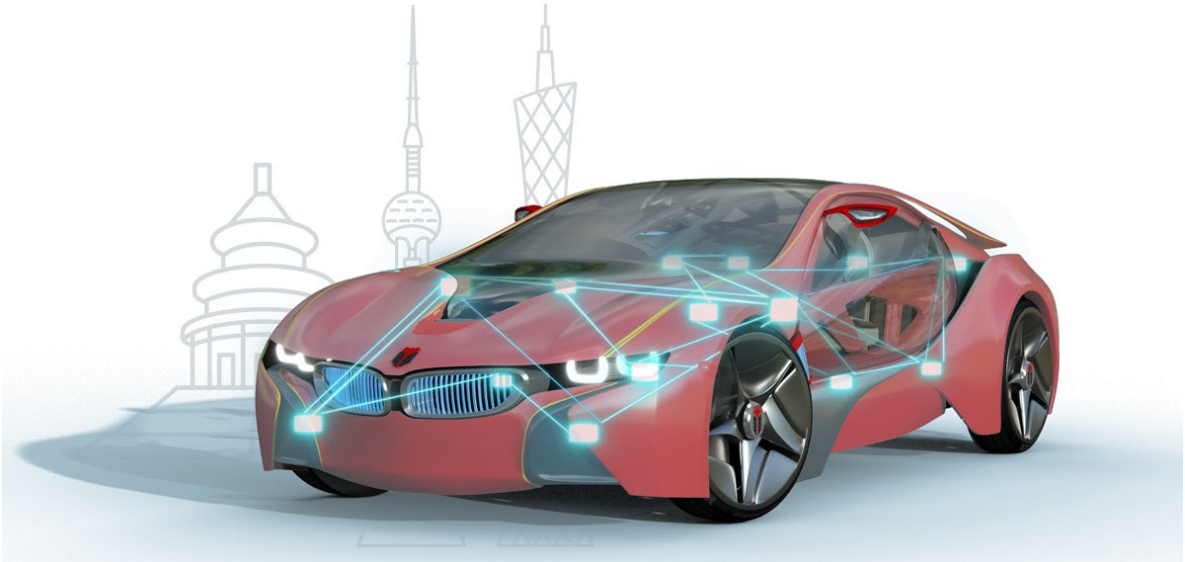
知从木牛 SAFETYLIBRARY 英飞凌 TC397 产品手册

ZC.MUNIU SAFETYLIBRARY PRODUCT MANUAL

BASED ON INFINEON TC397

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 英飞凌 TC397 产品手册
ZC.MUNIU SAFETYLIBRARY PRODUCT MANUAL BASED ON INFINEON TC397

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

TC397 Safety Library 用于帮助客户实现基于 AURIX TC397 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 TC397 Safety Library is designed to assist customers in achieving functional safety requirements based on the AURIX TC397 platform. The Safety Library offers high scalability, allowing for configuration and further development according to various customer project requirements, ultimately meeting the customers' functional safety requirements.

TC397 Safety Library 用于实现 TC397 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 TC397 Safety Library is used to implement software safety mechanisms for the TC397 series, including testing of internal MCU (Microcontroller Unit) modules and drivers for hardware safety mechanisms.

2 应用领域 APPLICATION FIELD

TC397 Safety Library 可应用于有功能安全等级需求的控制器。例如：

The TC397 Safety Library can be applied to controllers that require functional safety levels.

