工业设备的功能安全

中川 靖， 物联网及基础设施事业本部，瑞萨电子有限公司

2022 年 3 月

概要

近年来，“功能安全”正在成为工业设备领域中实现系统安全性的可靠方法。除了向来重视安全的汽车领域之外，在工业设备领域，也会因为机器故障和事故的发生以及人身伤害事件对工厂运转造成影响或引起社会关注，而且还导致了经济损失。为了避免这些情况，“功能安全”的重要性与日俱增。在通过人与机器人协同作业来提高作业效率的进程中，设备安全性越发受到关注。因此，越来越多的设备制造商以满足社会与用户的要求和提高商品竞争力为目的，开始研究功能安全设备。

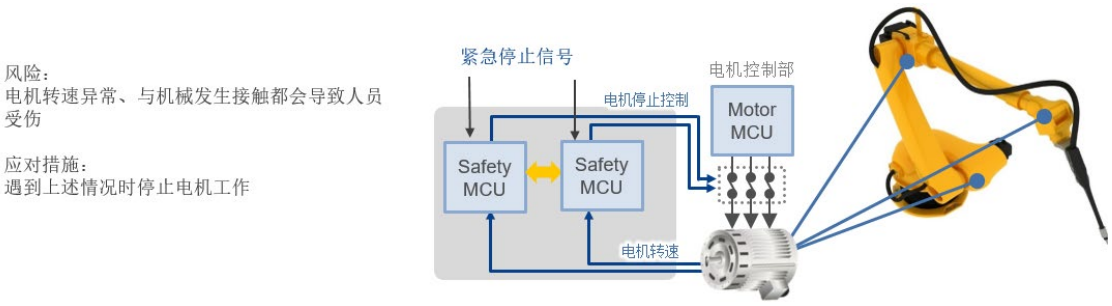
在本资料中，我们将对功能安全的定义和必要性，实际系统结构，开发中存在的课题以及瑞萨为解决这些课题而提供的功能安全解决方案进行说明。

什么是功能安全

功能安全的目的是，通过“功能”把因装置误动作，误操作而造成的人身伤害，财产损害或社会危害等风险控制在容许限度以内。

下面将以在机器人等电机控制装置中为避免出现危险状况而使电机停止工作的情况为例，进行具体说明。

图 1 是以通过 MCU 控制电机旋转的系统作为采取功能安全措施的例子。为了实现功能安全，首先要分析与装置相关的风险，并研究相应的措施。这被称为风险评估，而功能安全的装置（安全装置）能够通过电子电路等，实现以风险评估结果为基础制定的安全措施。在这里，功能安全与传统安全装置之间存在很大差异，即“安全装置”需要根据 IEC61508 等国际标准进行标准化，使“安全装置”规格的合理性能够通过客观，定量的方法来实现。



