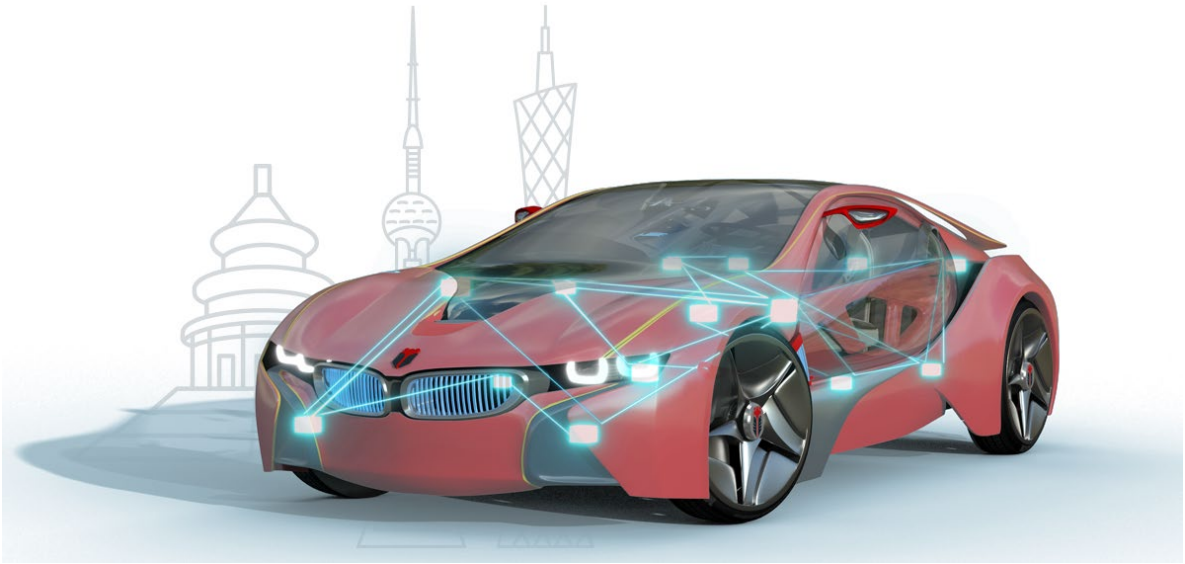
知从木牛 SAFETYFRAME 瑞萨 RH850/P1M-C 产品手册

ZC.MUNIU SAFETYFRAME PRODUCT MANUAL BASED ON RH850/P1M-C

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 RH850/P1M-C 产品手册

ZC.MUNIU SAFETYFRAME PRODUCT MANUAL BASED ON RH850/P1M-C

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

RH850/P1M-C SafetyFrame 用于帮助客户实现基于 RENESAS RH850/P1M-C 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 RH850/P1M-C SafetyFrame is designed to assist customers in achieving functional safety requirements based on the RENESAS RH850/P1M-C 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.

RH850/P1M-C SafetyFrame 用于实现 RH850/P1M-C 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 RH850/P1M-C SafetyFrame is used to implement software safety mechanisms for the RH850/P1M-C series, including fault testing of internal MCU modules and the driving functions of hardware safety mechanisms.

2 应用领域 APPLICATION FIELD

RH850/P1M-C SafetyFrame 可应用于有功能安全等级需求的控制器。例如：
The RH850/P1M-C 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 RH850/P1M-C 的控制中，可达到 ISO26262 ASIL-D 的等级要求。
By integrating the Safety Frame into RH850/P1M-C-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 RH850/P1M-C
Compilers Supported	GHS_For_RH850 Compiler v2020.1.5
Evaluation Hardware	RH850/P1M-C
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=rh850g3m -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。

