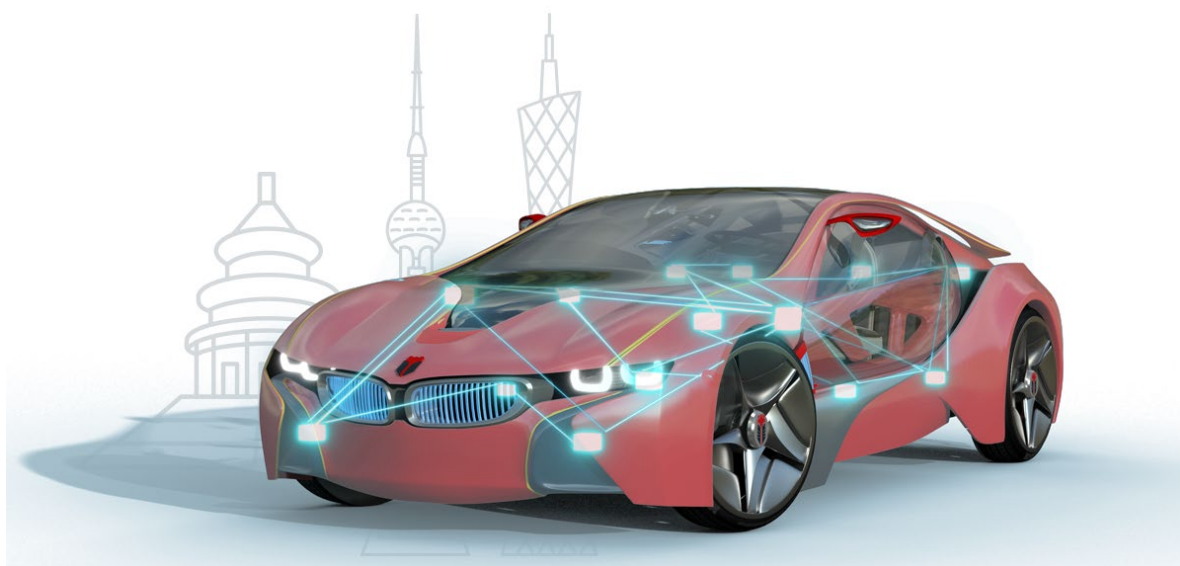


知从木牛 SAFETYLIBRARY 意法半导体 SPC58NN 产品手册
ZC.MUNIU SAFETYLIBRARY PRODUCT MANUAL
BASED ON ST SPC58NN

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 意法半导体 SPC58NN 产品手册

ZC.MUNIU SAFETYLIBRARY PRODUCT MANUAL BASED ON ST SPC58NN

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

ST SPC58NN Safety Library 用于帮助客户实现基于 SPC58NN 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 ST SPC58NN Safety Library is designed to assist customers in achieving functional safety requirements based on the SPC58NN 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.

SPC58NN Safety Library 用于实现 SPC58NN 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 SPC58NN Safety Library is used to implement the software safety mechanisms of the SPC58NN, including the testing of internal MCU modules and the driving of hardware safety mechanisms.

2 应用领域 APPLICATION FIELD

SPC58NN Safety Library 可应用于有功能安全等级需求的控制器。例如：

The SPC58NN Safety Library can be applied to controllers that require functional safety levels.

For example:

- 电机控制器
Motor Controller
- 电池管理系统(BMS)
Battery Management System
- 底盘系统应用
Chassis System Applications
- 电气稳定控制(ESC)
Electronic Stability Control
- 电动助力转向(EPS)
Electric Power Steering
- 安全气囊和传感器集成应用
Chassis Domain Line Control System Applications
- 雷达的应用
Radar Applications

通过将 Safety Library 集成到基于 SPC58NN 的控制器中，可达到 ISO26262 ASIL-D 的等级要求。

By integrating the Safety Library into the control based on SPC58NN, 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)	SPC58NN (SPC58NN84E7RMHBY)
Compilers Supported	Green Hills v7.1.4
Evaluation Hardware	SPC58NN84E7RMHBY
Debugger	Lauterbach (Trace32 R.2018.02) Isystem (IC5700)
Configuration Tools	Muniu_v5.0.0
Configuration Environment	Win10 64bit

