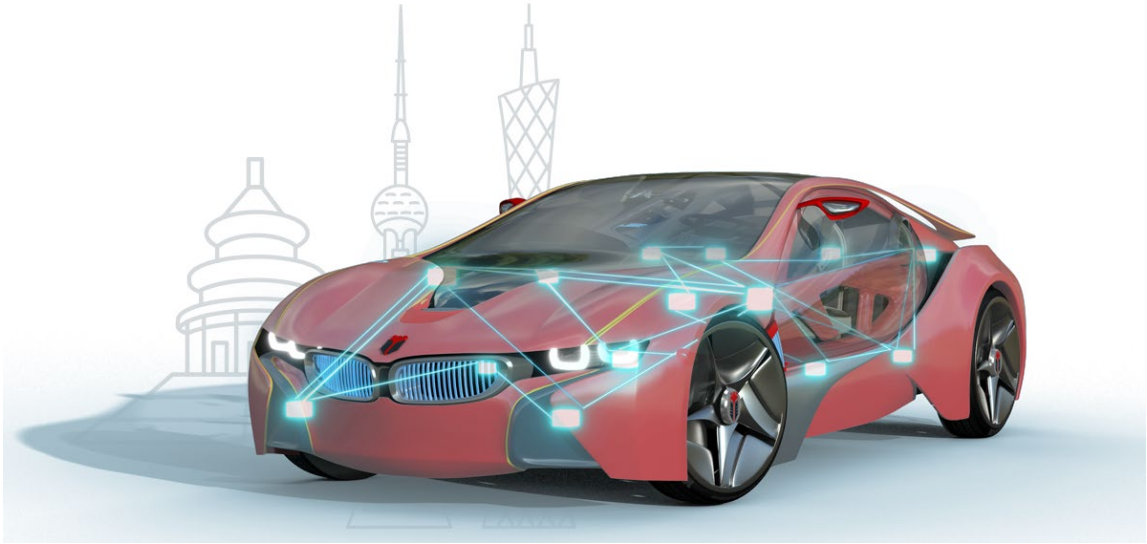
知从木牛 SAFETYLIBRARY 恩智浦 S32K14X 产品手册

ZC.MUNIU SAFETYLIBRARY PRODUCT MANUAL BASED ON NXP S32K14X

知从木牛基础软件平台功能安全库

ZC.MuNiu Basic Software Platform Safety Library



知从木牛 SAFETYLIBRARY 恩智浦 S32K14X 产品手册

ZC.MUNIU SAFETYLIBRARY PRODUCT MANUAL BASED ON NXP S32K14X

知从木牛基础软件平台功能安全库

ZC.MuNiu Basic Software Platform Safety Library

1 功能概述 FUNCTIONAL OVERVIEW

S32K14x Safety Library 用于帮助客户实现基于 S32K14x 平台的功能安全要求。Safety Library 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 S32K14x Safety Library is designed to assist customers in achieving functional safety requirements based on the S32K14x platform. The Safety Library is highly scalable and can be configured and redeveloped according to different customer project requirements, ultimately meeting the customers' functional safety requirements.

S32K14x Safety Library 用于实现 S32K14x 平台的软件安全机制，包括 MCU 内部模块的测试和硬件安全机制的驱动。

The S32K14x Safety Library is used to implement the software safety mechanisms of the S32K14x, including the testing of internal MCU modules and the driving of hardware safety mechanisms.

2 应用领域 APPLICATION FIELD

S32K14x Safety Library 可应用于有功能安全等级需求的控制器。例如：

The S32K14x Safety Library can be applied to controllers that require functional safety levels.

For example:

- 车身控制器
  Body Controller
- 电池管理系统(BMS)
  Battery Management System
- 网关控制器
  Gateway Controller
- 车载娱乐模块
  In-Vehicle Entertainment Module
- 胎压监控系统
  Tire Pressure Monitoring System
- 门控单元
  Gate Control Unit
- 车灯控制单元
  Lighting Control Unit
- 电子驻车制动系统
  Electronic Parking Brake System

通过将 Safety Library 集成到基于 S32K14x 平台的控制器中，可达到 ISO26262 ASIL-B 的等级要求。

By integrating the Safety Library into the control based on S32K14x, it is possible to meet the ISO 26262 ASIL-D level requirements.