For example:

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

通过将 Safety Library 集成到基于 TC397 的控制中，可达到 ISO26262 ASIL-D 的等级要求。

By integrating the Safety Library into the control based on TC397, 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 SAK-TC397T-64F300W
Compilers Supported	Tasking TriCore v6.2r2
Evaluation Hardware	TriBoard TC3X7
Debugger	Lauterbach (Trace32 R.2018.02) Isystem (IC5700)
Configuration Tools	Muniu_v5.1.3
Configuration Environment	Win7 64bit

编译器选项 Complier Options	
Tasking 编译选项 **Complier Options**	--cpu=tc39x --iso=99 --keep-temporary-files --integer-enumeration -Wa--emit-locals=+equ,+symbols -Wa--section-info=+list,-console -Wa--optimize=+generics,+instr-size -Wa--debug-info=+asm,+hll,+local,+smart -Wc--debug-info=default -Wc--align=4 -Wc--default-a0-size=0 -Wc--default-a1-size=0 -Wc--default-near-size=0 -Wc--optimize=aceFgIklMnopRsUvwy,+predict -Wc--tradeoff=2 -Wc--language=-gcc,+volatile,-strings,-comments
Tasking 链接选项 **Linker Options**	--cpu=tc39x -Wl--output=TC397_ADAS.hex:IHEX -Wl--optimize=1 --output=TC397_ADAS.elf --lsl-file=TC397_ADAS.lsl -Wl--map-file -Wl--map-file-format=2

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(2011) 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 in vehicles is becoming increasingly complex, and the requirements for the safety of automotive electronics are also rising. To meet these safety requirements, automotive functional safety is gaining more and more attention. When it comes to functional safety, the first thing that comes to mind is the functional safety standard ISO 26262. In particular, Clause 8 of ISO 26262-5 (2011) introduces two metrics: the Single-point fault metric (single-point fault metric) and the Latent-fault metric (latent fault metric). Depending on the different ASIL grade requirements, the single-point fault metric and the latent fault metric need to achieve the corresponding grade.

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 Library 安全库就是实现分配到软件上的安全机制。

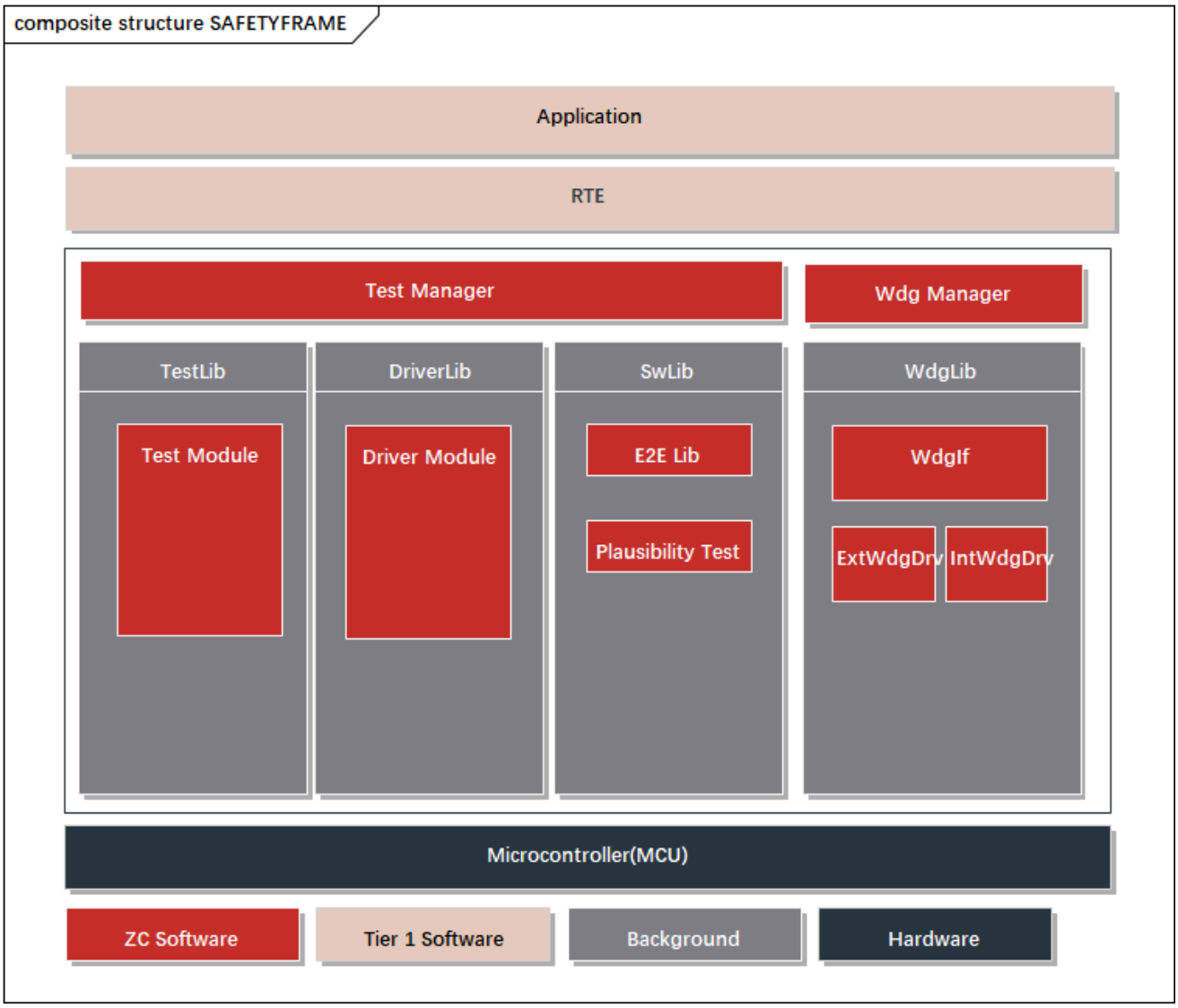
For microcontrollers (MCU, hereinafter referred to as MCU), in the electronic and electrical systems, they are designed and developed as SEooC (Safety Element out of Context). To meet the above-mentioned two metrics requirements, the MCU needs to implement corresponding safety mechanisms. Safety mechanisms can be allocated to hardware and software modules. The Safety Library of the MCU is the implementation of the safety mechanisms allocated to the 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 Features



