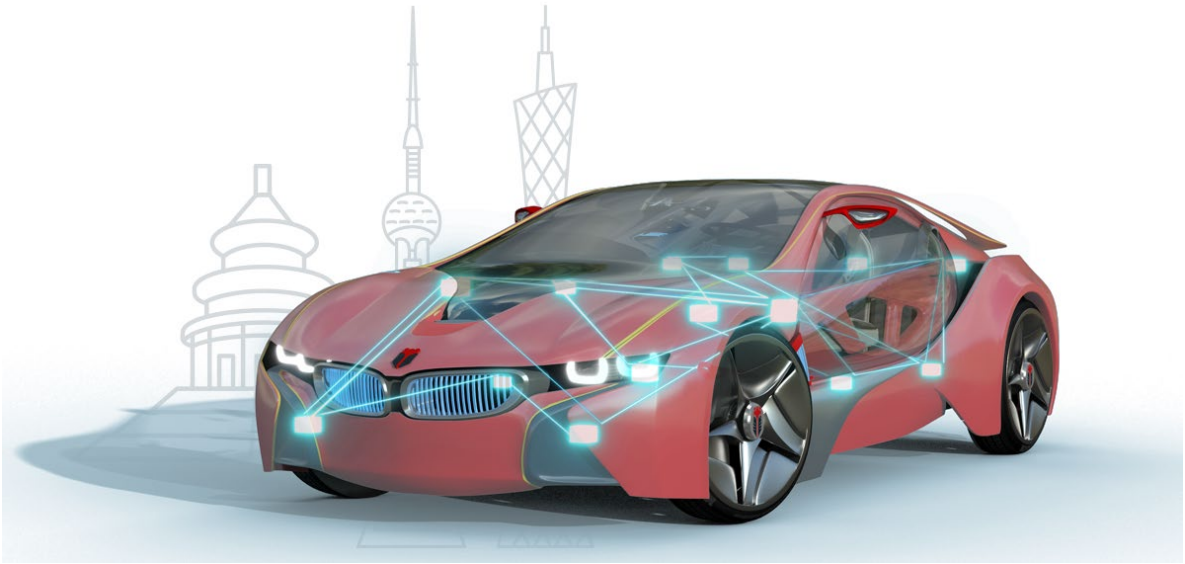
知从木牛 SAFETY FRAME 赛普拉斯

CYT2B7 产品手册

知从木牛基础软件平台功能安全库



知从木牛 SAFETY FRAME 赛普拉斯 CYT2B7 产品手册

知从木牛基础软件平台功能安全库

1 功能概述

CYT2B7 Safety Frame 用于帮助客户实现基于 CYT2B7 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。

CYT2B7 Safety Frame 用于实现 TRAVEO™ T2G 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。

© 2017-2024 上海知从科技有限公司

2 应用领域

CYT2B7 Safety Frame 可应用于有功能安全等级需求的控制器。

例如：

- 汽车车身电子设备
- 汽车车身控制模块（BCM）
- 带集成网关的车身控制模块（BCM）
- 汽车网关
- 汽车 LED 前照灯

通过将 Safety Frame 集成到基于 CYT2B7 的控制中，可达到 ISO26262 ASIL-B 的等级要求。

© 2017-2024 上海知从科技有限公司

3 配置环境

配置环境	
Hardware (Chip)	TRAVEO™ T2G -CYT2B7
Compilers Supported	IAR Embedded Workbench for ARM 8.40.1
Evaluation Hardware	KITBoard CYT2B7
Debugger	Lauterbach (Trace32 R.2023.02) Isystem IC5000/IC5700
Configuration Tools	Muniu_v5.1.0
Configuration Environment	Win10 64bit

编译器选项	
IAR 编译选项	--no_unroll --debug --endian=little --cpu=Cortex-M4 -e --fpu=None --debug --dlib_config --endian little --cpu_mode thumb -On --no_cse --no_unroll --no_inline --no_code_motion --no_tbaa --no_clustering --no_scheduling
IAR 链接选项	--cpu=Cortex-M4 -e --fpu=None DSTART_FROM_FLASH -DM4_DEVICE_RESERVED_ADDR