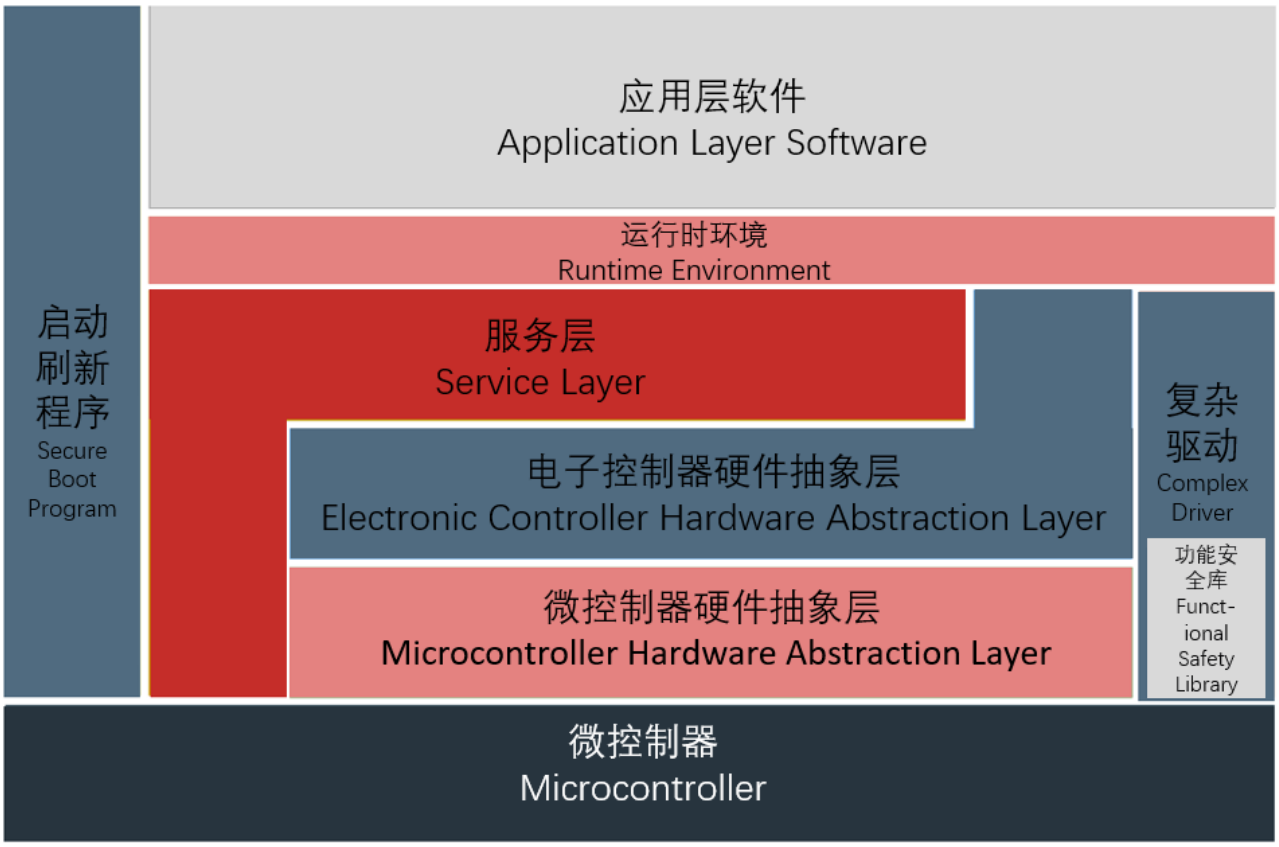
For microcontrollers (MCU, referred to as MCU below), within the electronic and electrical system, they are designed and developed as SEooC (safety element out of context). To meet the aforementioned metric requirements, MCUs need to implement corresponding safety mechanisms. These safety mechanisms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

