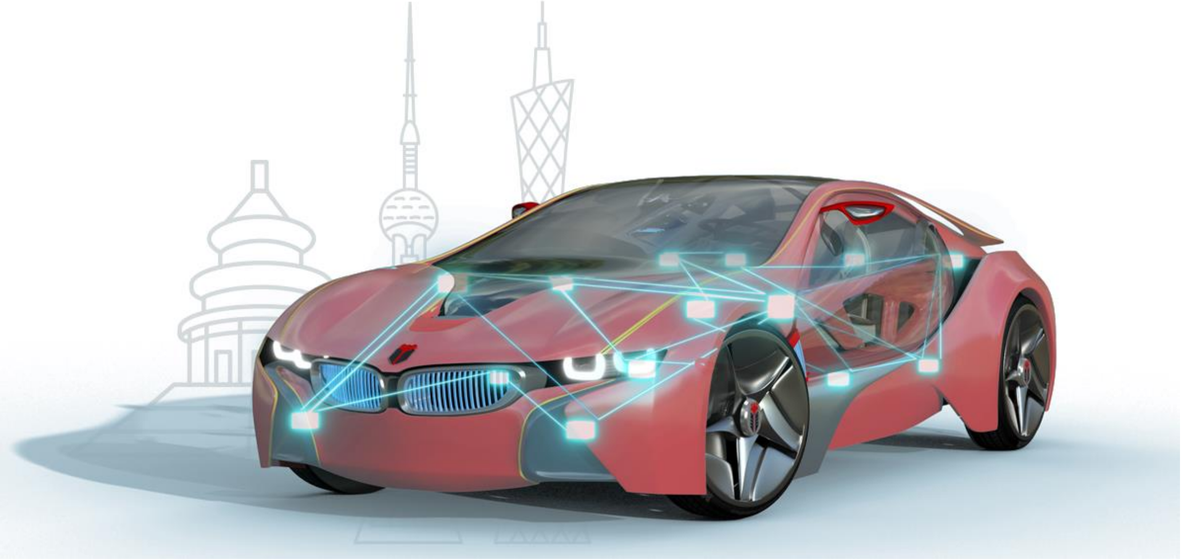
知从木牛 SAFETYFRAME 英飞凌 TLE9954 产品手册

ZC.MUNIU SAFETYFRAME PRODUCT MANUAL BASED ON INFINEON TLE9954

知从木牛基础软件平台功能安全库

ZC.MuNiu Basic Software Platform Safety Frame



知从木牛 SAFETYFRAME 英飞凌 TLE9954 产品手册

ZC.MUNIU SAFETYFRAME PRODUCT MANUAL BASED ON INFINEON TLE9954

知从木牛基础软件平台功能安全库

ZC.MuNiu Basic Software Platform Safety Frame

1 功能概述 FUNCTIONAL OVERVIEW

TLE9954 Safety Frame 用于帮助客户实现基于 Infineon TLE9954 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 TLE9954 Safety Frame is designed to assist customers in achieving functional safety requirements based on the TLE9954 platform. The Safety Frame is highly scalable and can be configured and redeveloped according to different customer project requirements, ultimately meeting the customers' functional safety requirements.

TLE9954 Safety Frame 用于实现 TLE9954 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 TLE9954 Safety Frame is used to implement the software safety mechanisms of the TLE9954, including the testing of internal MCU modules and the driving of hardware safety mechanisms.

2 应用领域 APPLICATION FIELD

TLE9954 Safety Frame 可应用于有功能安全等级需求的控制器。例如:

The TLE9954 Safety Frame can be applied to controllers that require functional safety levels.