© 2017-2024 上海知从科技有限公司

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(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。

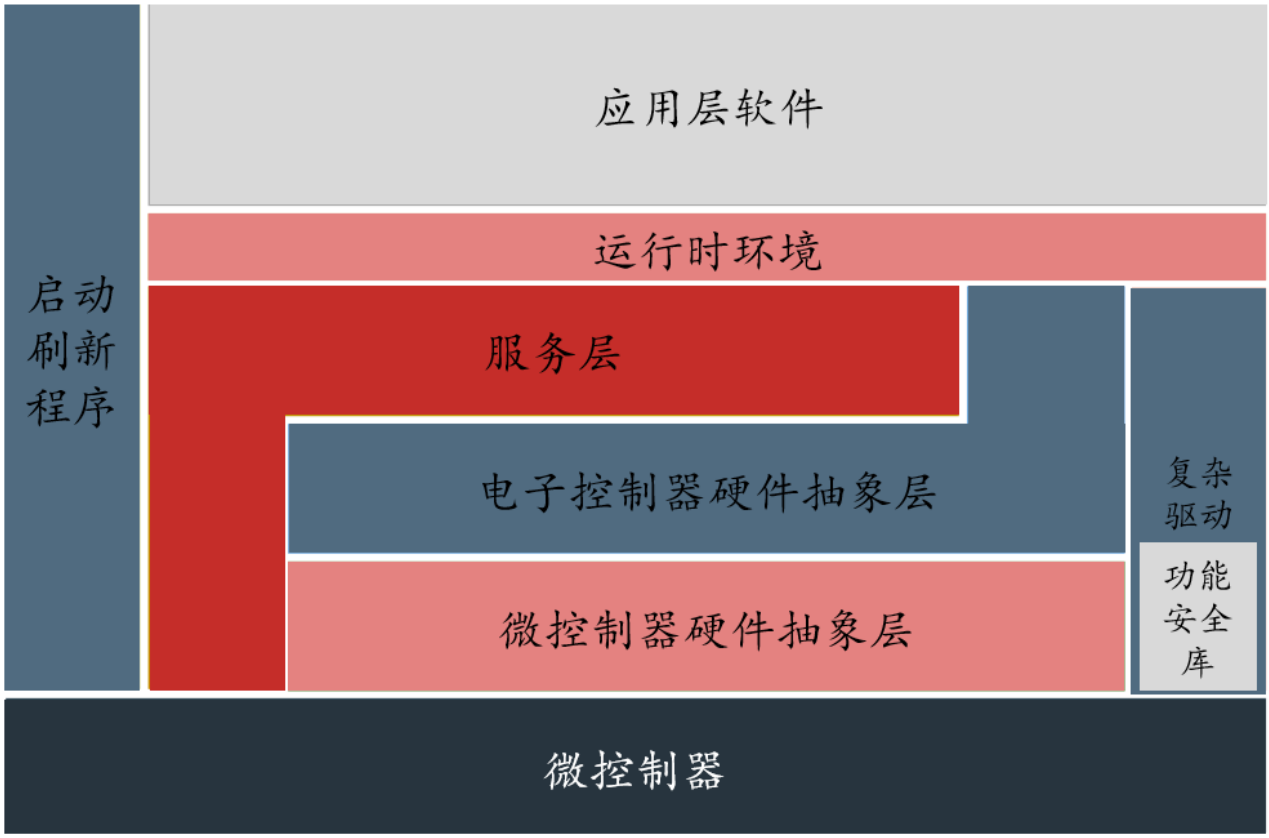
	ASIL B	ASIL C	ASIL D
Single-point fault metric	≥90 %	≥97 %	≥99 %