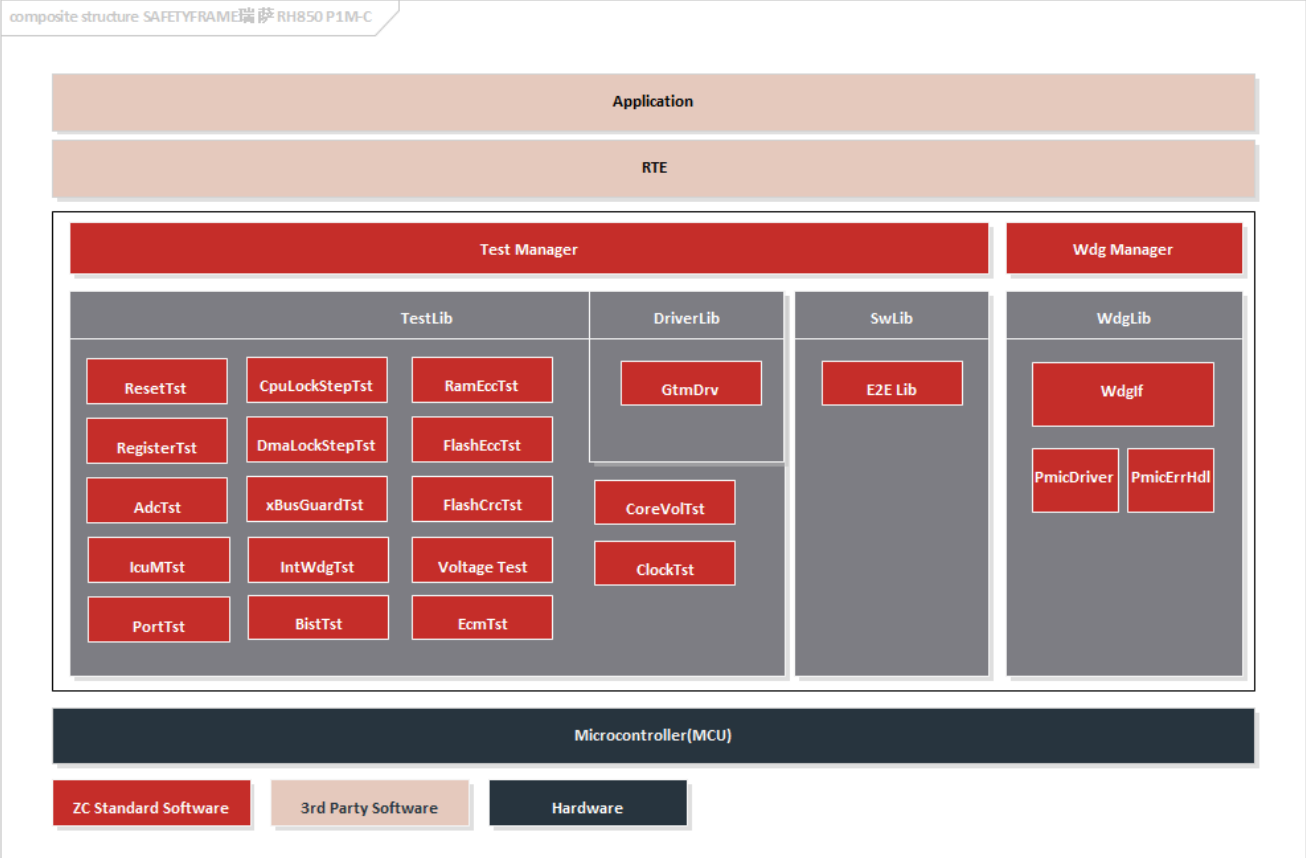
- Safety Frame 具有内部程序流监控

  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	CpuLockStepTst	Cpu lock step自检 CPU lock step self-check
	DmaLockStepTst	Dma lock step自检 DMA lock step self-check
	xBusGuardTst	x-Bus Guard自检(x:P、H、GRAM、PE) x-Bus Guard self-check (x: P, H, GRAM, PE)
	IntWdgTst	Wdg定时器自检 Wdg timer self-check
	BistTst	LBIST和MBIST自检 LBIST and MBIST self-check
	RamEccTst	RAM Ecc自检 RAM ECC self-check
	FlashEccTst	Flash Ecc自检(Code Flash、Data Flash、Data Flash

