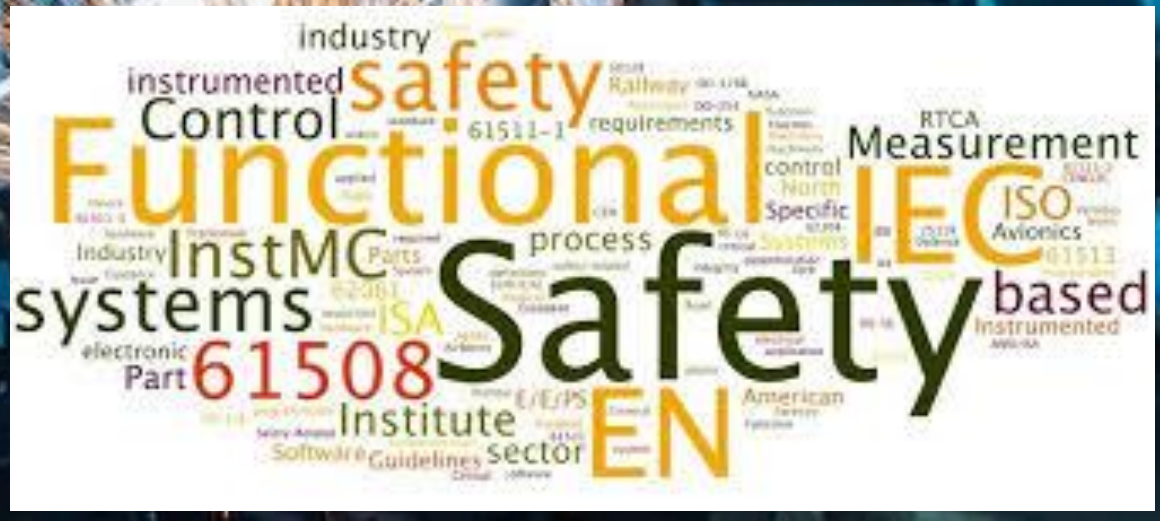
瑞萨功能安全解决方案
IEC61508

2023年5月
谭绍鹏 / JOHNSON TAN
MCU事业发展部
瑞萨电子（中国）有限公司



今天的议题

- 第一部分
  1. 符合IEC61508标准的功能安全介绍
  2. 功能安全市场趋势以及应用示例
  3. 工程师在功能安全设计上所面临的挑战,
  4. 瑞萨功能安全解决方案是如何应对这些挑战的
  5. 与瑞萨合作的模式
- 第二部分
  1. RX/RA自检库套件
  2. RX SIL3功能安全软件套件详解
  3. FSOE网络功能安全协议栈
  4. 功能安全参考文档及指南
  5. 参考板

功能安全

涉及应用领域	安全标准/等级	Renesas Safety Activity			
		瑞萨MCU	认证主体	安全等级	Notes
汽车	**ISO 26262** (ASIL A-D)	RH850	NA	ASIL D	Self certification by Renesas (certificate from 3rd party body is not required in ISO26262)
工业	**IEC 61508** (SIL 1-4) SIL1-3: FA/PA SIL4: train,infrastructure	RXv1, RXv2, RXv3, RA CM4 RA CM23/33	TUV	SIL3 (FA/PA)	EU directive forces certification to be done by certified body.
家电	**IEC 60730** (Class A/B/C) A: Lighting B: Washing machine C: Burner	RL78	VDE	Class B (appliance)	
		RX Synergy			

为什么功能安全非常重要

人会犯错，机器会出故障

- 随着越来越多的工业应用开始使用自动化技术，我们更加需要在设备中采取安全措施，从而防止或最大限度减少意外死亡和社会损失。
- 在向市场发布产品之前，当今的设备制造商要承担的任务是计算出发生故障的可能性，并为产品采取安全措施，以应对可能出现的故障。
- IEC61508是工业界具有代表性的安全标准，依照安全完整性等级(SIL)划分为SIL 1至SIL 4四个等级。最近，认证机构制定的SIL3标准正式成为工业设备的标准。
- **在工业应用中，第三方认证是必需的，不允许厂商自我声明。**