For example:

- 有刷直流电机
  Brushed DC Motors
- 无刷直流电机
  Brushless DC Motors
- 汽车网络安全
  Automotive Cybersecurity

通过将 Safety Frame 集成到基于 TLE9954 的控制器中，可达到 ISO26262 ASIL-D 的等级要求。

By integrating the Safety Frame into the control based on TLE9954, 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)	INFINEON TLE9954EQA40
Compilers Supported	IAR v9.50.1
Evaluation Hardware	TLE9954
Debugger	Jlink V8.76
Configuration Tools	ZCMuNiu v4.4.0
Configuration Environment	Win10 64bit

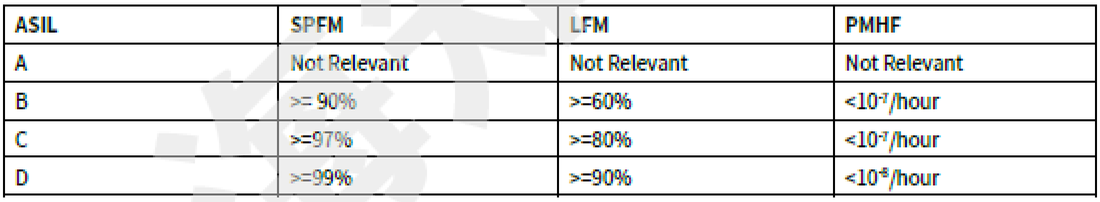
4 开发背景 DEVELOPMENT BACKGROUND

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 的功能安全框架就是实现分配到软件上的安全机制。

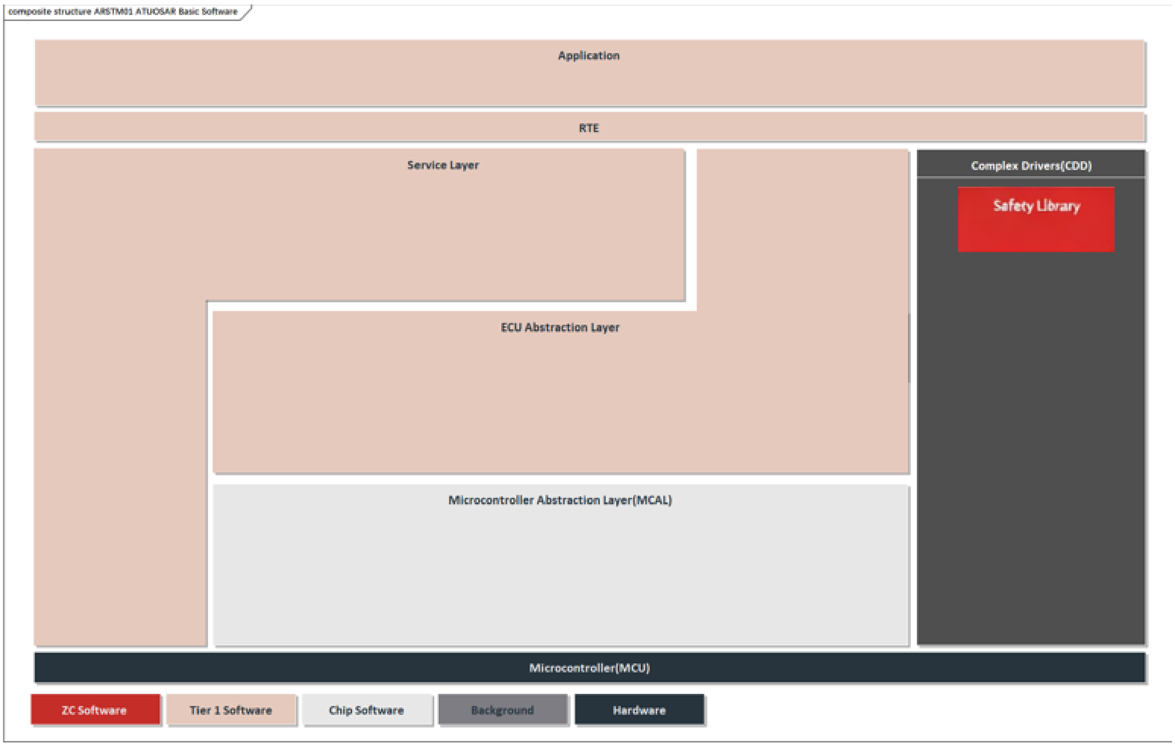
For microcontrollers (MCU, referred to as MCU below), within the electronic and electrical system, they are designed and developed as SEooC (safety element out of context). To meet the aforementioned metric requirements, MCUs need to implement corresponding safety mechanisms. These safety mechanisms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



ASIL	SPFM	LFM	PMHF
A	Not Relevant	Not Relevant	Not Relevant
B	>= 90%	>=60%	<10^{-7}/hour
C	>=97%	>=80%	<10^{-7}/hour
D	>=99%	>=90%	<10^{-8}/hour

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.