3 配置环境 CONFIGURATION ENVIRONMENT

配置环境 Configuration Environment	
Hardware (Chip)	S32K144/S32K146/S32K148
Compilers Supported	S32 Design Studio for ARM(2018.R1) 、IAR v8.40.1
Evaluation Hardware	S32K144 EVB
Debugger	Lauterbach (Trace32 R.2018.02) Isystem (IC5700)
Configuration Tools	Muniu_v5.0.5
Configuration Environment	Win7 64bit

S32DS 编译器选项 S32DS Compiler Options	
S32 Design Studio for ARM 编译选项 S32 Design Studio for ARM Compiler Options	-mcpu=cortex-m4 -c –Os -ggdb3 -mcpu=cortex-m4 -mthumb -mlittle-endian -fomit-frame-pointer -msoft-float -fno-common -Wall -Wextra -Wstrict-prototypes -Wno-sign-compare -fstack-usage -fdump-ipa-all -std=c99
S32 Design Studio for ARM 链接选项 S32 Design Studio for ARM Linker Options	-mcpu=cortex-m4 -msoft-float -mthumb -e _start -nostartfiles -static -lc -lm -lgcc -lnosys

IAR 编译器选项 IAR Compiler Options	
IAR 编译选项 **IAR Compiler Options**	--no_wrap_diagnostics --c++ -e --cpu Cortex-M4 --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 -DCPU_S32K146 -DAUTOSAR_OS_NOT_USED -DM4_DEVICE_RESERVED_ADDR=0x40080000 --diag_suppress Pa050 9
IAR 链接选项 **IAR Linker Options**	--cpu Cortex-M4 --fpu None -s+ -r -DSTART_FROM_FLASH -DM4_DEVICE_RESERVED_ADDR=0x40080000

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。

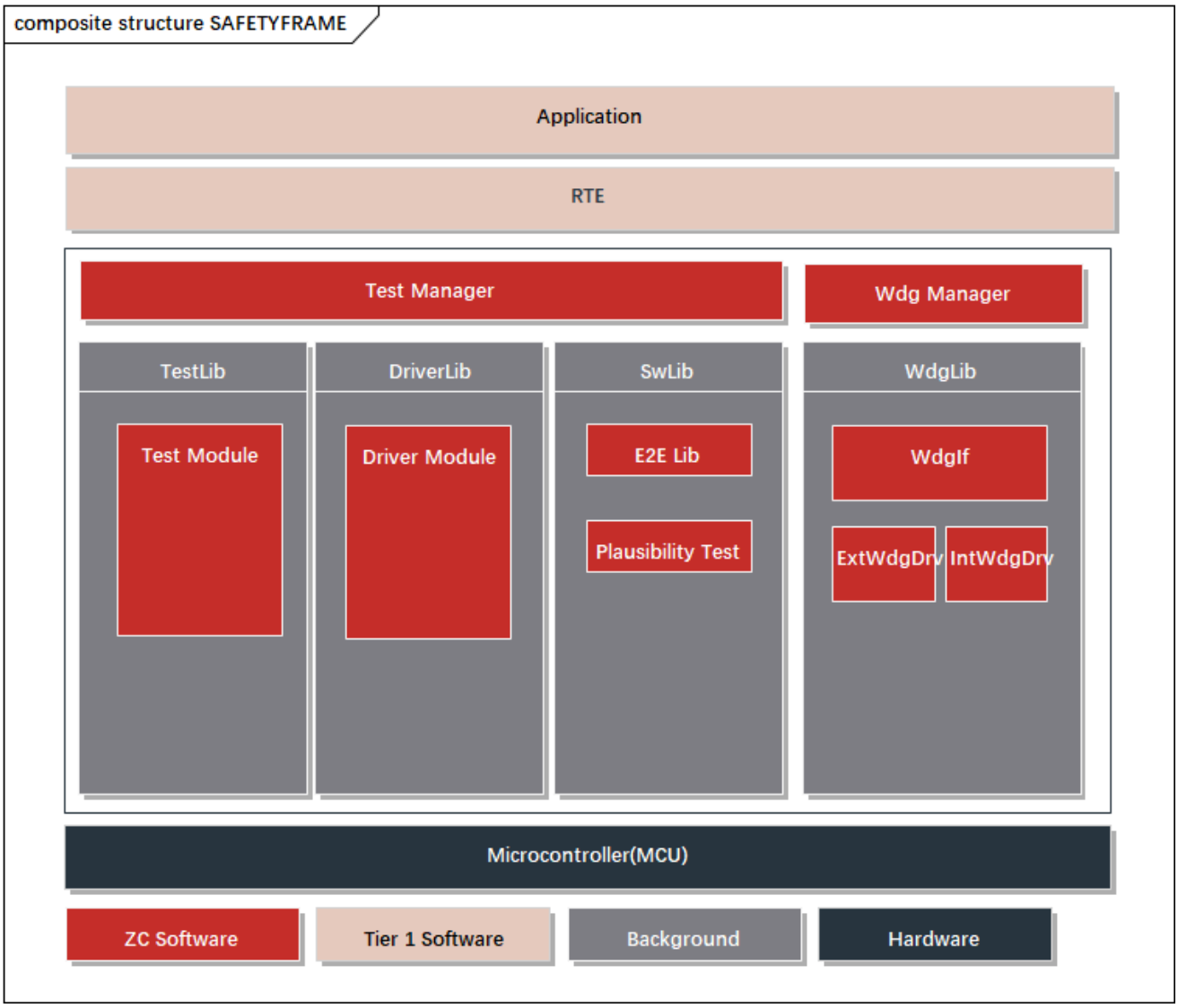
For microcontrollers (MCU, referred to as MCU below), within the electronic and electrical system, they are designed and developed as SEooC (safety element out of context). To meet the aforementioned metric requirements, MCUs need to implement corresponding safety mechanisms. These safety mechanisms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

