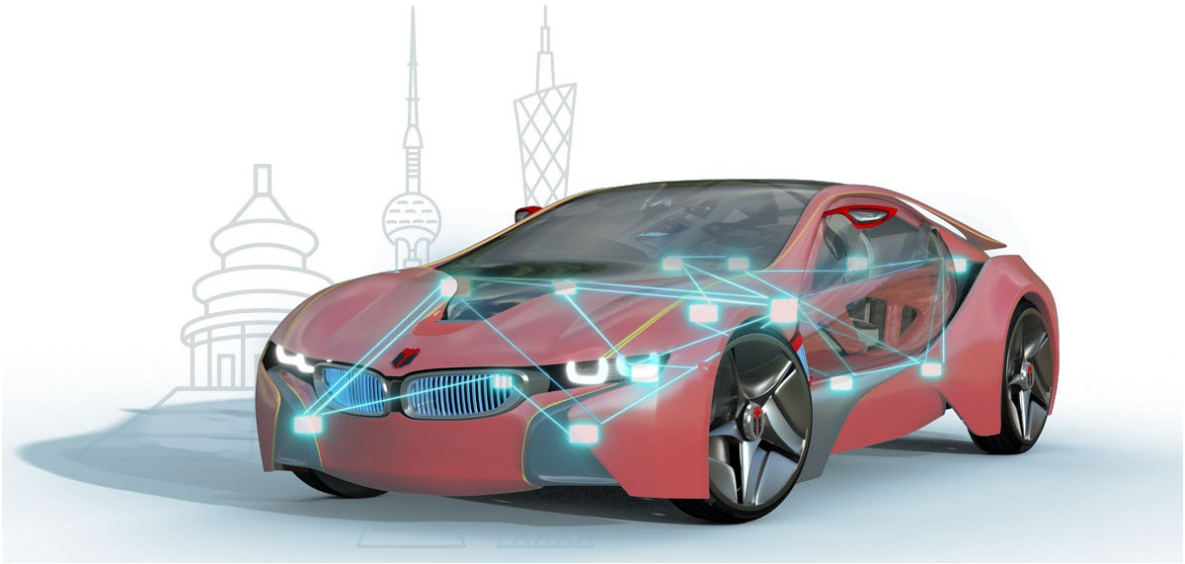
知从木牛 SAFETY FRAME 赛普拉斯 CYT2B7 产品手册

ZC.MUNIU SAFETYFRAME PRODUCT MANUAL

BASED ON CYPRESS CYT2B7

知从木牛基础软件平台功能安全库

ZC.MuNiu Basic Software Platform Functional Safety Library



知从木牛 SAFETY FRAME 赛普拉斯 CYT2B7 产品手册

ZC.MUNIU SAFETYFRAME PRODUCT MANUAL BASED ON CYPRESS CYT2B7

知从木牛基础软件平台功能安全库

ZC.MuNiu Basic Software Platform Functional Safety Library

1 功能概述 FUNCTIONAL OVERVIEW

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。

The CYT2B7 SafetyFrame is designed to assist customers in achieving functional safety requirements based on the RENESAS CYT2B7 platform. The SafetyFrame is highly scalable and can be configured and redeveloped according to different customer project requirements, ultimately meeting the functional safety requirements of the customers.

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。

The CYT2B7 SafetyFrame is used to implement software safety mechanisms for the TRAVEO™ T2G series, including fault testing of internal MCU modules and the driving functions of hardware safety mechanisms.

2 应用领域 APPLICATION FIELD

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

The CYT2B7 SafetyFrame can be applied to controllers that have functional safety level requirements. For example:

- 汽车车身电子设备
  Automotive Body Electronics
- 汽车车身控制模块 (BCM)
  Automotive Body Control Module (BCM)
- 带集成网关的车身控制模块 (BCM)
  Body Control Module with Integrated Gateway (BCM)
- 汽车网关
  Automotive Gateway
- 汽车 LED 前照灯
  Automotive LED Headlights

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。

By integrating the Safety Frame into CYT2B7 -based controls, it is possible to meet the ISO26262 ASIL-D level requirements.