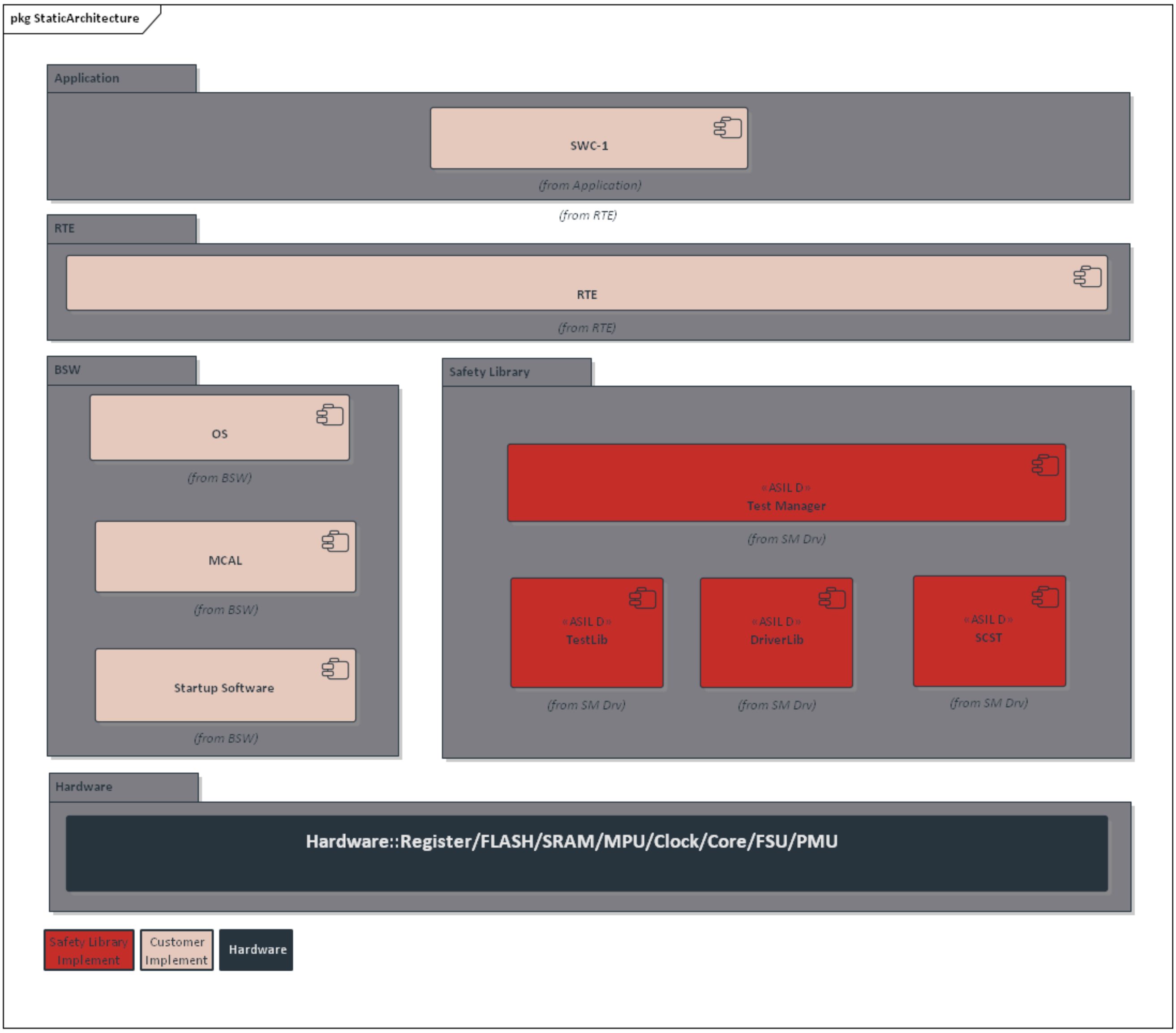
- ➢ Safety Frame 具有内部程序流监控

  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

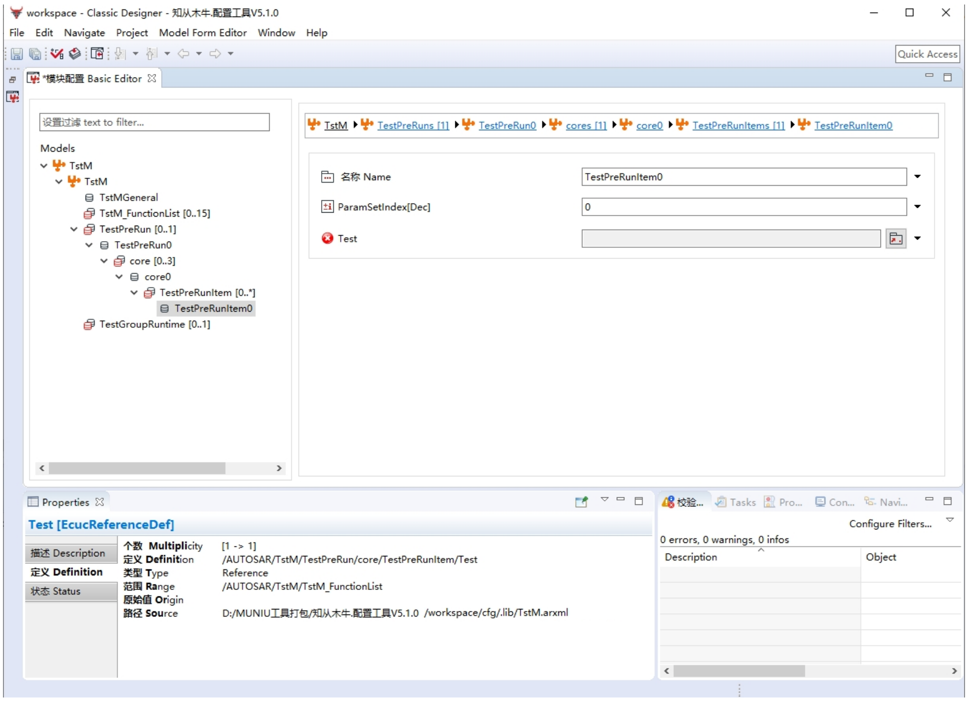
实现的功能模块:

Realized functional modules:

安全机制 Safety Mechanism	模块名称 Module Name	功能概述 Function Description
SA_11 SA_12 SA_17	Fsu Test	用于对FSU（故障安全单元）硬件进行测试、监控和管理。模块提供FSU初始化、启动时安全状态清除、潜在故障检测和安全状态监控功能 Used for testing, monitoring, and managing the FSU (Fail-Safe Unit) hardware. The module provides FSU initialization, safe state clearance during startup, latent fault detection, and safe state monitoring functions.
SA_16	Mpu Drv	用于对ARM Cortex-M处理器的MPU硬件进行配置和管理。该模块提供MPU初始化、使能/禁用、区域配置等功能，通过配置MPU区域实现对安全关键代码和数据的内存保护，防止未授权访问和意外修改 Used for configuring and managing the MPU hardware of the ARM Cortex-M processor. The module provides functions such as MPU initialization, enable/disable, and region configuration. By configuring MPU regions, it implements memory protection for safety-critical code and data, preventing unauthorized access and unintended modifications.
SA_10	OverVolTst	过压状态检测模块，通过故障注入、寄存器状态判断等方法判断当前芯片是否处于过压状态。 The overvoltage detection module determines whether the current chip is in an overvoltage state through methods such as fault injection and register status judgment.
ESM_regulation_check_validation	EsmTst	电机转速控制单元：通过一个阶段的转速采样值来判断当前电机转速是否

