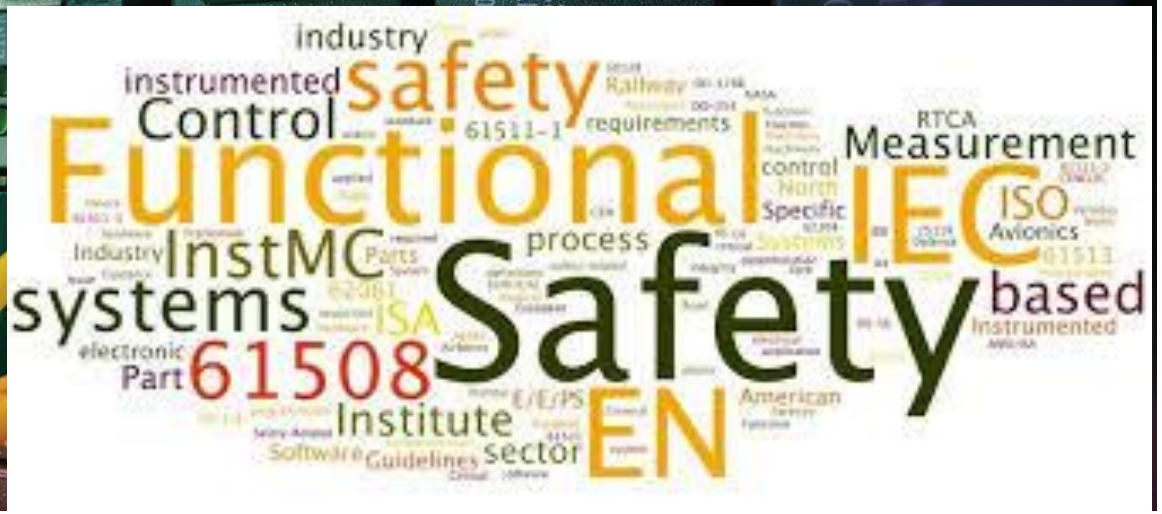
Renesas Functional Safety 功能安全解决方案 IEC61508

2023年5月
孙炜 MCU AE
MCU事业发展部
瑞萨电子（中国）有限公司



Renesas Functional Safety 功能安全

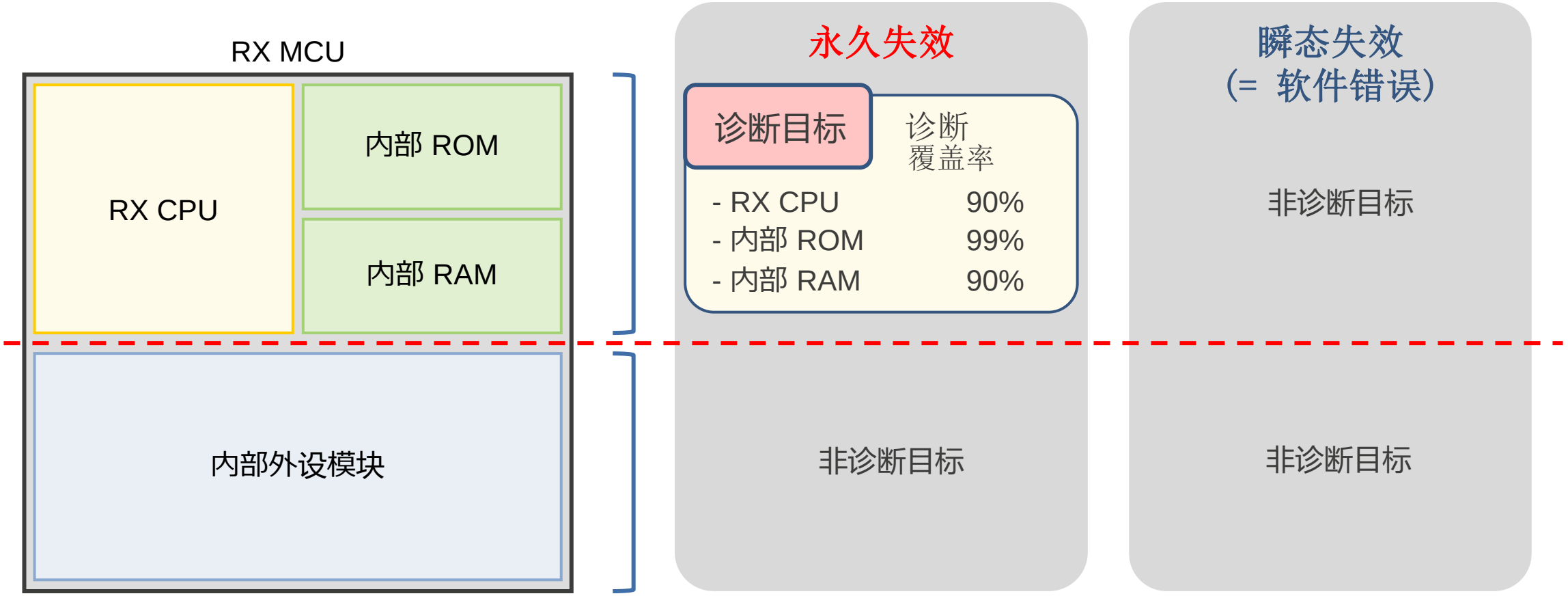
1. Renesas RX系列MCU功能安全解决方案
   - 1-1. Self-Test 软件包
     - 1-1-1. 概述
     - 1-1-2. 功能
   - 1-2. SIL3 系统软件包
   - 1-3. FSoE 功能软件包
   - 1-4. 参考文档
   - 1-5. 参考硬件
2. Renesas RA系列MCU功能安全解决方案
   - 2-1. Self-Test 软件包

RX系列Self-Test软件包：内容

No.	内容	
1	RX系列MCU诊断软件	TÜV Rheinland IEC61508 SIL3 认证的对象
2	安全手册	
3	用户指南	
4	IEC61508 认证文档(证书, 测试报告)	

RX系列MCU诊断软件 ： 概要

RX 系列MCU针对CPU, RAM, 和ROM 的永久失效诊断软件



RX系列MCU诊断软件 ：必要的资源

No.	目标	软件	ROM	RAM	端子	外设
1	RX100 系列*1	RX系列MCU诊断软件	39Kbyte	16byte	0	CRC
2	RX200 系列*2 RX600 系列*3 RX700 系列*4	RX系列MCU诊断软件	57Kbyte	16byte	0	CRC

*1:兼容RX111, RX113, RX130
*2:兼容RX24U, RX24T, RX230/RX231, RX23T, RX23W, RX23E-A
*3:兼容RX66T, RX66N, RX651/RX65N, RX64M
*4:兼容RX72M, RX72T, RX72N, RX71M

Self-Test 软件包 : 订购号码

No.	系列	编译器	订购号码
1	RX100 系列*1	CC-RX 编译器 V2.03.00	RTK0EF0059F31001SJ
2		IAR-EWRX编译器V3.10.5	RTK0EF0060F31001SJ
3	RX200 系列*2	CC-RX编译器V3.01.00	RTK0EF0054F32002SJ
4		IAR-EWRX编译器V4.14.2	RTK0EF0055F32002SJ
5	RX600 系列*3	CC-RX编译器V3.01.00	RTK0EF0054F36002SJ
6		IAR-EWRX编译器V4.14.2	RTK0EF0055F36002SJ
7	RX700 系列*4	CC-RX编译器V3.01.00	RTK0EF0054F37002SJ
8		IAR-EWRX编译器V4.14.2	RTK0EF0055F37002SJ

*1:兼容RX111, RX113, RX130
*2:兼容RX24U, RX24T, RX230/RX231, RX23T, RX23W, RX23E-A
*3:兼容RX66T, RX66N, RX651/RX65N, RX64M
*4:兼容RX72M, RX72T, RX72N, RX71M

RX系列MCU诊断软件 ：CPU 内核的诊断

项目	描述									
目标区域	CPU 核, 通用寄存器									
目标失效类型	永久失效									
诊断方法	“CPU指令代码组合的有效值”与“期望值”的比较									
诊断覆盖率	90%									
测试单元的数量, 总执行时间 *1	核	RXv3			RXv2					RXv1
	MCU 组	RX72M RX72N RX66N	RX72T	RX66T	RX71M	RX651 RX65N	RX64M	RX24U RX24T	RX230 RX231 RX23T RX23W	RX23E-A	RX111 RX113 RX130
	测试单元的数量	249	243	210	210	210	210	209	209	209	76
	总执行时间	187,266	176,084	171,138	171,590	204,515	156,238	211,751	185,675	154,957	45,178

*1: Unit = CPU clock cycles

RX系列MCU诊断软件 ：内部ROM诊断

<table>
<tr><th>项目</th><th colspan="4">描述</th></tr>
<tr><td>目标区域</td><td colspan="4">内部 ROM</td></tr>
<tr><td>目标失效类型</td><td colspan="4">永久失效</td></tr>
<tr><td>诊断方法</td><td colspan="4">“ROM数据的CRC计算值”与“期望值”的比较</td></tr>
<tr><td rowspan="4">诊断多项式,
诊断覆盖率</td><td colspan="4">从以下选项中选择</td></tr>
<tr><td></td><td colspan="2">诊断多项式</td><td>诊断覆盖率</td></tr>
<tr><td>1</td><td colspan="2">CRC-16 $(X^{16}+X^{15}+X^{2}+1)$</td><td>99%</td></tr>
<tr><td>2</td><td colspan="2">CRC-CCITT $(X^{16}+X^{12}+X^{5}+1)$</td><td>99%</td></tr>
<tr><td rowspan="5">执行时间[*1] [*2]</td><td colspan="2">Core</td><td>多项式</td><td>执行时间</td></tr>
<tr><td rowspan="2">RXv2
RXv3</td><td>CRC-16</td><td>34,234</td></tr>
<tr><td>CRC-CCITT</td><td>34,234</td></tr>
<tr><td rowspan="2">RXv1</td><td>CRC-16</td><td>81,996</td></tr>
<tr><td>CRC-CCITT</td><td>81,996</td></tr>
</table>

*1: Unit = CPU clock cycles
*2: 当ROM诊断的大小为 4 Kbyte

RX系列MCU诊断软件 ：内部RAM诊断

<table>
<tr><th>Item</th><th colspan="5">描述</th></tr>
<tr><td>目标区域</td><td colspan="5">内部 RAM</td></tr>
<tr><td>目标失效类型</td><td colspan="5">永久失效</td></tr>
<tr><td>诊断方法</td><td colspan="5">使用标准RAM测试算法进行诊断</td></tr>
<tr><td rowspan="4">诊断算法,
诊断覆盖率</td><td colspan="5">从以下选项中选择</td></tr>
<tr><td></td><td colspan="2">诊断算法</td><td colspan="2">诊断覆盖率</td></tr>
<tr><td>1</td><td colspan="2">Extended March C-</td><td colspan="2">90%</td></tr>
<tr><td>2</td><td colspan="2">WALPAT</td><td colspan="2">90%</td></tr>
<tr><td>诊断类型</td><td colspan="5">从以下选项中选择
1. 数据非破坏性测试
2. 数据破坏性测试</td></tr>
<tr><td rowspan="5">执行时间*1 *2</td><td colspan="2">核</td><td>算法</td><td>非破坏性测试</td><td>破坏性测试</td></tr>
<tr><td rowspan="2">RXv2
RXv3</td><td>Extended March C-</td><td>83,465</td><td>81,314</td></tr>
<tr><td>WALPAT</td><td>6,600,290</td><td>6,598,157</td></tr>
<tr><td rowspan="2">RXv1</td><td>Extended March C-</td><td>92,597</td><td>95,411</td></tr>
<tr><td>WALPAT</td><td>8,692,445</td><td>8,695,768</td></tr>
</table>

*1: Unit = CPU clock cycles
*2:当RAM诊断的大小为 1Kbyte

Renesas Functional Safety功能安全

1. Renesas RX系列MCU功能安全解决方案
    - 1-1. Self-Test软件包
    - 1-2. SIL3 系统软件包
        - 1-2-1. 概述
        - 1-2-2. 功能 1 (MCU 诊断)
        - 1-2-3. 功能 2 (调度器)
        - 1-2-4. 功能 3 (分区)
        - 1-2-5. 评估版本.
    - 1-3. FSoE 应用软件包
    - 1-4. 参考文档
    - 1-5. 参考硬件
2. Renesas RA系列MCU功能安全解决方案
    - 2-1. Self-Test 软件包

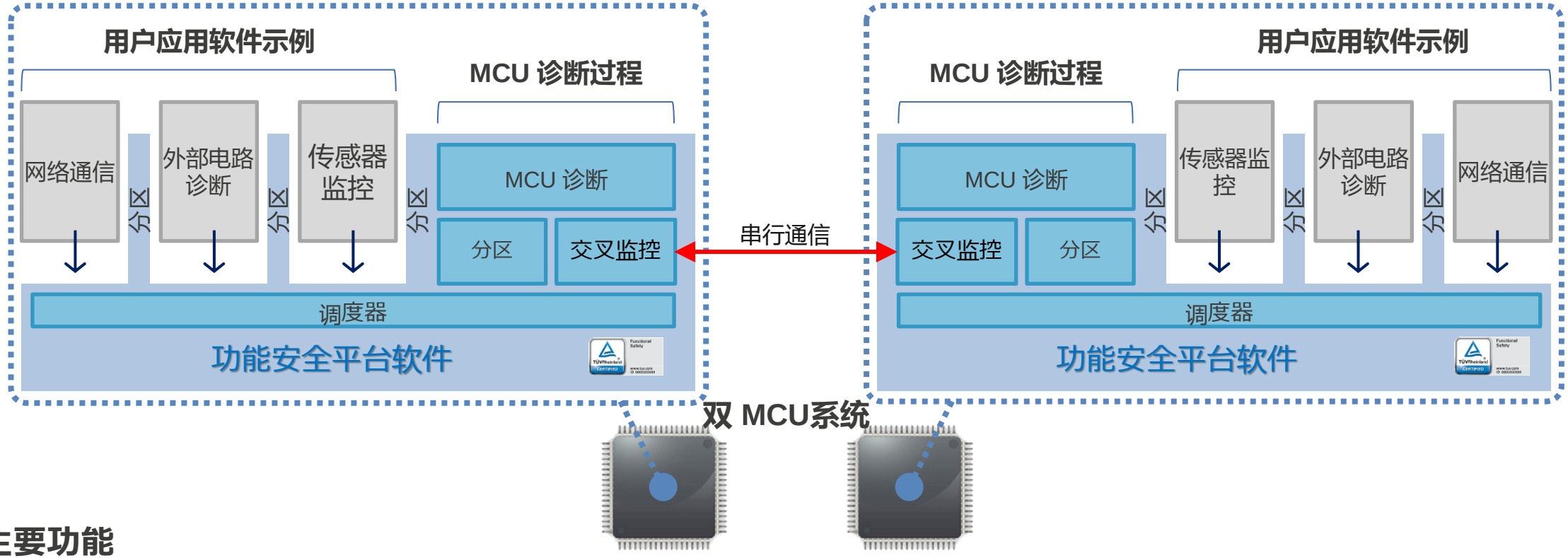
SIL3 系统软件包 ： 内容

No.	内容		商业版本	评价版本
1	**功能安全平台软件**	IEC61508 SIL3 认证目标	✓	✓*1
2	**安全手册**		✓	✓
3	**用户指南**		✓	✓
4	**IEC61508 认证文档(证书, 测试报告)**		✓	–
5	**软件开发手册** 介绍如何使用功能安全平台软件的指南 如何将其应用于用户系统		✓	✓
6	**配置工具** 检查“配置文件”设置的工具 决定功能安全平台软件的行为		✓	✓
7	**配置工具手册**		✓	✓
8	**用于信息输出的PC工具** 显示功能安全平台软件运行状态的工具		–	✓
9	**Self-Test 软件包** *2			
	- RX系列MCU诊断软件	IEC61508 SIL3 认证目标	✓	✓
	- 安全手册		✓	✓
	- 用户指南		✓	✓
	- IEC61508 认证文档(证书, 测试报告)		✓	–

*1: 仅在评估和开发阶段使用的未经认证的软件.
*2: 功能安全平台软件与RX诊断软件结合使用.

功能安全平台软件 ： 概述

使用双MCU轻松开发功能安全系统的软件



主要功能

1. MCU 诊断 (自诊断, 交叉监控)
2. 调度器 (用户应用软件的执行控制)
3. 分区　(用户应用程序之间、用户应用程序和功能安全平台软件之间)

功能安全平台软件 ：必要的资源

No.	软件	ROM	RAM	端子	外设
1	功能安全平台软件 (包含诊断软件)	96Kbyte	4Kbyte	5	SCI:1ch *1 MTU:3ch*1 CRC:1ch*2

*1: 用户不能使用功能安全平台软件使用的串行和定时器通道。
*2: 用户可以使用功能安全平台软件使用的CRC模块.

SIL3 系统软件包：订购号码

No.	RX 组	编译器	商业版本	评估版本
1	RX72M RX72T RX72N RX71M RX66T RX66N RX651/RX65N RX64M	CC-RX编译器 V3.01.00	RTK0EF0061F22002SJ	RTK0EF0061F32002SJ
2	RX24U RX24T RX230/RX231 RX23T RX23W RX23E-A	IAR-EWRX编译器 V4.14.2	RTK0EF0062F22002SJ	RTK0EF0062F32002SJ

注意：SIL3系统软件包 为每个RX MCU组提供不同的程序。
请指定RX MCU组并获取SIL3系统软件包.

