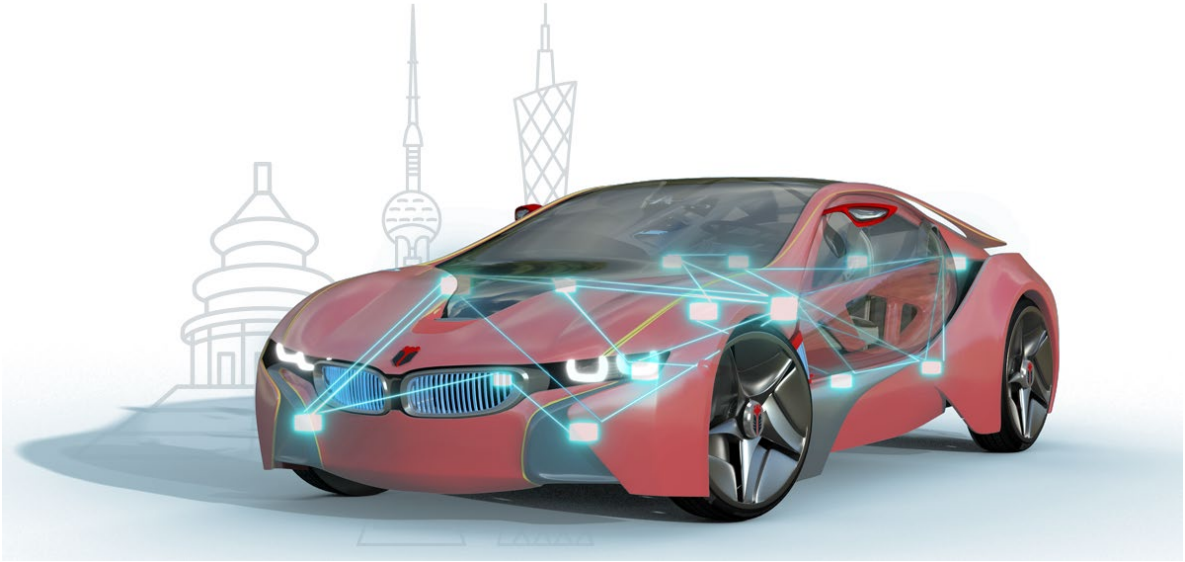
知从木牛 SAFETYFRAME 瑞萨 RH850F1KM 产品手册

ZC.MUNIU SAFETYFRAME PRODUCT MANUAL BASED ON RH850F1KM

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 SAFETYFRAME 瑞萨 RH850F1KM 产品手册
ZC.MUNIU SAFETYFRAME PRODUCT MANUAL BASED ON RH850F1KM

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

RH850F1KM SafetyFrame 用于帮助客户实现基于 RENESAS RH850F1KM 平台的功能安全要求。SafetyFrame 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 RH850F1KM SafetyFrame is designed to assist customers in achieving functional safety requirements based on the RENESAS RH850F1KM 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.

RH850F1KM SafetyFrame 用于实现 RH850F1KM 系列的软件安全机制，包括 MCU 内部模块的故障测试和硬件安全机制的驱动功能。

The RH850F1KM SafetyFrame is used to implement software safety mechanisms for the RH850F1KM series, including fault testing of internal MCU modules and the driving functions of hardware safety mechanisms.

2 应用领域 APPLICATION FIELD

RH850F1KM SafetyFrame 可应用于有功能安全等级需求的控制器。例如:
The RH850F1KM SafetyFrame can be applied to controllers that have functional safety level requirements. For example:

- 电池管理系统(BMS)
  Battery Management System (BMS)
- 智能驾驶控制器(ADAS)
  Advanced Driver Assistance Systems (ADAS)
- 智能网关控制器(Gateway)
  Smart Gateway Controller (Gateway)
- 智能刹车系统(iBooster)
  Intelligent Braking System (iBooster)
- 车身稳定控制(ESC/Onebox)
  Vehicle Stability Control (ESC/Onebox)
- 电动助力转向(EPS)
  Electric Power Steering (EPS)
- 车身控制器(BCM)
  Body Control Module (BCM)
- 发动机管理系统(EMS)
  Engine Management System (EMS)
- 底盘域线控系统应用
  Chassis Domain Control System Applications
- 区域控制器
  Regional Controllers

通过将 Safety Frame 集成到基于 RH850F1KM 的控制中，可达到 ISO26262 ASIL-D 的等级要求。
By integrating the Safety Frame into RH850F1KM-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)	RENESAS RH850F1KM
Compilers Supported	GHS_For_RH850 Compiler v2020.1.5
Evaluation Hardware	FG2 RH850F1KM U2Ax_C and U2Ax_3
Debugger	Lauterbach (Trace32 R.2024.02) Isystem (IC5700)
Configuration Tools	知从木牛.配置工具V5.1.0 ZC.Muniu Configuration Tool V5.1.0
Configuration Environment	Win10 64bit