		处于预期范围内。 Motor speed control unit: judges whether the current motor speed is within the expected range through a stage of speed sampling values.
iAoU_02 **iAoU_03** **iAoU_04**	SCST	内核自检库是一种基于软件的重要安全机制，其核心功能是在微控制器运行时检测CPU内核中的永久性硬件故障，以支持系统满足功能安全标准的要求。它通过预定义的测试向量激励MCU内核的各个子模块（如算术逻辑单元、寄存器、程序计数器、存储单元等），并观察和评估其逻辑响应，从而诊断出单点故障或潜在故障。 The kernel self-test library is a critical security mechanism based on software, with its core function being the detection of permanent hardware faults in the CPU core during microcontroller operation to ensure the system meets functional safety standards. It diagnoses single-point or potential faults by applying predefined test vectors to stimulate various submodules of the MCU core (such as the arithmetic logic unit, registers, program counter, memory units, etc.) and observing and evaluating their logical responses.

5.3 配置工具 Configuration Tool


workspace - Classic Designer - 知从木牛.配置工具V5.1.0
File Edit Navigate Project Model Form Editor Window Help
Quick Access
*模块配置 Basic Editor
设置过滤 text to filter...
Properties
校验... Tasks Pro... Con... Navi...
Configure Filters...

```
Models
  TstM
    TstM
      TstMGeneral
      TstM_FunctionList [0..15]
      TestPreRun [0..1]
        TestPreRun0
          core [0..3]
            core0
              TestPreRunItem [0..*]
                TestPreRunItem0
      TestGroupRuntime [0..1]
```

TstM ▸ TestPreRuns [1] ▸ TestPreRun0 ▸ cores [1] ▸ core0 ▸ TestPreRunItems [1] ▸ TestPreRunItem0

名称 Name	TestPreRunItem0
ParamSetIndex[Dec]	0
Test	

Test [EcucReferenceDef]

描述 Description
定义 Definition
状态 Status

个数 Multiplicity	[1 -> 1]
定义 Definition	/AUTOSAR/TstM/TestPreRun/core/TestPreRunItem/Test
类型 Type	Reference
范围 Range	/AUTOSAR/TstM/TstM_FunctionList
原始值 Origin	
路径 Source	D:/MUNIU工具打包/知从木牛.配置工具V5.1.0 /workspace/cfg/.lib/TstM.arxml

0 errors, 0 warnings, 0 infos

Description	Object

为了满足客户的不同项目需求，提高 Safety Frame 的扩展性，TLE9954 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 diverse project requirements of customers and enhance the scalability of the Safety Frame, the TLE9954 Safety Frame has implemented the configurability of each module and has developed a configuration tool for the Safety Frame. Customers can complete the configuration of various modules of the Safety Frame using the configuration tool according to different needs. They can generate configuration code files, and integrate the generated configuration files into the project.

6 过程文档 PROCESS DOCUMENTATION

以下是英飞凌 TLE9954 功能安全产品在开发流程中的输出产物，其中需求文档、集成手册和测试相关文档可作为产品发布物提供给客户，设计相关的文档如有需要可以和我们进一步的沟通。

The following are the deliverables of the Infineon TLE9954 functional safety product in the development process. The requirements document, integration manual, and test-related documents can be provided to customers as product deliverables. Design-related documents can be further discussed with us if needed.