- 支持多核测试及应用

  Support multi-core testing and applications.

- Safety Library 具有内部程序流监控

  Safety Frame has internal program flow monitoring.

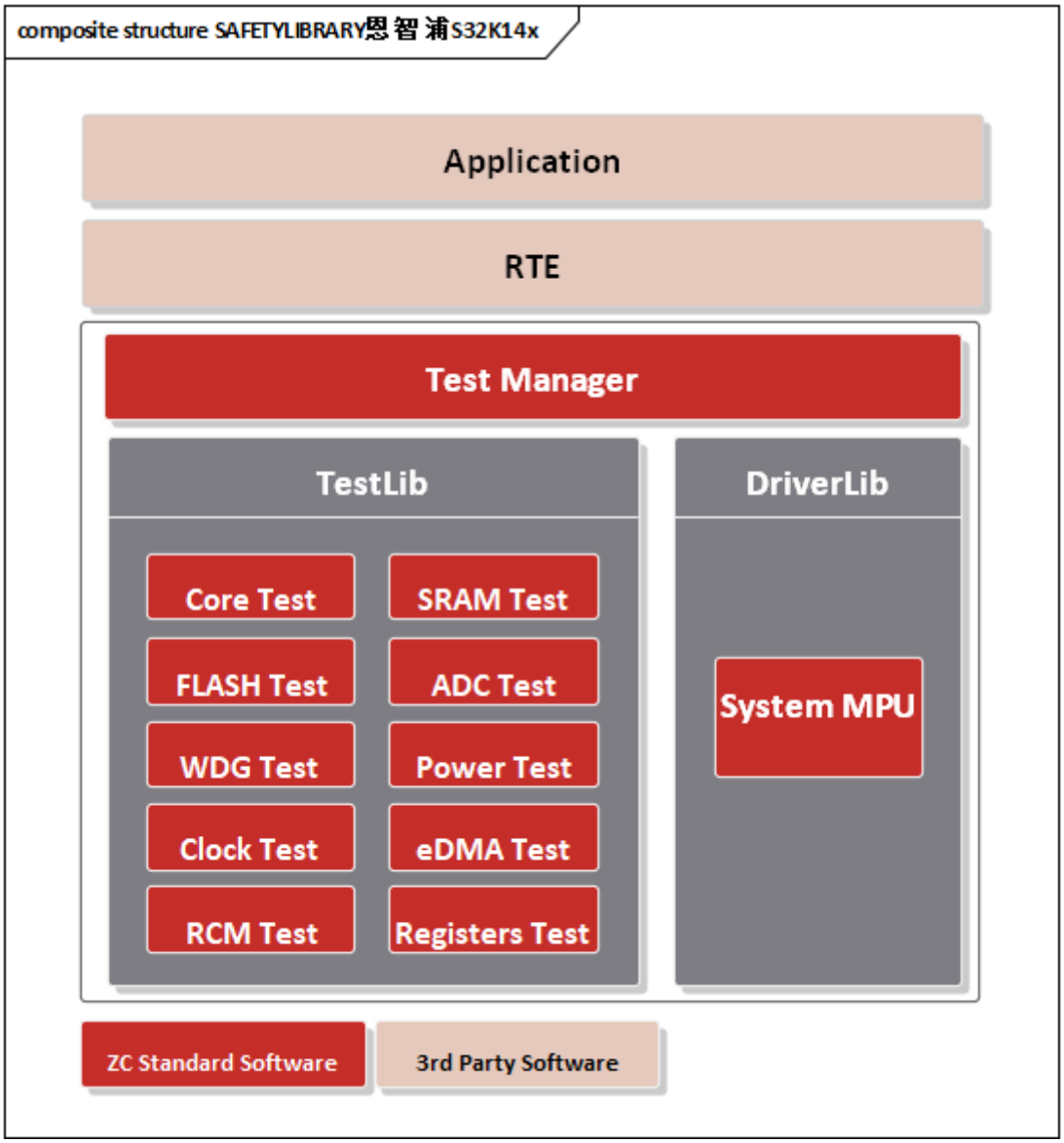
- 高安全性：支持多核自检测试，搭配知从科技 TLF35584Lib 可实现高达 ASIL-D 需求