3 配置环境 CONFIGURATION ENVIRONMENT

配置环境 Configuration Environment	
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 Compiler Option	
IAR 编译选项 **IAR Compiler Options**	--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 **IAR Linker Options**	--cpu=Cortex-M4 -e --fpu=None DSTART_FROM_FLASH -DM4_DEVICE_RESERVED_ADDR

4 开发背景 DEVELOPMENT BACKGROUND

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。

Currently, the electronic and electrical architecture of automobiles is becoming increasingly complex, and the safety requirements for automotive electronics are also rising. To meet the safety requirements of automobiles, functional safety is gaining more attention. When it comes to functional safety, the first thing that comes to mind is the functional safety standard ISO 26262. In particular, ISO 26262-5(2018) Clause 8 introduces two metrics: Single-point fault metric (single-point fault metric) and Latent-fault metric (latent fault metric). Depending on the required ASIL level, the single-point fault metric and latent fault metric must meet the corresponding levels.

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。

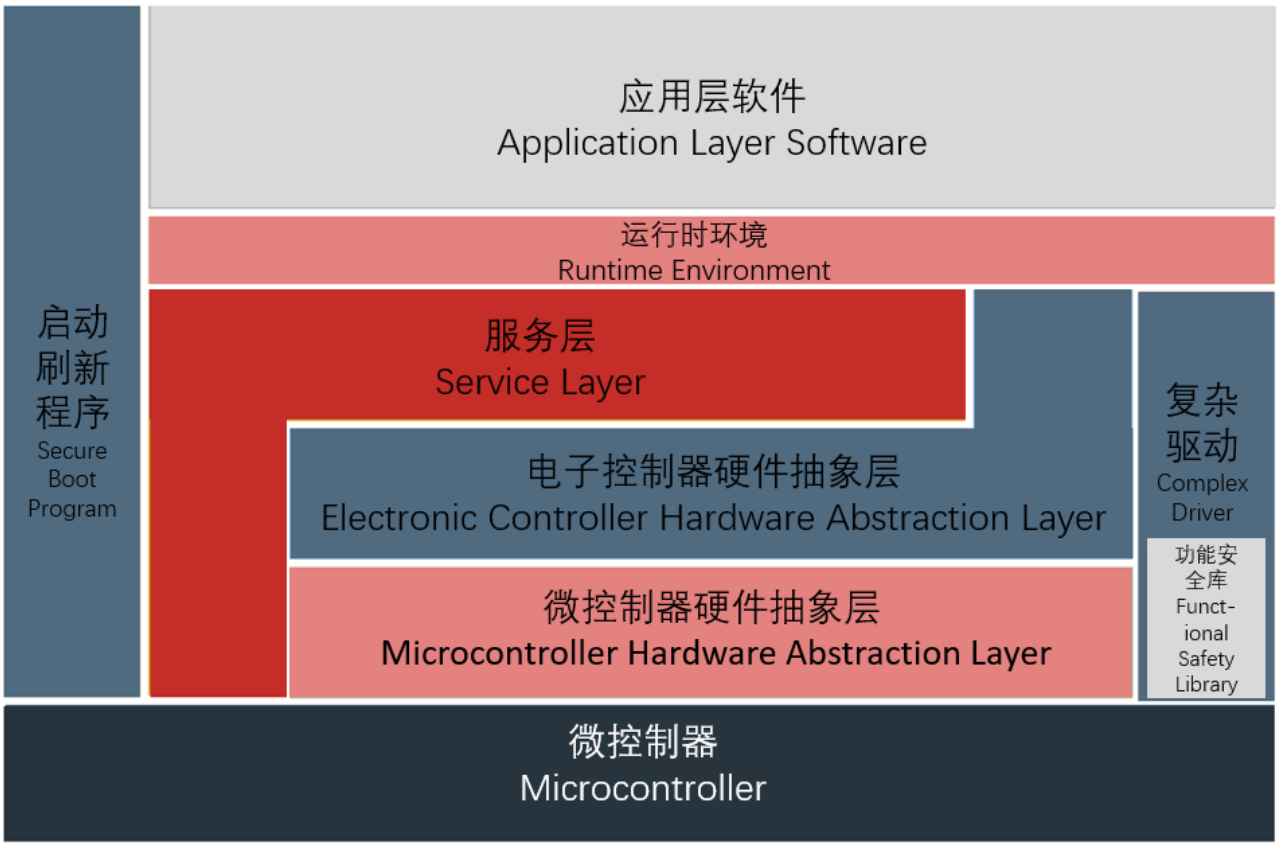
For microcontrollers (MCU, referred to as MCU below), within the electronic and electrical system, they are designed and developed as SEooC (safety element out of context). To meet the aforementioned metric requirements, MCUs need to implement corresponding safety mechanisms. These safety mechanisms can be allocated to both hardware and software modules. The Safety Frame safety library for MCUs is the implementation of safety mechanisms allocated to software.