- 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 applications.

- Safety Library 具有内部程序流监控

  The Safety Library has internal program flow monitoring.

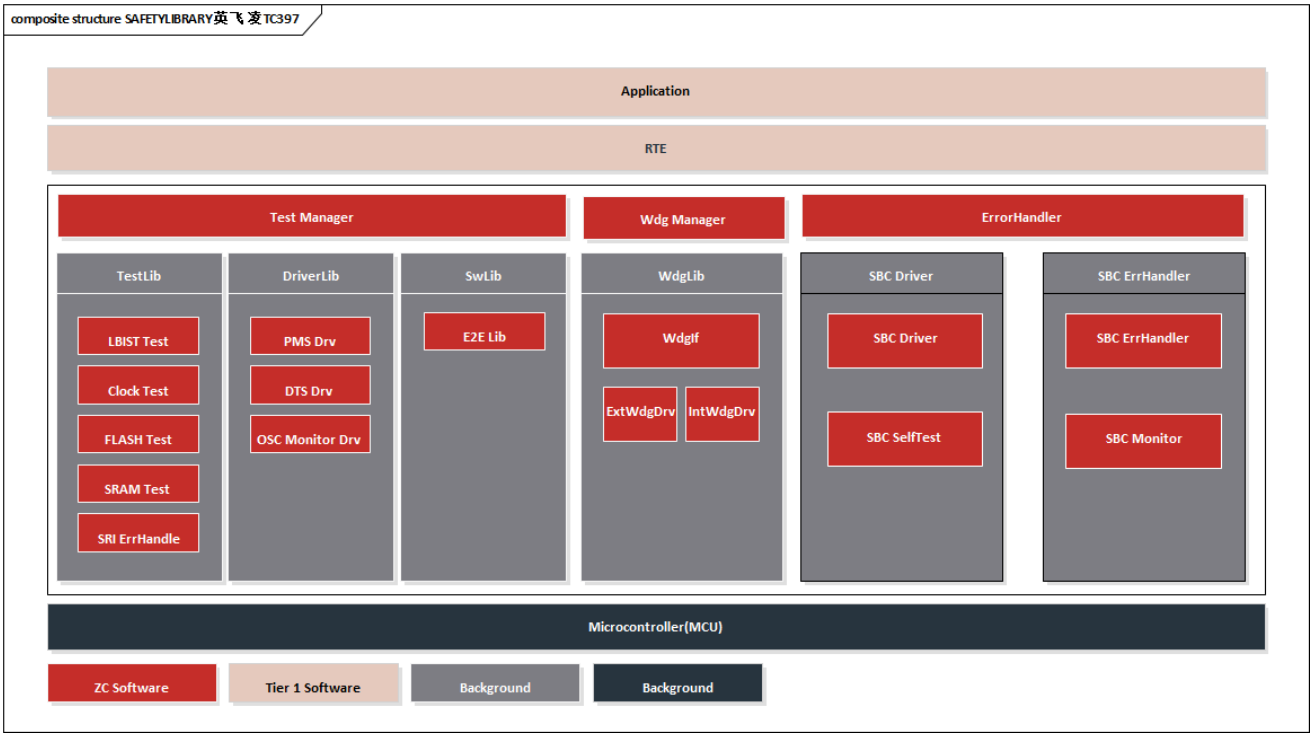
- 高安全性：支持多核自检测试，搭配知从科技 TLF35584Lib 可实现高达 ASIL-D 需求