什么是IEC61508？

1. 该标准涵盖与安全相关的系统，包括电气/电子/可编程电子器件，例如MCU、MPU、ASIC和FPGA。

2. 该标准专门针对当安全功能发生故障时出现的危害。

3. 该安全标准的主要目标是将故障风险降低到可接受的水平。但是，开发稳固的安全系统可能是非常复杂的过程。

自2014年以来，瑞萨电子按照IEC61508标准提供功能安全解决方案。这些解决方案经过TUV莱茵认证。

应用实例

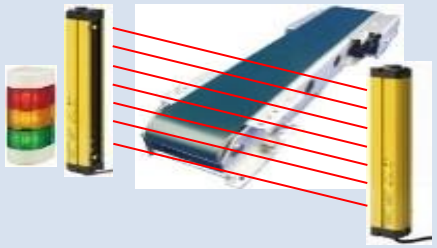
功能安全应用

工厂自动化和流程自动化

交流伺服系统/逆变器
机器人、数控机床

PLC（控制器）

FA传感器



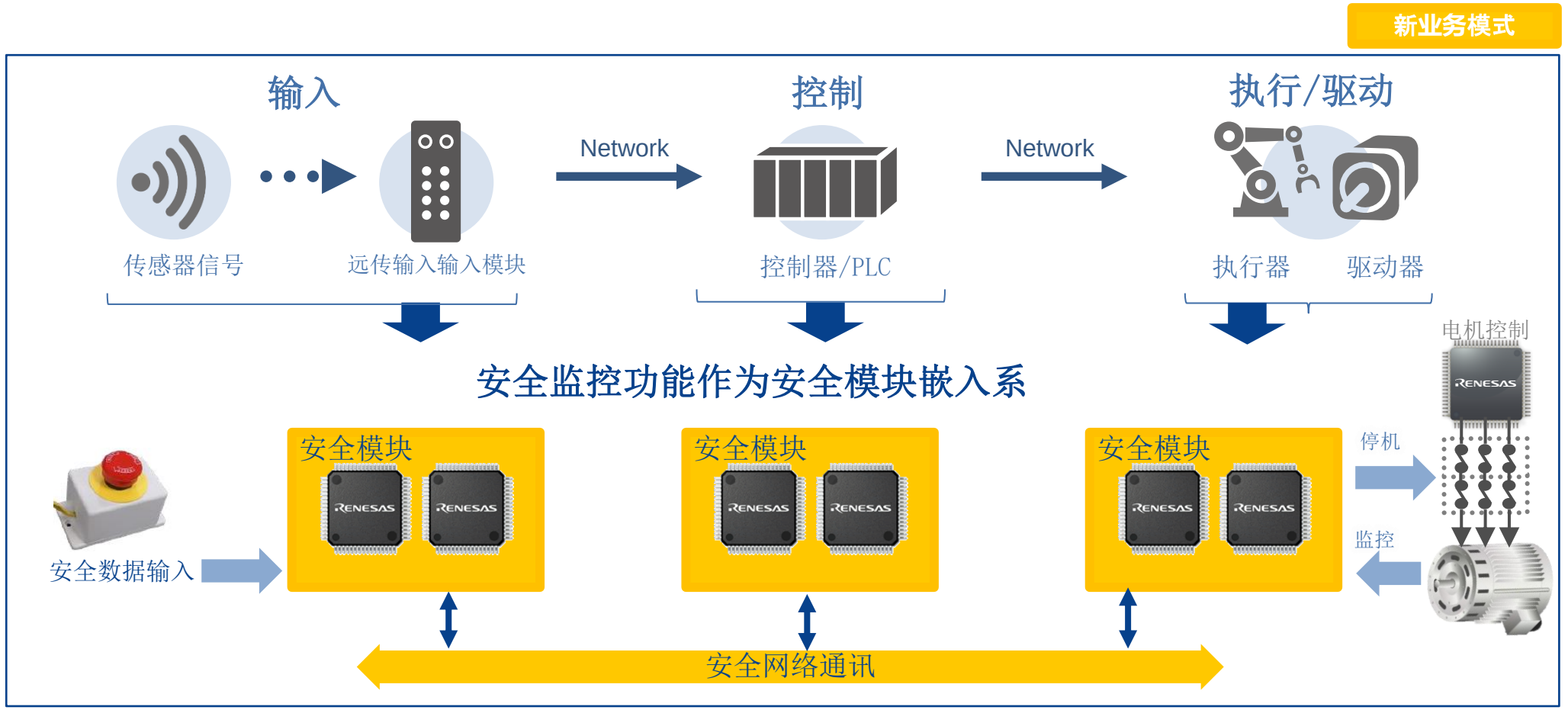
DCS
（工厂控制器）

PA传感器

远程IO

功能安全在工业自动化领域的典型应用

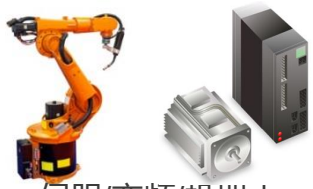
- 功能安全作为必要的系统安全措施，广泛应用在机器设备工厂自动化、过程自动化系统领域



功能安全在其他领域的应用

工厂/过程自动化(IEC61508, others)

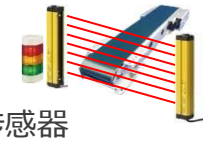
PLC(主控)



伺服/变频/机器人

DCS(工厂控制器)

远程IO



传感器

PA传感器

服务型机器人 (ISO13482)

Bed equipment

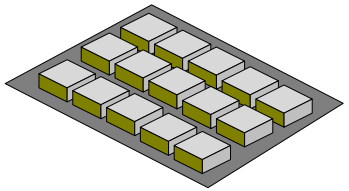
Electric cart

Transport robot

自动门 (EN16005)

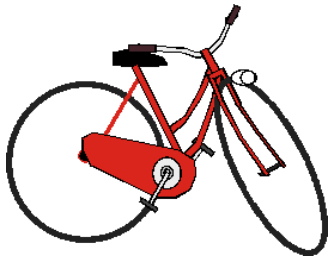
电池系统 (IEC62133, others)

家用燃料电池



蓄电池

助力自行车 (EN15194)