	ASIL B	ASIL C	ASIL D
Latent-fault metric	≥60 %	≥80 %	≥90 %

© 2017-2024 上海知从科技有限公司

5 功能描述

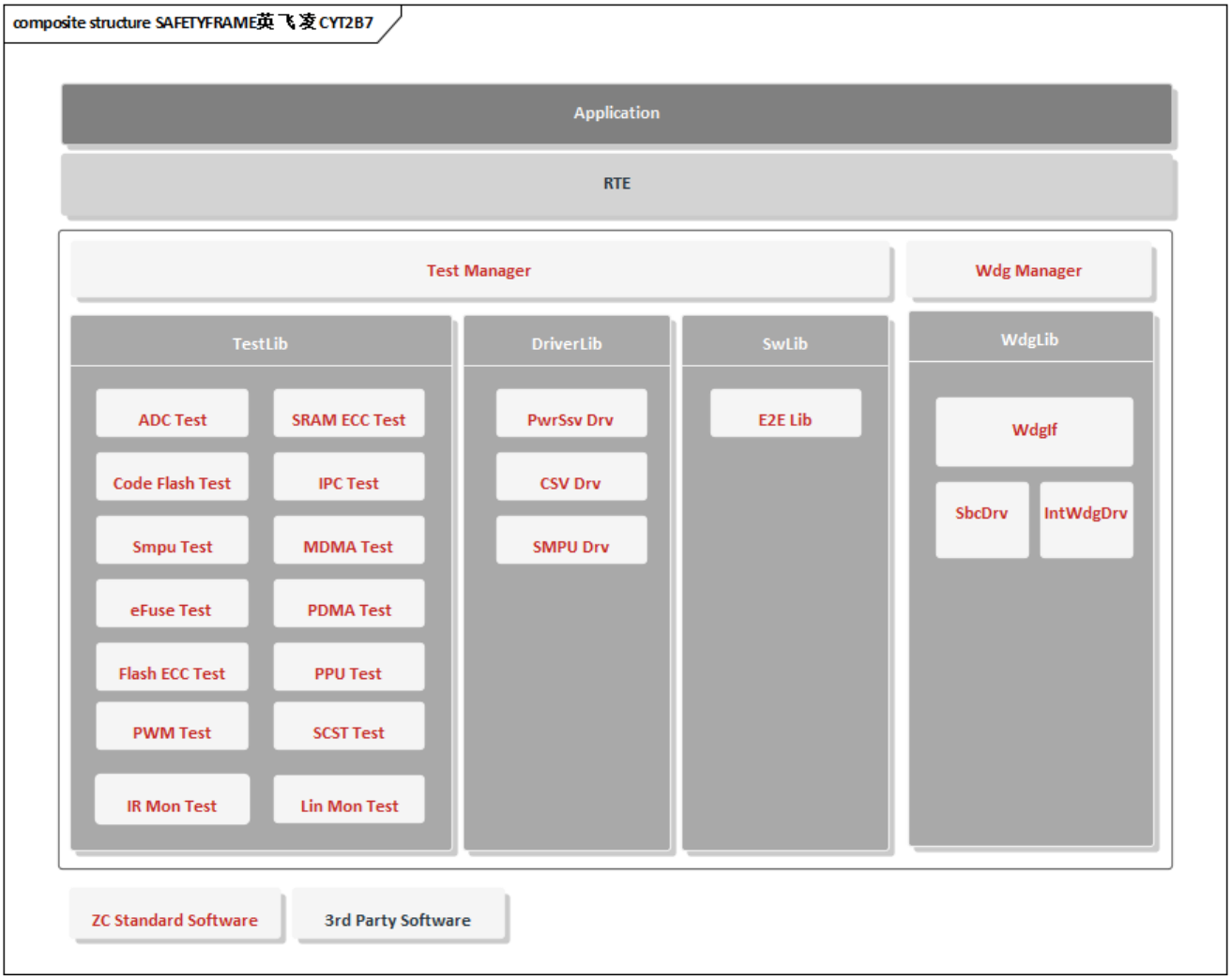
5.1 产品特点



- 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：支持自检测试，搭配知从科技 SBC 复杂驱动可实现高达 ASIL-B 需求
- 高扩展性：各模块可配置满足不同客户的应用需求