		Transfer Path自检) Flash ECC self-check (Code Flash, Data Flash, Data Flash Transfer Path self-check)
	FlashCrcTst	Flash CRC自检 Flash CRC self-check
	EcmTst	Ecm 模块自检 ECM module self-check
	CoreVolTst	Core Voltage自检 Core Voltage self-check
	ClockTst	Clock Monitor自检 Clock Monitor self-check
	PortTst	I/O Port自检，依赖于客户的硬件电路 I/O Port self-check (dependent on customer hardware circuit)
	RegisterTst	INTC静态寄存器自检、Power Down Modes静态寄存器自检 INTC static register self-check, Power Down Modes static register self-check
	AdcTst	Adc自检，包含ADC电路诊断，ADC电平诊断，ADC Pin断路诊断，ADC双路冗余（依赖客户硬件环境） ADC self-check, including ADC circuit diagnosis, ADC level diagnosis, ADC Pin open-circuit diagnosis, ADC dual-redundant (dependent on customer hardware environment)
	ResetTst	复位自检，包含软件复位自检，ECM复位自检 Reset self-check, including software reset self-check, ECM reset self-check
	IcuMTst	ICU-M的功能验证，需要考虑客户是否使用ICU-M ICU-M functionality verification, considering whether the customer uses ICU-M
驱动库 Driver Library	GtmDrv	Gtm驱动 GTM driver
SwLib	E2E	End to End通信保护 End-to-End communication protection
Wdg 驱动库 Wdg Driver	PmicDriver/PmicErrHdl	SBC监控机制，依赖于客户使用的SBC型号 SBC monitoring mechanism (dependent on the SBC model used by the customer)
Wdg Manager	WdgM/WdgIf	看门狗管理，支持内外看门狗 Watchdog management, supporting internal and external watchdogs

满足的 RH850/P1M-C Safety Application Note 中的 Safety Mechanism：

Safety Mechanisms Satisfied in the RH850/P1M-C Safety Application Note:

安全机制 Safety Mechanism	描述 Description
SAN-P1xC-0101	[LOCK STEP DUAL CORE]Each RH850G3M CPU shall be implemented redundant based on a lock step structure. The
SAN-P1xC-0101	[LOCK STEP DUAL CORE]Each RH850G3M CPU shall be implemented redundant based on a lock step structure. The redundant CPU architecture consists of the master and the checker core. The execution in the master core is followed by the checker core in lockstep mode. All output signals (data, address and control) are compared by a compare unit. Any comparison mismatch is reported to the ECM module. The inputs to the checker are delayed by two clocks to reduce their susceptibility to common mode failures due to clock and noise on power and spikes in voltage and current.
SAN-P1xC-0201	[DMA REDUNDANCY]HW redundancy shall be implemented to detect data fault inside DMA.
SAN-P1xC-0301	[P-BUS GUARD]P-Bus Guard protects single peripherals and/or groups against access from other bus masters at P-Bus interface
SAN-P1xC-0302	[H-Bus Guard]H-Bus Guard protects single peripherals and/or groups against access from other bus masters at H-Bus interface. System level SM such as E2E protection should be considered when H-Bus Guard cannot work properly.
SAN-P1xC-0303	[GRAM guard]GRAM guard protects data in global RAM against memory write access from other bus masters .
SAN-P1xC-0304	[PE GUARD]PE-Guard in DCLS protects PE internal resources against access from other bus masters via system interconnect.
SAN-P1xC-0305	[INTERNAL PERIPHERAL GUARD]Unauthorized accesses to peripherals from the CPU core should be prevented according to the attributes (including address, transfer type, and access right) by IPG.

SAN-P1xC-0401	[WATCHDOG TIMER]Window watchdog timer for temporal and logical program monitoring shall recover CPU deadlock due to unexpected instruction fetch from cache or other memories.
SAN-P1xC-0501	[FIELD BIST]Start-up BIST can work as generic measure for latent fault as same as start-up functional test for each safety mechanism. BIST coverage can be claimed as diagnostic coverage for LFm, and over 90% is required in ASIL-D for LFm. Logic BIST (LBIST) covers logic circuits with scan techniques. Memory BIST(MBIST) covers SRAM hard macro components such as address decoder, sense amplifier or data selector where is difficult to be checked by LBIST. If Start-up BIST cannot work properly, BIST sequence cannot end or cannot output correct result. As a result, BIST shall judge as fail and MCU shall not start anymore(i.e.safe state inSRS.)
SAN-P1xC-0601	[INSTRUCTION CACHE RAM EDC]The integrity of the data stored in the Instruction Cache Data/Tag shall be ensured by an error detection and correction code. EDC SED/DED with 64 bit data and 8 bits for cache data EDC or 32 bit data and 7 bit for cache tag EDC is able to detect faults in data with high coverage.
SAN-P1xC-0602	[LOCAL RAM ECC]The integrity of the data stored in the LRAM shall be ensured by an error detection and correction code. ECC SEC/DED with 32 bit data and 7 bits for ECC is able to detect up to two bit errors and to correct one bit error in a logical word. When considering multibit errors, the max coverage of error detection can be given by {1-2^(data bits)/2^(data+ecc bits)} and user can be noticed by error signal. In case of one bit error notification, user needs to classify that cause is not coming from multi bit corruption in that memory. Fault inside ECC decoder has risk to wrongly change correct data. Such direct violation, however, can be notified to ECC error flag or detected by other SM.

