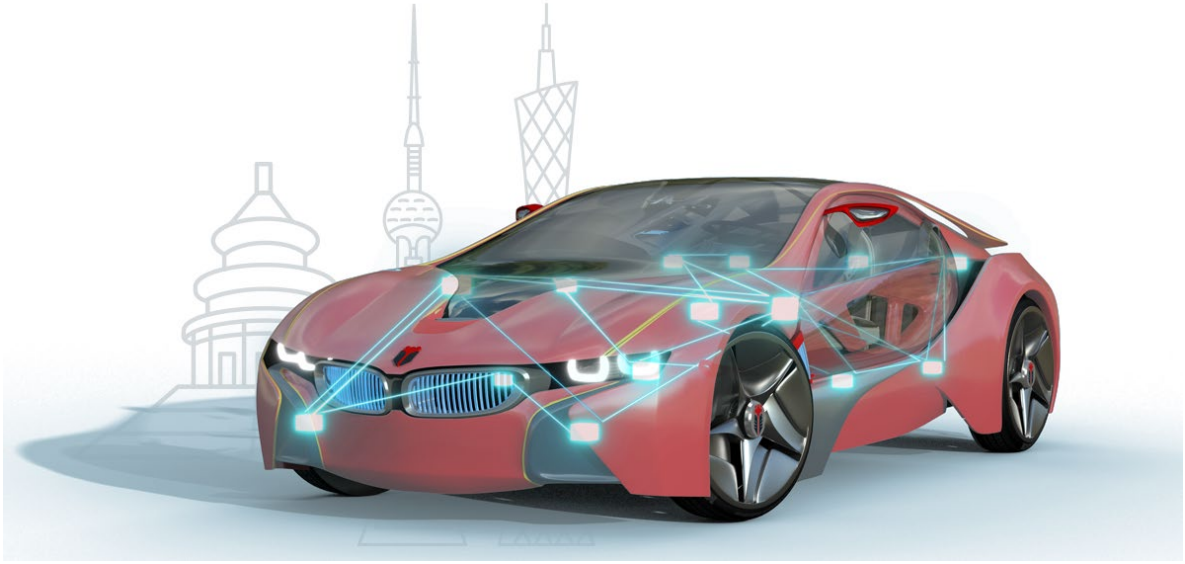
知从木牛功能安全 E2E 应用手册

ZC.MUNIU SAFETYLIBRARY E2E APPLICATION MANUAL

知从木牛基础软件平台功能安全库

ZC.MuNiu Basic Software Platform SafetyLibrary



知从木牛功能安全 E2E 应用手册

ZC.MUNIU SAFETYLIBRARY E2E APPLICATION MANUAL

知从木牛基础软件平台功能安全库

ZC.MuNiu Basic Software Platform SafetyLibrary

1 方案介绍 INTRODUCTION TO THE SOLUTION

随着汽车行业的发展，汽车电子产品设计的复杂程度，特别是软件开发的复杂程度也随之大幅提升，行业对于安全性(Safety)的重视程度也越来越高。知从科技具备多年符合 ISO 26262 功能安全要求的控制器开发经验，并和国内知名汽车的公司建立战略合作伙伴关系。

针对满足 ISO 26262 功能安全要求过程中的痛点——E2E 具体的项目实施，知从科技提供了相应的解决方案。

为了检测出信息交换中的各种失效状态，AUTOSAR 提出了 E2E 机制，通过对通信数据增加 DataID、CRC、Counter 等控制字段，使得软件可以在运行时检测和处理通信链路故障。E2E 保护可以实现：

1) 通过附加的控制数据来保护要通过 RTE 发送的安全相关的数据元素（data element）。
2) 通过控制数据来验证从 RTE 接收到的安全相关的数据元素。
3) 当接收到的安全相关的数据元素发生错误时，可以发出通知并由相关的 SWC 处理。

In order to detect various failure states in information exchange, AUTOSAR puts forward the E2E mechanism, which adds DataID, CRC, Counter and other control fields to the communication data, so that the software can detect and deal with communication link failures at runtime. E2E protection enables:

1) Security related data elements to be sent via RTE are protected by additional control data.
2) Verify security related data elements received from RTE through control data.