© 2017-2024 上海知从科技有限公司

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	ADCTst	ADC模块采样检测
	CodeFlsTst	Code Flash的完整性检测
	SmpuTst	MPU/Smpu功能检测
	eFuseTst	eFuse trim values冗余存储检测
	FlashECCTst	Flash ECC驱动和ECC功能检测
	IpcTst	通信数据的完整性校验和通信时间超时检测
	MDmaTst	MDMA冗余通道传输检测
	PDmaTst	PDMA冗余通道传输检测
	PPUTst	外设/系统组件的权限保护检测
	PwmTst	Pwm输出回读检测

© 2017-2024 上海知从科技有限公司

	SCST	内核自检
	SramEccTst	SRAM ECC功能检测
	IRMonTst	中断监控
	LinMonTst	Lin传输监控检测
驱动库	PwrSsvDrv	VDDD和VDDA电压监控驱动
	CsvDrv	时钟监控模块驱动
	SmpuDrv	Smpu 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

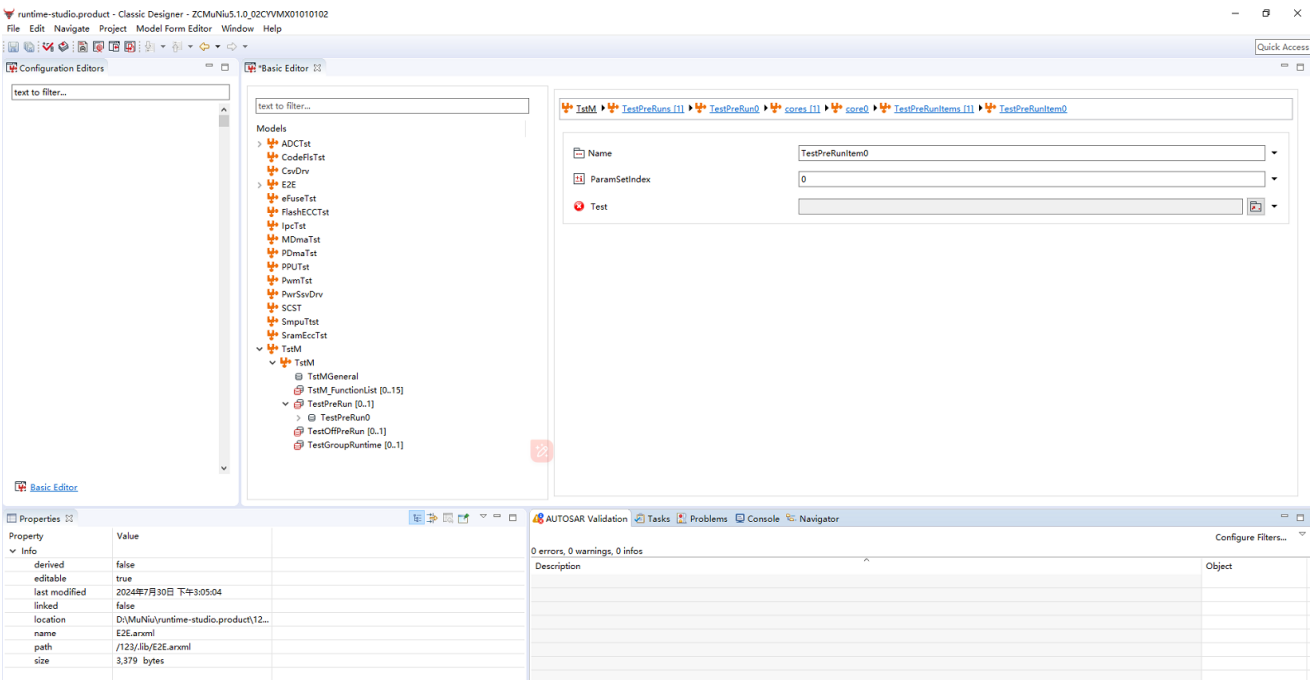
满足 CYT2B7 Safety Manual 中的 MXS：

安全机制	描述
MXS40-9165	ADC 配置保护
MXS40-12752	ADC MUX 测试
MXS40-298	ADC 采样测试
MXS40-235	停电检测阈值配置
MXS40-5641	BOD 低电压检测
MXS40-233	时钟监控器检测
MXS40-226	时钟监控器窗口配置
MXS40-193	Code Flash 完整性校验
MXS40-184	内核自检
MXS40-9167	BOD 、OVD 冗余存储
MXS40-5625	eFuse 用户数据完整性校验
MXS40-287	E2E 保护
MXS40-190	Flash Ecc 配置使能
MXS40-185	FPU 检测
MXS40-9163	IPC 消息保护
MXS40-9162	IPC 超时保护
MXS40-9058	Lin 传输监控
MXS40-424	MDMA 传输检测
MXS40-318	中断监控
MXS40-138	MPU、SMPU 检测
MXS40-5644	VCCD 电压监控
MXS40-238	过压检测阈值配置