	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 FUNCTIONAL DESCRIPTION

5.1 产品特点 Product Feature



- 可作为复杂驱动集成到 AUTOSAR 中

  Can be integrated as a complex driver into AUTOSAR.

- 可集成到非 AUTOSAR 软件架构中，灵活适配

  Can be integrated into non-AUTOSAR software architectures, with flexible adaptation.

- 支持多核测试及应用

  Supports multi-core testing and application.

- Safety Frame 具有内部程序流监控

  Safety Frame has internal program flow monitoring.

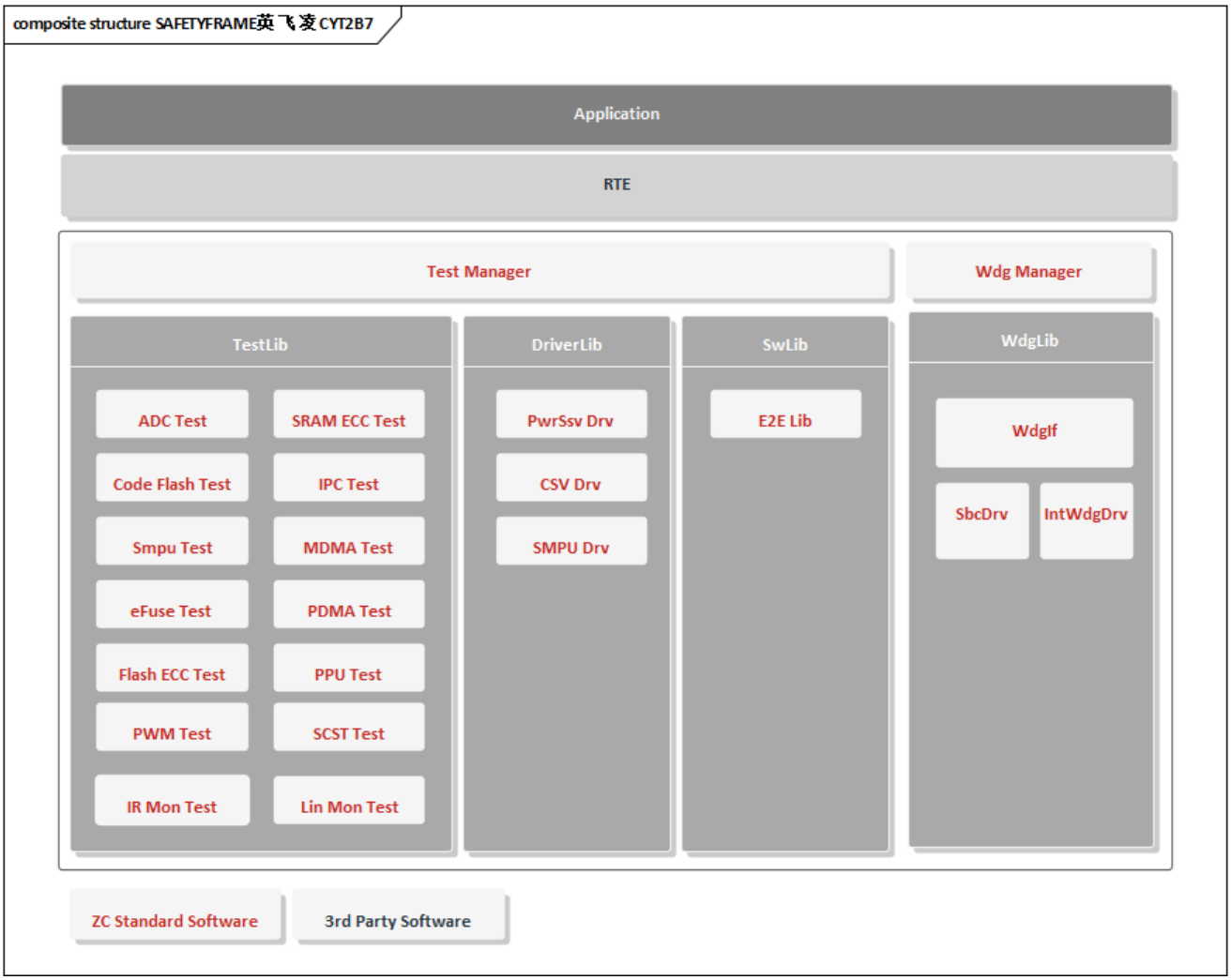
- 高安全性：支持自检测试，搭配知从科技 SBC 复杂驱动可实现高达 ASIL-B 需求