Green Hills v7.1.4 编译器选项 Green Hills v7.1.4 Compiler Options	
编译选项 Compiler options	-c99 -cpu=core_ppce200z42 - DNOT_READY_FOR_TESTING_OR_DEPLOYMEN - DDISABLE_MCAL_INTERMODULE_ASR_CHECK - DAUTOSAR_OS_USED -DEU_DISABLE_ANSILIB_CALLS -DGHS - DI_CACHE_DISABLE -dual_debug -G -- incorrect_pragma_warnings --no_commons --no_exceptions - noSPE -nostartfile -preprocess_assembly_files --prototype_errors -sda=all --short_enum --unsigned_fields -vle -Wimplicit-int - Wshadow -Wtrigraphs -Wundef -passsource -c99 -Onone
链接选项 Linker Options	-dwarf2 -e _start :binDirRelative=../output/ - object_dir=../output/objs -list_dir=../output/lst - object_dir=\${%option_value(-object_dir)} - noentry ./autosar_flash.ld ./bhd.ppc

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。

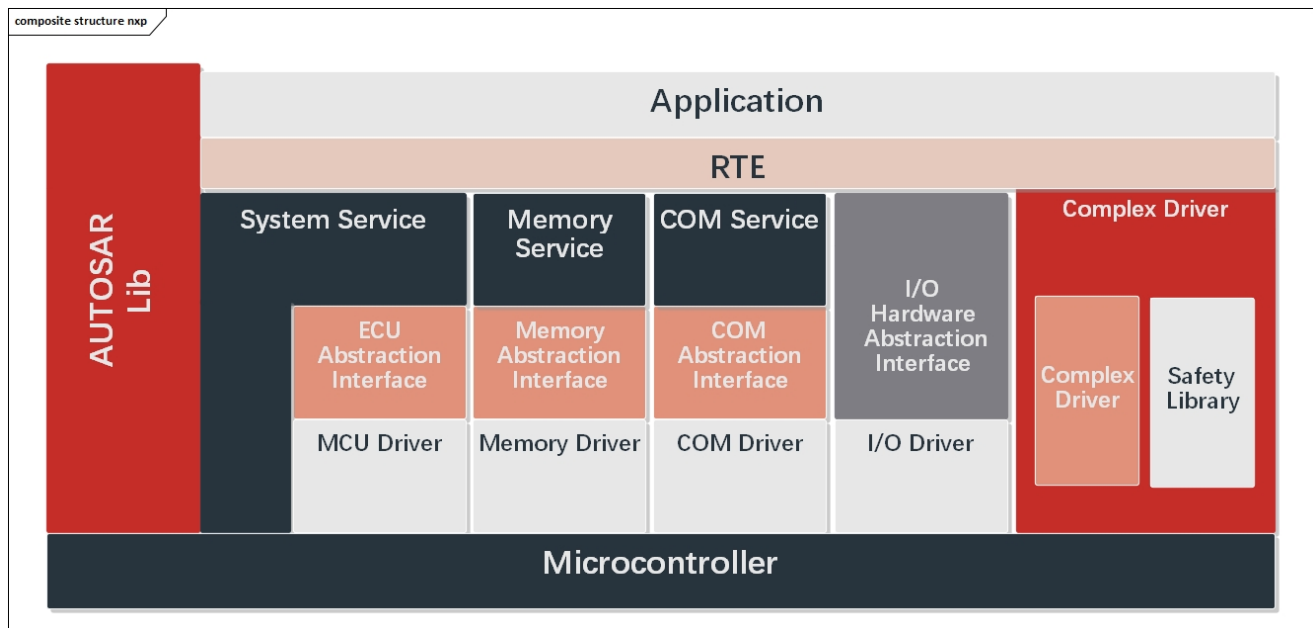
For microcontrollers (MCU, referred to as MCU below), within the electronic and electrical system, they are designed and developed as SEooC (safety element out of context). To meet the aforementioned metric requirements, MCUs need to implement corresponding safety mechanisms. These safety mechanisms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

- 满足控制器 ASIL-D 需求

Meet the ASIL-D requirements of the controller.

- 可集成到非 AUTOSAR 软件架构中

Can be integrated into non-AUTOSAR software architecture.