MXS40-8996	PDMA 传输检测

© 2017-2024 上海知从科技有限公司

MXS40-181	程序流监控
MXS40-294	PWM 输出回读检测
MXS40-348	RAM ECC 检测使能
MXS40-279	SCB 监控
MXS40-8092	SMPU 配置
MXS40-208	SRAM ECC 检测
MXS40-319	中断有效性检测
MXS40-186	Work Flash 数据完整性校验
MXS40-13046	CXPI 监控
MXS40-12756	HVD 配置
MXS40-12754	LVD 配置
MXS40-148	PPU 检测
MXS40-258	GPIO 回读检测
MXS40-21241	VDDIO 监控

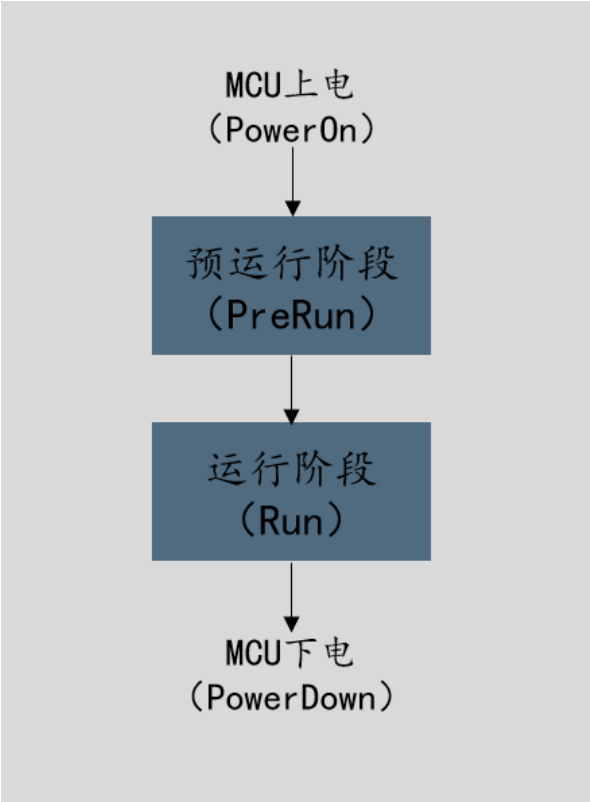
5.3 配置工具



为了满足客户的不同项目需求，提高 Safety Frame 的扩展性，CYT2B7 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。

© 2017-2024 上海知从科技有限公司

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，同时部分 MCU 的安全机制在此阶段进行测试。

© 2017-2024 上海知从科技有限公司

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	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	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

© 2017-2024 上海知从科技有限公司

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.

© 2017-2024 上海知从科技有限公司

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

© 2017-2024 上海知从科技有限公司



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

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

© 2017-2024 上海知从科技有限公司