High security: Supports multi-core self-testing, and can achieve up to ASIL-D requirements when paired with ZC 's TLF35584Lib.

- 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.

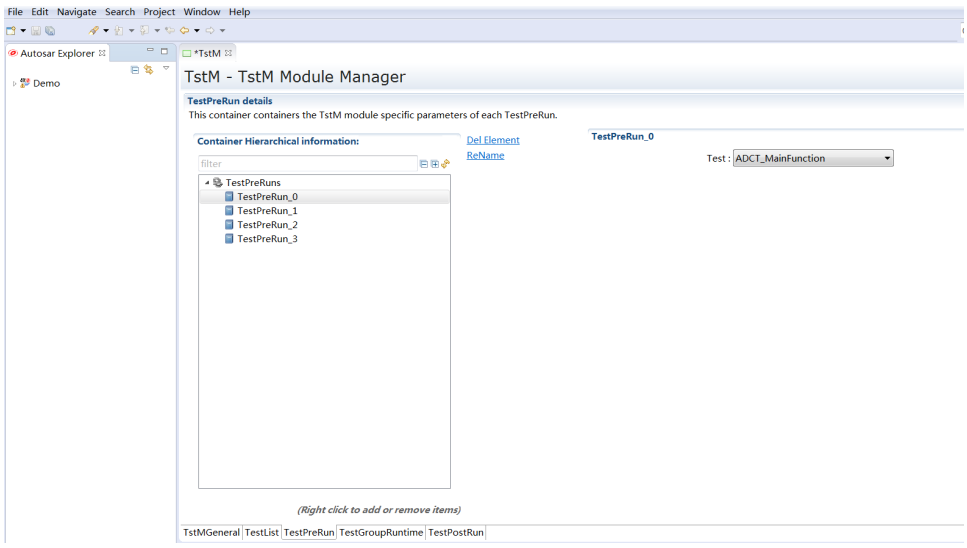
5.2 软件架构 Software Architecture



模块 Module	子模块 Sub-module	描述 Description
管理模块 Management Module	Test Manager	Safety Library 的管理模块 Safety Library Management Module