楼宇自动化

报警器

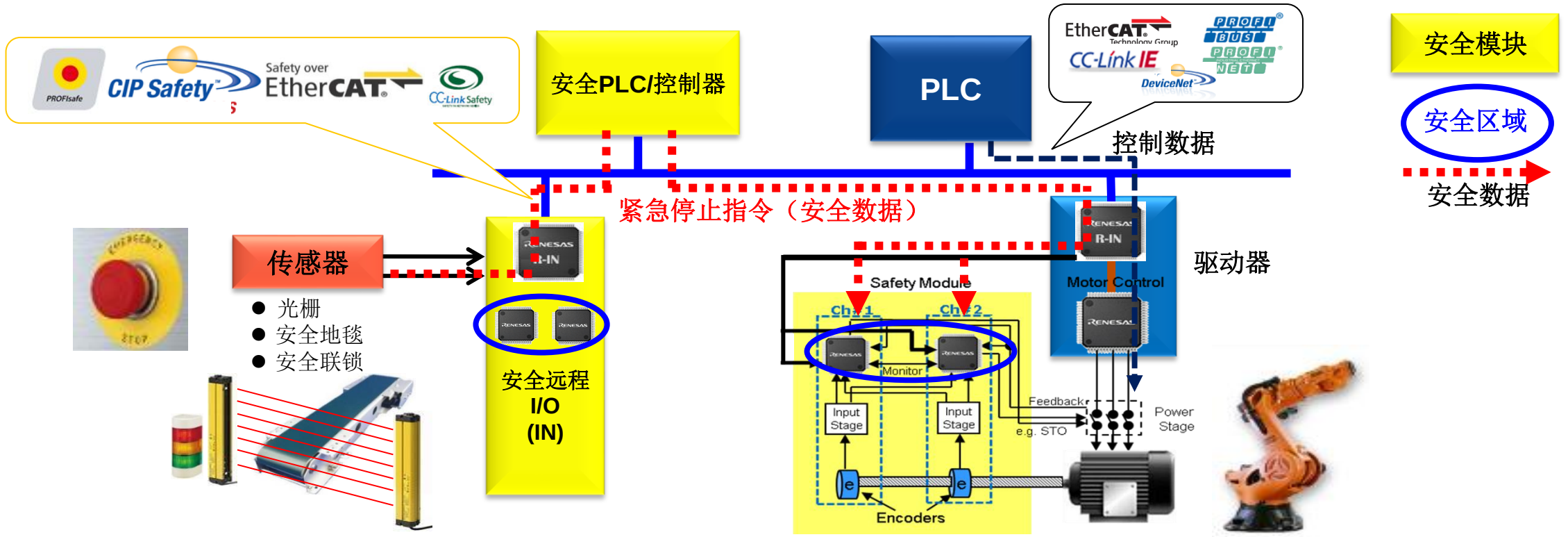
打印机

办公室打印机

工业打印机

一个典型的工业自动化安全系统

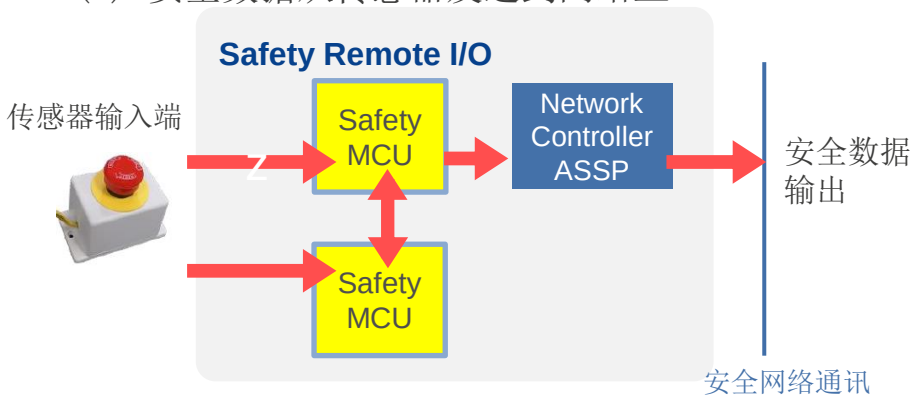
- 如今，机器都要通过工业以太网进行连接，包括在传感器、PLC、驱动器之间。
- 由于每个系统都要通过网络进行控制和监控，因此系统安全和网络协议本身都必须具有安全控制。