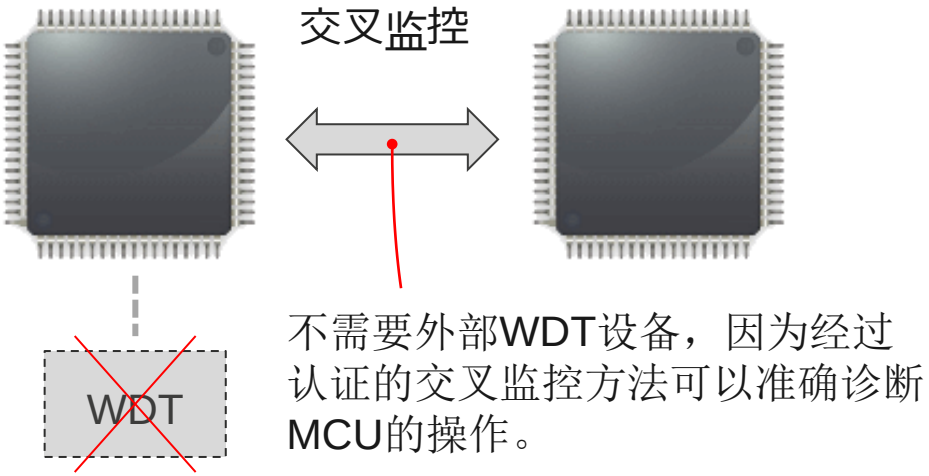
功能安全平台软件 :功能1 (MCU 诊断)

■ 根据IEC61508标准进行诊断

经证明，功能安全平台软件执行的自我诊断和交叉监测的诊断覆盖率可以达到90%。

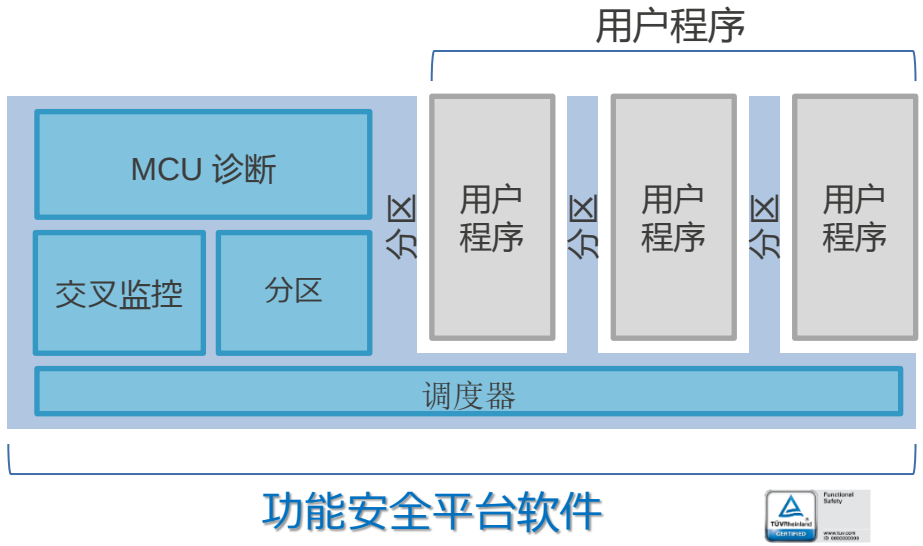
■ 交叉监控

不需要外部WDT设备



功能安全平台软件 :功能 1（MCU 诊断）

■诊断目标区域



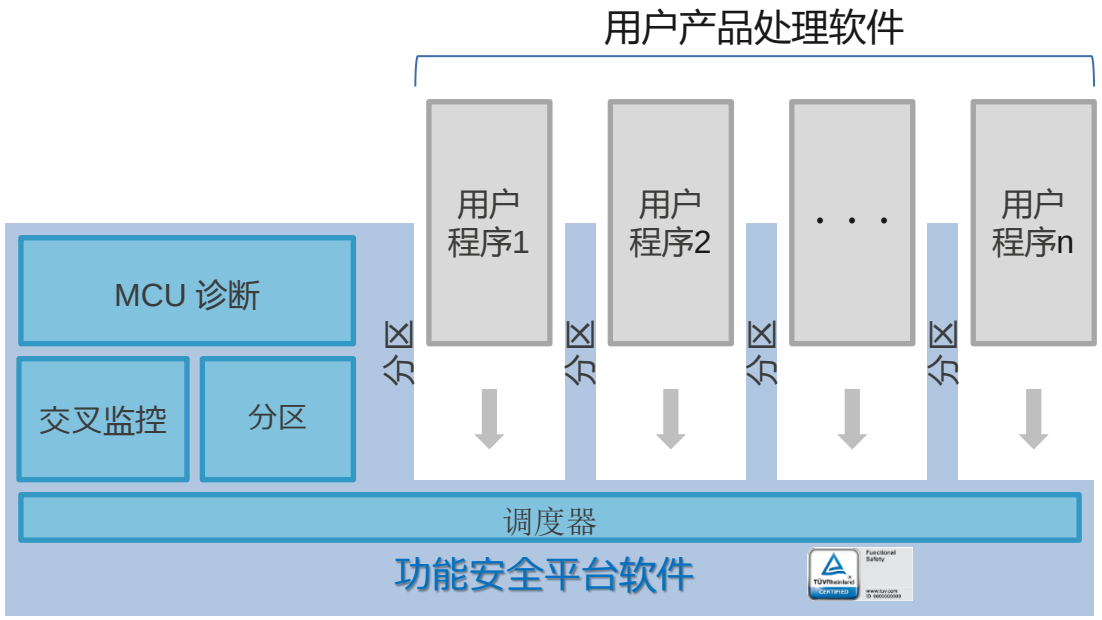
✓: 功能安全平台软件执行诊断

区域		永久失效	瞬态失效
ROM	功能安全平台软件区域	✓	无需诊断
	用户程序区域	✓	无需诊断
RAM	功能安全平台软件区域	✓	✓
	用户程序区域	✓	*1
外设	功能安全平台软件区域	✓	✓
	用户程序区域	*2	

用户只需要执行以下MCU诊断：
*1：用户应用程序完成RAM的瞬态失效检测
*2：用户应用程序完成的外设的永久和瞬态失效

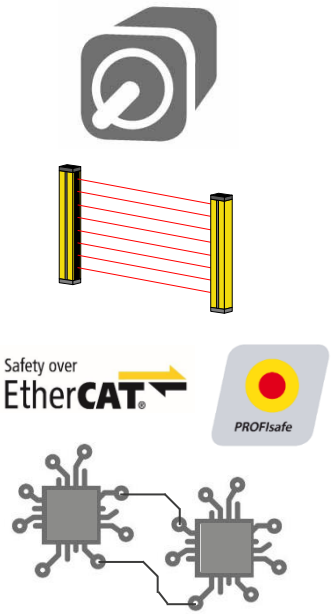
功能安全平台软件 :功能 2 (调度器)

■ 用户应用软件的执行控制



用户应用程序示例：

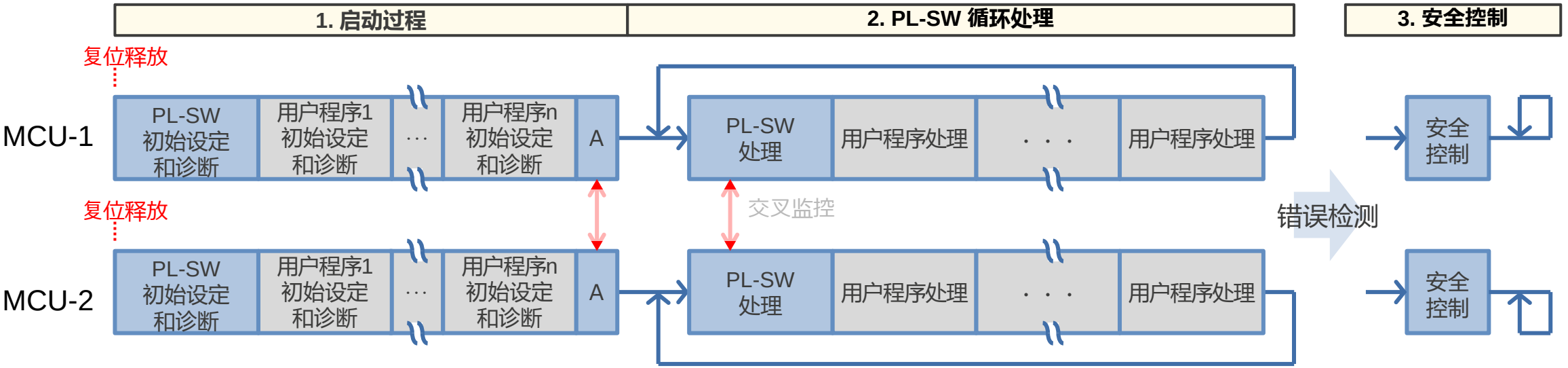
- 电机转速监测
- 传感器输入监测
- 安全网络协议控制
- 外部电路诊断



用户应用程序功能
- 最多可以注册16种类型的用户应用程序
- 可以混合使用安全和非安全应用
- 用户应用程序的执行顺序在专用配置文件中指定.

功能安全平台软件 :功能 2 (调度器)

■ 安全控制



:功能安全平台软件（PL-SW）处理
A : MCU 同步操作
n :用户应用程序的数量(max.16)

[操作总结]

1. 执行启动处理（初始设定/功能安全平台软件和用户应用程序1~n的诊断/MCU之间的同步）
2. 重复PL-SW循环处理（功能安全平台软件和用户应用程序的过程）。
   可以在用户应用程序处理过程中接受来自其他用户应用程序的中断请求。
3. 如果检测到任何错误或故障，则执行安全控制处理并保持状态.

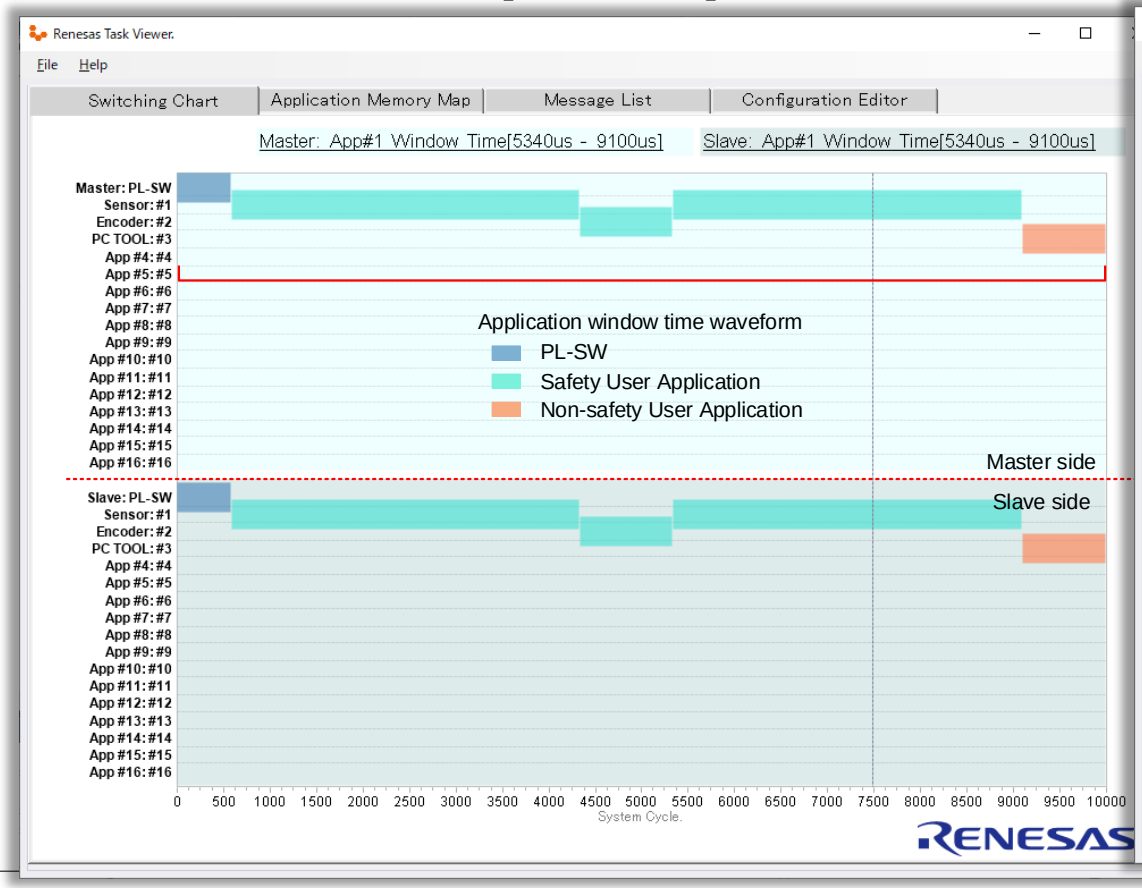
.

功能安全平台软件 :功能 2 (调度器)

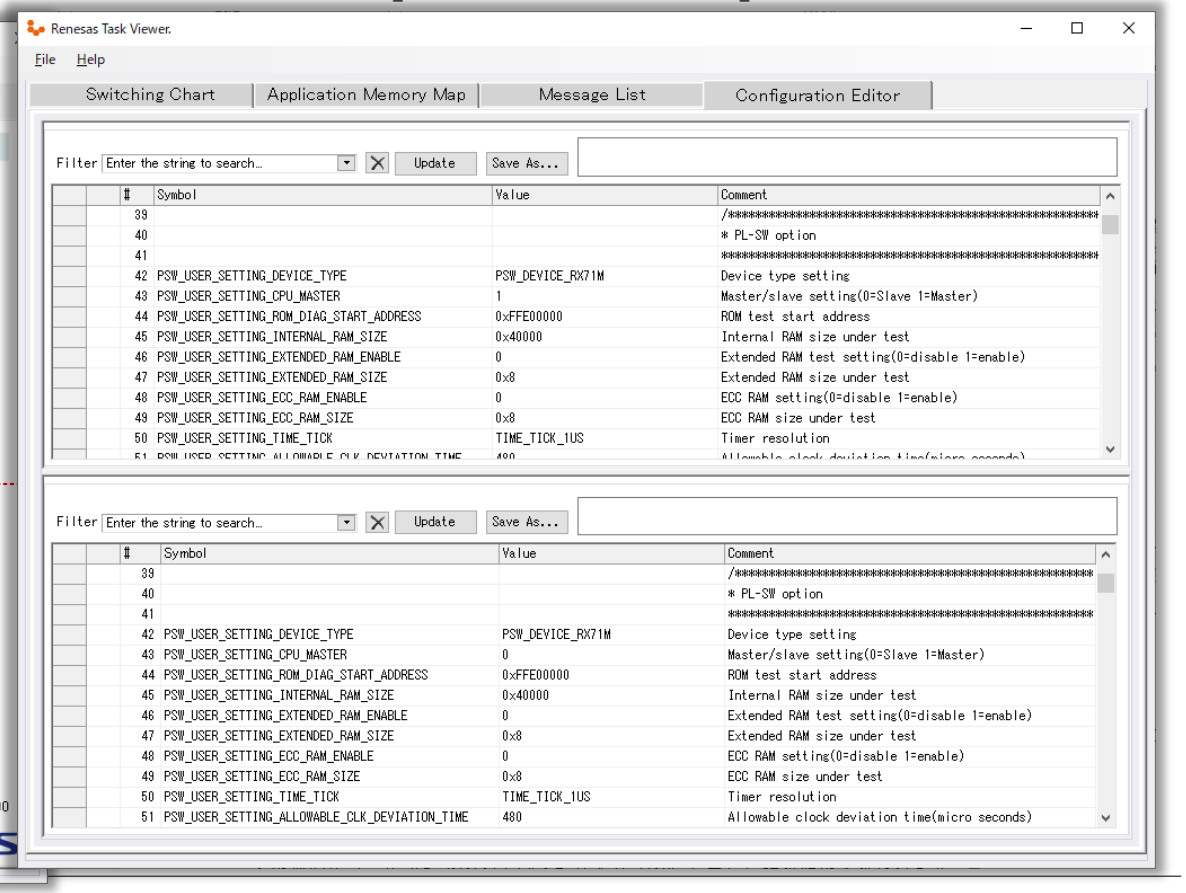
■ 配置工具

SIL3系统软件包与“配置工具”捆绑在一起，该工具可在PC监控软件上显示配置文件中设置的内容。

[波形显示]



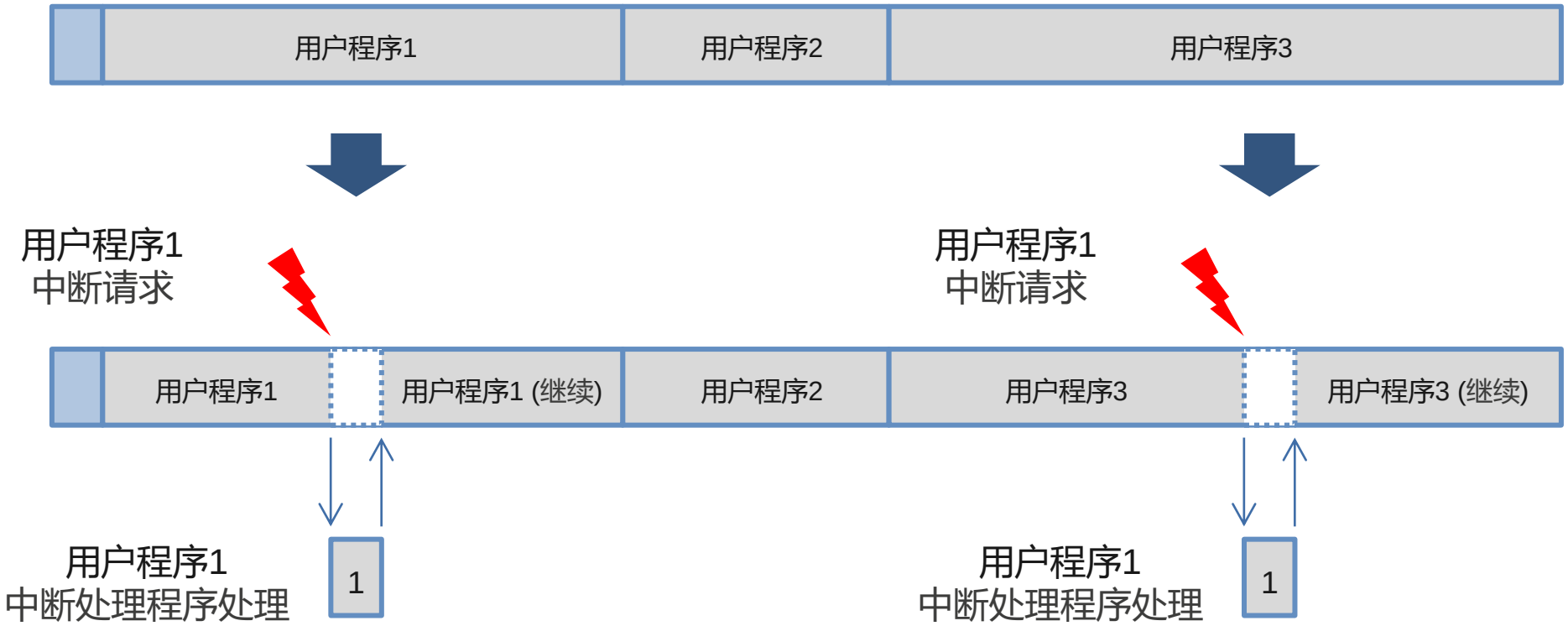
[配置文件编辑器]