  High Safety: Supports self-diagnostics, and when paired with Zhicong Technology's SBC complex drivers, it can meet the high ASIL-B requirements

- 高扩展性：各模块可配置满足不同客户的应用需求

High scalability: Each module can be configured to meet the application requirements of different customers.

5.2 软件架构 Software Architecture



软件架构 Software Architecture

实现的功能模块:

Implemented functional modules:

模块 Module	子模块 Sub-module	描述 Description
测试库 Test Library	ADCTst	ADC模块采样检测 ADC Module Sampling Inspection
	CodeFlsTst	Code Flash的完整性检测 Code Flash Integrity Check
	SmpuTst	MPU/Smpu功能检测

		MPU/Smpu Functionality Test
	eFuseTst	eFuse trim values冗余存储检测 eFuse Trim Values Redundant Storage Check
	FlashECCTst	Flash ECC驱动和ECC功能检测 Flash ECC Driver and ECC Feature Detection
	IpcTst	通信数据的完整性校验和通信时间超时检测 Communication Data Integrity Verification and Communication Timeout Detection
	MDmaTst	MDMA冗余通道传输检测 MDMA Redundant Channel Transmission Test
	PDmaTst	PDMA冗余通道传输检测 PDMA Redundant Channel Transmission Test
	PPUTst	外设/系统组件的权限保护检测 Peripheral/System Component Access Rights Protection Test
	PwmTst	Pwm输出回读检测 PWM Output Readback Detection
	SCST	内核自检 Kernel Self-Check
	SramEccTst	SRAM ECC功能检测 SRAM ECC Feature Detection
	IRMonTst	中断监控 Interrupt Monitoring
	LinMonTst	Lin传输监控检测 LIN Transmission Monitoring and Detection
驱动库 Driver Library	PwrSsvDrv	VDDD和VDDA电压监控驱动 VDDD and VDDA Voltage Monitoring Driver
	CsvDrv	时钟监控模块驱动 Clock Monitoring Module Driver
	SmpuDrv	Smpu 配置驱动 Smpu Configuration Driver
SwLib	E2E Lib	E2E保护协议库 E2E protection protocol library
Wdg 驱动库 Wdg Driver	WdgIf	看门狗驱动接口 Watchdog driver interface
	SbcDrv	SBC芯片驱动

		SBC chip driver
	IntWdg Drv	内部看门狗驱动 Internal watchdog driver
Wdg Manager	Wdg Manager	看门狗管理模块 Watchdog management module
Test Manager	Test Manager	测试管理模块 Test management module