SAN-P1xC-0603	[GLOBAL RAM ECC]The integrity of the data stored in the GRAM shall be ensured by an error detection and correction code. ECC SEC/DED with 32 bit data and 7 bits for ECC is able to detect up to two bit errors and to correct one bit error in a logical word. When considering multibit errors, the max coverage of error detection can be given by {1- 2^(data bits)/2^(data+ecc bits)} and user can be noticed by error signal.Fault inside ECC decoder has risk to wrongly change correct data. Such direct violation,however, can be notified to ECC error flag or detected by other SM.
SAN-P1xC-0604	[DTS RAM ECC]The integrity of the data stored in the DTS RAM shall be ensured by an error detection and correction code. ECC SEC/DED with 32 bit data and 7 bits for ECC is able to detect up to two bit errors and to correct one bit error in a logical word. When considering multibit errors, the max coverage of error detection can be given by {1- 2^(data bits)/2^(data+ecc bits)} and user can be noticed by error signal. In case of one bit error notification, user needs to classify that cause is not coming from multi bit corruption in that memory. Fault inside ECC decoder has risk to wrongly change correct data. Such direct violation, however, can be notified to ECC error flag or detected by other SM.
SAN-P1xC-0605	[PERIPHERAL RAM ECC]The integrity of the data stored in the CSIH RAM shall be ensured by an error detection and correction code. ECC SEC/DED with 32 bit data and 7 bits for ECC is able to detect up to two bit errors and to correct one bit error in a logical word. When considering multibit errors, the max coverage of error detection can be given by {1-2^(data bits)/2^(data+ecc bits)} and user can be noticed by error signal.
SAN-P1xC-0606	[CODE FLASH ECC AND ADDRESS PARITY]The MCU shall be moved into the safe state when an ECC 2-bit error, ECC 1-bit error overflow or an address parity error is detected. In the case 1-bit error is flagged by the ECC logic, user shall execute Code-Flash Data CRC test to check whether the error is multi-bit fault or not.
SAN-P1xC-0607	[DATA FLASH ECC AND SIGNATURE TEST]ECC is enabled by HW as initial state and shall not be disabled by SW. ECC 1-bit error notification should be enabled if application requires.