功能安全平台软件 :功能 2 (调度器)

■ 用户应用程序执行期间的中断

可以在用户应用程序执行期间进行中断处理。



: Functional Safety Platform Software processing

功能安全平台软件 :功能 3 (分区)

■ 功能安全系统开发中的问题

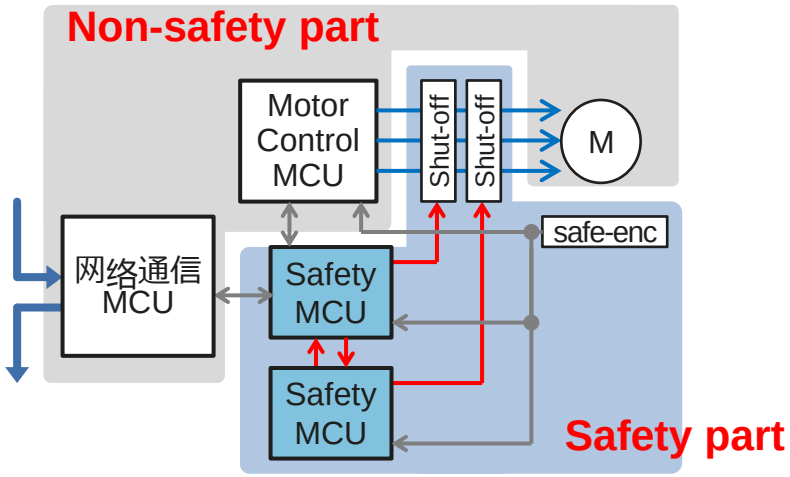
开发功能安全认证产品有些重大问题.

问题 1. 更改安全部件的软件时需要重新认证

例如,
- 如果检测到软件Bug，则不能立即重新发布，因为MCU中的整个软件都需要进行影响分析和重新认证.
- 在衍生产品开发的情况下，只有一些功能不同，所有软件都要经过重新认证，因此开发需要很长时间.

问题 2. 由于需要将安全部件和非安全部件分开，部件成本增加。

功能安全平台软件的分区功能解决了这些挑战。

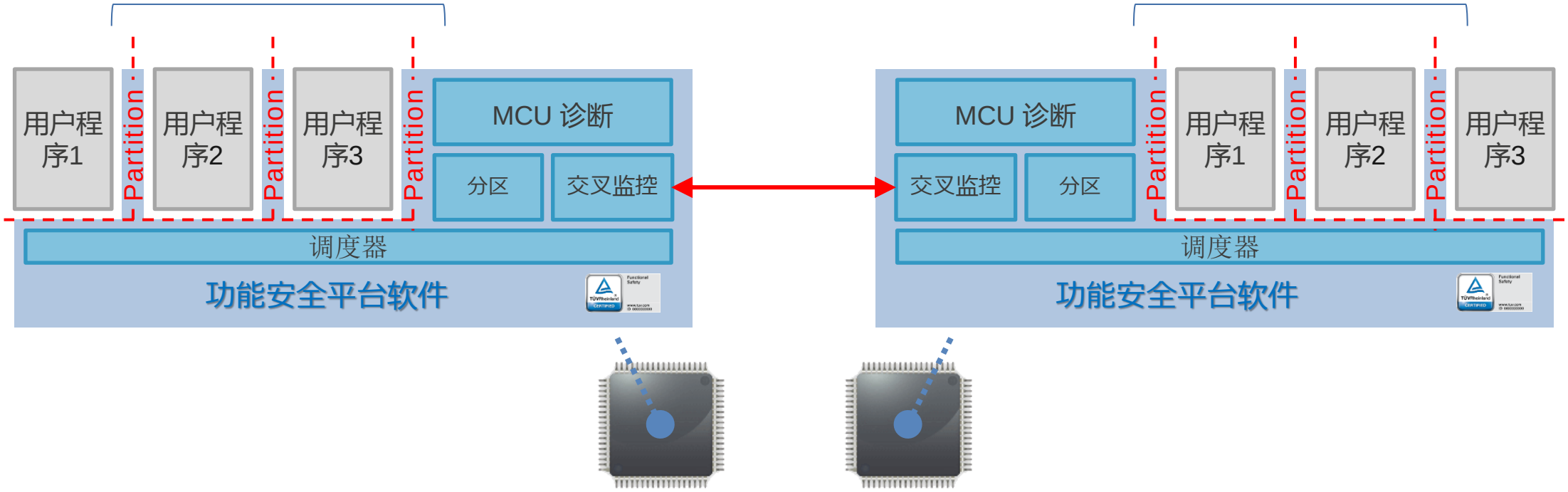


功能安全平台软件 :功能 3 (分区)

■ 关于分区

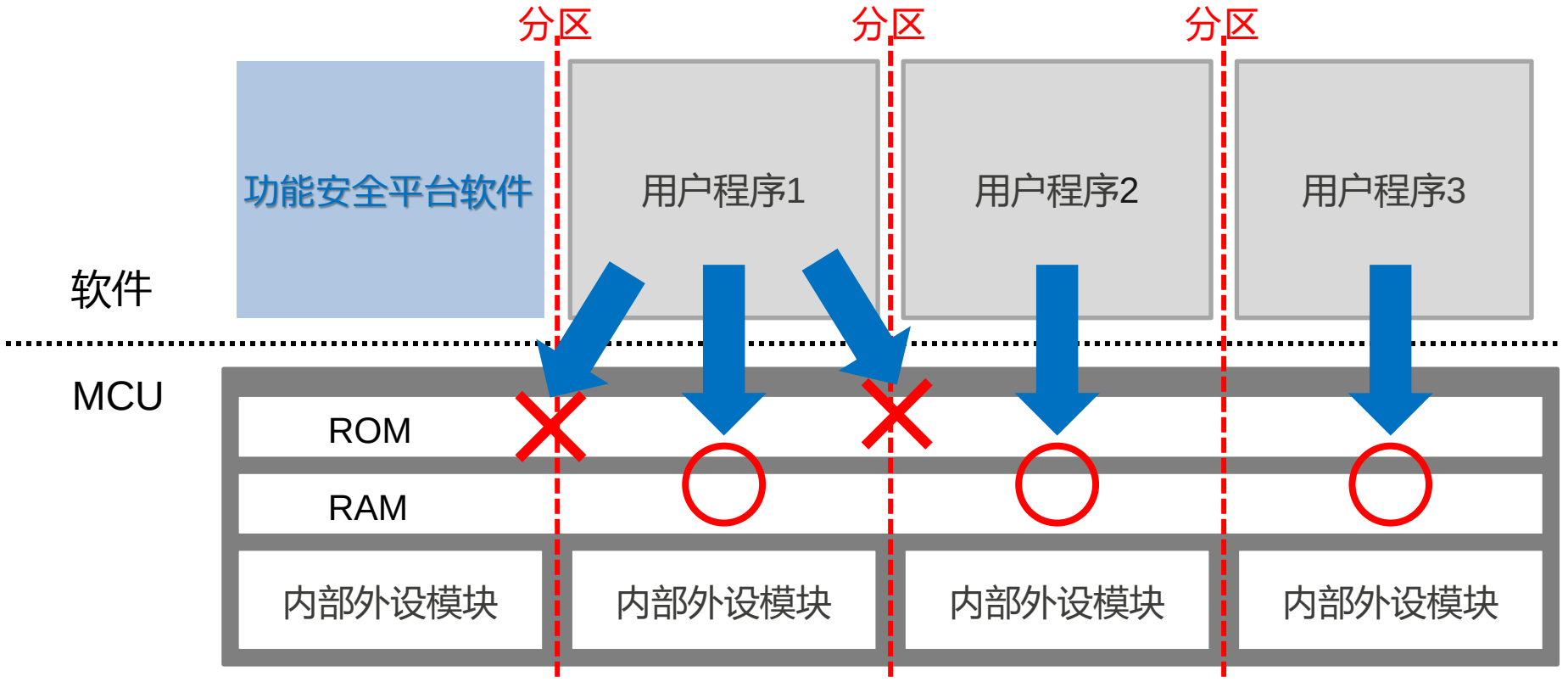
即使一个应用程序发生错误，也不会影响其他应用程序的操作

- 用户应用程序之间的分区
- 功能安全平台软件和用户应用程序之间的划分



功能安全平台软件 :功能 3 (分区)

■ 分区数据保护

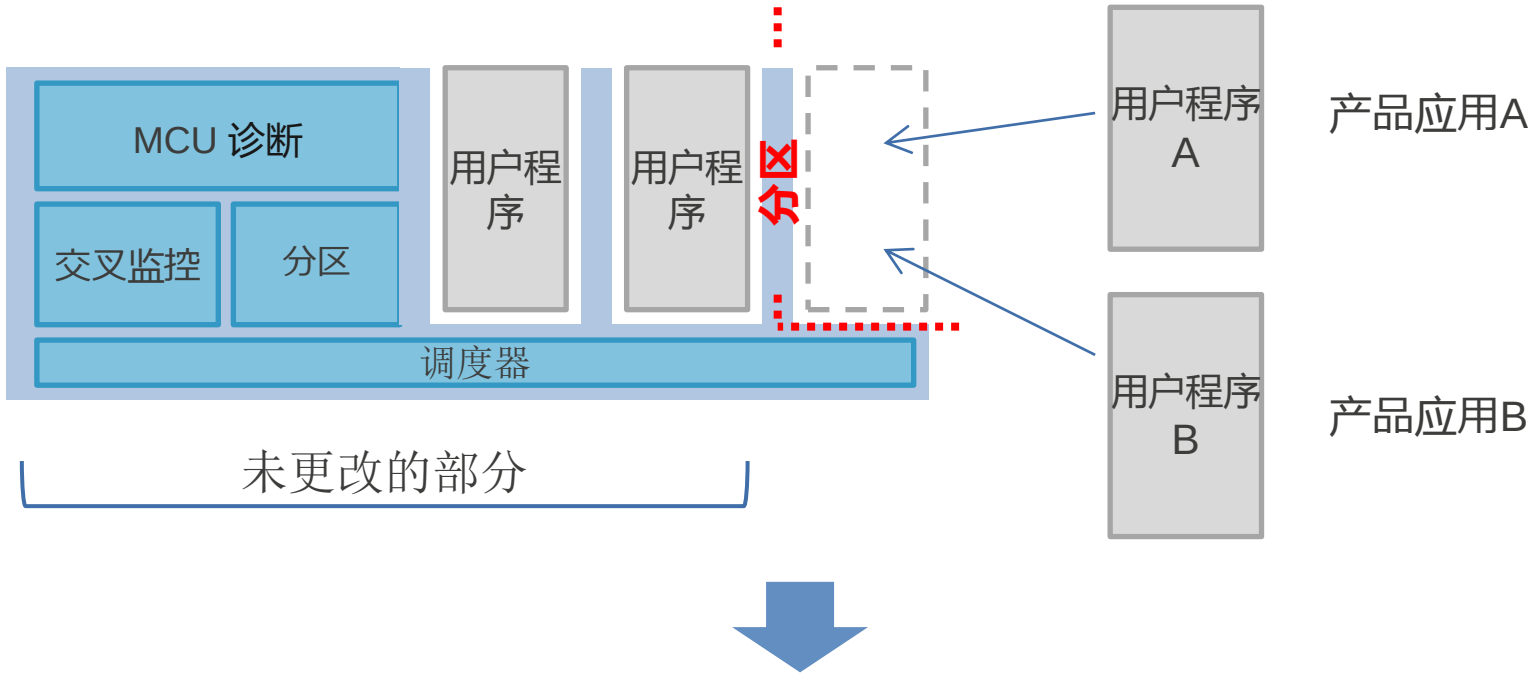


-每个用户应用程序只能访问预先注册的区域。
-功能安全平台软件在检测到违规访问时执行安全控制。
-即使一个应用程序发生错误，也不会影响其他应用程序的操作.

功能安全平台软件 :功能 3 (分区)

■分区的好处: 1

即使某些安全软件发生了更改，功能安全平台软件的“分区功能”也可保证未更改软件的操作没有问题。



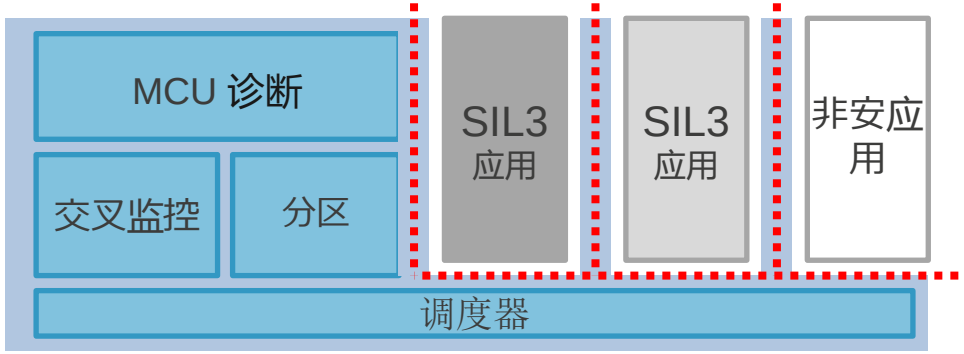
减少了重新认证所需的工作量。

功能安全平台软件 :功能 3 (分区)

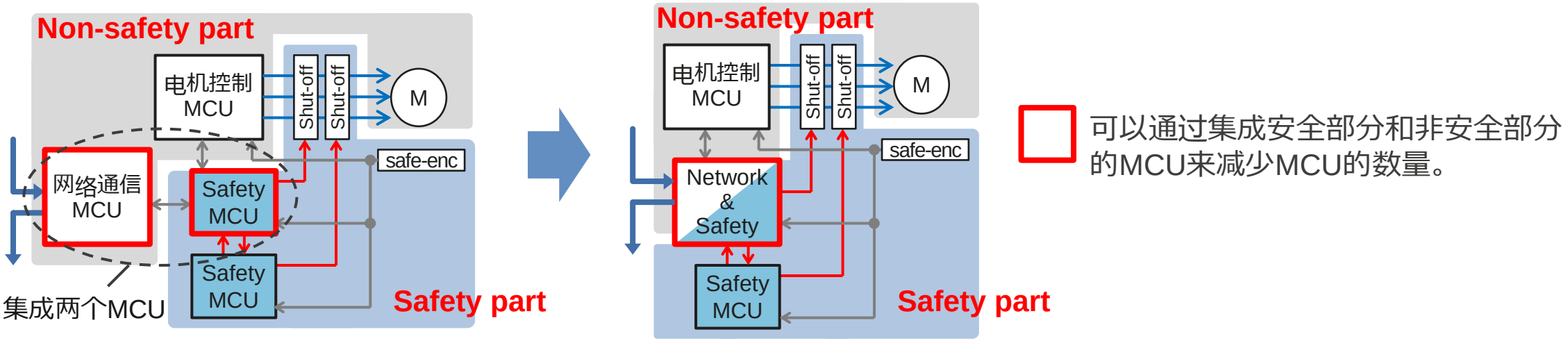
■ 分区的好处: 2

功能安全平台软件的“分区功能”使具有不同安全级别的软件能够混合在一个MCU中。

- 安全和非安全软件可以混合在一个MCU中.
- 对非安全软件的更改不需要重新认证。



[Ex. SIL3, SS1, SLS, 安全网络兼容电机控制单元]



功能安全平台软件 ：评估软件

■ 商业版本和评估版本的比较.

- 提供评估版本用于检查功能安全平台软件的规格和性能。
- 评估版本也可以在产品开发阶段使用。

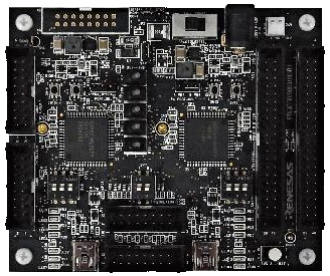
Item	商业版	评估版
IEC61508 认证	认证 	非认证
	- 可用于产品	- 仅在评估和开发阶段可用
评估功能	Debug 模式 : 不支持	Debug 模式 : 支持
	- 开发工具的软件中断、跟踪和步骤执行功能不可用 - 功能安全平台软件专用的PC监控工具*不可用	- 提供开发工具的软件中断、跟踪和步骤执行功能 - 功能安全平台软件专用的PC监控工具*可用

* : 用于输出信息的PC监控工具

功能安全平台软件 ：评估软件.