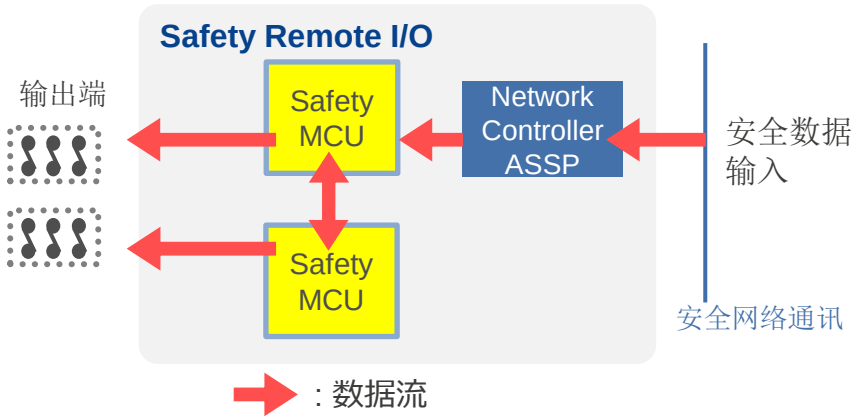
其他工业自动化安全功能应用示例

安全的远程I/O模块

(1) 安全数据从传感器发送到网络上

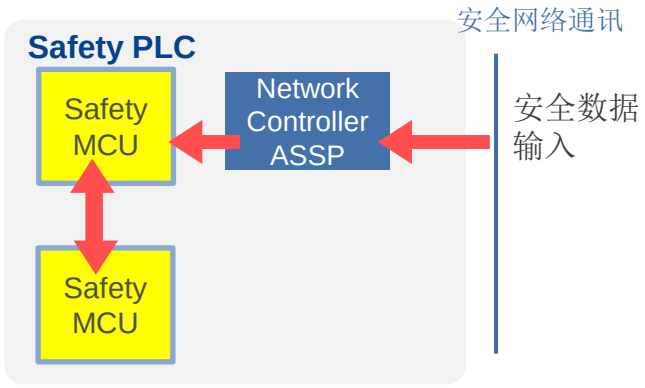


(2) 安全数据从网络再到执行器

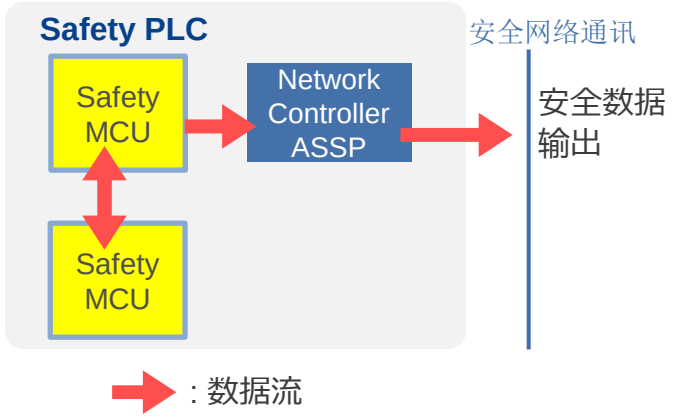


安全功能PLC

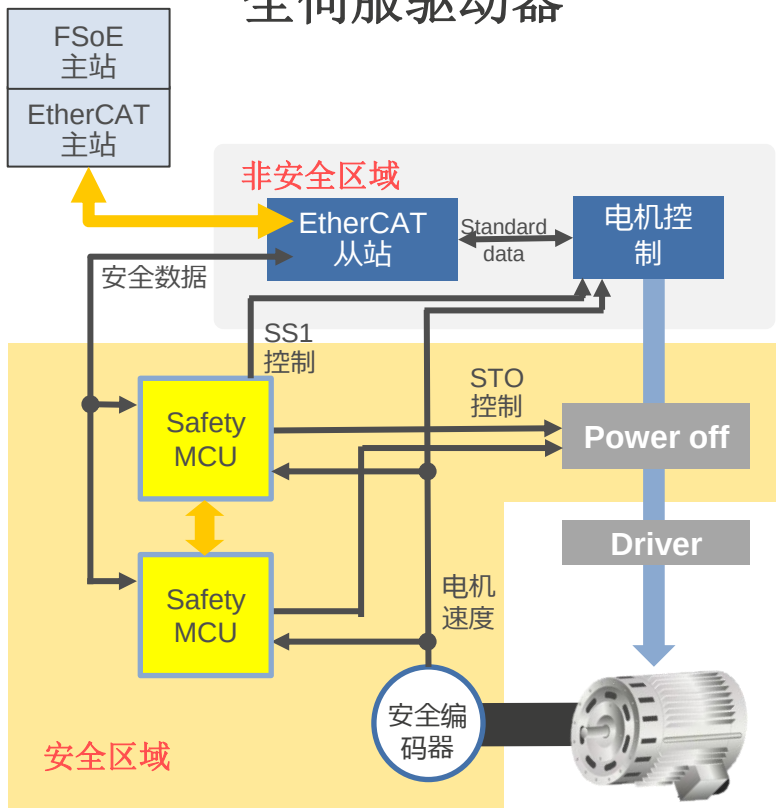
(1) 从网络输入安全的数据



(2) 将安全的控制数据发送到网络上



带网络安全（FSOE）的安全伺服驱动器



功能安全的设计所面临的挑战

IEC61508认证流程

从开始开发到认证，需要很长的过程，还要付出高昂的成本

SIL认证流程：从开始开发到认证，需要很长的过程，还要付出高昂的成本

功能安全系统开发中存在的问题

- 安全系统流程可能导致整个产品开发的成本大幅增加。

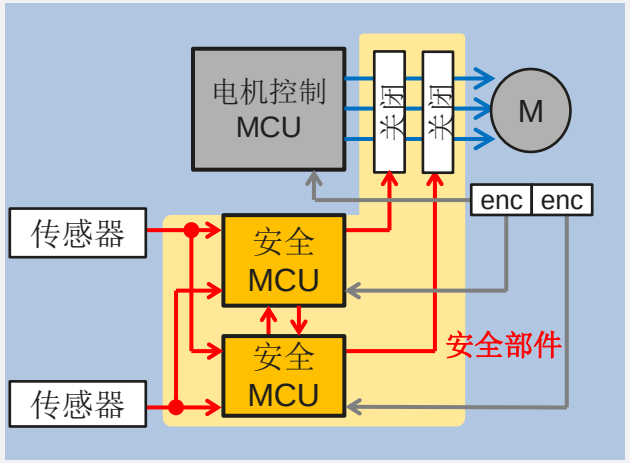
开发成本

- 理解功能安全标准
- 理解MCU规范
- MCU诊断方法检查
- 外设功能诊断方法检查
- 编写认证文档
- 安全软件/硬件的开发和评估
- 重复试生产

认证成本

- 参加功能安全研讨会
- 与认证机构磋商
- 概念检测
- 安全软件检测
- 安全硬件检测
- 文档检测
- 开发流程检测
- 更改软件/硬件时进行重新认证

物料成本



安全电路添加

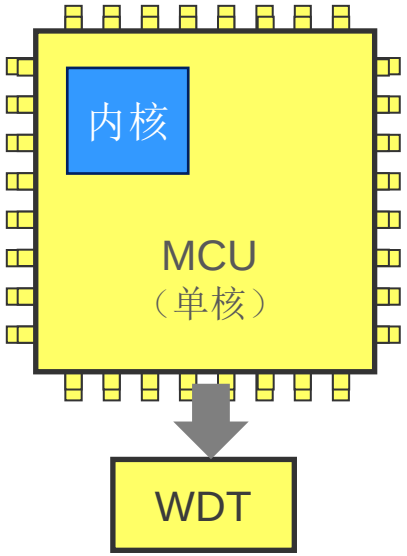
瑞萨提出的解决方案

硬件方案
MCU安全系统架构

- 通过采用双MCU配置，使用通用MCU，可以达到SIL3等级。

单MCU配置

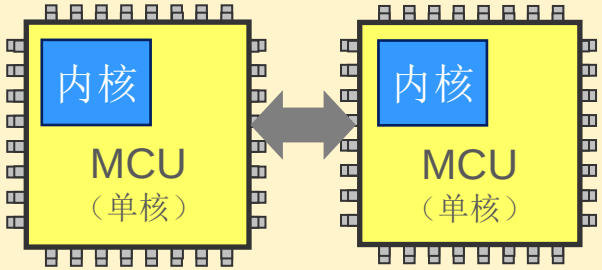
（SIL2等级，HFT=0）



最佳架构

双MCU配置

（SIL3等级，HFT=1）

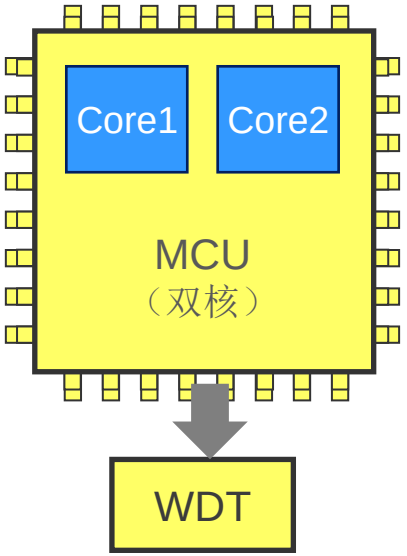


使用双MCU配置可以：

1. 简化安全认证
2. 降低诊断频率
3. 提升系统性能

双核和单MCU配置

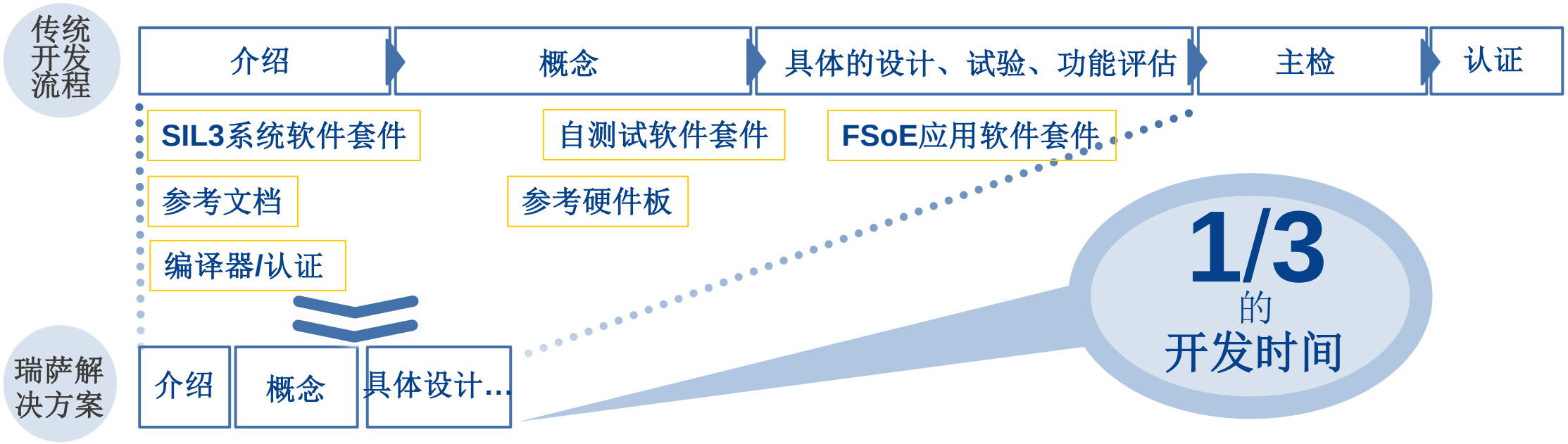
（SIL3等级，HFT=0）



HFT：硬件故障容错

软件方案
安全解决方案可以缩短开发和认证流程

- 瑞萨电子提供功能安全解决方案，利用瑞萨电子MCU的认证状态，缩短安全系统开发流程。
- 这让客户可以确信功能安全将会正确实施，并且达到认证要求，从而专注于应用开发工作。