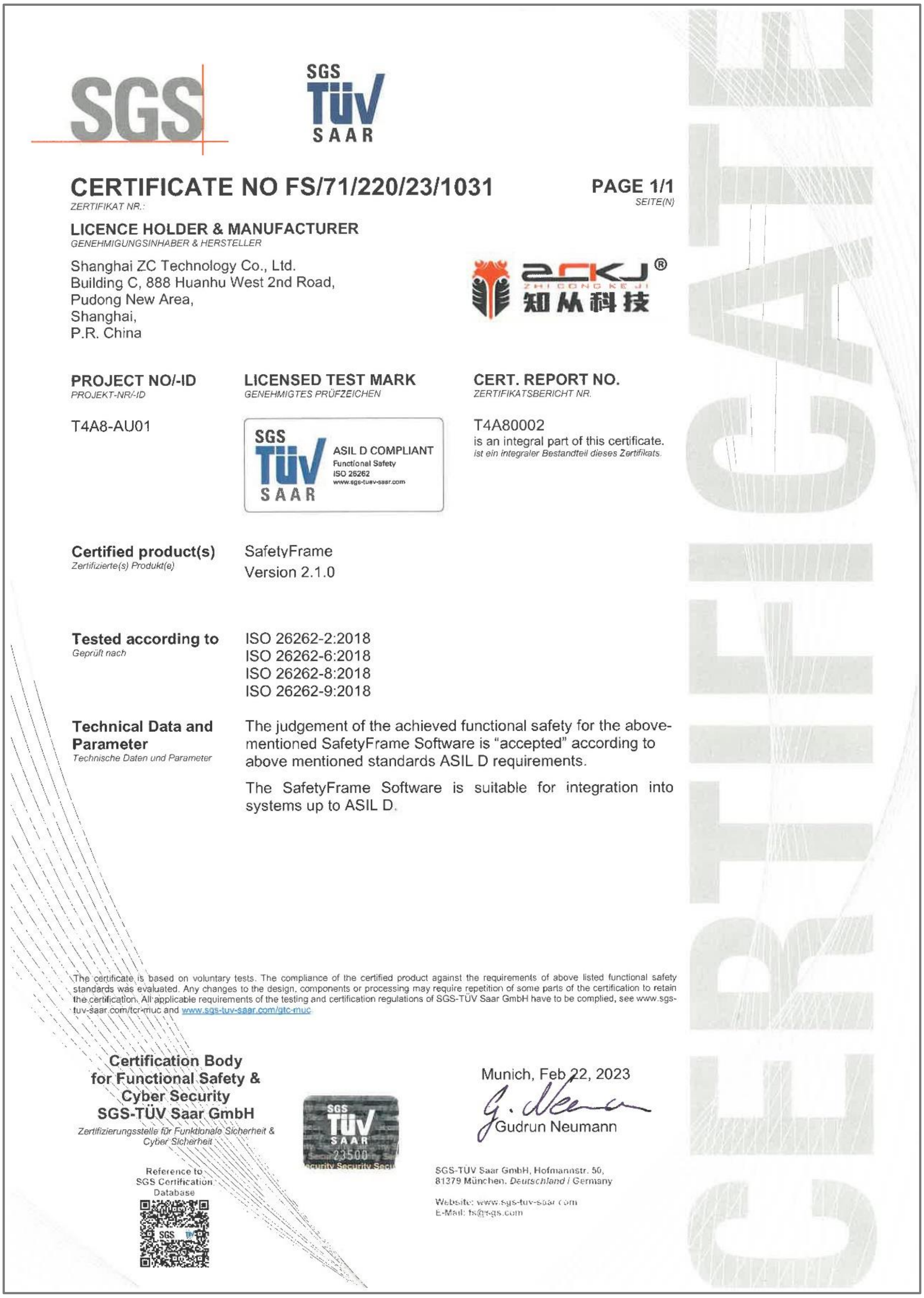
开发流程 Development Process	文档描述 Document Description
需求收集 Requirement Collection	客户的需求文档 Customer Requirements Document
软件需求分析 Software Requirement Analysis	软件需求分析 Software Requirements Analysis
	需求分析规格书 Requirements Analysis Specification
	软件需求追踪表 Software Requirements Traceability Matrix
	客户的问题沟通表 Customer 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
	软件安全分析 Software Failure Mode and Effect Analysis
	软件相关性失效分析 Software Dependent Failure Analysis
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

开发流程 Development Process	文档描述 Document Description
	SafetyFrame Engineering Review
软件单元测试 **Software Unit Testing**	软件静态分析报告 Software Unit Analysis Report
	软件动态测试报告 Software Unit Dynamic Test Report
	软件单元验证策略 Software Unit Verification Strategy
	软件单元验证策略 Software Unit Verification Strategy
软件集成和集成测试 **Software Integration and Integration Testing**	集成策略 Integration Strategy
	集成手册 pdf Integration Manual (PDF)
	软件安全手册 Software Safety Manual
	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.SafetyFrame 配置工具使用指导书 MuNiu.SafetyFrame Configuration Tool User Guide
	木牛.SafetyFrame 配置工具软件配置管理文档 MuNiu.SafetyFrame 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