■ 用于信息输出的PC监控工具

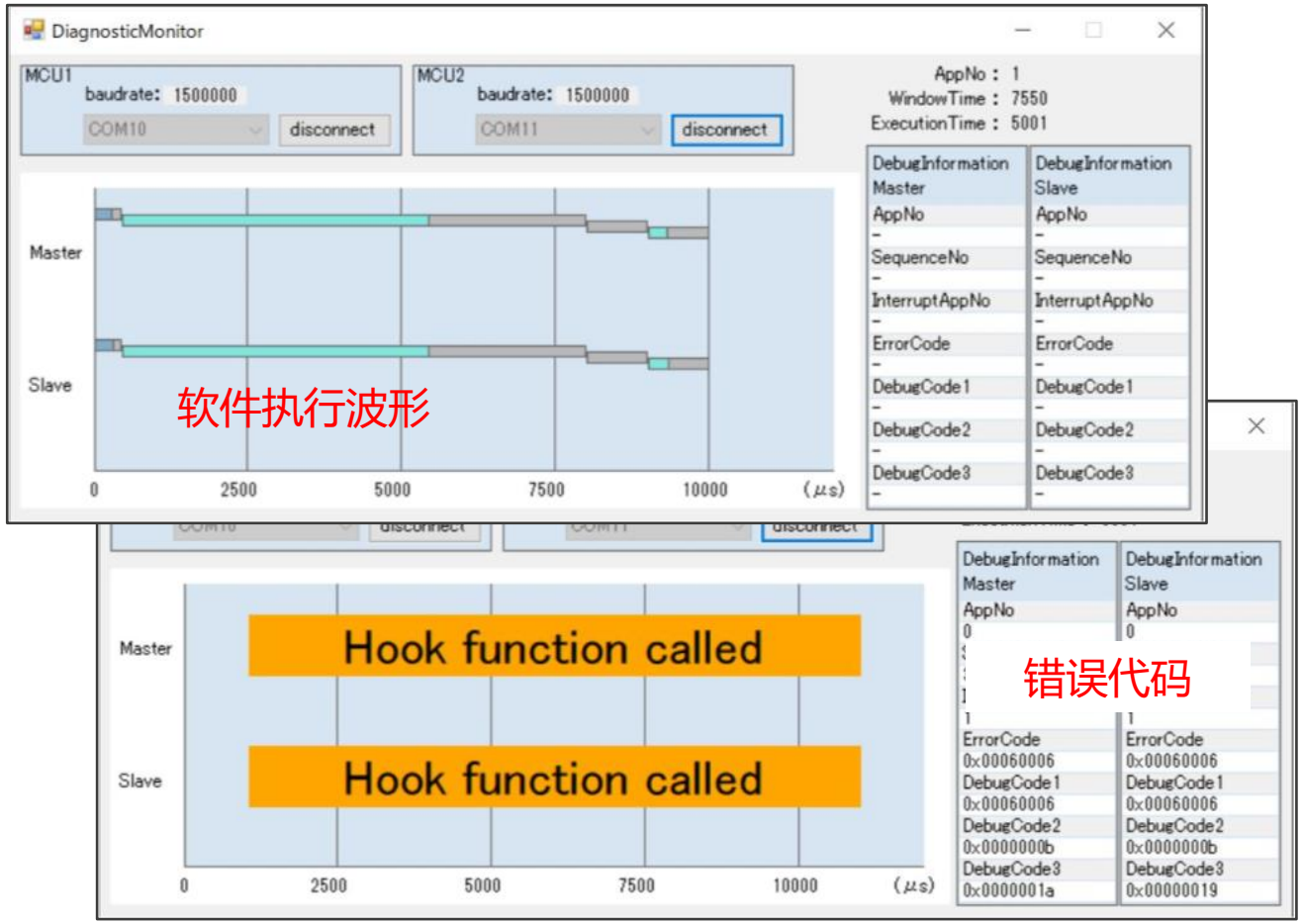
这个工具显示两个MCU在PL-SW循环阶段的操作以及故障发生时的原因。



冗余MCU结构Demo板

正常工作

检测到错误

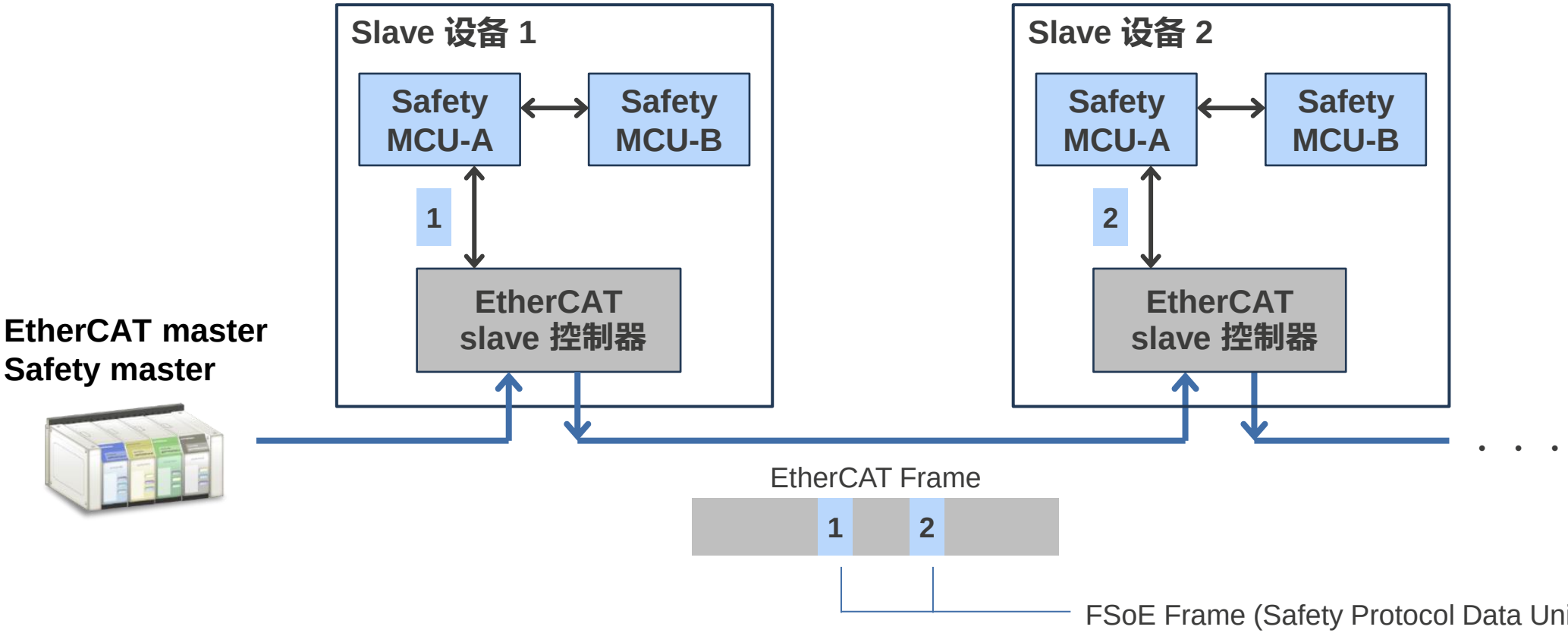


Renesas Functional Safety

1. Renesas RX系列MCU功能安全解决方案
    - 1-1. Self-Test 软件包
    - 1-2. SIL3 系统软件包
    - 1-3. FSoE 应用软件包
        - 1-3-1. 概述
        - 1-3-2. 功能
        - 1-3-3. 评价版本
    - 1-4. 参考文档
    - 1-6. 参考硬件
2. Renesas RA系列MCU功能安全解决方案
    - 2-1. Self-Test 软件包

什么是FSoE

FSoE（Safety over EtherCAT）定义了一个安全的通信层，用于在EtherCAT设备之间传输安全的过程数据。
FSoE是一项由EtherCAT技术集团（ETG）支持的开放技术。
FSoE安全协议处理需要冗余硬件配置。



FSoE 应用软件包：内容

No.	内容		商业版本	评估版本
1	FSoE 应用软件	TÜV Rheinland IEC61508 SIL3 认证目标	✓	✓
2	安全手册		✓	✓
3	用户指南		✓	✓
4	IEC61508 认证文档 (证书, 测试报告)		✓	- *2
5	(样例应用) *1 网络通信IC接口 数据 I/O 接口		✓	✓
6	软件开发手册		✓	✓

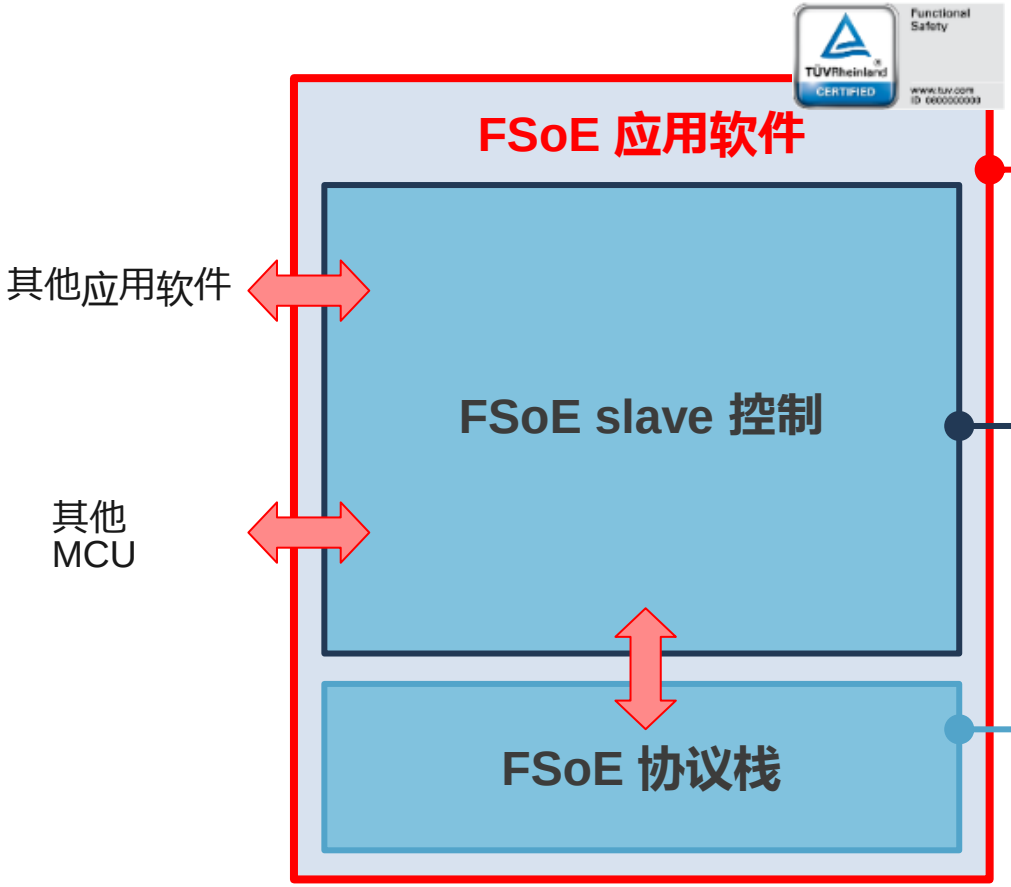
*1：捆绑了两个示例应用程序，以检查FSoE应用程序软件的操作.

- **网络通信IC接口** ：演示网络通信IC与RX MCU之间的数据交换
- **数据 I/O 接口** ：演示安全数据输入/输出

*2：不包括功能安全认证文件

FSoE应用软件包: 概述

认证不仅包括协议栈部分，还包括FSoE Slave控制部分



- **ETG.5100 S (R) V1.2.0** FSoE Slave兼容软件
- **需要 IEC61508 SC3/SIL3 认证** 包含FSoE slave控制部分

功能：
1. FSoE slave 状态管理和数据流控制
2. 与其他用户应用程序的数据传输/接收控制
3. 两个MCU之间的FSoE数据交换
4. FSoE应用软件本身的运行诊断

功能：
1. 输入安全PDU*的诊断和安全数据的提取
2. 输入安全数据的CRC计算和返回安全PDU的生成

* : PDU : Protocol Data Unit

FSoE 应用软件包：必要的资源

No.	软件	ROM	RAM	端子	外设
1	FSoE 应用软件	22K byte	Min 1K byte*1	2 (TxD,RxD)	SCI:1ch *2 DTC:1ch*3 CRC:1ch*4

*1: RAM大小根据要通信的安全数据的大小而增加.
*2: SCI = 串行通信接口
用户不能使用FSoE应用软件使用的SCI通道.
*3: DTC = 数据传输控制器
用户不能使用FSoE应用软件使用的DTC通道.
*4: CRC = 循环冗余检查
用户可以使用FSoE应用软件使用的CRC模块。

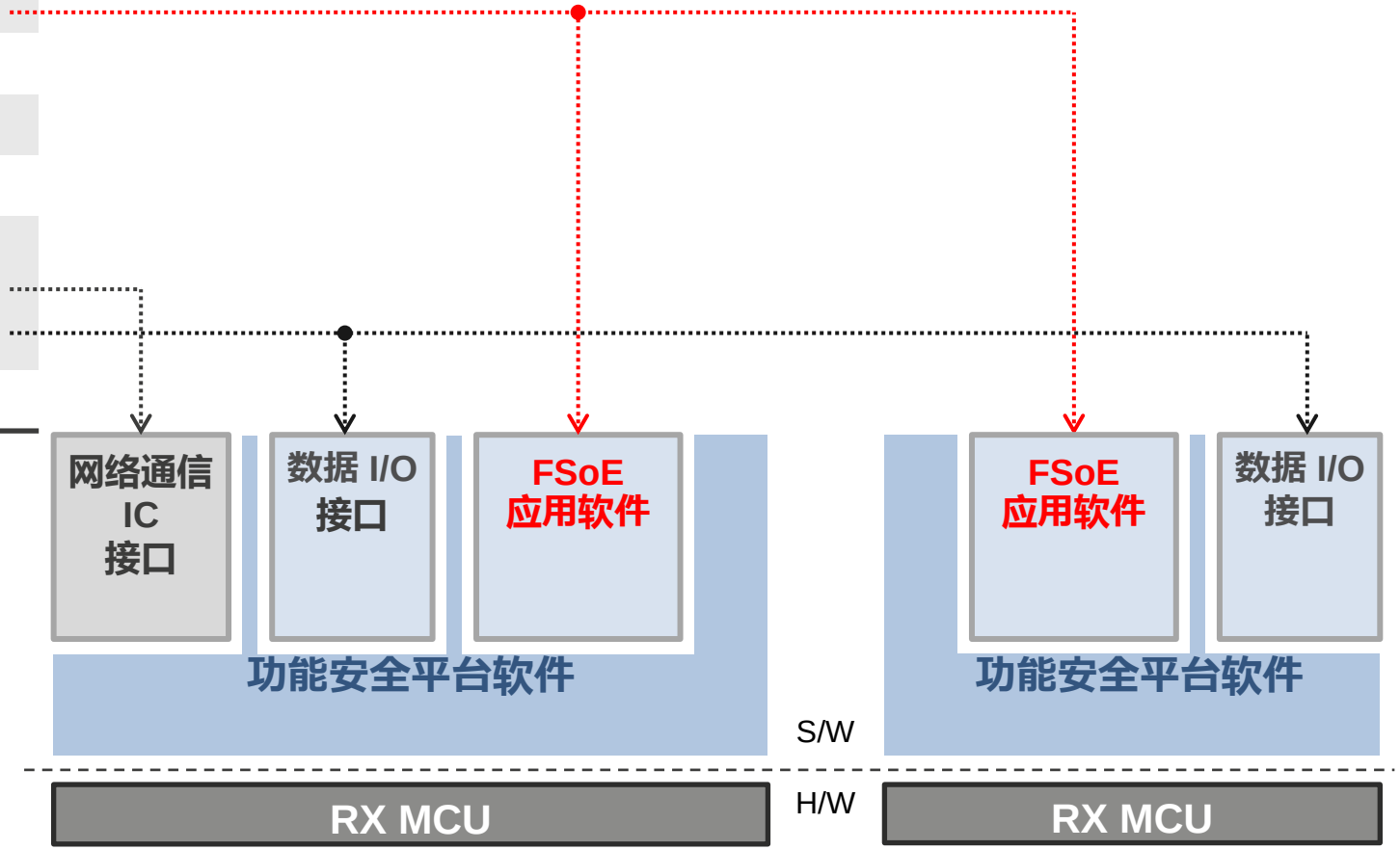
FSoE 应用软件包：订购号码

No.	RX 组	编译器	商业版本	评估版本
1	RX72M RX72T RX72N RX71M RX66T RX66N RX651/RX65N RX64M	CC-RX 编译器 V3.01.00	RTK0EF0080F21001SJ	RTK0EF0080F31001SJ
2	RX24U RX24T RX230/RX231 RX23T RX23W RX23E-A	IAR-EWRX 编译器 V4.14.2	RTK0EF0081F21001SJ	RTK0EF0081F31001SJ