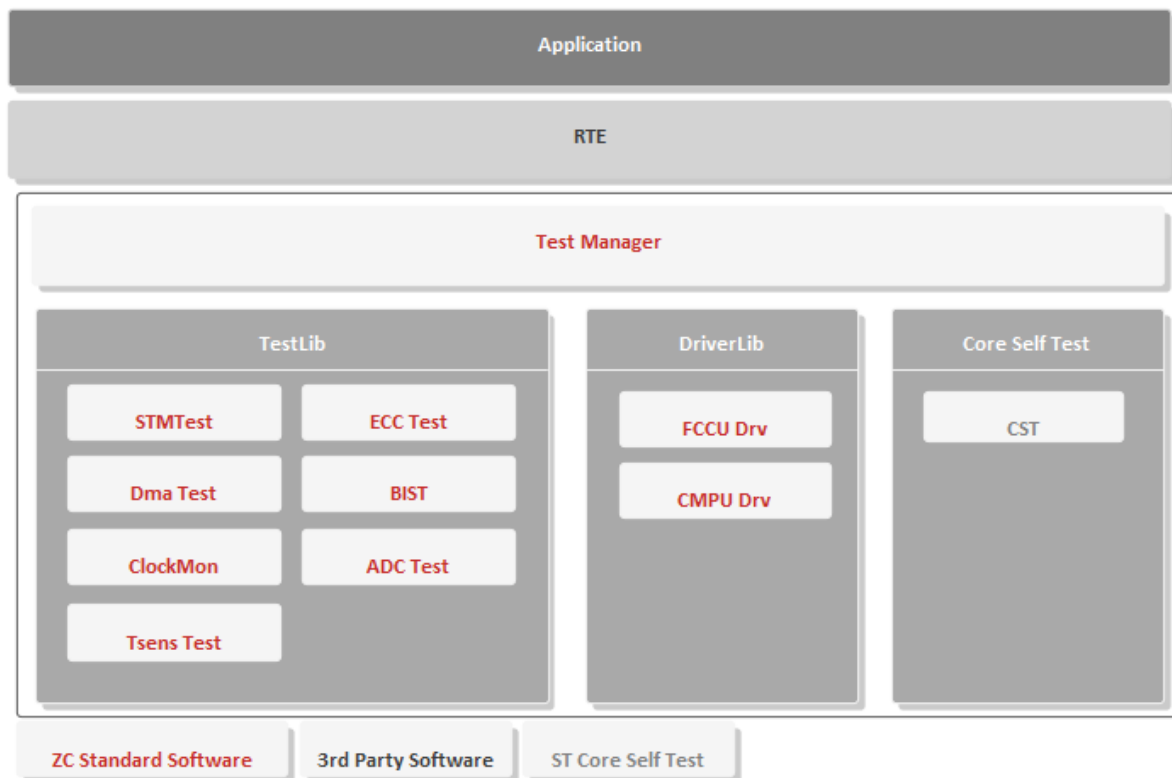
- 高扩展性：每个模块实现可配置性，满足不同的客户需求

High scalability: Each module is configurable to meet different customer requirements.