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

ZCKJ® ZHI CONG KE JI 知从科技

PROJECT NO/-ID
PROJEKT-NR/-ID

T4A8-AU01

LICENSED TEST MARK
GENEHMIGTES PRÜFZEICHEN

SGS TÜV SAAR
ASIL D COMPLIANT
Functional Safety
ISO 26262
www.sgs-tuev-saar.com

CERT. REPORT NO.
ZERTIFIKATSBERICHT NR.

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

SGS TÜV SAAR 23500 Security Security Sec

Munich, Feb 22, 2023

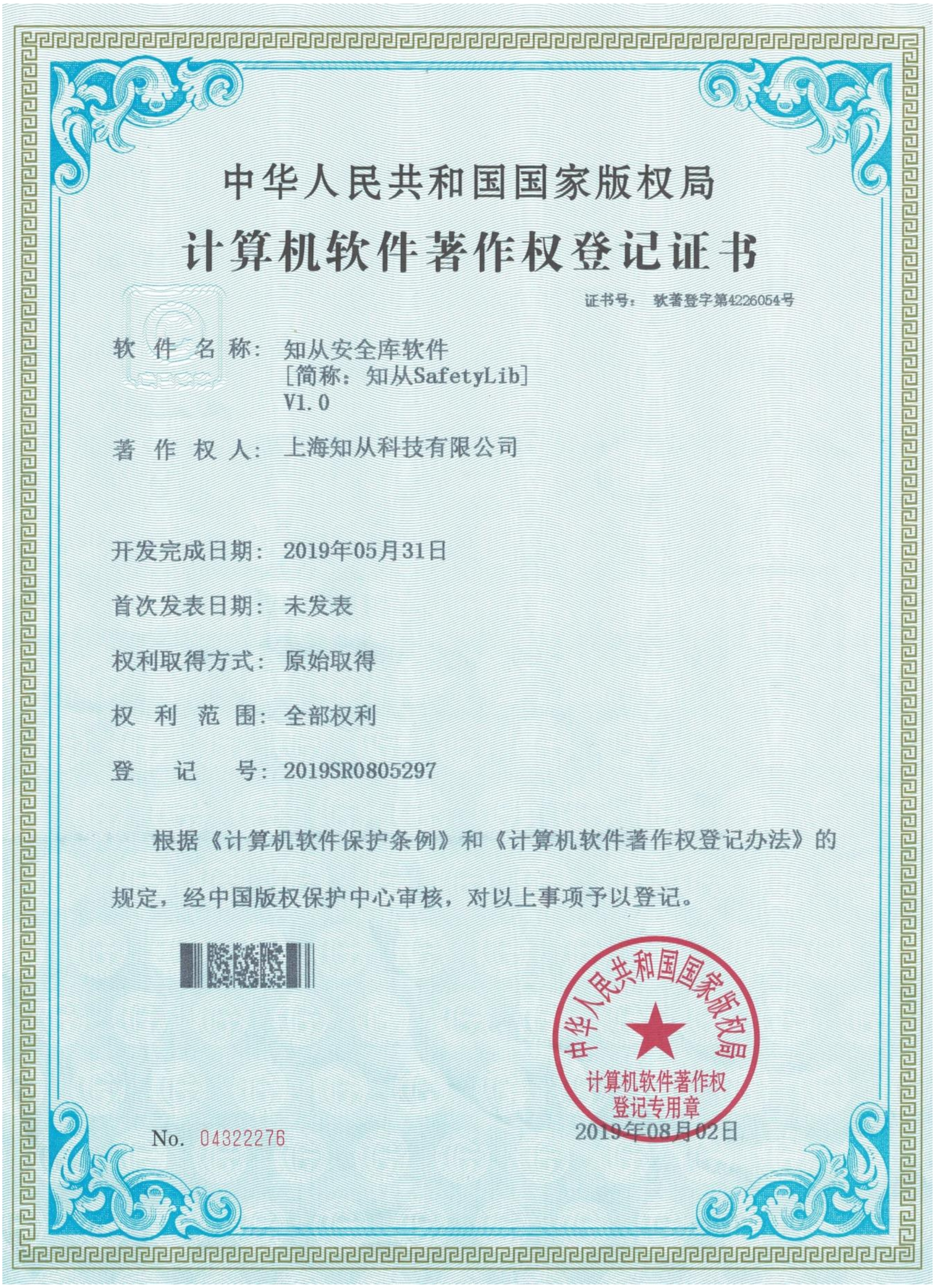