编译器选项 Compiler Option	
GreenHills 编译选项 **GreenHills Compiler Options**	-Onone -OB -no_data_delete -delete -dual_debug -ignore_debug_references -object_dir=objs -init_ram_at_startup {optgroup=GhsCommonOptions} -o RH850_SafetyFrame.elf :postexec='gsrec -B -hex386 ./out/RH850_SafetyFrame.elf -o RH850_SafetyFrame.hex' -full_debug_info -G -gnu99 -cpu=rh850g4kh -bsp generic
GreenHills 链接选项 **GreenHills Linker Options**	-e _RESET

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。

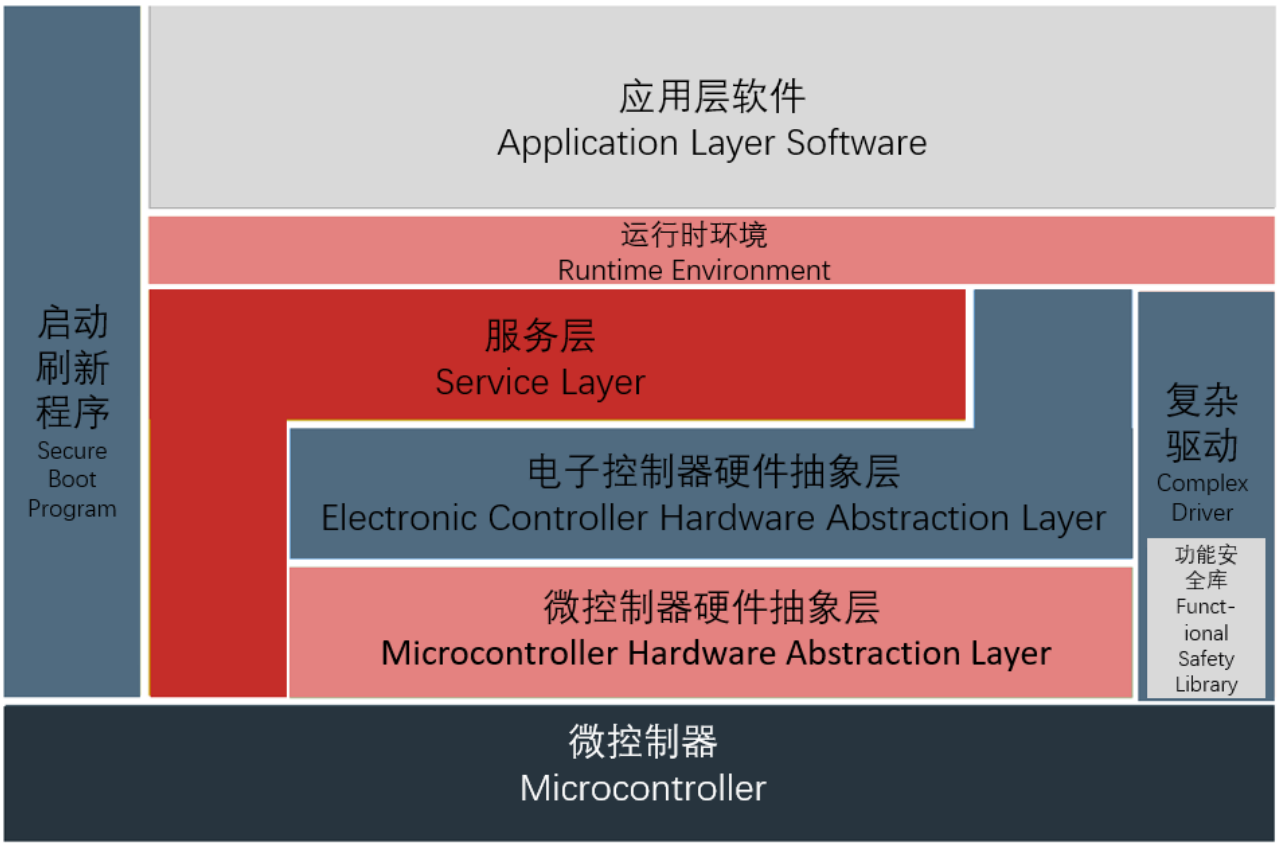
For microcontrollers (MCU, referred to as MCU below), within the electronic and electrical system, they are designed and developed as SEooC (safety element out of context). To meet the aforementioned metric requirements, MCUs need to implement corresponding safety mechanisms. These safety mechanisms 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.