High safety: Supports multi-core self-test, and when combined with ZC's TLF35584Lib, it can meet up to ASIL-D requirements.

- 高扩展性：各模块可配置满足不同客户的应用需求

  High scalability: Modules 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 Submodule	描述 Description
测试库 Test Library	LBIST Test	Logic BIST配置和结果检测 Configuration and result detection for Logic BIST (Built-In Self-Test).
	SRAM Test	MBIST SRAM 数据检测 Data detection for MBIST (Memory Built-In Self-Test) SRAM.

	FLASH Test	FLASH数据检测 Data detection for FLASH memory.
	FW Test	MCU Firmware启动检测 Boot detection for MCU Firmware.
	Clock Test	时钟合理性模块检测 Detection of clock rationality module.
	Register Test	寄存器检测 Detection of registers.
	DMA Test	DMA传输过程检测 Detection of DMA transfer process.
	SRI ErrHandle	SRI错误处理 Error handling for SRI (System Resource Interface).
	MONBIST	Power BIST配置和结果检测 Configuration and result detection for Power BIST (Built-In Self-Test).
	RegMon Test	寄存器监控检测 Detection of register monitoring.
驱动库 Driver Library	PMS Driver	PMS监控配置驱动 Configuration driver for PMS (Power Management System) monitoring.
	DTS Driver	温度监控配置和检测驱动 Configuration and detection driver for temperature monitoring.
	OSC Monitor Drv	OSC监控配置驱动 Configuration driver for OSC (Oscillator) monitoring.
SwLib	E2E Lib	E2E保护协议库 End-to-End protection protocol library.
Wdg 驱动库 Wdg Driver Library	WdgIf	看门狗驱动接口 Watchdog driver interface.
	SbcDrv	SBC芯片驱动 Driver for SBC (System Basis Chip).
	IntWdg Drv	内部看门狗驱动 Driver for internal watchdog.
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.