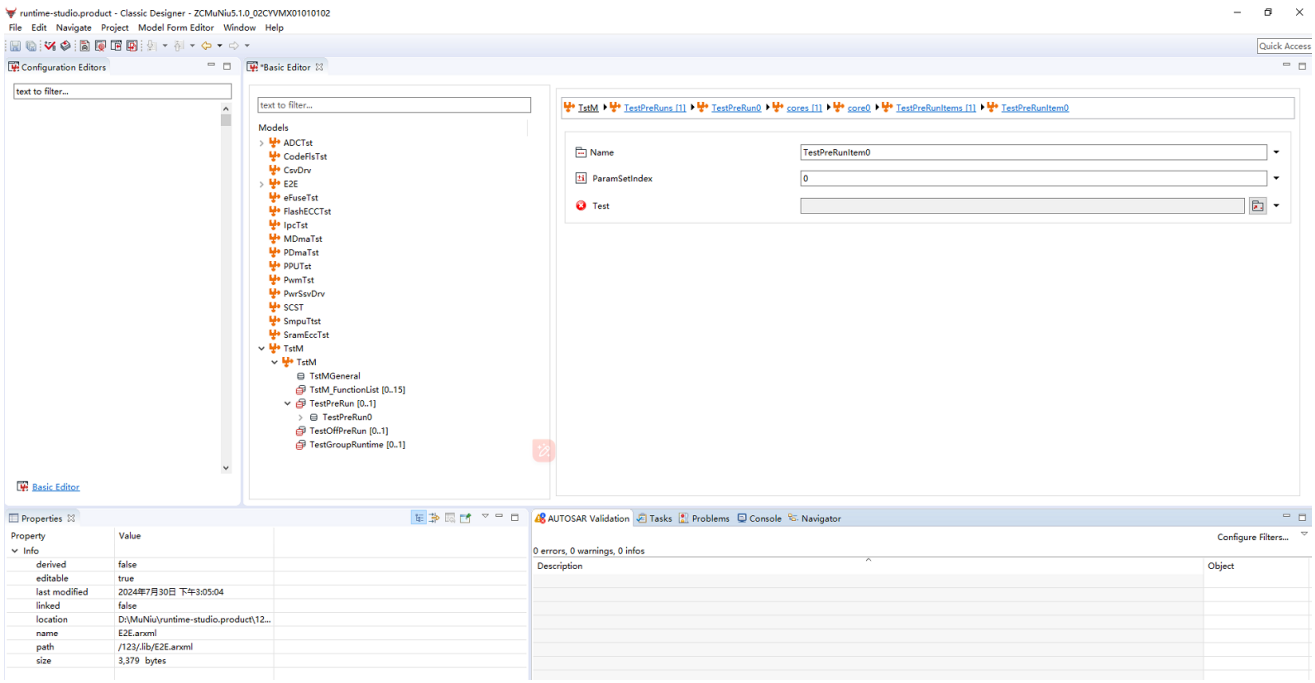
满足 CYT2B7 Safety Manual 中的 MXS:

安全机制 Safety Mechanism	描述 Description
MXS40-9165	ADC 配置保护 ADC Configuration Protection
MXS40-12752	ADC MUX 测试 ADC MUX Test
MXS40-298	ADC 采样测试 ADC Sampling Test
MXS40-235	停电检测阈值配置 Power Loss Detection Threshold Configuration
MXS40-5641	BOD 低电压检测 BOD Low Voltage Detection
MXS40-233	时钟监控器检测 Clock Monitor Detection
MXS40-226	时钟监控器窗口配置 Clock Monitor Window Configuration
MXS40-193	Code Flash 完整性校验 Code Flash Integrity Check
MXS40-184	内核自检 Kernel Self-Check
MXS40-9167	BOD 、OVD 冗余存储 BOD, OVD Redundant Storage
MXS40-5625	eFuse 用户数据完整性校验 eFuse User Data Integrity Check
MXS40-287	E2E 保护 E2E Protection
MXS40-190	Flash Ecc 配置使能 Flash ECC Configuration Enable
MXS40-185	FPU 检测 FPU Detection