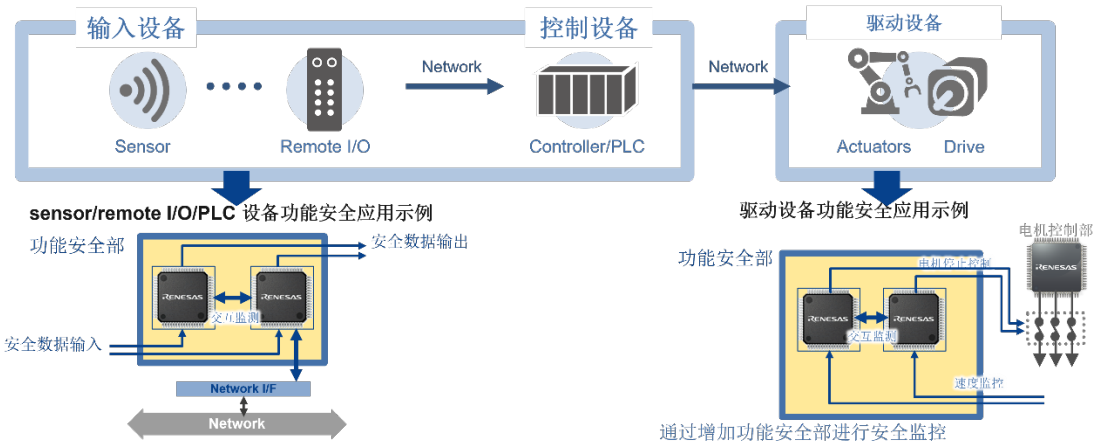
1: 功能安全的电机驱动装置结构示例

功能安全规格的要求事项有许多，如通过分析因安全装置故障造成的误动作的影响，设计基于诊断功能的，在安全装置故障时也能引导至安全状态的措施；通过做出设计方法和设计流程的相关规定，避免因软硬件设计缺陷等原因导致的误动作等。通过这些要求事项，便可更加客观地判断其安全规格以及作为安全装置的动作准确性（可靠性）。另外，此类 FA 系统还要求采用类似图 1 所示的双配置 MCU 结构，在系统结构上实现即使一个 MCU 在动作期间出现故障等动作不良，也能通过正常动作的另一个 MCU 执行可靠的安全动作。

工业领域功能安全系统的具体示例

下面将用 FA 系统来说明实际应用中的功能安全系统结构示例。

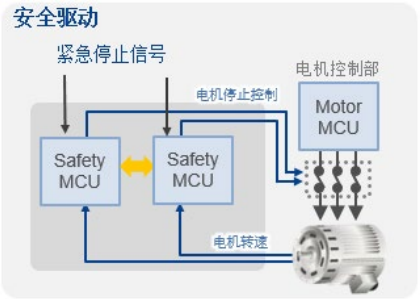
图 2 是功能安全相关系统结构示例。该 FA 系统由以下部分构成：检测是否有人进入危险区域的安全传感器等输入设备，由整体控制安全系统的安全 PLC 等构成的控制设备，驱动具体设备的驱动设备以及连接以上设备的网络。其内部结构如图 2 下半部分所示，是由 2 个 MCU 构成的双配置 MCU 结构。采用这种机构的目的是，即使在安全功能的某处发生故障，也能通过正常动作的 MCU 准确执行用于避免危险的动作，从而使设备能够可靠地执行安全动作。



2: FA 系统的结构示例

接下来将说明构成该 FA 系统的各类设备，即安全驱动设备，安全 IO 设备以及安全网络设备。

安全驱动设备

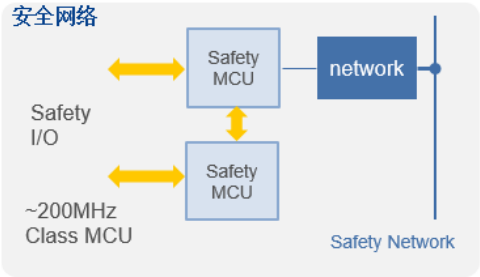


驱动设备的基本安全规格是通过监控电机是否安全受控来实现的。在开头的图 1 中也已经对它的结构作了说明，一般采用在使电机旋转的机构外侧加装监控单元的结构，用于监控电机安全动作。该监控单元通过双配置 SafetyMCU 监控电机转速以及用于在紧急等时候紧急停止装置的紧急停止信号，并在这些状态被判断为危险状态时，执行向电机控制端发送电机停止信号的动作。设计这些动作时采用了双配置结构，因此即使监控单元内发生故障，也可以通过其中一个正常动作的 SafetyMCU 转移到安全动作。此外，根据 FA 系统的用途，有多种电机的监控方法和停止方法，其规格已在电机驱动设备的安全标准 IEC61800-5-2 中定义。

安全远程 I/O 设备

安全远程 I/O 设备是传输信号的设备，这些信号包括根据安全传感器等的输入信号向需要紧急停止的设备输出的信号等。它的内部结构是双配置 MCU 结构，即使安全装置发生故障，也能可靠地执行安全动作。此外，通过用双 SafetyMCU 执行用于安全控制程序，也能以同样结构实现安全 PLC（主要是低端型）。