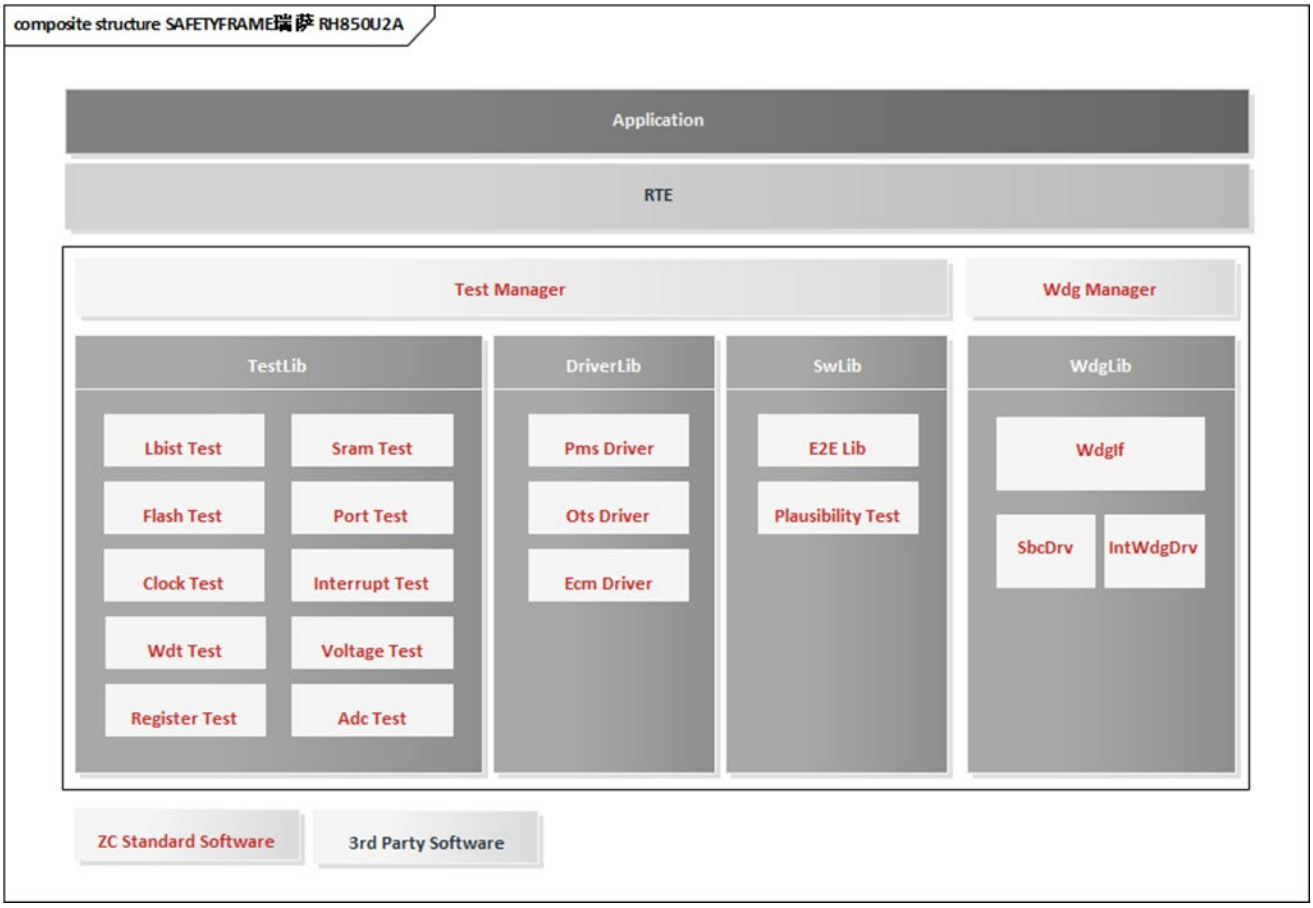
- Safety Frame 具有内部程序流监控

  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	Lbist Test	Logic BIST和Memory配置和结果检测 Logic BIST and Memory configuration and result detection
	Sram Test	Sram 数据检测 Sram data detection
	Flash Test	Flash数据检测 Flash data detection
	Port Test	Port模块启动检测 Port module startup detection
	Clock Test	时钟合理性模块检测 Clock rationality module detection
	Interrupt Test	中断检测 Interrupt detection