MXS40-9163	IPC 消息保护 IPC Message Protection
MXS40-9162	IPC 超时保护 IPC Timeout Protection
MXS40-9058	Lin 传输监控 LIN Transmission Monitoring
MXS40-424	MDMA 传输检测 MDMA Transmission Detection
MXS40-318	中断监控 Interrupt Monitoring
MXS40-138	MPU、SMPU 检测 MPU, SMPU Detection
MXS40-5644	VCCD 电压监控 VCCD Voltage Monitoring
MXS40-238	过压检测阈值配置 Overvoltage Detection Threshold Configuration
MXS40-8996	PDMA 传输检测 PDMA Transmission Detection
MXS40-181	程序流监控 Program Flow Monitoring
MXS40-294	PWM 输出回读检测 PWM Output Readback Detection
MXS40-348	RAM ECC 检测使能 RAM ECC Detection Enable
MXS40-279	SCB 监控 SCB Monitoring
MXS40-8092	SMPU 配置 SMPU Configuration
MXS40-208	SRAM ECC 检测 SRAM ECC Detection
MXS40-319	中断有效性检测 Interrupt Validity Detection
MXS40-186	Work Flash 数据完整性校验 Work Flash Data Integrity Check
MXS40-13046	CXPI 监控 CXPI Monitoring
MXS40-12756	HVD 配置 HVD Configuration
MXS40-12754	LVD 配置 LVD Configuration
MXS40-148	PPU 检测 PPU Detection
MXS40-258	GPIO 回读检测

	GPIO Readback Detection
MXS40-21241	VDDIO 监控 VDDIO Monitoring

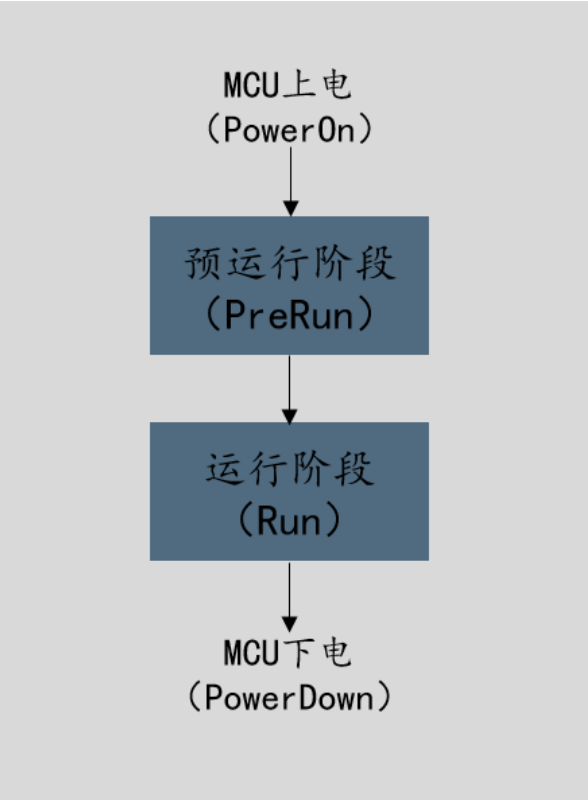
5.3 配置工具 Configuration Tool



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。

To meet the varying project requirements of customers and enhance the extensibility of SafetyFrame, the CYT2B7 SafetyFrame has implemented configurable modules and has developed a configuration tool for SafetyFrame. Customers can complete the configuration of various SafetyFrame modules according to different requirements using the configuration tool, generate configuration code files, and integrate the generated configuration files into the project.

5.4 运行阶段 Run Phase



- 预运行阶段 PreRun Phase

  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。

  This phase involves testing the safety mechanisms of the MCU, which is generally conducted before the OS starts up.

- 运行阶段 Run Phase

  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。

  This phase takes place during task execution, while the OS is running, and some of the MCU's safety mechanisms are tested during this phase.