- Safety Library 内部程序流监控

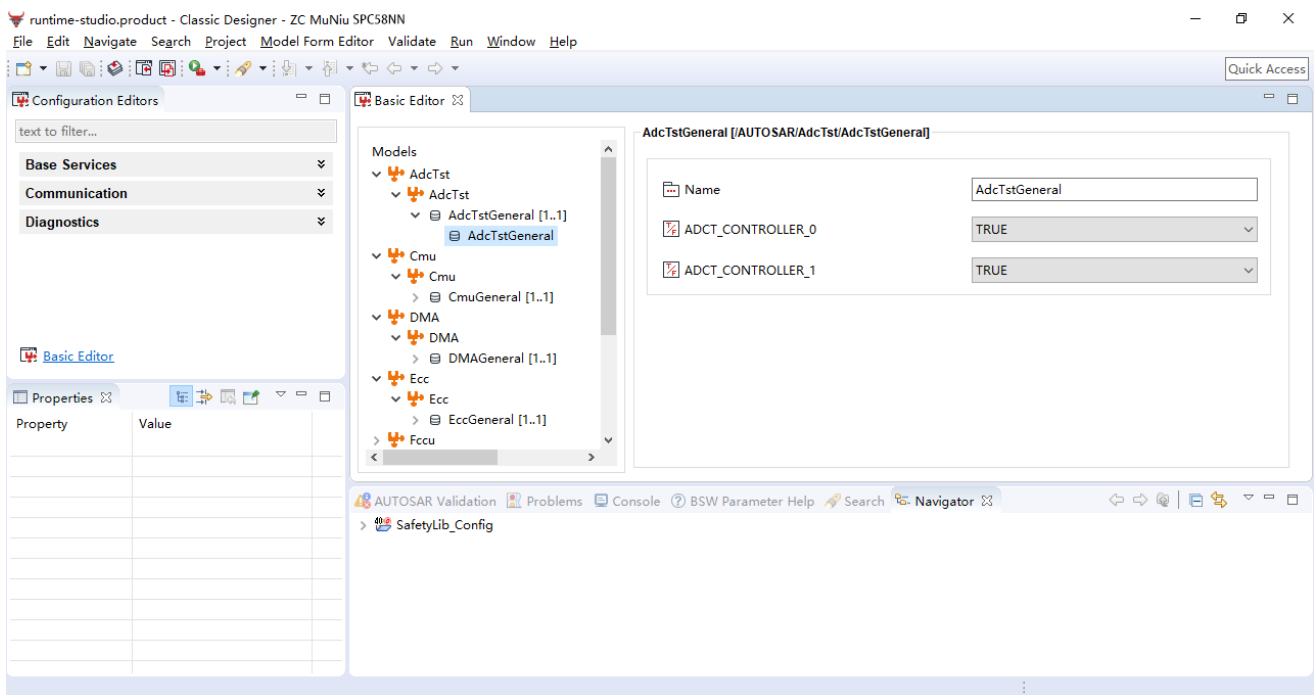
Internal Program Flow Monitoring of the Safety Library.

composite structure SAFETYLIBRARY意法 半导体 SPC58NN



模块 Module	子模块 Sub-module	描述 Description
管理模块 Management Module	Test Manager	Safety Library 的管理 Management of the Safety Library
测试库 Test Library	BIST Test	BIST检测模块 BIST Detection Module
	Dma Monitor	DMA检测模块 DMA Detection Module
	ECC Test	ECC检测模块 ECC Detection Module
	CMU Test	CMU时钟检测模块 CMU Clock Detection Module
	ADC Test	ADC检测模块 ADC Detection Module
	STM Test	STM检测模块 STM Detection Module
	TSENS Test	温度检测模块 Temperature Detection Module
驱动库 Driver Library	Core MPU Driver	CMPU驱动 CMPU Driver
	FCCU Driver	FCCU驱动 FCCU Driver
Core 自检模块 Core Self-Check Module	Core self Test	执行Core 自检 Execute Core Self-Check
通用模块 Common Module	Common	通用类型定义、MemMap定义等 General Type Definitions, MemMap Definitions, etc.

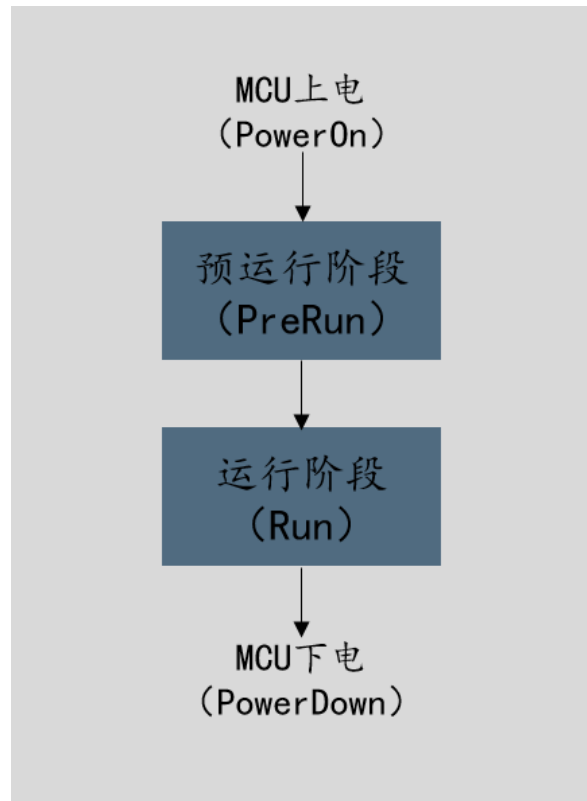
5.2 配置工具 Configuration Tool



为了满足客户的不同项目需求，提高 Safety Library 的扩展性，SPC58NN 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 SPC58NN 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.