3) When an error occurs in the received security-related data element, a notification can be issued and processed by the relevant SWC.

With the development of the automotive industry, the complexity of the design of automotive electronic products, especially the complexity of software development, has also been greatly improved, and the industry has paid more and more attention to Safety. ZC Technology has many years of experience in controller development in line with ISO 26262 functional safety requirements, and has established strategic partnerships with well-known domestic automotive companies.

To meet the ISO 26262 functional safety requirements in the process of pain point - E2E specific project implementation, ZC technology provides the corresponding solution.

E2E 保护是关键系统通信安全的基石，能够有效应对数据传输和处理过程中的多种风险，常见 E2E 保护方案如下：

E2E protection is the cornerstone of communication security for critical systems and can effectively address multiple risks during data transmission and processing， the common E2E protection schemes are as follows:

- CRC 校验+计数器 CRC check + counter：
  - 使用 CRC(Cyclic Redundancy Check)校验数据完整性 Cyclic Redundancy Check (CRC) is used to verify data integrity
  - 添加计数器检测数据新鲜度(防止重放攻击) Add counters to detect data freshness (prevent replay attacks)
  - 简单易实现，适用于多数 ASIL B-D 应用 Simple to implement and suitable for most ASIL B-D applications
- 安全协议(如 AUTOSAR E2E) Security protocols (such as AUTOSAR E2E)：
  - AUTOSAR 标准定义的 E2E 保护库 E2E protected library defined by AUTOSAR standard
  - 提供多种 Profile(如 Profile1-5 等)适应不同 ASIL 等级 Various profiles (such as Profile1-5, etc.) are available for different ASIL levels
  - 包含数据 ID、计数器、CRC 等机制 Includes data ID, counter, CRC and other mechanisms
  - 提供多种 Profile 变体(如 Profile1A 1B 1C 等) Multiple Profile variants available (e.g., Profile1A 1B 1C, etc.)
- 能够检测出来的失效状态 A failure state that can be detected：
  - 信息重复（Repetition of information）：信息被接收到不止一次 The message is received more than once
  - 信息丢失（Loss of information）：信息或部分信息从传输的信息流中删除 The information or part of the information is deleted from the transmitted information flow

- 信息延迟（Delay of information）：接收到的信息晚于预期 The message received was later than expected
- 信息插入（Insertion of information）：将附加信息插入到所传输的信息流中 Inserts additional information into the transmitted information stream
- 信息伪装（Masquerading）：非真实信息被接收者接受为真实信息 Inauthentic information is accepted by the recipient as true information
- 信息的不正确寻址（Incorrect addressing）：信息从错误的发送方发送或被错误的接收方接收 The message was sent from the wrong sender or received by the wrong receiver
- 信息次序不正确（Incorrect sequence of information）：修改传输信息流中的信息顺序 Modify the order of information in the transmission flow
- 信息损坏（Corruption of information）：信息被改变内容 Information is changed content
- 从发送方传送到多个接收方的信息不对称（Asymmetric information sent from a sender to multiple receivers）：多个接收方从同一发送方接收到不同的信息 Multiple receivers receive different messages from the same sender
- 发送方发送的信息只能被部分接收方接收（Information from a sender received by only a subset of the receivers）：部分接收方没有接收到信息 Some recipients did not receive the message
- 通信信道阻塞（Blocking access to a communication channel）：对通信通道的访问被阻塞 Access to the communication channel is blocked

Secure Update ensures that only authorized software can be used by the controller, and when paired with Secure Boot, it can effectively prevent the execution of unofficial programs by the controller.