	Register Test	寄存器检测 Register detection
	Wdt Test	看门狗检测 Watchdog detection
	Voltage Test	电压监控检测 Voltage monitoring detection
	Adc Test	Adc模块检测 Adc module detection
驱动库 Driver Library	Pms Driver	电源监控配置驱动 Power monitoring configuration driver
	Ots Driver	温度监控配置驱动 Temperature monitoring configuration driver
	Ecm Driver	Ecm模块配置驱动 Ecm module configuration driver
SwLib	E2E Lib	E2E保护协议库 E2E protection protocol library
	Plausibility Test	数据合理性校验库 Data plausibility verification 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

满足的 RH850F1KM Safety Application Note 中的 Safety Mechanism：

Safety Mechanisms Satisfied in the RH850F1KM Safety Application Note:

安全机制 Safety Mechanism	子安全机制 Sub-security Mechanism
Core [SAN-F1KM-0010]	
Overview of RH850/F1KM ECC Functiosn [SAN-F1KM-0020]	
Code Flash ECC [SAN-F1KM-0030]	
Data Flash ECC [SAN-F1KM-0040]	
Local (Retention) RAM ECC [SAN-F1KM-0050]	

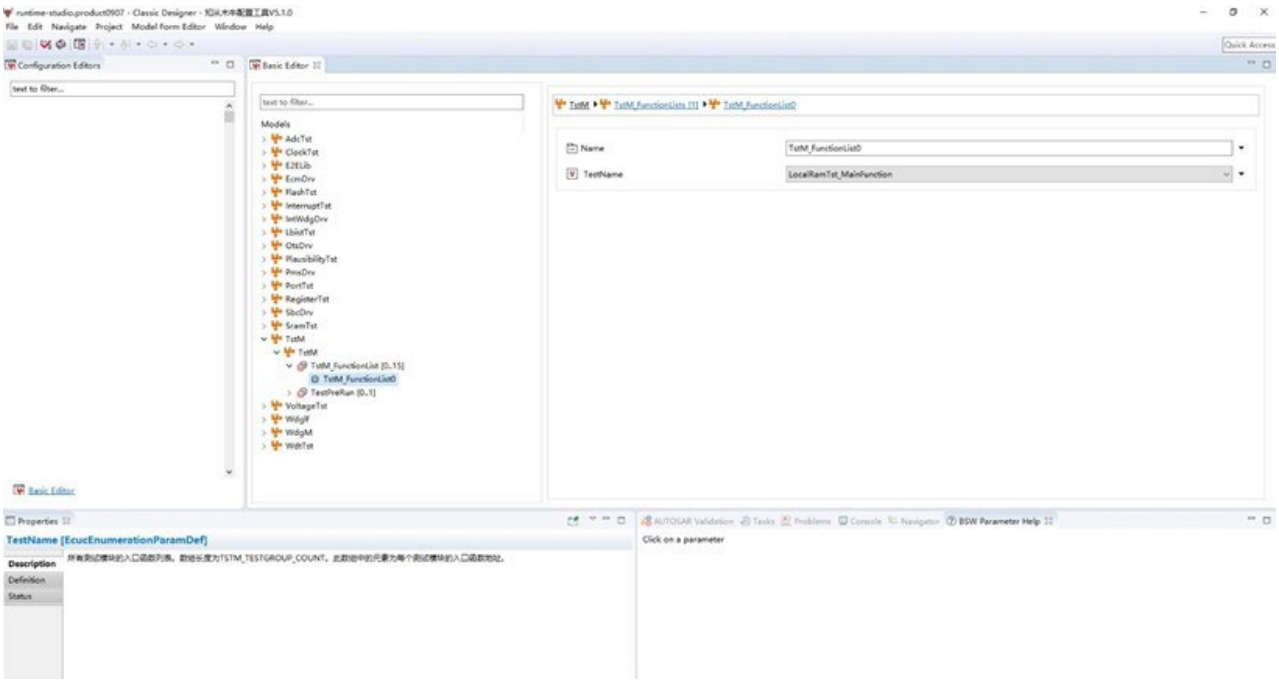
安全机制 Safety Mechanism	子安全机制 Sub-security Mechanism
Peripheral RAM ECC of RS-CANFD [SAN-F1KM-0060]	
Peripheral RAM ECC of CSIH [SAN-F1KM-0070]	
DMA [SAN-F1KM-0080]	
RESET [SAN-F1KM-0090]	
CRC (DCRA) [SAN-F1KM-0100]	
Clock Monitor [SAN-F1KM-0110]	
Watchdog Timer [SAN-F1KM-0120]	
A/D Converter [SAN-F1KM-0130]	
CSI (CSIH) [SAN-F1KM-0140]	
CSI (CSIG) [SAN-F1KM-0150]	
LIN (RLIN2) [SAN-F1KM-0160]	
LIN (RLIN3) [SAN-F1KM-0170]	
CAN (RS-CANFD) [SAN-F1KM-0180]	
Memory Protection Unit Test [SAN-F1KM-0190]	
Data Flash Write / Verify [SAN-F1KM-0200]	
Memory Test [SAN-F1KM-0210]	
Configuration Register Read/Verify [SAN-F1KM-0220]	
Interrupt Consistency Check [SAN-F1KM-0230]	
Timer Protection Function [SAN-F1KM-0240]	
Loopback of Timer [SAN-F1KM-0250]	
Loopback of PWM [SAN-F1KM-0260]	External loop back and comparison with other timer [SAN-F1KM-0261]
	External loop back for PWM with ADC [SAN-F1KM-0262]
E2E Protection [SAN-F1KM-0270]	
I/O Port Diagnosis [SAN-F1KM-0280]	
Multiple Operation [SAN-F1KM-0290]	
Voltage Monitoring [SAN-F1KM-0300]	
Core Voltage Monitor [SAN-F1KM-0310]	
Slave guard [SAN-F1KM-0320]	P-Bus Guard (PBG/PBGC) [SAN-F1KM-0321]
	Processing Element Guard (PEG) [SAN-F1KM-0322]
	Internal Peripheral Guard (IPG) [SAN-F1KM-0323]
	Global RAM Guard (GRG) [SAN-F1KM-0324]