FSoE应用软件包: 软件配置

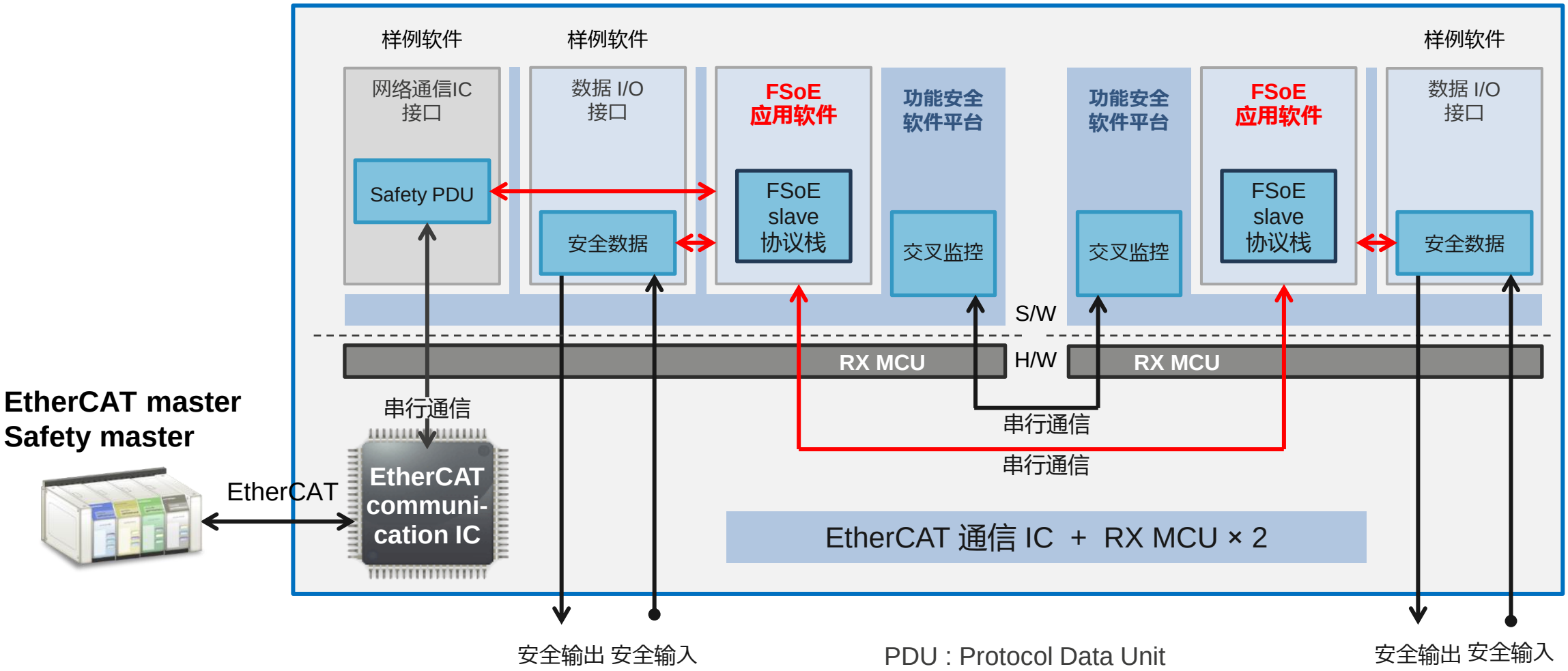
FSoE应用软件与功能安全平台软件结合使用

No.	内容
1	FSoE 应用软件
2	安全手册
3	用户指南
4	IEC61508 认证文档
5	(样例软件) 网络通信IC接口 数据 I/O接口
6	软件开发手册



FSoE应用软件包: System Configuration

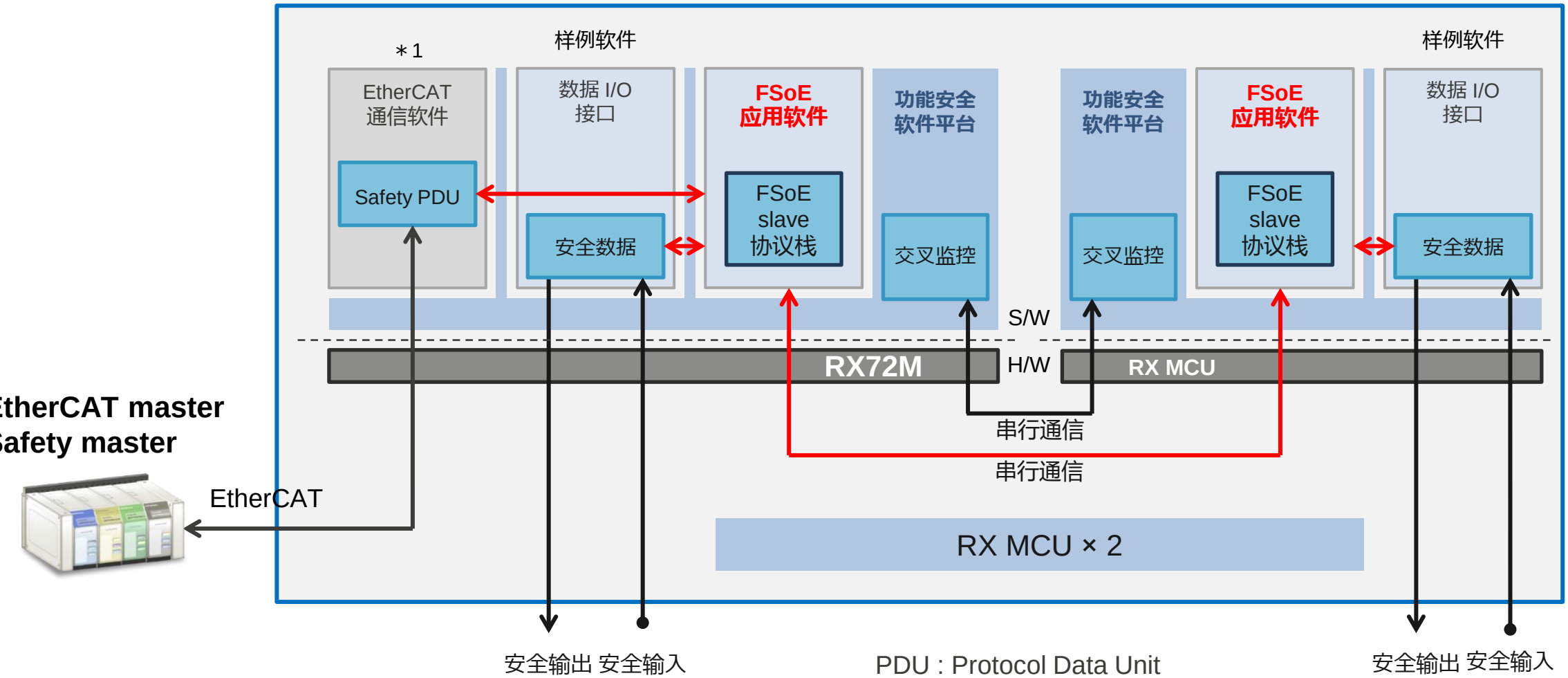
示例1 : Safety 远程 I/O 配置



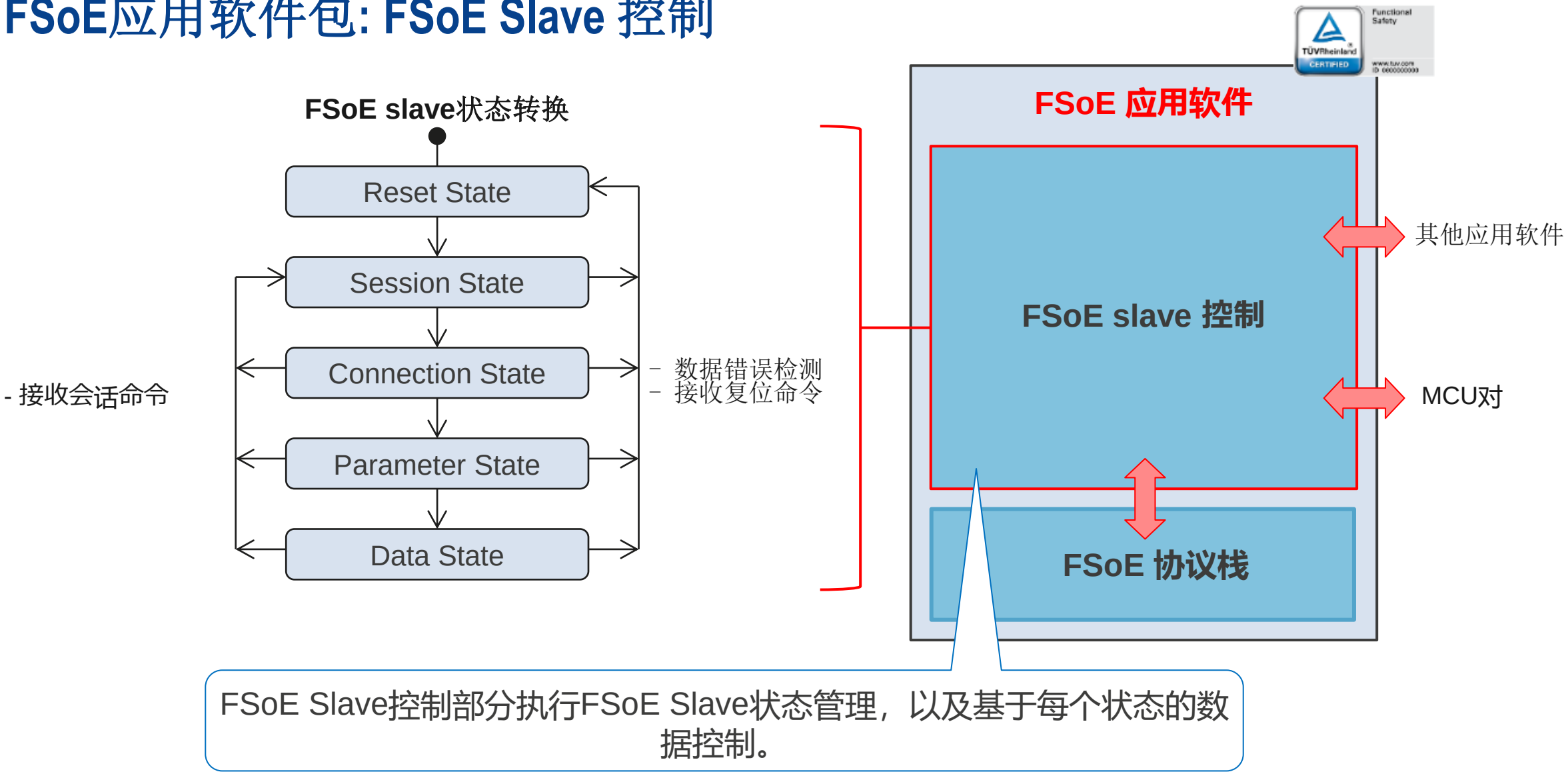
FSoE应用软件包: System Configuration

示例2 : Safety 远程 I/O 配置 (使用RX72M)

＊1: 此软件未在FSoE应用程序中绑定



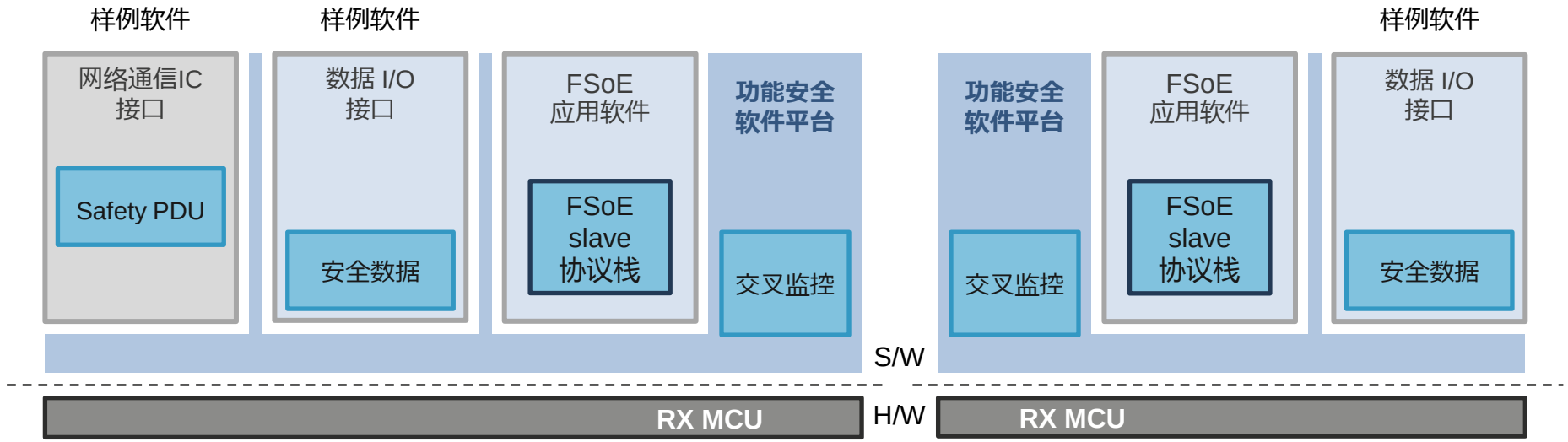
FSoE应用软件包: FSoE Slave 控制



FSoE Slave控制部分执行FSoE Slave状态管理，以及基于每个状态的数据控制。

FSoE应用软件包: 数据流

[数据状态]安全数据输出操作的数据流：0



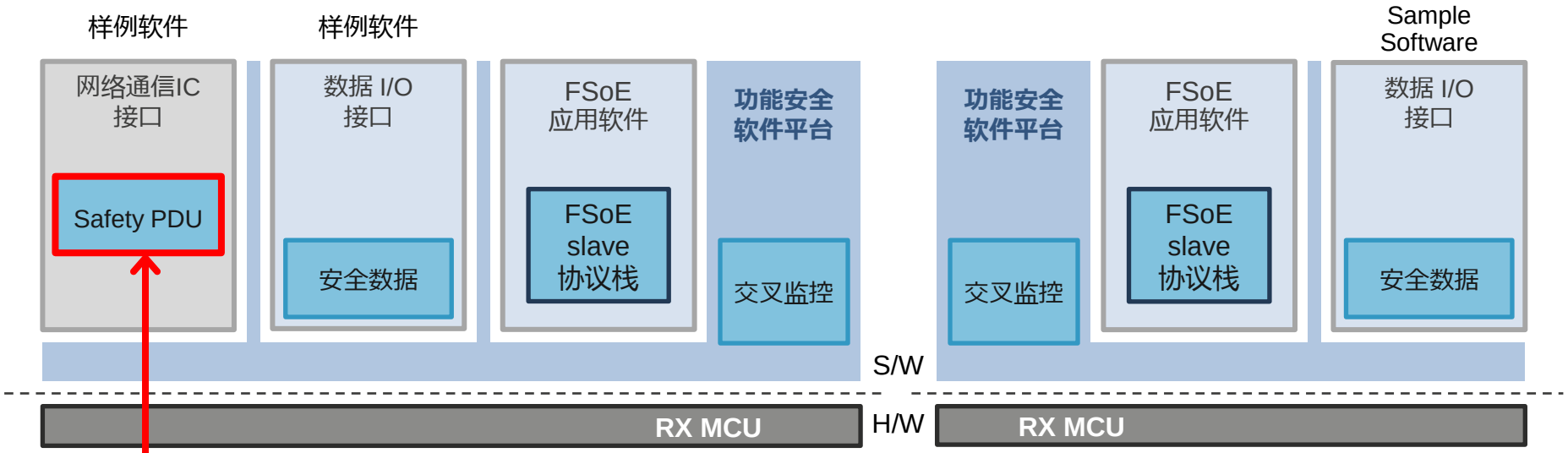
EtherCAT master
Safety master

1. 从外部IC接收Safety PDU
2. 发送Safety PDU 到MCU对
3. 分析两个MCU上的Safety PDU
4. 将安全数据发送到数据I/O接口
5. 将安全数据输出到外部端口

PDU : Protocol Data Unit

FSoE应用软件包:数据流

[数据状态] 安全数据输出操作的数据流：1



Safety Protocol Data Unit

EtherCAT master
Safety master

EtherCAT

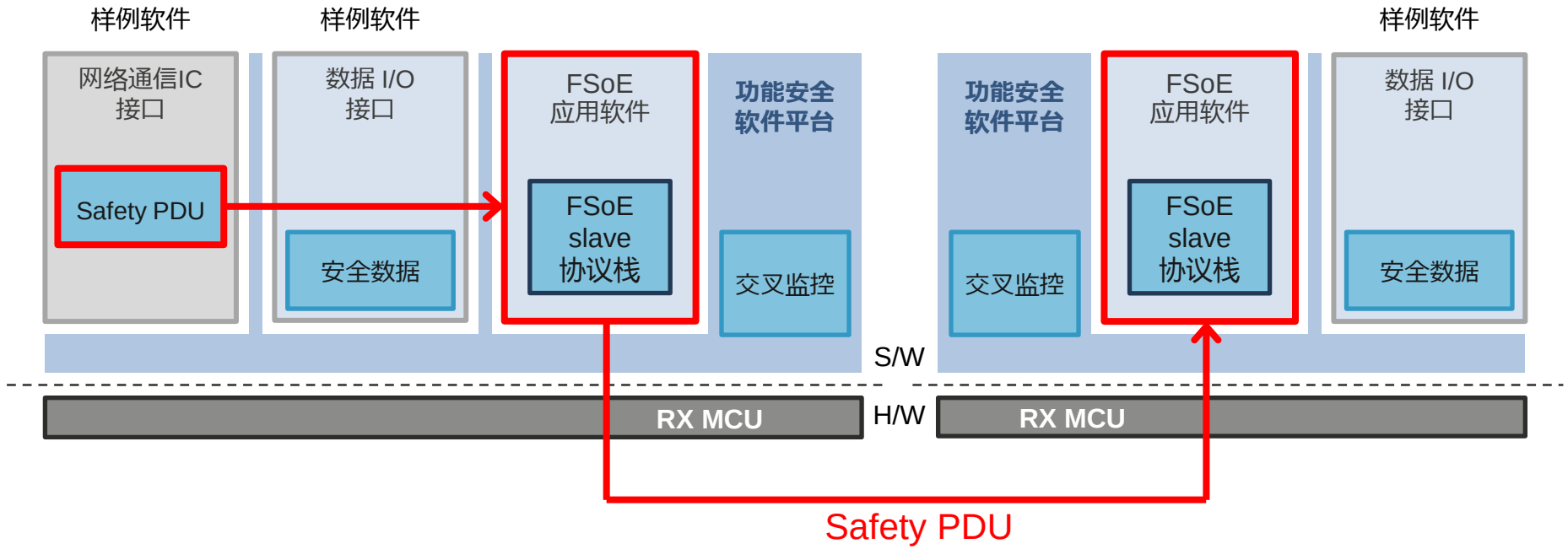
EtherCAT commu-nication IC

1. 从外部IC接收Safety PDU
2. 发送Safety PDU 到两个MCU
3. 分析两个MCU上的Safety PDU
4. 将安全数据发送到数据I/O接口
5. 将安全数据输出到外部端口