G. Neumann
Gudrun Neumann

SGS-TÜV Saar GmbH, Hofmannstr. 50,
81379 München, *Deutschland* / Germany

Website: www.sgs-tuv-saar.com
E-Mail: fs@sgs.com

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

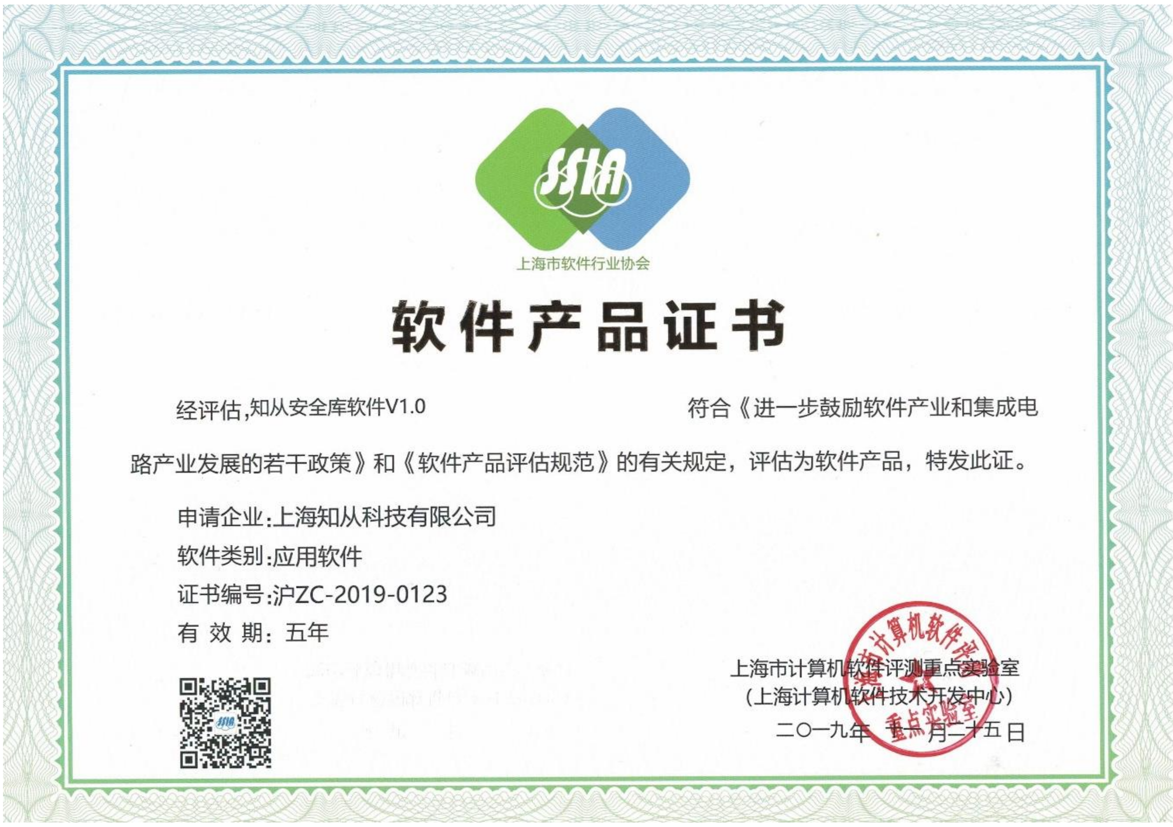
根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。

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 十一月二十五日

海计算机软件评
重点实验室

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