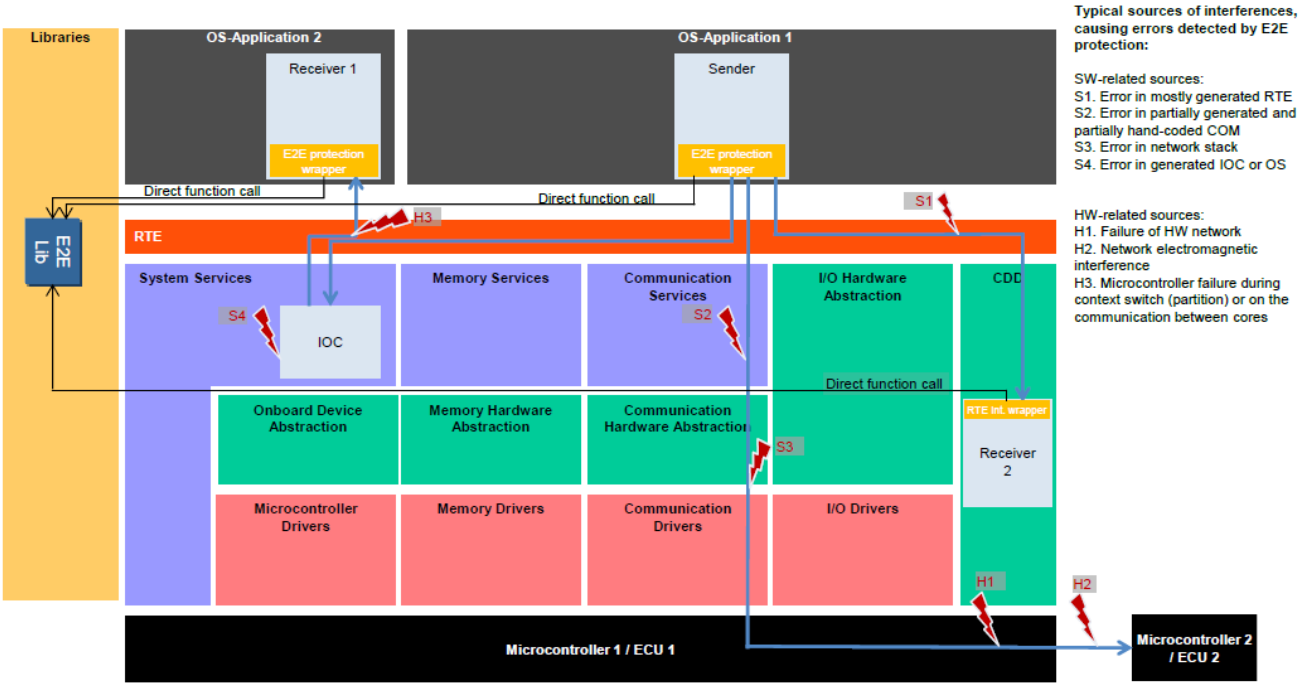


Figure 1： Example of faults mitigated by E2E protection

2 E2E APPLICATIONS

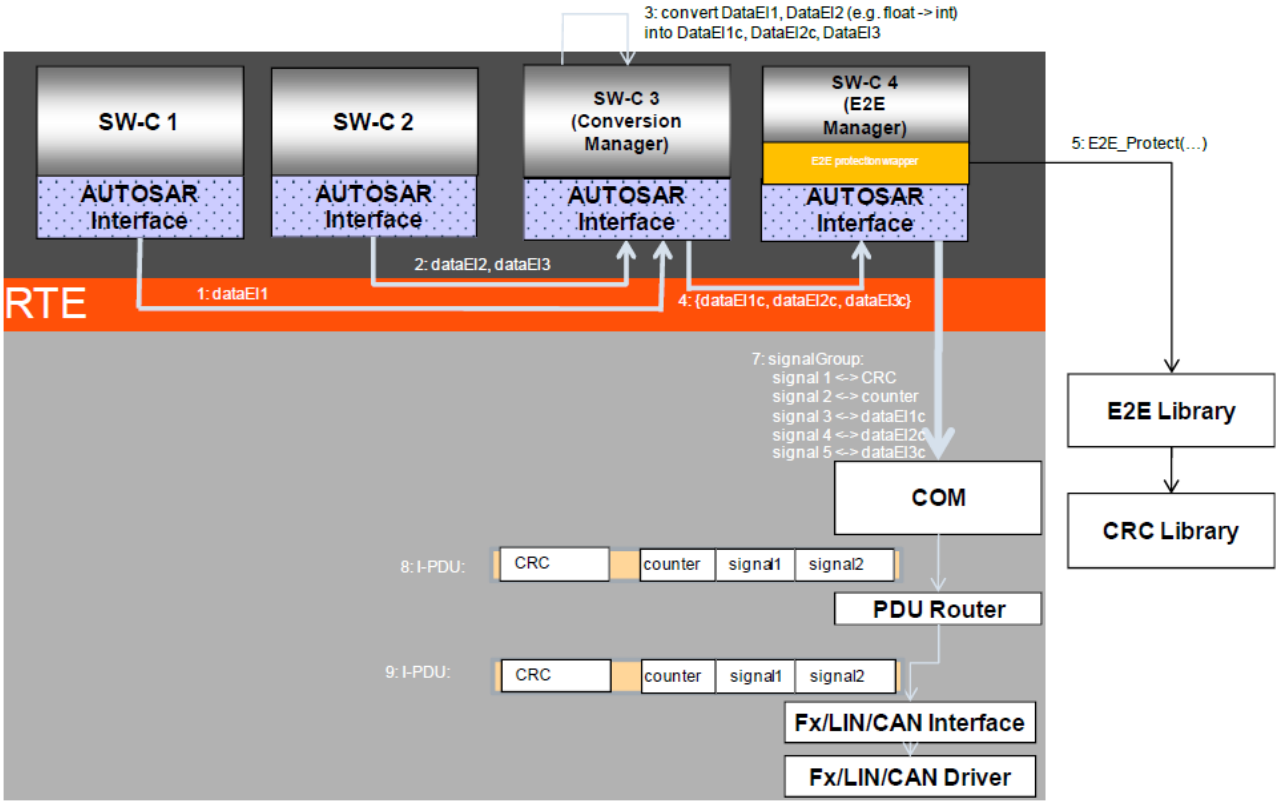


Figure 2： E2E Manager and Conversion Manager – sender ECU

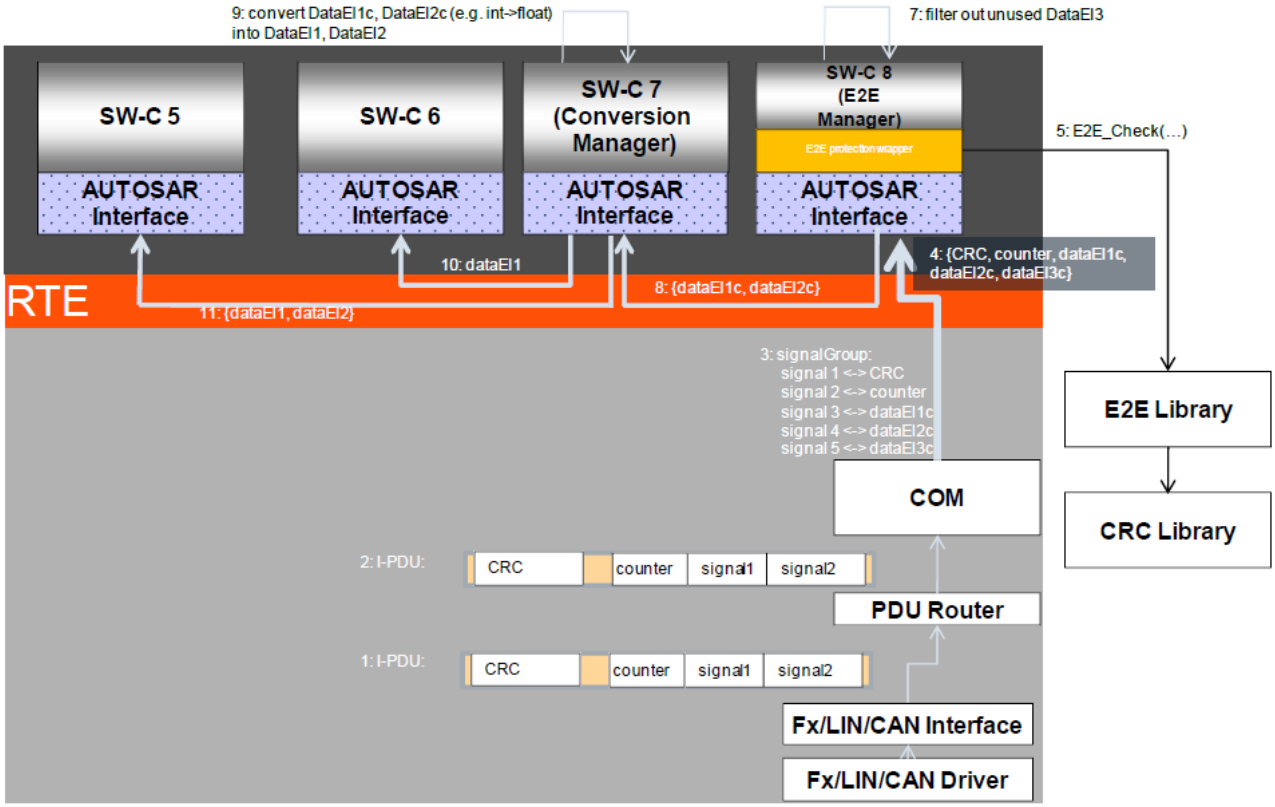


Figure 3： E2E Manager and Conversion Manager – receiver ECU

知从科技可以为客户提供 E2E 完整方案，并可针对项目特定需求定制开发：

ZC Technology can provide customers with a complete E2E solution, and can be customized for the specific needs of the project:

- 基于 CAN/CANFD/LIN/ FlexRay 通信保护方案
  Communication protection scheme based on CAN/CANFD/LIN/ FlexRay
- 基于 UART/SPI 等通信保护方案
  Communication protection scheme based on UART/SPI etc
- 基于 ETH 通信保护方案
  Communication protection scheme based on ETH

3 知从木牛 E2E 功能安全库 ZC.MuNiu E2E SafetyLibrary

3.1 E2E 协议栈 E2E Protocol Stack

知从木牛 E2E 协议栈主要由 E2E、CRC 两个模块构成。E2E 模块通过配置实现用户所需的通信保护等，并且调用接口进行发送或接收。CRC 模块功能为 E2E 模块进行 CRC 运算，得到具体 CRC 的结果。

The E2E stack is mainly composed of E2E and CRC modules. The E2E module is configured to implement the communication protection required by the user, etc., and calls the interface to send or receive. The CRC module performs CRC operations for the E2E module and obtains specific CRC results.