PDU : Protocol Data Unit

FSoE应用软件包:数据流

[数据状态] 安全数据输出操作的数据流：2

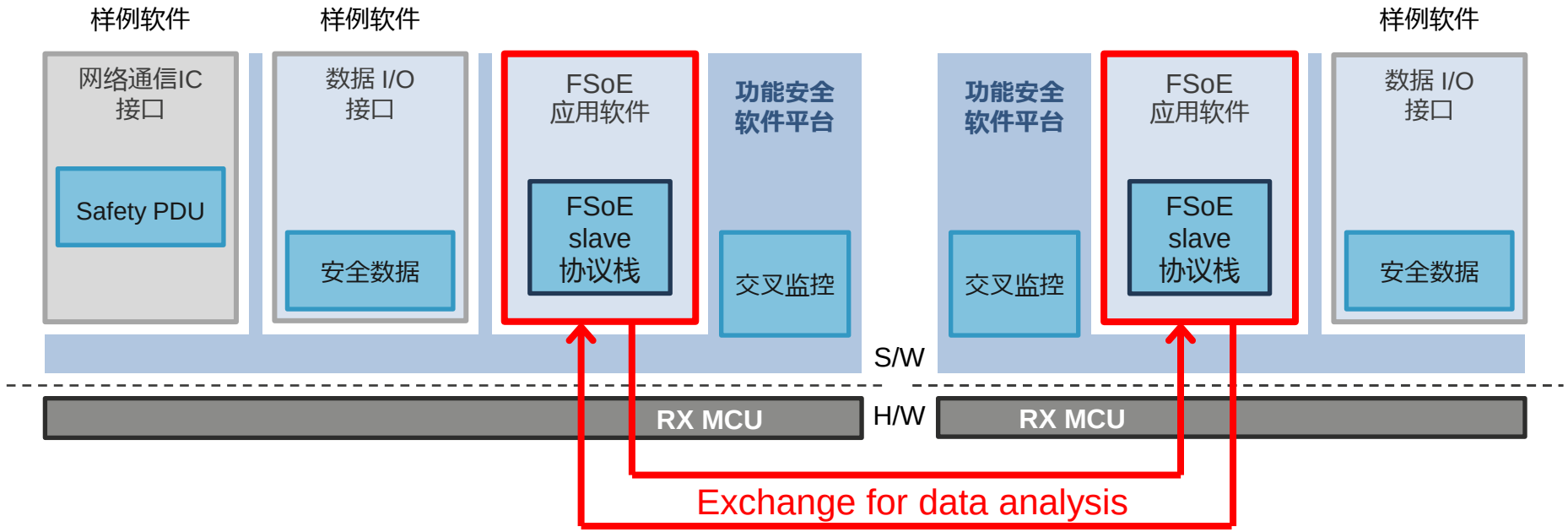


1. 从外部IC接收Safety PDU
2. 发送Safety PDU 到两个MCU
3. 分析两个MCU上的Safety PDU
4. 将安全数据发送到数据I/O接口
5. 将安全数据输出到外部端口

PDU : Protocol Data Unit

FSoE应用软件包:数据流

[数据状态] 安全数据输出操作的数据流：3

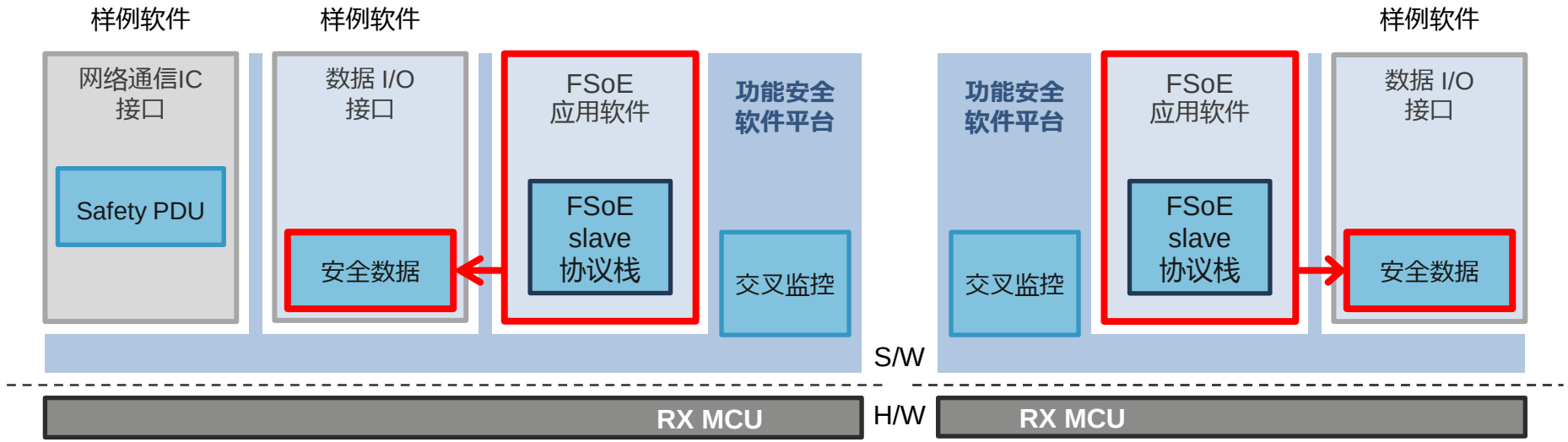


1. 从外部IC接收Safety PDU
2. 发送Safety PDU 到两个MCU
3. 分析两个MCU上的Safety PDU
4. 将安全数据发送到数据I/O接口
5. 将安全数据输出到外部端口

PDU : Protocol Data Unit

FSoE应用软件包:数据流

[数据状态] 安全数据输出操作的数据流：4

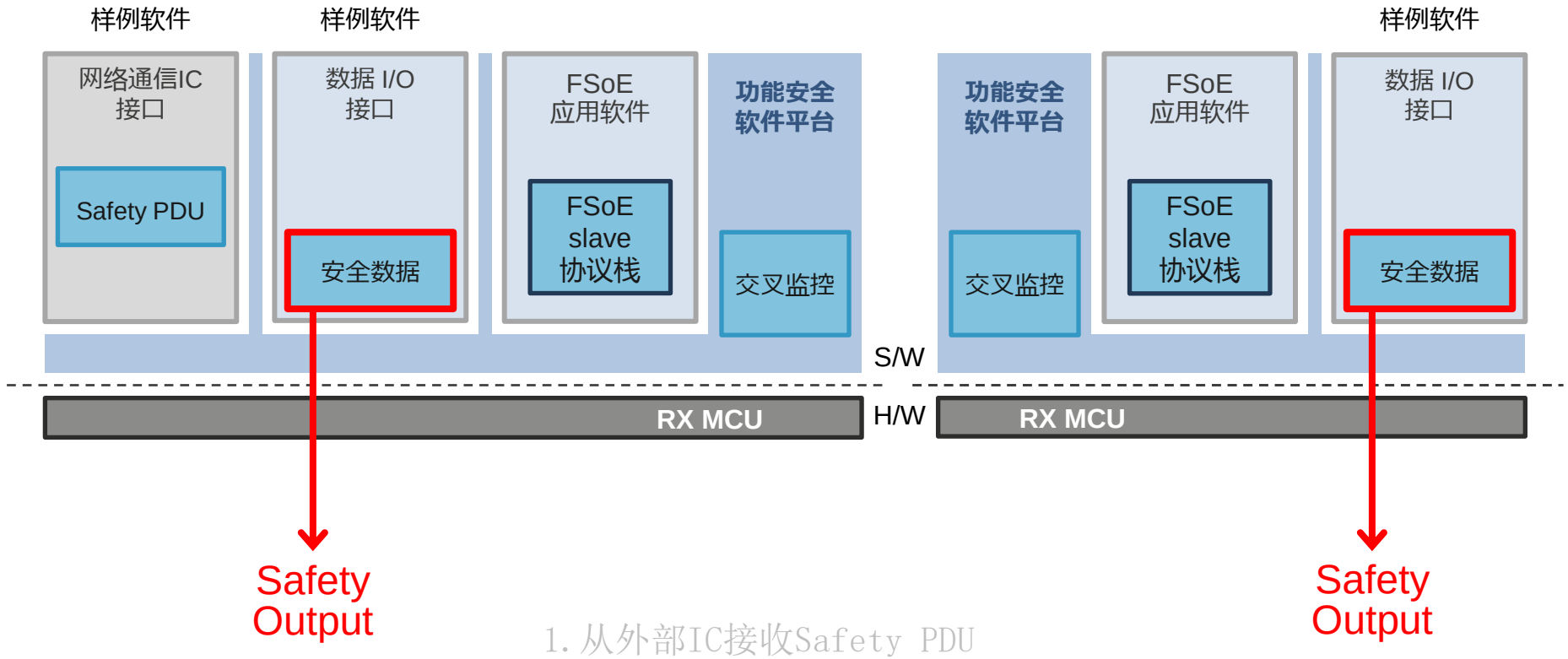


1. 从外部IC接收Safety PDU
2. 发送Safety PDU 到两个MCU
3. 分析两个MCU上的Safety PDU
4. 将安全数据发送到数据I/O接口
5. 将安全数据输出到外部端口

PDU : Protocol Data Unit

FSoE应用软件包:数据流

[数据状态] 安全数据输出操作的数据流：5

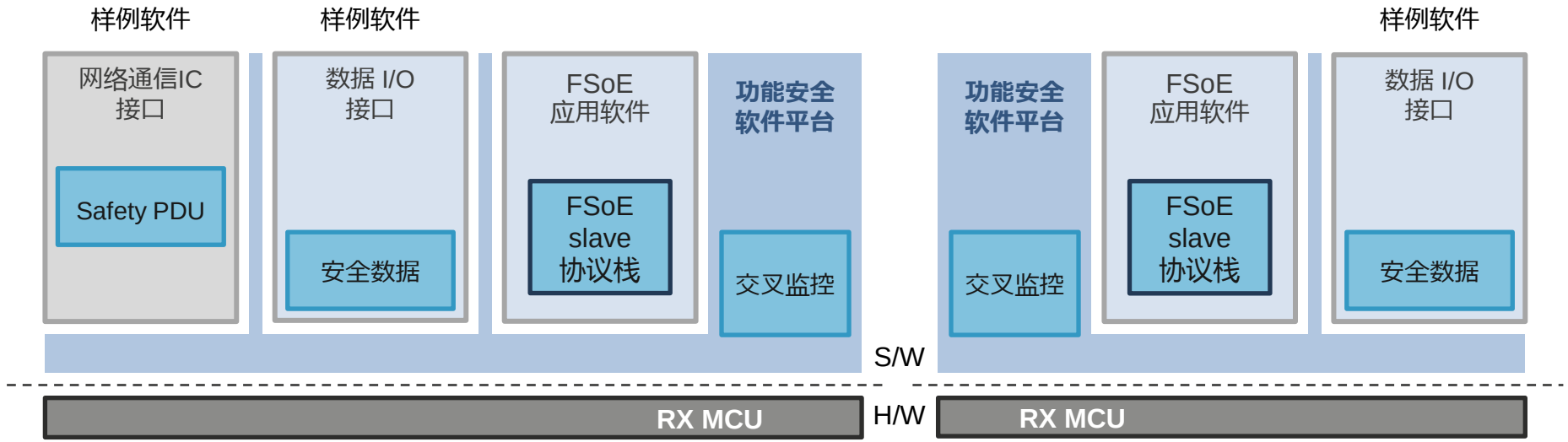


1. 从外部IC接收Safety PDU
2. 发送Safety PDU 到两个MCU
3. 分析两个MCU上的Safety PDU
4. 将安全数据发送到数据I/O接口
5. 将安全数据输出到外部端口

PDU : Protocol Data Unit

FSoE应用软件包:数据流

[数据状态] 安全数据输入操作数据流：0

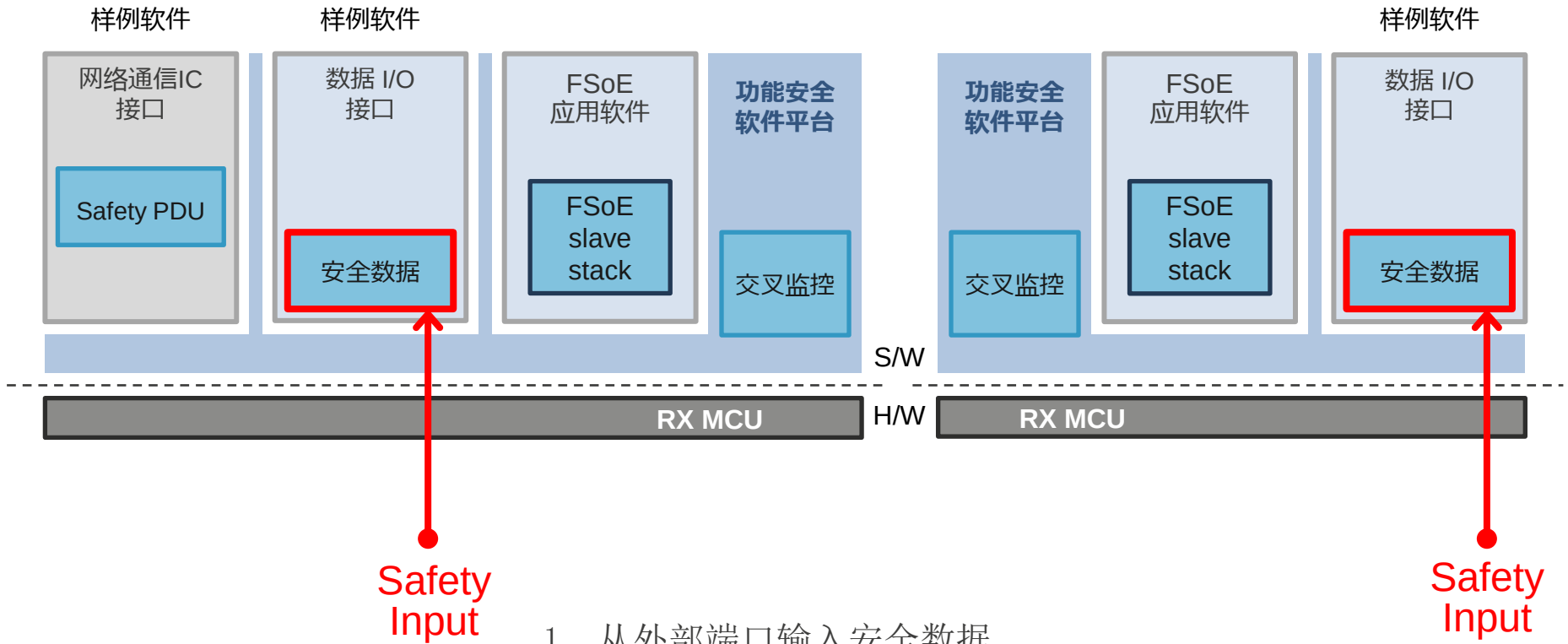


1. 从外部端口输入安全数据
2. 向FSoE应用软件发送安全数据
3. 数据交换和处理，CRC计算
4. 生成Safety PDU格式
5. 将Safety PDU发送到外部IC.

PDU : Protocol Data Unit

FSoE应用软件包:数据流

[数据状态] 安全数据输入操作数据流：1

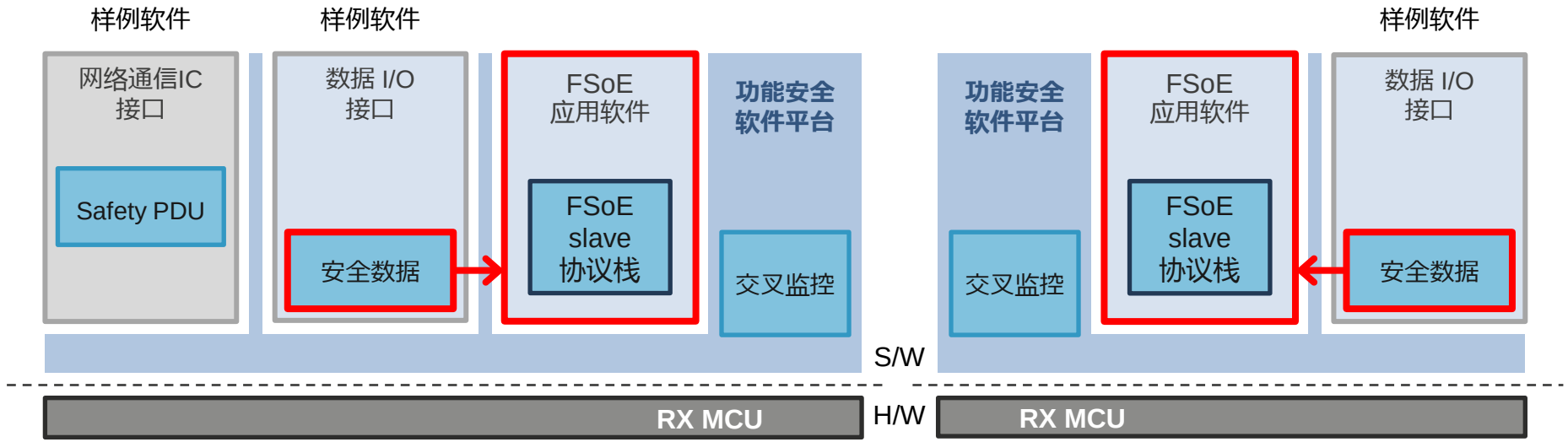


1. 从外部端口输入安全数据
2. 向FSoE应用软件发送安全数据
3. 数据交换和处理，CRC计算
4. 生成Safety PDU格式
5. 将Safety PDU发送到外部IC.