测试库 Test Library	Core Test	Core检测模块 Core Detection Module
	eDMA Monitor	DMA检测模块 DMA Detection Module
	SRAM Test	SRAM检测模块 SRAM Detection Module
	FLASH Test	FLASH检测模块 FLASH Detection Module
	Power Test	供电检测模块 Power Supply Detection Module
	Clock Test	时钟检测模块 Clock Detection Module
	WDG Test	WDG检测模块 WDG Detection Module
	ADC Test	ADC检测模块 ADC Detection Module
	RCM Test	复位检测模块 Reset Detection Module
	Register Test	寄存器检测模块 Register Detection Module
驱动库 Driver Library	System MPU Driver	SMPU驱动 SMPU Driver
通用模块 Common Module	Common	通用类型定义、MemMap定义等 General Type Definitions, MemMap Definitions, etc.

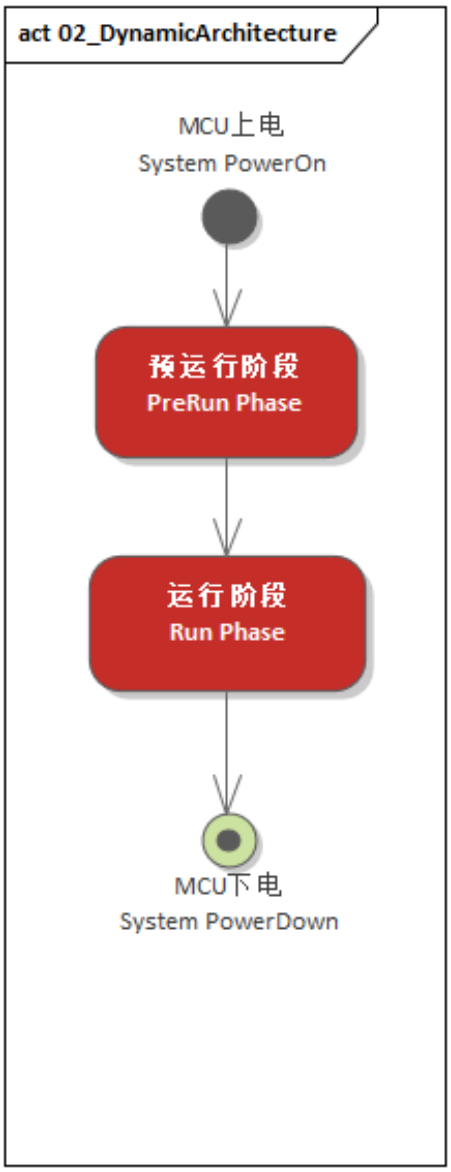
5.3 配置工具 Configuration Tool



为了满足客户的不同项目需求，提高 Safety Library 的扩展性，S32K14X Safety Library 实现了各个模块可配置性，并且实现了 Safety Library 的配置工具。客户可根据不同需求，在配置工具上完成 Safety Library 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 diverse project requirements of customers and enhance the scalability of the Safety Library, the S32K14X Safety Library has implemented the configurability of each module and has developed a configuration tool for the Safety Library. Customers can complete the configuration of various modules of the Safety Library using the configuration tool according to different needs. They can 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 Requirements Document
软件需求分析 Software Requirement Analysis	软件的需求分析 Software Requirements Analysis
	需求分析规格书 Requirements Analysis Specification
	软件需求追踪表 Software Requirements Traceability Matrix
	客户的问题沟通表 Customer Issue Communication Form
软件架构设计 Software Architecture Design	软件架构说明书 Software Architecture Specification
	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 Document
	配置工具评审 Configuration Tool Review
	软件详细设计追踪表 Software Detailed Design Traceability Matrix
	SafetyLib 工程评审 SafetyLib Engineering 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	集成策略 Integration Strategy
	集成手册 pdf Integration Manual (PDF)

开发流程 Development Process	文档描述 Document Description
Software Integration and 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.SafetyLibrary 配置工具使用指导书 MuNiu.SafetyLibrary Configuration Tool User Guide
	木牛.SafetyLibrary 配置工具软件配置管理文档 MuNiu.SafetyLibrary 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	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: fs@ts-gs.com

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 五月二十五日

木牛软件产品登记证书
ZC. MUNIU SOFTWARE PRODUCT REGISTRATION CERTIFICATE