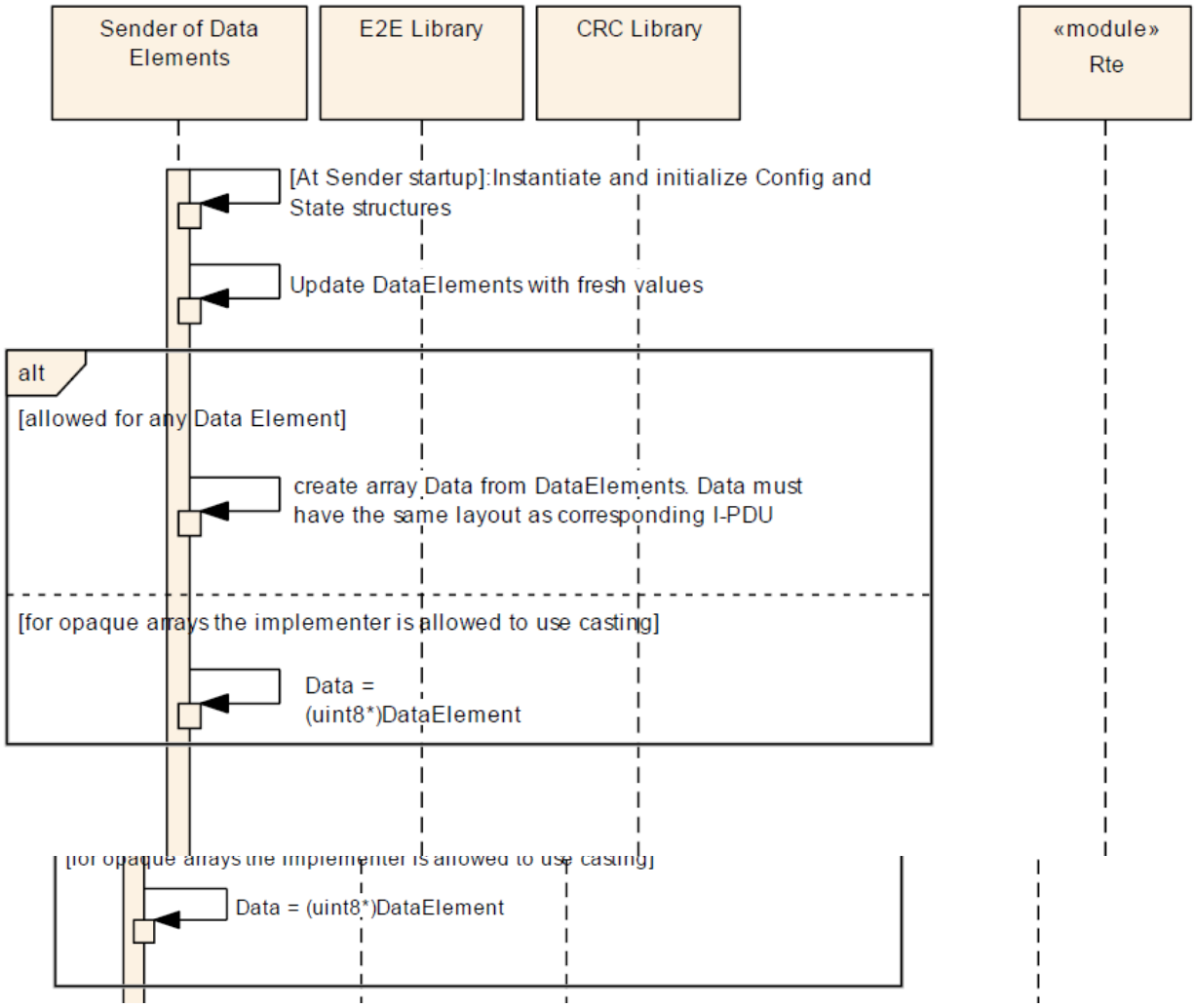


Figure 5： Receiver of data

4 证书 CERTIFICATE

SGS TÜV SAAR

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	LICENSED TEST MARK	CERT. REPORT NO.
PROJEKT-NR/-ID	GENEHMIGTES PRÜFZEICHEN	ZERTIFIKATSBERICHT NR.
T4A8-AU01	SGS TÜV SAAR ASIL D COMPLIANT Functional Safety ISO 26262	T4A80002 is an integral part of this certificate. ist ein integraler Bestandteil dieses Zertifikats.

Certified product(s) (Zertifizierte(s) Produkt(e)): SafetyFrame (compliant with Infineon TC3xx/TC2xx/TLF35584 and NXP FS6500 Safety Requirements)

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@sgs.com

Figure 6： ISO 26262 ASIL D