安全机制 Safety Mechanism	子安全机制 Sub-security Mechanism
	H-Bus Guard (HBG) [SAN-F1KM-0325]
Loopback of TAPA [SAN-F1KM-0330]	External loop back for TAPA with ADC [SAN-F1KM-0331]
	External loop back with TAPAxESO [SAN-F1KM-0332]
Alternative safety measure of the external voltage monitor for AWOVCL and ISOVCL [SAN-F1KM-0360]	
Register protection test [SAN-F1KM-0380]	
Local RAM ECC [SAN-F1KM-0390]	
Global (Retention) RAM ECC [SAN-F1KM-0400]	
Peripheral RAM ECC of FlexRay [SAN-F1KM-0410]	
Peripheral RAM ECC of Ethernet AVB [SAN-F1KM-0420]	
FlexRay [SAN-F1KM-0430]	
Ethernet AVB [SAN-F1KM-0440]	

注: 标注颜色部分安全机制由 BIST 模块实现.

Note: Safety mechanisms highlighted in color are implemented by the BIST module.

5.3 配置工具 Configuration Tool

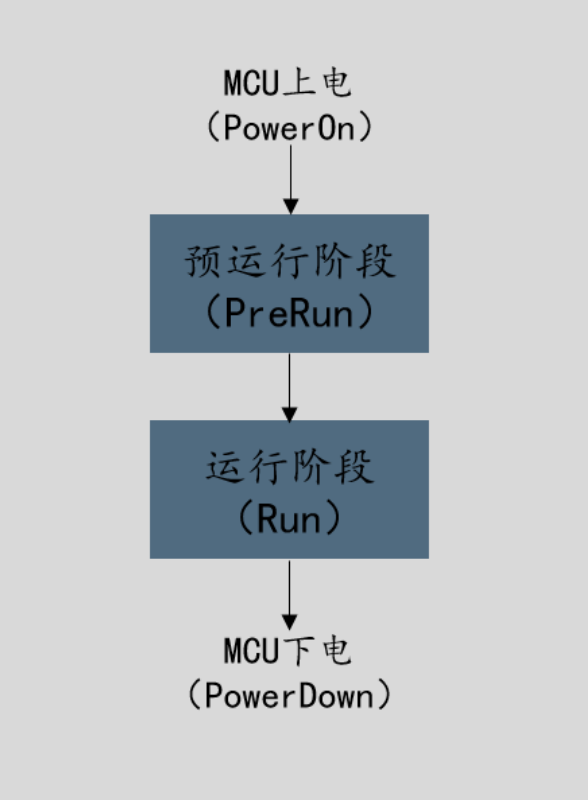


运行阶段为了满足客户的不同项目需求，提高 SafetyFrame 的扩展性，RH850F1KM SafetyFrame 实现了各个模块可配置性，并且实现了 SafetyFrame 的配置工具。客户可根据不

同需求，在配置工具上完成 SafetyFrame 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。

During the operation phase, to meet the varying project requirements of customers and enhance the extensibility of SafetyFrame, the RH850F1KM 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
ZERTIFIKAT NR.:

PAGE 1/1
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-tuev-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: ts@t-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