5.3 运行阶段 Run Phase



➤ 预运行阶段 Pre-Run Phase

此阶段是对 MCU 的安全机制进行测试，此阶段下 FCCU 为 Normal 状态，一般此阶段在 OS 启动之前进行。

This phase is for testing the safety mechanisms of the MCU. During this phase, the Fault Control and Communication Unit (FCCU) is in the Normal state, and this phase is generally performed before the operating system (OS) starts up.

➤ 运行阶段 Run Phase

此阶段是在任务运行时进行，此阶段下 FCCU 为 Normal 状态，在 OS 运行时进行。

This phase occurs while tasks are running. The FCCU remains in the Normal state, and this phase takes place during the operation of the OS.

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 软件详细设计和单元设计 Detailed Software Design and Unit Design	FCCU 详细设计说明书 FCCU Detailed Design Document
	FCCU 错误处理列表 FCCU Error Handling List
	FCCU 模块评审记录 FCCU Module Review Record
	STM 详细设计说明书 STM Detailed Design Specification
	STM 评审记录 STM Review Record
	CMPU 详细设计说明书 CMPU Detailed Design Specification
	CMPU 评审记录 CMPU Review Record
	ECC 详细设计说明书 ECC Detailed Design Specification
	ECC 模块评审记录 ECC Module Review Record
	DMA 详细设计说明书

开发流程 Development Process	文档描述 Document Description
	DMA Detailed Design Specification
	DMA 模块评审记录 DMA Module Review Record
	TSENS 模块详细设计说明书 TSENS Module Detailed Design Specification
	TSENS 模块评审记录 TSENS Module Review Record
	ADC 模块详细设计说明书 ADC Module Detailed Design Specification
	ADC 模块评审记录 ADC Module Review Record
	Test Manger 详细设计说明书 Test Manger Detailed Design Specification
	Test Manger 模块评审记录 Test Manger Module Review Record
	BIST 详细设计说明书 BIST Detailed Design Specification
	BIST 模块评审记录 BIST Module Review Record
	CMU 详细设计说明书 CMU Detailed Design Specification
	CMU 模块评审记录 CMU Module Review Record
	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 Project Review
软件单元测试 Software Unit Testing	单元测试的 QAC 分析报告 Unit Test QAC Analysis Report
	Tessy 测试报告 Tessy Test Report
	软件单元验证策略 Software Unit Verification Strategy
	集成策略

开发流程 Development Process	文档描述 Document Description
软件集成和集成测试 Software Integration and Integration Testing	Integration Strategy
	集成手册 pdf Integration Manual (PDF)
	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
软件系统测试 Software System Testing	BIST 软件测试报告 BIST Software Test Report
	FCCU 软件测试报告 FCCU Software Test Report
	STM 软件测试报告 STM Software Test Report
	CMPU 软件测试报告 CMPU Software Test Report
	TSENS 软件测试报告 TSENS Software Test Report
	ECC 软件测试报告 ECC 软件测试报告
	DMA 软件测试报告 DMZ 软件测试报告
	CMU 软件测试报告 CMU 软件测试报告
	ADC 软件测试报告 ADC 软件测试报告
	Test Manger 软件测试报告 Test Manger Software Test Report
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

			
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		T4A80002 is an integral part of this certificate. <i>Ist ein integraler Bestandteil dieses Zertifikats.</i>	
Certified product(s) Zertifizierte(s) Produkt(e)	SafetyFrame Version 2.1.0		
Tested according to Gepprüft 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.		
This 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@sgs.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。	
	
No. 04322276	 2019年08月02日

木牛软件著作权登记证书
ZC.MUNIU SOFTWARE COPYRIGHT REGISTRATION CERTIFICATE



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



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