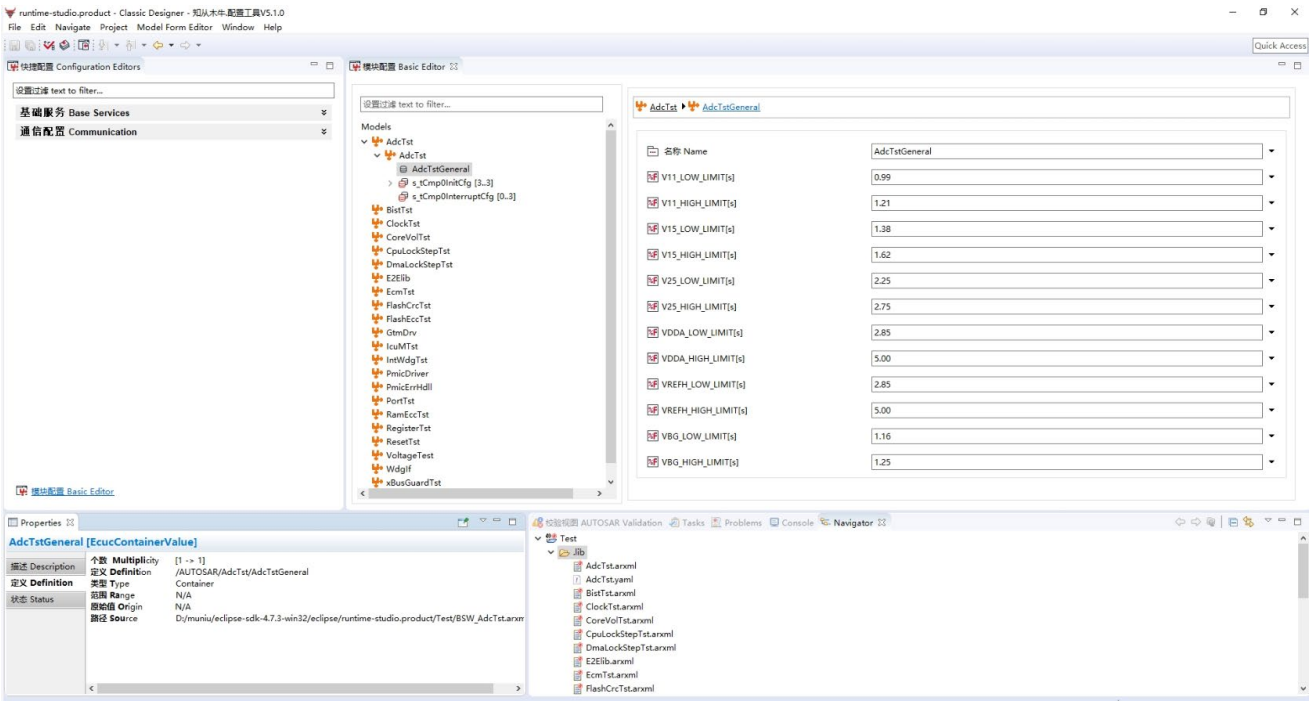
SAN-P1xC-0608	[DATA TRANSFER PATH]Flowing address through the P-Bus shall be ensured by an error detection and correction code. EDC SED/DED with 32 bit address and 7 bits for ECC is able to detect up to two bit errors in a logical address. When considering multibit errors, the max coverage of error detection can be given by {1-2^(data bits)/2^(data+ecc bits)} and user can be noticed by error signal.
SAN-P1xC-0701	[DATA CRC FUNCTION]The CRC result of Code Flash contents is read by CPU from Data CRC macro and compared against the reference CRC stored in Code-Flash memory. The reference CRC should be calculated by user at Flash Programming. If there is a difference among these CRC values,the content of the Code-Flash (or the CRC macro) may have failures
SAN-P1xC-0801	[ERROR CONTROL MODULE]ECM should be implemented redundant for assumed failure mode and LBIST(P1xC_SRS_SM_7) also covers this SM as a part of measures for latent fault.
SAN-P1xC-0901	[CORE VOLTAGE MONITOR]The core voltage monitor (referred to as CVM) shall detect abnormalities in the core power supply while the microcontroller is operating. It detects under/overvoltage/drift/oscillation of the core with related coverage. Threshold should be within the safe range of the voltage with a margin to be justified.
SAN-P1xC-1001	[CLOCK MONITOR]Clock monitoring of Main OSC output by sampling with On-chip OSC shall be provided.Clock monitoring of Peripheral Clock of Window Watch Dog Count Clock and PE1/PE2 Checker CPU S/S System Clock are also provided by sampling with Main OSC. PE2 is not available for P1M-C product
SAN-P1xC-1101	[I/O PORTS]Ports where have possibility to violate safety goal defined by customer should be verified by using SW measures or AoU like E2E protection.
SAN-P1xC-1201	[INTERRUPT CONTROLLER]Following checks should be implemented by SW according to user application. - Periodic check of the configuration registers - Interrupt consistency check - Periodic check of not executed interrupt requests - Check the correct interrupt order priority