瑞萨功能安全解决方案
缩短开发/认证流程

开发功能安全产品的各种解决方案

1. 自检库套件 RA/RX

用于诊断MCU内部的CPU、ROM、RAM和永久故障

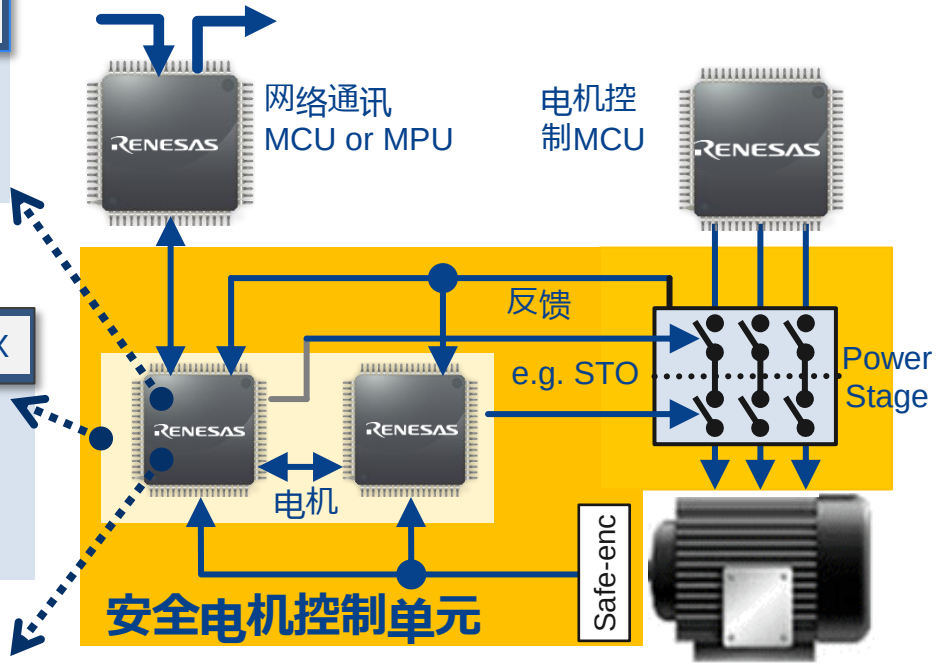
2. SIL3系统软件套件 RX

适用于双MCU系统，具有MCU诊断功能、调度程序和分区功能

3. FSoE 安全功能通讯软件套件 RX

适用于安全网络通讯的从站通讯协议栈

示例
带安全网络通讯的安全电机控制



4. 参考文档 RA/RX

-包含将要提交给认证机构的示例文档的指导书，以及准备指南
-技术文档，用于安全部件开发，例如输入和输出电路诊断、电源监控。

5. 参考板 RX

双MCU配置的硬件评估套件

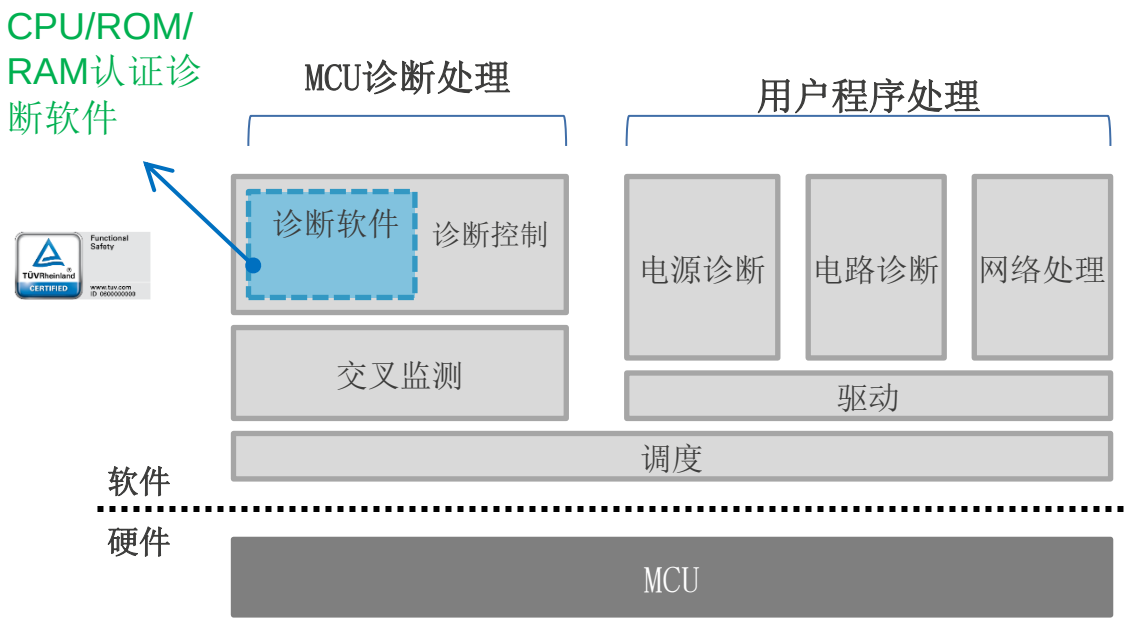
6. 符合IEC61508认证的编译器 RA/RX

- 瑞萨电子编译器的认证套件 "CC-RX" (RX)
- 或者从IAR购买经过认证的编译器 (RX/RA)