PDU : Protocol Data Unit

FSoE应用软件包:数据流

[数据状态] 安全数据输入操作数据流：2

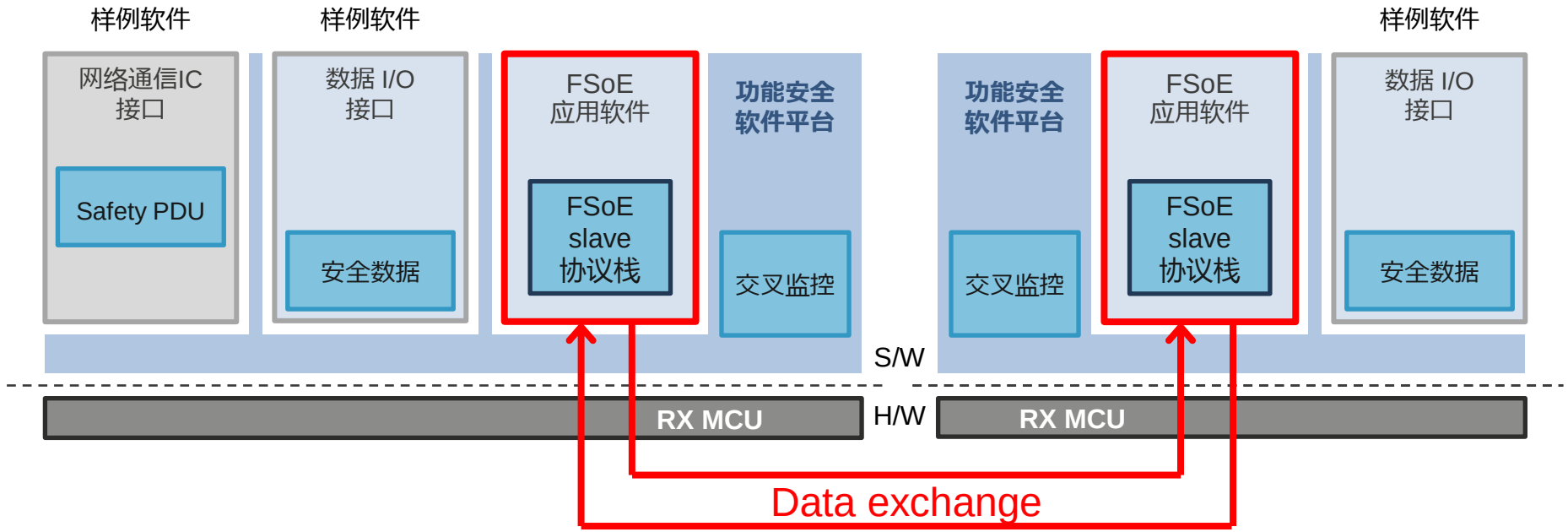


1. 从外部端口输入安全数据
2. 向FSoE应用软件发送安全数据
3. 数据交换和处理，CRC计算
4. 生成Safety PDU格式
5. 将Safety PDU发送到外部IC.

PDU : Protocol Data Unit

FSoE应用软件包:数据流

[数据状态] 安全数据输入操作数据流：3

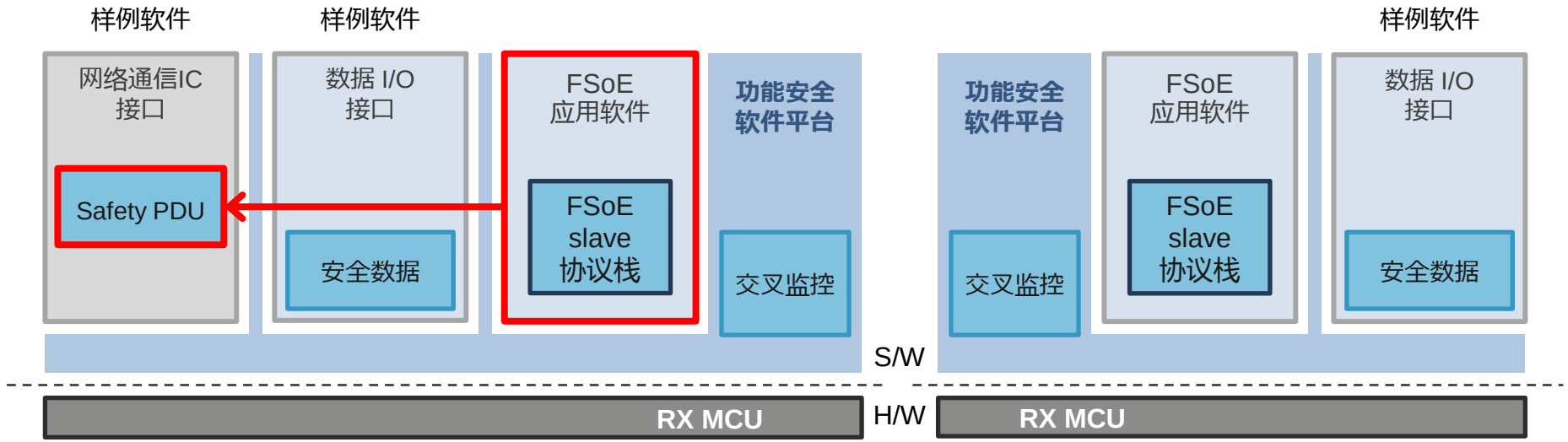


1. 从外部端口输入安全数据
2. 向FSoE应用软件发送安全数据
3. 数据交换和处理，CRC计算
4. 生成Safety PDU格式
5. 将Safety PDU发送到外部IC.

PDU : Protocol Data Unit

FSoE应用软件包:数据流

[数据状态] 安全数据输入操作数据流：4

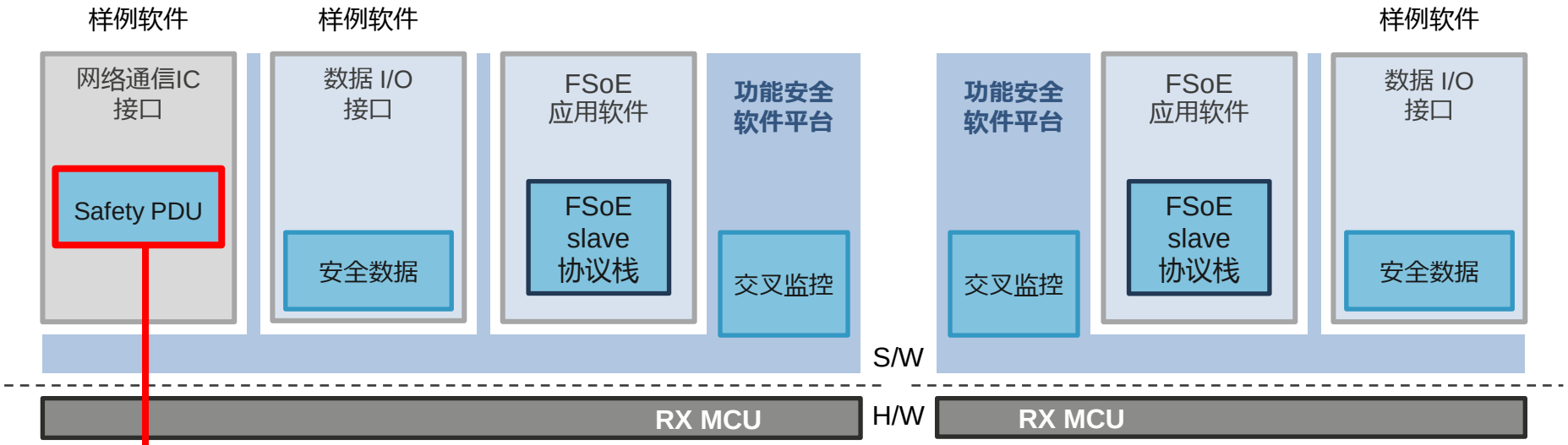


1. 从外部端口输入安全数据
2. 向FSoE应用软件发送安全数据
3. 数据交换和处理，CRC计算
4. 生成Safety PDU格式
5. 将Safety PDU发送到外部IC.

PDU : Protocol Data Unit

FSoE应用软件包:数据流

[数据状态] 安全数据输入操作数据流：5



Safety
Protocol
Data Unit

EtherCAT master
Safety master

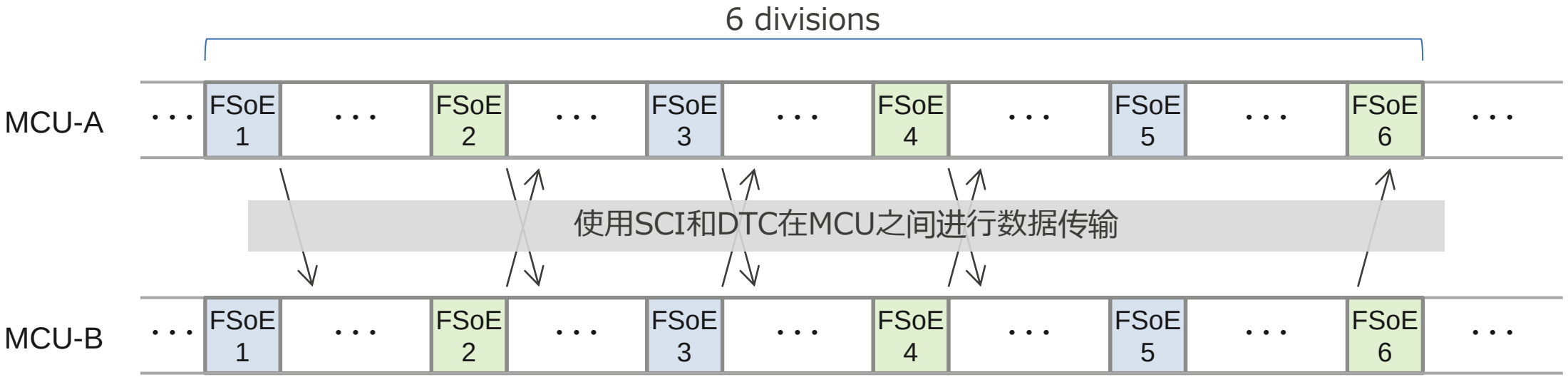
EtherCAT

1. 从外部端口输入安全数据
2. 向FSoE应用软件发送安全数据
3. 数据交换和处理，CRC计算
4. 生成Safety PDU格式
5. 将Safety PDU发送到外部IC.

PDU : Protocol Data Unit

FSoE应用软件包: 执行控制

拆分流程以最大限度地减少对其他应用程序流程的影响



: FSoE 应用软件 : 安全数据输出处理

: FSoE 应用软件 : 安全数据输入处理

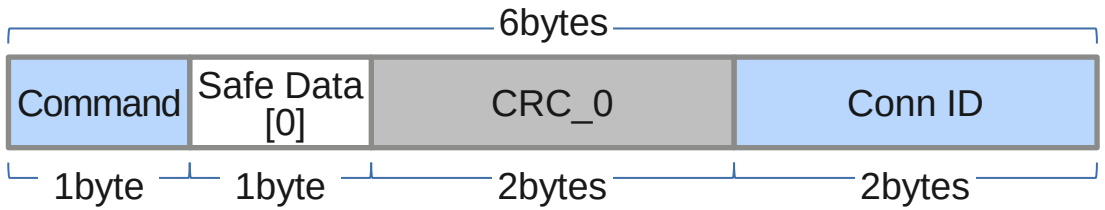
: 其他应用软件

FSoE应用软件包: 数据格式

可以在设置文件中更改安全PDU大小

例如. 安全 PDU：6 bytes 设定

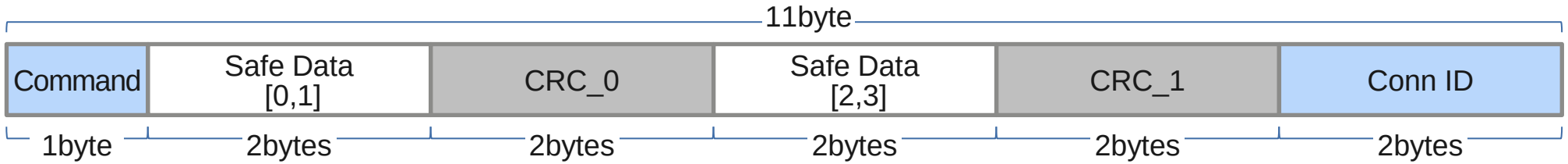
```
#define FSOEIF_INTERFACE_SAFETY_PDU_INPUT_SIZE     (6U)
#define FSOEIF_INTERFACE_SAFETY_PDU_OUTPUT_SIZE    (6U)
```



= Safe Data 1byte

例如. Safety PDU：11 bytes 设定

```
#define FSOEIF_INTERFACE_SAFETY_PDU_INPUT_SIZE     (11U)
#define FSOEIF_INTERFACE_SAFETY_PDU_OUTPUT_SIZE    (11U)
```



= Safe Data 4bytes

FSoE应用软件包: 评估版本

No.	内容		商业版本	评估版本
1	FSoE 应用软件	TÜV Rheinland IEC61508 SIL3 认证目标	✓	✓
2	安全手册		✓	✓
3	用户指南		✓	✓
4	IEC61508 认证文档(证书, 测试报告)		✓	-
5	(样例软件) 网络通信IC接口 数据I/O接口		✓	✓
6	软件开发手册		✓	✓

Same software

Renesas Functional Safety

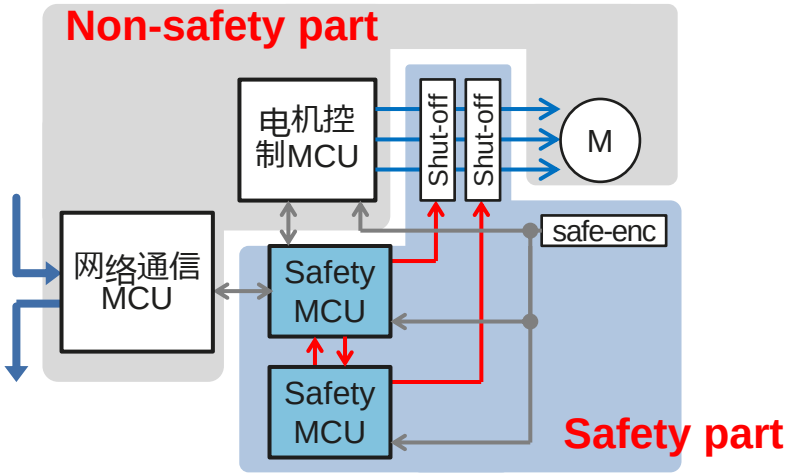
1. Renesas RX系列MCU功能安全解决方案
   - 1-1. Self-Test 软件包
   - 1-2. SIL3 系统软件包
   - 1-3. FSoE 应用软件包
   - 1-4. 参考文档
   - 1-5. 参考硬件
     - 1-5-1. 概述
     - 1-5-2. 电机控制系统文档
     - 1-5-3. 概念阶段文档
     - 1-5-4. 安全验证文档
     - 1-5-5. MCU 内部诊断文档
     - 1-5-6. MCU 外部诊断文档
2. Renesas RA系列MCU功能安全解决方案
   - 2-1. Self-Test 软件包

参考文档: 概述

参考文档定义了一个虚拟电机控制系统，并描述了获得该虚拟系统功能安全认证所需的以下技术信息。

- 如何编写提交给认证机构的文件
- 如何实现安全MCU执行的诊断和监控功能

本文件的内容可用于各种功能安全产品。



	内容
1	电机控制系统文档
	- 虚拟电机控制系统安全控制器规范
2	概念阶段文档
	- 功能安全认证概念阶段所需文件的编写指南 - 功能安全认证概念阶段所需的文件样本
3	安全验证文档
	- 使用自下而上方法的硬件FMEA的概念和示例 - 软件FMEA的概念和示例 - 用于确认SIL有效性的计算示例 (SFF, PFDavg, PFH)
4	MCU 内部诊断文档
	- 解释MCU内部模块诊断方法的文档
5	MCU 外部诊断文档
	- 解释MCU外部电路诊断方法的文档

总计：20 个文档和 6个 Excel 文件

参考文档: 订购号码

No.	RX 组	编译器	订购号码	备注
1	- *1	- *1	RTK0EF0005Z21001ZJ	20 文档 + 6 excel 文件

*1 : 由于这是一份解释处理功能安全的技术方法的文件，因此它不取决于MCU或编译器的类型。

参考文档: 内容简介

	内容
1	电机控制系统文档
	- 虚拟电机控制系统安全控制器规范
2	概念阶段文档
	- 功能安全认证概念阶段所需文件的编写指南 - 功能安全认证概念阶段所需的文件样本
3	安全验证文档
	- 使用自下而上方法的硬件FMEA的概念和示例 - 软件FMEA的概念和示例 - 用于确认SIL有效性的计算示例 (SFF, PFDavg, PFH)
4	MCU 内部诊断文档
	- 解释MCU内部模块诊断方法的文档
5	MCU 外部诊断文档
	- 解释MCU外部电路诊断方法的文档

电机控制系统文档

电机控制系统安全控制器规范

概念阶段文档

文档指南

安全计划/验证和确认计划(样例文档)