SAN-P1xC-1301	[POWER DOWN MODES]Configuration registers of Power Down Modes of peripherals which are used in SR application should be read back and compared with expected value.
SAN-P1xC-1401	[EXTERNAL MEMORY CONTROLLER]It is highly recommended to use E2E protection to ensure the safety integrity of the External_Memory_Controller module
SAN-P1xC-1411	[CLOCKED SERIAL INTERFACE H]It is highly recommended to use E2E protection to ensure the safety integrity of the CSIH module.
SAN-P1xC-1421	[HIGH SPEED USRT]It is highly recommended to use E2E protection to ensure the safety integrity of the USART module.
SAN-P1xC-1431	[LIN/UART INTERFACE]It is highly recommended to use E2E protection to ensure the safety integrity of the RLIN module.
SAN-P1xC-1441	[CAN CONTROLLER]It is highly recommended to use E2E protection to ensure the safety integrity of the MCAN module.
SAN-P1xC-1451	[FLEXRAY]It is highly recommended to use E2E protection to ensure the safety integrity of the FlexRay module.
SAN-P1xC-1461	[ETHERNET CONTROLLER]It is highly recommended to use E2E protection to ensure the safety integrity of the Ethernet module.
SAN-P1xC-1471	[SINGLE EDGE NIBBLE TRANSMISSION]It is highly recommended to use E2E protection to ensure the safety integrity of the SENT module.
SAN-P1xC-1501	[SYSTEM TIMER]To detect missing and delayed synchronous interrupts application level safety measures are recommended:For example program flow monitoring and/or plausibility check within the control loop,timeout supervision, interrupt requests counting within time windows.
SAN-P1xC-1601	[A/D CONVERTER]Open wiring and break detection self-diagnostic function provides a discharge enable bit to discharge analog pins for which A/D conversion should be performed.If any of the A/D input pin becomes floating, the value of the conversion result would become close to H' 0000 after several sampling in continuous scan mode. Consequently a condition whereby a pin is open can be detected.

SAN-P1xC-1701	[RESET CONTROLLER]A start-up test can be executed to ensure that the reset can be asserted correctly. Also when reset is occurred, ERROROUT pin is working.If SW reset is used in SR application, SUST of SW reset can be executed.If terminal reset is used to bring the MCU safe state, a start-up test toggling the terminal reset 1 to 0 is highly recommended. The user can monitor ERROROUT pin to 0 when terminal reset is toggled from 1 to 0
SAN-P1xC-1801	[OPERATING MODE]Unintended flash programming mode or test mode activation while in single chip mode respectively its deactivation shall be detected and signaled to ECM.
SAN-P1xC-A001	[ASSUMPTIONS ON SAFETY MEASURES EXTERNAL TO MCU (1)]As AoU, it is highly recommended to monitor whether the supplied voltage on VCC outside MCU is within safe range as defined by Renesas.
SAN-P1xC-A002	[ASSUMPTIONS ON SAFETY MEASURES EXTERNAL TO MCU (2)]As AoU, it is highly recommended to monitor whether the supplied voltage on EnVCC (n = 0,1) outside MCU is within safe range as defined by Renesas.
SAN-P1xC-A003	[ASSUMPTIONS ON SAFETY MEASURES EXTERNAL TO MCU (3)]As AoU, it is highly recommended to monitor whether the supplied voltage on AnVREFH (n =0, 1) outside MCU is within safe range as defined by Renesas.
SAN-P1xC-A004	[ASSUMPTIONS ON SAFETY MEASURES EXTERNAL TO MCU (4)]It is recommended to use an external window watchdog timer to monitor the operation of the MCU by assuming exit from user mode at worst. This external monitoring function at system expects activated immediately after start-up.
SAN-P1xC-A005	[ASSUMPTIONS ON SAFETY MEASURES EXTERNAL TO MCU (5)]Monitoring circuit to evaluate the ERROROUT status and CVMOUT status(*) .
SAN-P1xC-A006	[ASSUMPTIONS ON SAFETY MEASURES EXTERNAL TO MCU (6)]The user must not exceed the electrical specification and the environmental limits defined by Renesas in order to guarantee the safety integrity of the product.
SAN-P1xC-A007	[ASSUMPTIONS ON SAFETY MEASURES EXTERNAL TO MCU (7)]Customer should test mechanical stress test in ECU level.