功能安全软件取决于客户的需求

自检软件包

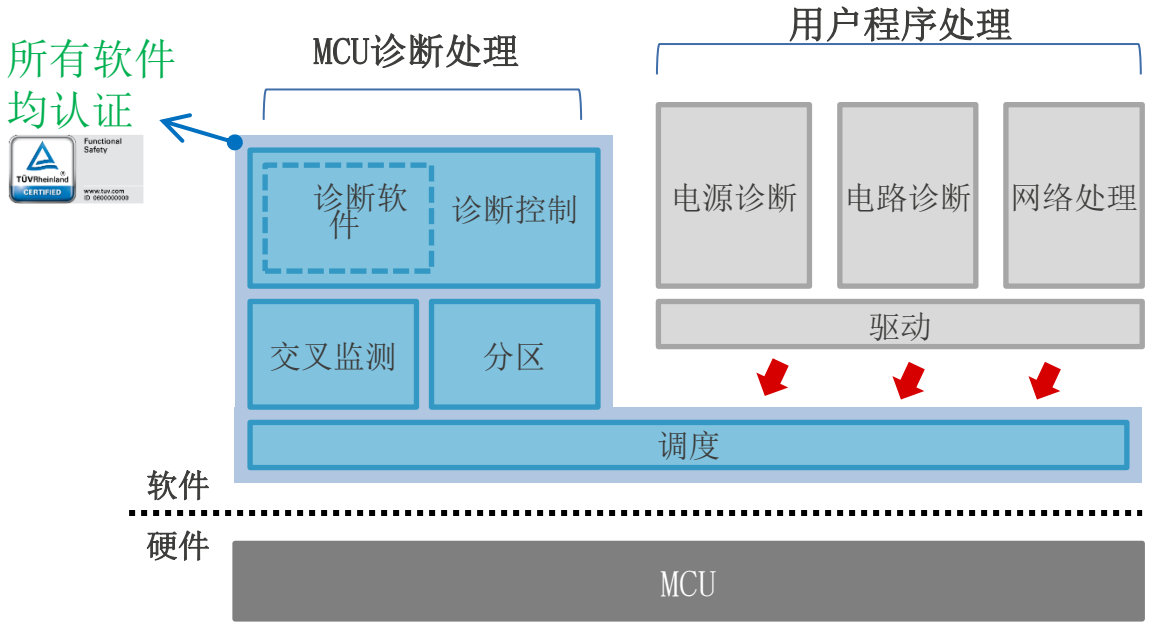
- 所有软件开发和认证工作需要，诊断软件除外



产品名称：自检软件包

SIL3功能安全系统软件包

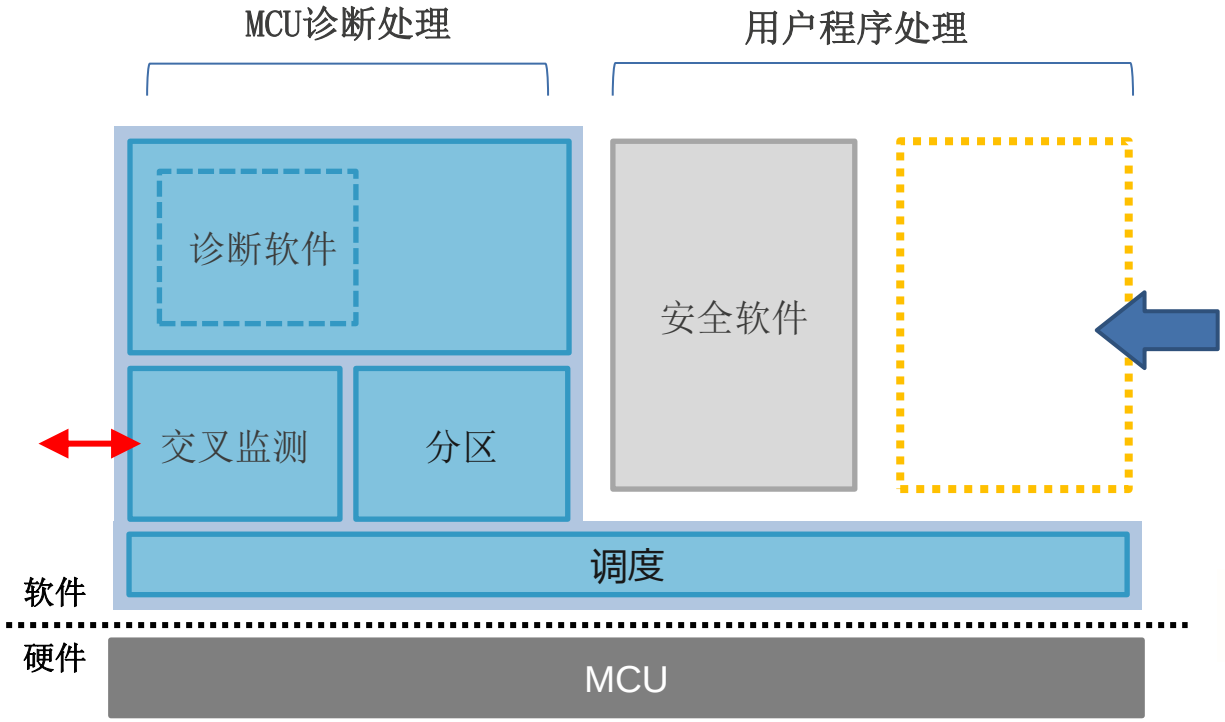
- 功能安全平台S/W执行所有诊断，如自我诊断以及交叉监控等。
- 用户只需开发用户产品处理软件