安全要求规范(样例文档)

安全概念(样例文档)

安全验证文档

FMEA 文档(硬件)

安全完整性等级计算

代码规范

FMECA 文档(软件)

检查安全等级的计算公式

MCU 内部诊断文档

区块式自我诊断

如何实现软件错误诊断

如何实现MCU间的通信诊断

RX MCU内置ECC电路的诊断

MCU 外部诊断文档

如何实现MCU电源电压的监测

如何实现网络通信部分的诊断

利用编码器脉冲进行电机诊断

如何实现安全输出电路诊断

如何实现安全输入电路诊断

安全控制

Renesas Functional Safety功能安全

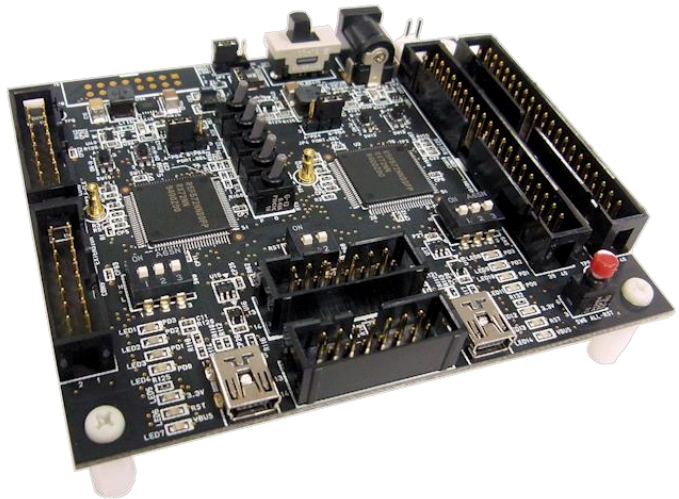
1. Renesas RX系列MCU功能安全解决方案
    - 1-1. Self-Test 软件包
    - 1-2. SIL3 系统软件包
    - 1-3. FSoE 应用软件包
    - 1-4. 参考文档
    - 1-5. 参考硬件
        - 1-6-1. 概述
        - 1-6-2. RXv2 参考板
        - 1-6-3. RXv3 参考板
2. Renesas RA系列MCU功能安全解决方案
    - 2-1. Self-Test 软件包

RX 参考硬件: 内容

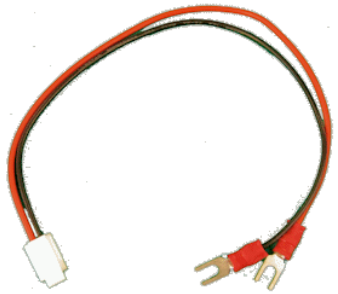
No.	内容	RXv2 Board	RXv3 Board
1	**参考板**	✓	✓
2	**电源线**	✓	✓
3	**用户手册(CD-R)** **(包括原理图和零件清单)**	✓	✓

注意：参考硬件未捆绑任何软件.

1. 参考板



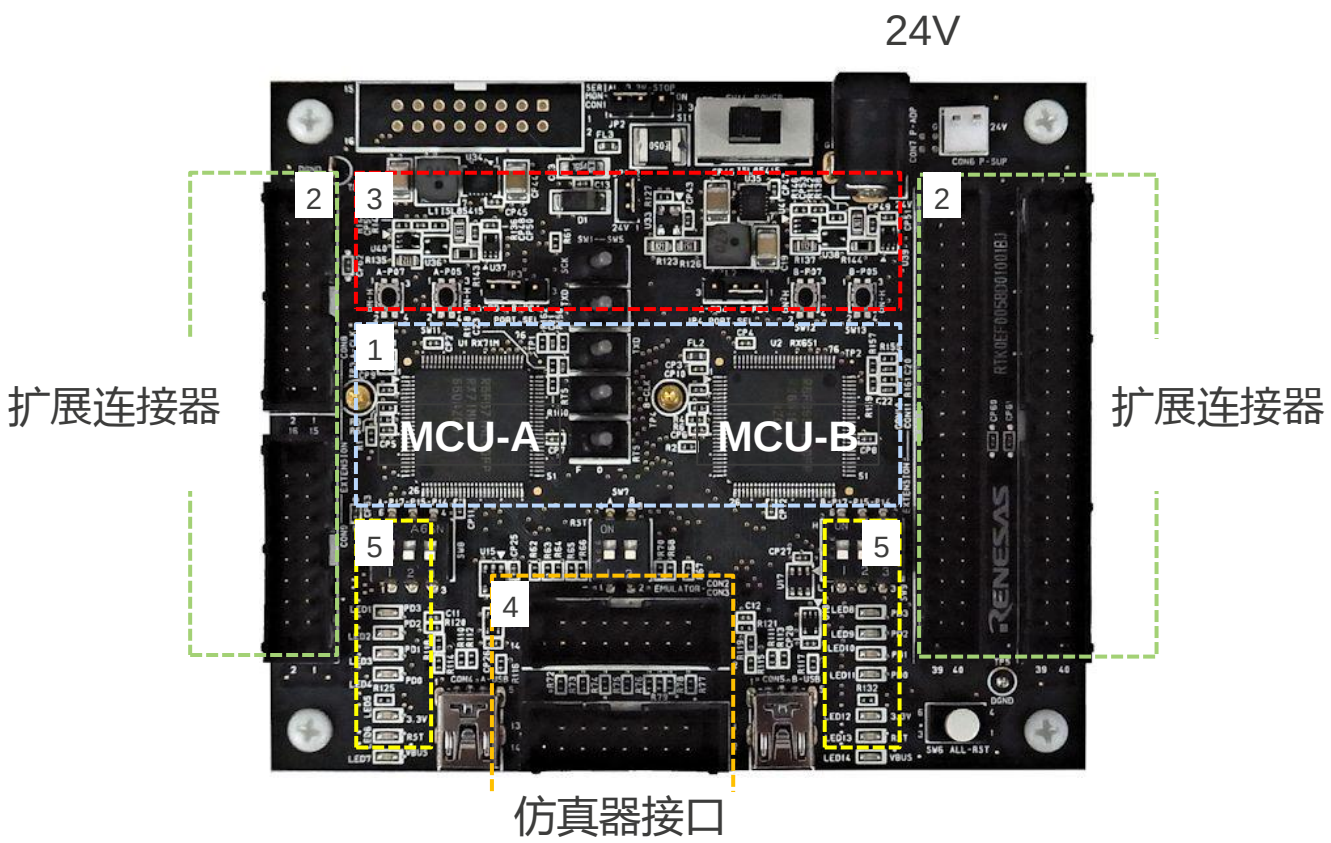
2. 电源线



3. 用户手册(CD-R)

RX参考硬件: 概述

具有双MCU配置的功能安全评估板



1. 双MCU

   -RXv2 参考板
   MCU-A : **RX71M** / MCU-B : **RX651**

   -RXv3参考板
   MCU-A : **RX72N** / MCU-B : **RX72N**

2. 配备用于功能扩展的连接器

3. 配备24V和MCU电源监控电路

4. 配备E1或E2 Lite仿真器的连接器

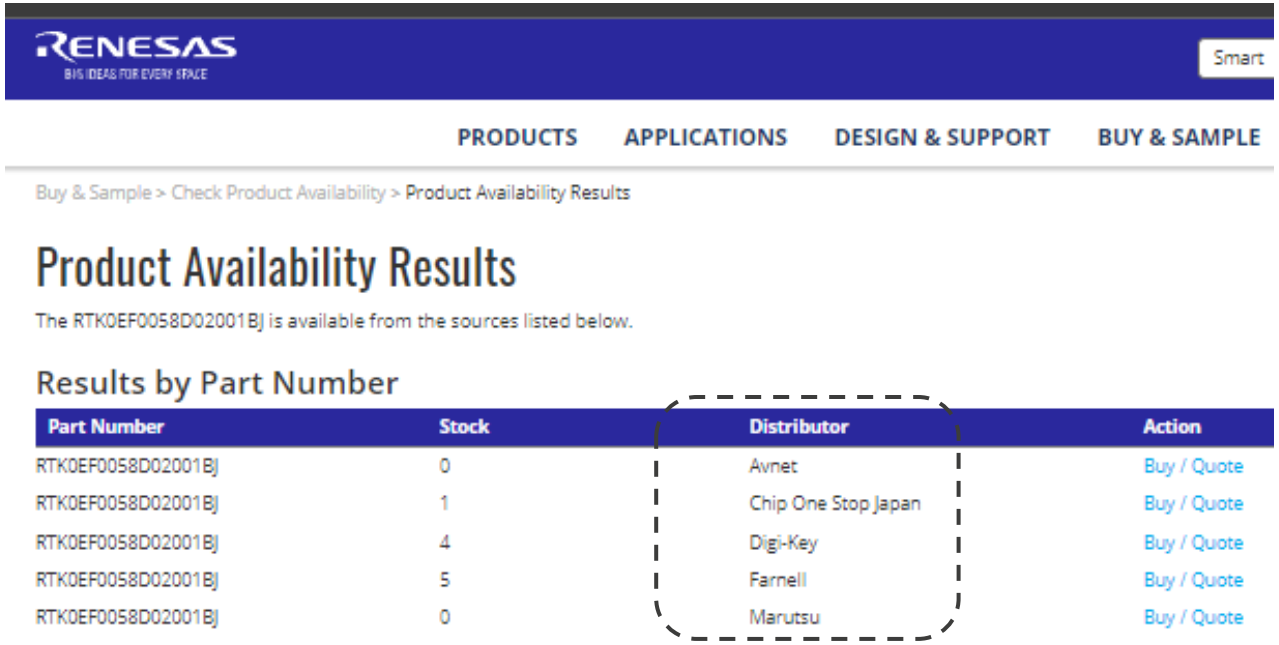
5. 配备通用开关和LED，可用于评估

RX参考硬件: 订购号码

No.	类别	MCU	订购号码
1	RXv2 Board	RX71M - RX651	RTK0EF0058D01001BJ
2	RXv3 Board	RX72N - RX72N	RTK0EF0058D02001BJ

Note: RXv3参考硬件不仅通过瑞萨分销商销售，还通过多个在线购物网站销售.

URL : Product Availability Results | Renesas Electronics Corporation



Renesas Functional Safety 功能安全

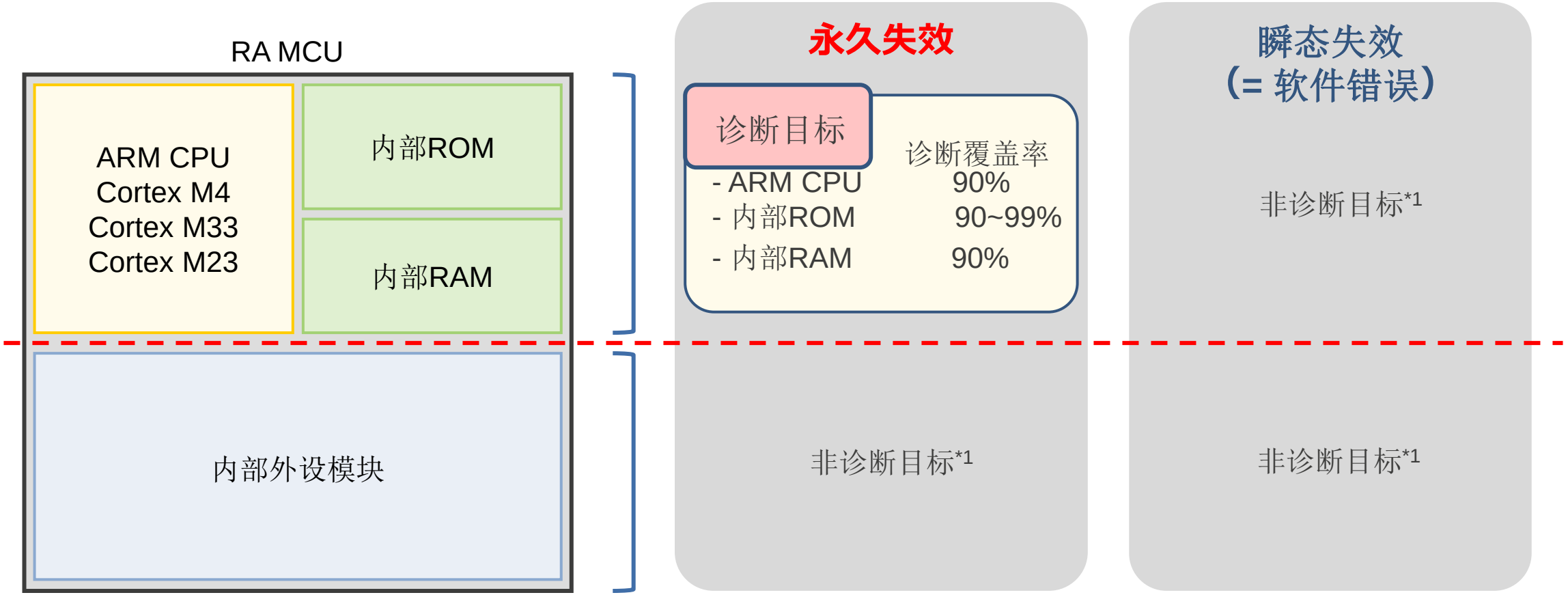
1. Renesas RX系列MCU功能安全解决方案
2. Renesas RA系列MCU功能安全解决方案
   - 2-1. Self-Test 软件包
     - 2-1-1. 概述
     - 2-1-2. 功能

RA系列MCU Self-Test 软件包 ：内容

No.	Contents	
1	RA系列MCU诊断软件for RA	TÜV Rheinland IEC61508 SIL3 认证目标
2	安全手册	
3	用户指南	
4	IEC61508 认证文档(证书, 测试报告)	

RA系列MCU 诊断软件: 概述

RA MCU中CPU、RAM和ROM的永久失效诊断软件



*1:Refer to the reference document for the diagnostic method

RA系列MCU 诊断软件: 必要的资源

No.	CPU	软件	ROM	RAM	端子	外设
1	Cortex-M4 *1	RA系列MCU诊断软件	55Kbyte	16byte	0	CRC
2	Cortex-M33 *2		27Kbyte	0.5Kbyte	0	CRC
3	Cortex-M23 *3		7Kbyte	0.5Kbyte	0	CRC

*1:Compatible with RA6M1, RA6M2, RA6M3, RA6T1, RA4M1
*2:Compatible with RA6M4, RA6M5, RA4M2, RA4M3
*3:Compatible with RA2A1, RA2L1, RA2E1

RA系列MCU Self-Test软件包 ：订购号码

No.	CPU	MCU	编译器	订购号码
1	Cortex-M4	RA6系列 *1	IAR-EWARM V8.22.3	RTK0EF0090F60001SJ
2		RA4系列*2		RTK0EF0090F40001SJ
3	Cortex-M33	RA6系列*3	IAR-EWARM V8.50.10	RTK0EF0104F01001SJ
		RA4系列*4		
	Cortex-M23	RA2系列*5		

*1:兼容RA6M1, RA6M2, RA6M3, RA6T1
*2:兼容RA4M1
*3:兼容RA6M4, RA6M5
*4:兼容RA4M2, RA4M3
*5:兼容RA2A1, RA2L1, RA2E1

RA系列MCU 诊断软件: CPU内核的诊断

项目	描述				
目标区域	CPU 核，通用寄存器				
目标失效类型	永久失效				
诊断方法	“CPU指令代码组合的有效值”与“期望值”的比较				
诊断覆盖率	90%				
测试单元的数目，总执行时间	CPU	Cortex-M4		Cortex-M33		Cortex-M23
	MCU 组	RA6M1 RA6M2 RA6M3 RA6T1	RA4M1	RA6M4 RA6M5	RA4M2 RA4M3	RA2A1 RA2L1 RA2E1
	测试单元的数目	32	32	25	25	10
	总执行时间*1	125,410	125,410	19,121	19,121	6,721

*1: Unit = CPU clock cycles

RA系列MCU 诊断软件: 内部ROM诊断

项目	描述		
目标区域	内部 ROM		
目标失效类型	永久失效		
诊断方法	“ROM数据的CRC计算值”与“期望值”的比较		
诊断多项式, 诊断覆盖率	从以下选项中选择		
		诊断多项式	诊断覆盖率
	1	CRC-8 *1 (X^8+X^2+X+1)	90%
	2	CRC-16 *1 $(X^{16}+X^{15}+X^2+1)$	99%
	3	CRC-CCITT $(X^{16}+X^{12}+X^5+1)$	99%
执行时间*2	CPU	多项式	执行时间
	Cortex-M4	CRC-16	25,601 *3
	Cortex-M33	CRC-CCITT	14,015* 4
	Cortex-M23	CRC-CCITT	27,959 *4

*1: 只能选择Cortex-M4的诊断软件
*2: Unit = CPU clock cycles
*3: 当诊断ROM大小为1K字节时
*4: 当诊断ROM大小为4K字节时

RA系列MCU 诊断软件: 内部RAM诊断

项目	描述			
目标区域	内部 RAM			
目标失效类型	永久失效			
诊断方法	使用标准RAM测试算法进行诊断			
诊断算法, 诊断覆盖率	从以下选项中选择			
		诊断算法	诊断覆盖率	
	1	Extended March C-	90%	
	2	WALPAT	90%	
诊断类型	从以下选项中选择 1.非破坏性测试 2.破坏性测试			
执行时间*1 *2	CPU	算法	非破坏性测试	破坏性测试
	Cortex-M4	Extended March C-	184,377	180,538
		WALPAT	113,347,652	113,343,045
	Cortex-M33	Extended March C-	122,957	118,415
		WALPAT	9,132,152	9,127,766
	Cortex-M23	Extended March C-	169,403	164,580
		WALPAT	14,942,718	14,937,893

*1: Unit = CPU clock cycles
*2: 当诊断RAM大小为1 KB时