6 过程文档 PROCESS DOCUMENTATION

开发流程 Development Process	文档描述 Document Description
需求收集 Requirement Collection	客户的需求文档 Customer's requirement document
软件需求分析 Software Requirement Analysis	需求分析规格书 Requirement analysis specification
	软件需求追踪表 Software requirement traceability matrix
	客户问题沟通表 Customer issue communication form
软件架构设计 Software Architecture Design	软件架构说明书 Software architecture manual
	软件架构的追踪表 Software architecture traceability matrix
软件详细设计和单元设计 Detailed Software Design and Unit Design	软件模块详细设计说明书 Software module detailed design manual
	配置工具设计 Configuration tool design
	软件详细设计追踪表 Software detailed design traceability matrix
	Safety Frame 工程评审 Safety Frame project review
软件单元测试 Software Unit Testing	QAC 分析报告 QAC analysis report
	Tessy 测试报告 Tessy test report
	软件单元验证策略 Software unit verification strategy
软件集成和集成测试 Software Integration and	集成策略 Integration strategy
	集成手册 pdf Integration manual (PDF)

Integration Testing	集成测试策略 Integration test strategy
	集成测试报告 Integration test report
	资源分析报告 Resource analysis report
	木牛.Safety Frame 配置工具使用指导书 Muniu.Safety Frame configuration tool user guide
	木牛.Safety Frame 配置工具软件配置管理文档 Muniu.Safety Frame configuration tool software configuration management document
软件认可测试 Software Qualification Testing	软件测试报告 Software test report
	软件测试策略 Software test strategy
发布 Release	发布文档 Release documentation

7 功能安全 FUNCTIONAL SAFETY

7.1 功能安全评估报告 Functional Safety Assessment Report

7.2 功能安全证书 Functional Safety Certificate

SGS TÜV SAAR

CERTIFICATE NO FS/71/220/23/1031 **PAGE 1/1**
ZERTIFIKAT NR.: *SEITE(N)*

LICENCE HOLDER & MANUFACTURER
GENEHMIGUNGSINHABER & HERSTELLER

Shanghai ZC Technology Co., Ltd.
Building C, 888 Huanhu West 2nd Road,
Pudong New Area,
Shanghai,
P.R. China

PROJECT NO/-ID *PROJEKT-NR/-ID*	LICENSED TEST MARK *GENEHMIGTES PRÜFZEICHEN*	CERT. REPORT NO. *ZERTIFIKATSBERICHT NR.*
T4A8-AU01	SGS TÜV SAAR ASIL D COMPLIANT Functional Safety ISO 26262 www.sgs-tuv-saar.com	T4A80002 is an integral part of this certificate. *ist ein integraler Bestandteil dieses Zertifikats.*

Certified product(s)
Zertifizierte(s) Produkt(e)
SafetyFrame
Version 2.1.0

Tested according to
Geprüft nach
ISO 26262-2:2018
ISO 26262-6:2018
ISO 26262-8:2018
ISO 26262-9:2018

Technical Data and Parameter
Technische Daten und Parameter
The judgement of the achieved functional safety for the above-mentioned SafetyFrame Software is "accepted" according to above mentioned standards ASIL D requirements.

The SafetyFrame Software is suitable for integration into systems up to ASIL D.

The certificate is based on voluntary tests. The compliance of the certified product against the requirements of above listed functional safety standards was evaluated. Any changes to the design, components or processing may require repetition of some parts of the certification to retain the certification. All applicable requirements of the testing and certification regulations of SGS-TÜV Saar GmbH have to be complied, see www.sgs-tuv-saar.com/tcr-muc and www.sgs-tuv-saar.com/gtc-muc

Certification Body for Functional Safety & Cyber Security SGS-TÜV Saar GmbH
Zertifizierungsstelle für Funktionale Sicherheit & Cyber Sicherheit

Reference to SGS Certification Database

Munich, Feb 22, 2023
Gudrun Neumann

SGS-TÜV Saar GmbH, Hofmannstr. 50, 81379 München, *Deutschland* / Germany
Website: www.sgs-tuv-saar.com
E-Mail: fs@ts-gs.com

ISO26262 ASIL D CERTIFICATE

8 证书 CERTIFICATE

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

ZC.MUNIU SOFTWARE COPYRIGHT REGISTRATION CERTIFICATE

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

ZC. MUNIU SOFTWARE PRODUCT REGISTRATION CERTIFICATE