产品名称：SIL3系统软件包

网络安全软件

使用功能安全平台软件的多协议



通过交换网络协议栈应用程序，轻松更改协议

FSoE

NEW
PROFI Safe

CIP Safety*

CC-Link IE Safety

Safety over EtherCAT

PROFIsafe

CIP Safety

CC-Link IE Safety

*: 开发中

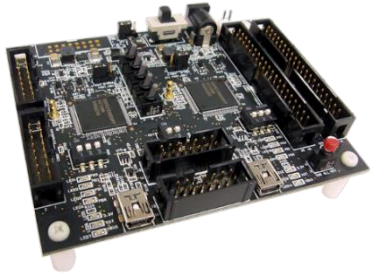
功能安全参考板

- 以下评估板均经过第三方安全功能认证机构验证并通过
- 设计包括功能安全标准要求的诊断和监控电路。
- 快速切入原型机和软件的开发！

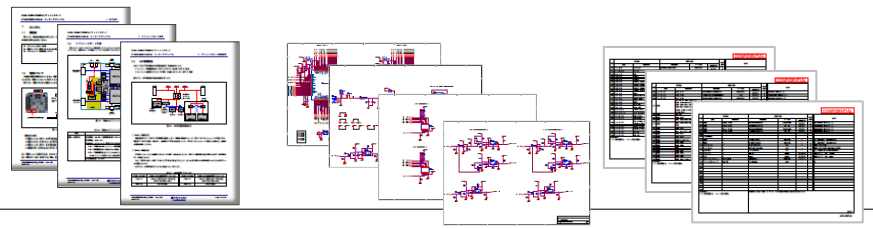
RXv1内核
RX111 - RX111参考板

RXv2内核
RX71M - RX651参考板

RXv3内核
RX72N – RX72N参考板



✓ 包括标准物料的各种电路设计以及用户手册



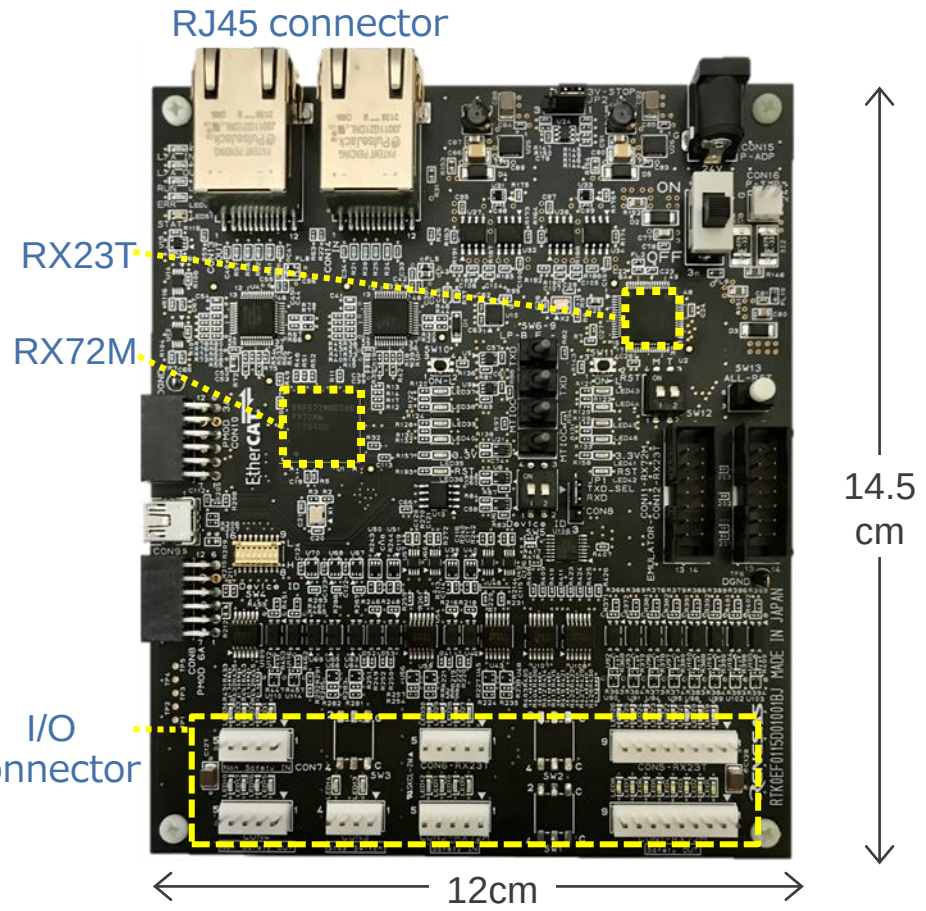
MCU引脚连接到扩展连接器:
✓ 快速启动软件原型开发或评估安全功能软件套件.
✓ 方便连接到原系统，以便扩展安全功能原型机开发

FSOE参考设计板

- 用于评估FSoE功能安全通讯从站评估板，适用于安全远程I/O等。

- 硬件功能包括
  - HFT(硬件故障裕度)=1 符合SIL3安全级别
  - 利用RX72M内置的EtherCAT双端口从控制器（ESC）实现EtherCAT从站安全功能通讯
  - 双MCU架构，符合FSoE从站安全功能，无需外部网络通信IC
  - 安全输入：5通道，安全输出：8通道；非安全I/O：4通道

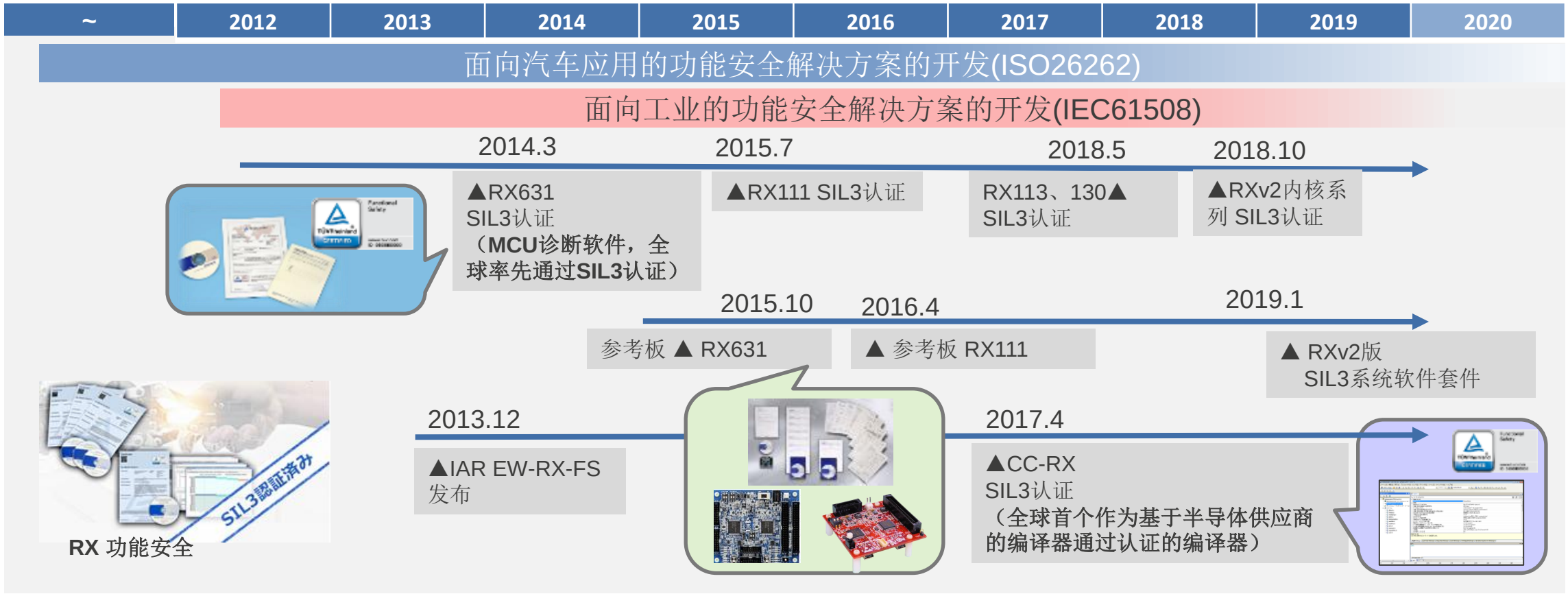
- 软件及文档
  - 自检软件库
  - SIL3系统软件库
  - FSoE 应用软件库（评估版本）
  - 用户手册、原理图、BOM清单



RX72M-RX23T FSOE安全功能评估板
(Order number：RTK0EF0115D01001BJ)