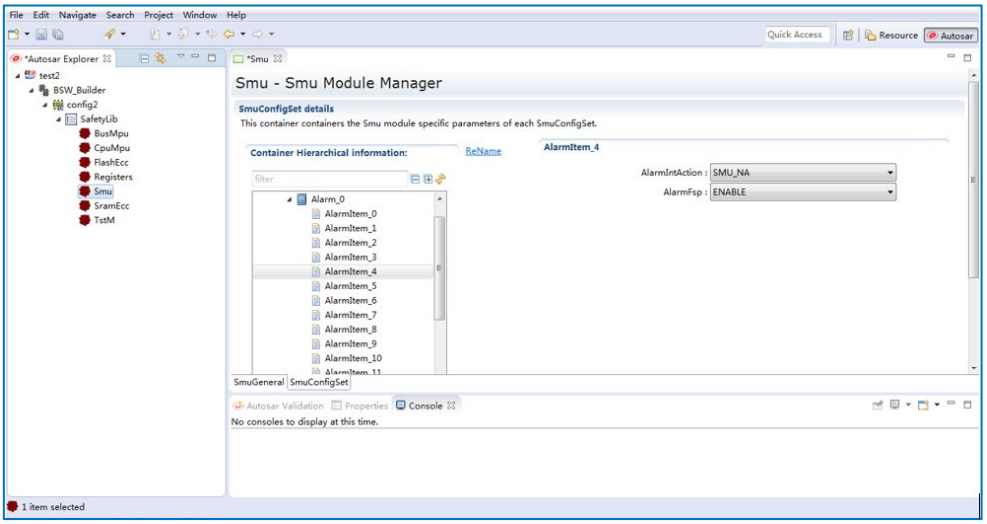
满足的 TC397 Safety Manual 中的 ESM：

Meets the ESM in the TC397 Safety Manual:

SMC[SW]:MCU:LBIST_CFG
ESM[SW]:MCU:LBIST_RESULT
ESM[SW]:DMA:ADDRESS_CRC
ESM[SW]:DMA:DATA_CRC
ESM[SW]:DMA:ERROR_HANDLING
ESM[SW]:DMA:SUPERVISION
ESM[SW]:DMA:TIMESTAMP
ESM[SW]:PMS:MONBIST_RESULT
SMC[SW]:PMS:MONBIST_CFG
SMC[SW]:PMS:MON_REDUNDANCY_CFG
SMC[SW]:PMS:VX_MONITOR_CFG
SMC[SW]:DTS:DTS_CFG
ESM[SW]:DTS:DTS_RESULT
SMC[SW]:CLOCK:OSC_MONITOR
ESM[SW]:CLOCK:PLAUSIBILITY
ESM[SW]:SYS:MCU_FW_CHECK
ESM[SW]:SRI:ERROR_HANDLING
ESM[SW]:NVM.PFLASH:WL_FAIL_DETECT
ESM[SW]:VMT:MBIST
SMC[SW]:VMT:MBIST
AMU.LMU_DAM:REG_MONITOR_TEST
CIF.RAM:REG_MONITOR_TEST
CPU.DCACHE:REG_MONITOR_TEST
CPU.DLMU:REG_MONITOR_TEST
CPU.DSPR:REG_MONITOR_TEST
CPU.DTAG:REG_MONITOR_TEST
CPU.PCACHE:REG_MONITOR_TEST
CPU.PSPR:REG_MONITOR_TEST
CPU.PTAG:REG_MONITOR_TEST
DMA.RAM:REG_MONITOR_TEST
EMEM.RAM:REG_MONITOR_TEST
ERAY.RAM:REG_MONITOR_TEST
GETH.RAM:REG_MONITOR_TEST
GTM.RAM:REG_MONITOR_TEST
HSPDM.RAM:REG_MONITOR_TEST
LMU.RAM:REG_MONITOR_TEST
MCMCAN.RAM:REG_MONITOR_TEST
PSI5.RAM:REG_MONITOR_TEST
SCR.RAM:REG_MONITOR_TEST
SDMMC.RAM:REG_MONITOR_TEST

SPU.BUFFER:REG_MONITOR_TEST
SPU.CONFIG:REG_MONITOR_TEST
SPU.FFT:REG_MONITOR_TEST
TRACE.TRAM:REG_MONITOR_TEST

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，TC397 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 TC397 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 requirements. They can generate configuration code files, and integrate the generated configuration files into the project.

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
	配置工具设计 Configuration Tool Design
	软件详细设计追踪表 Software Detailed Design Traceability Matrix
	Safety Library 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 Release	发布文档 Release documentation

7 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