SAN-P1xC-U001	[USE CASES]Loop back test is effective to ensure core IP and glue logics at once.etc
SAN-P1xC-U002	[RECOMMENDED USAGE (1) for USE CASES]In case of each usecases, the ports for intended function and safety mechanism should not be neighbored.
SAN-P1xC-U003	[RECOMMENDED USAGE (2) for USE CASES]In case of usecase2, should be confirmed the sum of conversion value for input signal and another input signal.
SAN-P1xC-U004	[RECOMMENDED USAGE (3) for USE CASES]In case of Usecase1-2, one additional channel should be monitoring a known voltage.etc
SAN-P1xC-U005	[RECOMMENDED USAGE (4) for USE CASES]In case of Usecase3-6,Port Group of both elements should be divided. (e.g. GPIO for output on Port Group0 and GPIO for loop back on Port Group 1)Data bits of both elements should be mapped into different bit. (e.g. GPIO for output on data bit 15 and GPIO for loop back on data bit 0)
SAN-P1xC-U006	[RECOMMENDED USAGE (5) for USE CASES]In case of Usecase 6,Control Register of both elements should be divided. (e.g. ENP2TIM0 for Element A and ENP2TIM1 for Element B). Data bits of ENP2TIM0 and ENP2TIM1 should be mapped into different bit.
SAN-P1xC-U007	[RECOMMENDED USAGE (6) for USE CASES]In case of Usecase6,one additional pin (ref) should be monitoring a known frequency
SAN-P1xC-U008	[RECOMMENDED USAGE (7) for USE CASES]The ARU cycle time can be checked using one free channel of a connected MCS.
SAN-P1xC-U009	[RECOMMENDED USAGE (8) for USE CASES]Different channel of TIM between main function and safety mechanism should be used to mitigate CCF for the failure of TIM.
SAN-P1xC-S001	[SECURITY USE CASE ASSUMPTIONS]Ciphering technique provides not only secure comunication but also end to end protection from safety point of view. Example of ICUMC usecase assumed by Renesas is described in safety application note as safety mechanism.

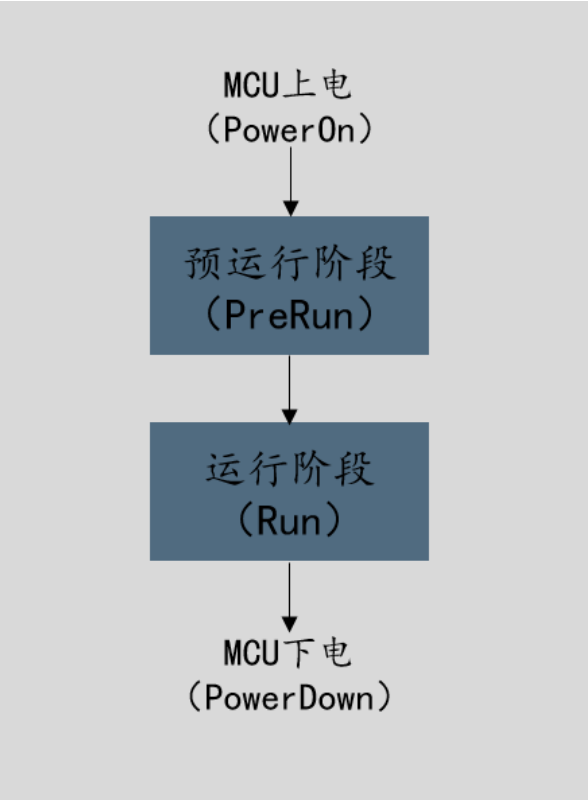
5.3 配置工具 Configuration Tool



运行阶段为了满足客户的不同项目需求，提高 SafetyFrame 的扩展性，RH850/P1M-C 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 RH850/P1M-C 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 重点实验室 月二十五日

木牛软件产品登记证书

ZC. MUNIU SOFTWARE PRODUCT REGISTRATION CERTIFICATE