与瑞萨的合作模式

瑞萨在工业自动化功能安全领域的经验



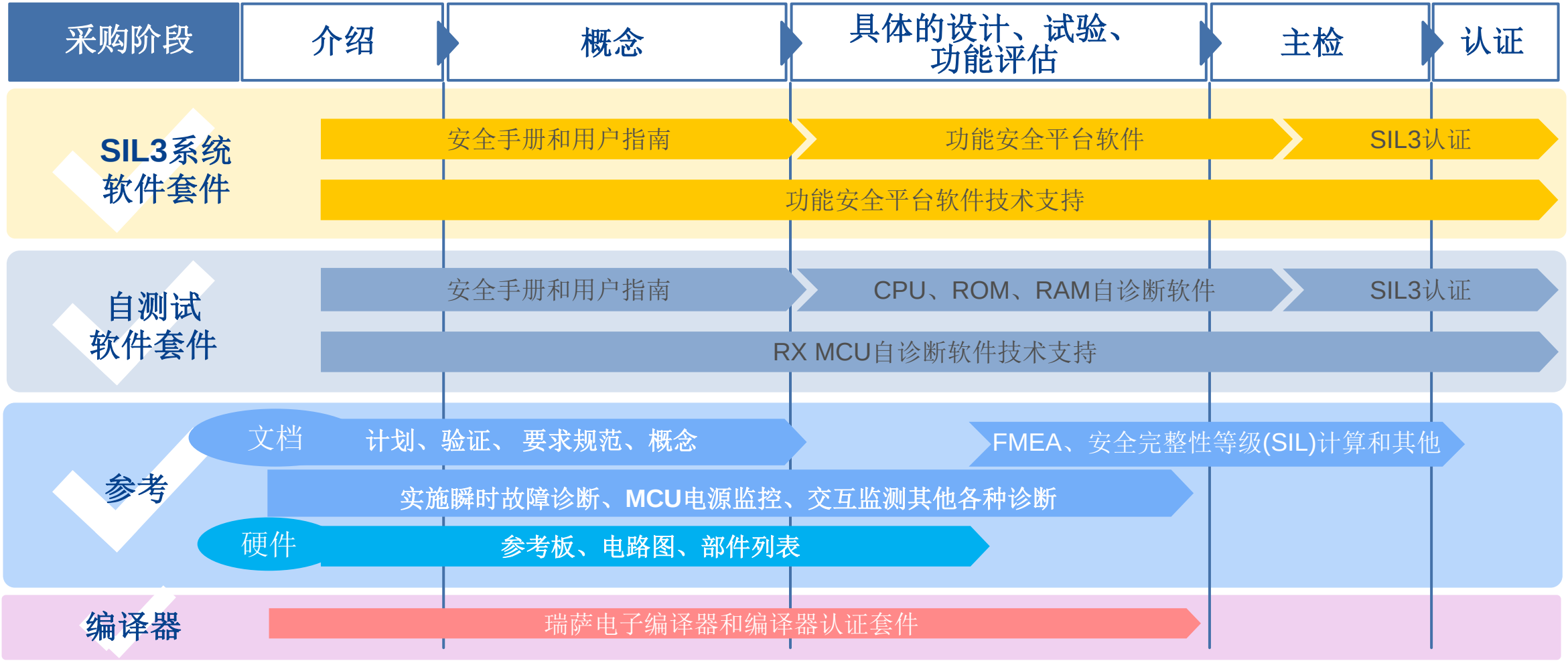
各产品系列的支持

*1： 虽然在使用RX MCU的示例中进行了描述，但它可以用于其他MCU，因为它是功能安全标准本身的技术文件，与专用MCU系列无关。
*2： 可以使用IAR系统编译器

No	Product	Family	RX			RA			
		Core	RXv1	RXv2	RXv3	CM4	CM23	CM33	
		Group	RX111 RX113 RX130	RX71M RX651/N RX64M RX24U RX24T RX230/1 RX23T RX23W RX23E-A	RX72M RX72N RX72T RX66N RX66T	RA6M1 RA6M2 RA6M3 RA6T1 RA4M1	NEW RA2A1 RA2L1 RA2E1	NEW RA6M4 RA6M5 RA4M2 RA4M3	More to come !
1	Self-Test Software Kit		✓	✓	✓	✓	✓	✓	
2	SIL3 System Software Kit			✓	✓				
3	FSoE Application Software Kit			✓	✓				
4	PROFIsafe Application Software Kit NEW			✓	✓				
5	Reference Document		✓	✓	✓	✓*1	✓*1	✓*1	
6	Reference Hardware		✓	✓	✓				
7	IEC61508 Certification Kit for RX Compilers		✓	✓	✓	*2	*2	*2	

瑞萨解决方案涵盖所有认证流程

客户可以专注于应用开发，而不会在没有预先认证的硬件、软件和文档的情况下，
在学习和完成安全认证流程时出现延误



瑞萨电子提供的灵活产品

- 标准解决方案 - **免费的认证自测试软件套件，带证书**

  ②自测试软件套件*

- 高级**认证解决方案**，帮助用户更简单快速地进行安全系统开发。
  - ✓ SIL3系统软件套件的**试用版本**和参考文档，**免费**提供，帮助开始评估

    ①SIL3系统软件套件*

    ③FSoE应用软件套件*

    ④参考文档*

    ⑤参考硬件板

    ⑥编译器，认证套件*

  - ✓ 年度支持服务包为选购

*需要事先获得软件许可证协议

瑞萨与其他品牌MCU的比较

MCU供应商	解决方案比较				有效缩短产品上市时间	分析
	认证CPU诊断	开发和认证指导文档	SIL3认证冗余系统软件	认证编译器		
瑞萨	✓	✓	✓	✓ CC-RX 和 IAR	1年	瑞萨电子解决方案比竞品更加全面，每个解决方案的技术含量都更高。
A	✓			✓ IAR ARM	2年或3年	CPU的已发布自测试软件。在支持服务方面，他们依赖于第三方。
B	✓			✓ IAR ARM	2年或3年	提供基于硬件的诊断，速度比软件快，但并非基于冗余系统。
C				✓ IAR ARM	2年或3年	提供MCU诊断软件，但没有经过认证。另外没有安全支持服务。
D				N/A	2年或3年	将双核锁步产品引入IA安全领域，但没有经过认证。仅提供器件支持，其他支持依赖于第三方。
E				✓ GHS	2年或3年	提供来自第三方的CPU诊断软件，而不是自有的软件。

总结

要点

- 瑞萨电子的经过认证的安全解决方案涵盖了开发和认证流程，帮助用户更简单快速地将产品推向市场。

✓经过认证的安全软件：使用经过认证的安全软件和安全协议，用户无需再开发自己的安全功能软件，而能够专注于用户应用软件的开发。

✓参考硬件板： 双MCU安全系统板，包含可供用户参考的安全电路，缩短产品开发时间。

✓参考文档：完整的安全指导书，包括有关IEC61508标准的设计专业知识。

✓认证编译器：实现顺畅快速的开发。

THANK YOU