安全网络设备



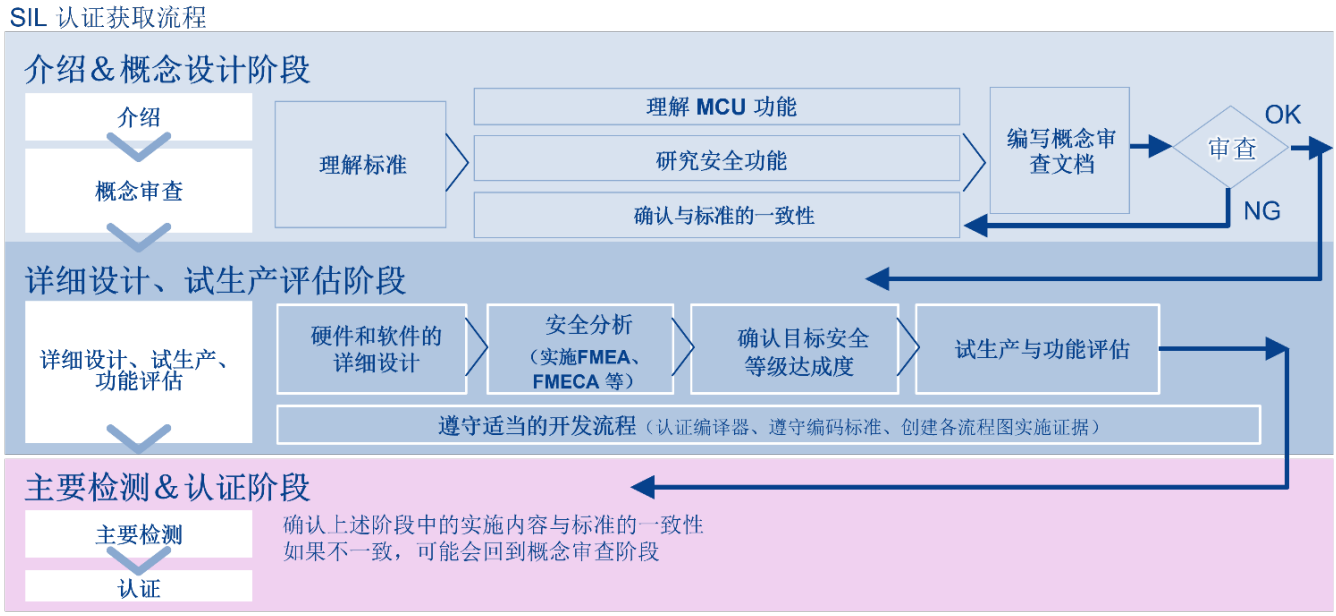
安全网络设备是可以通过工业网络实现安全数据通信的设备。这里也采用了 2 个 SafetyMCU，除了安全 IO 处理，还能根据安全网络标准进行通信安全数据处理。右侧的网络设备被称为“黑色通道（Black Channel）”，是非安全处理的一部分。黑色通道意味着不安全，不过安全网络中的标准化安全协议有方法确认从黑色通道接收的数据是否被正确传送，即通过用 2 个 SafetyMCU 进行确认来实现。

功能安全系统开发中遇到的问题

功能安全系统的开发分为规格研究（介绍 & 概念阶段），详细设计/评估（详细设计与试生产评估阶段），第三方认证（主要检测 & 认证阶段）等三个开发认证阶段进行，并对传统开发流程中没有的技术条件和流程提出了要求。

图 3 显示了功能安全系统开发的典型流程。在第一阶段——介绍 & 概念阶段，在学习了功能安全标准，MCU 规格等基础性知识之后，对危险进行分析（被称为安全分析），确定避免危险的方法，研究设定作为具体安全系统规格研究的概念。此外，还要创建必要的文档，并接受认证机构的概念审查。这里的安全系统规格应该是接下来的原型机详细设计，试作评估阶段的详细设计以及试生产评估阶段中可实现的规格。通过认证机构的审查后，进入第二阶段——原型机详细设计，试作评估阶段的详细设计以及试生产评估阶段，根据在概念设计阶段确定的规格进行详细的软硬件设计评估。这一系列设计流程需要按照功能安全标准 IEC61508 所要求的开发流程进行。在设计时，必须在准确把握功能安全标准的内容之后进行开发。此外，还需要分析硬件故障，研究故障的诊断方法，并执行适当的开发流程以避免软件出现问题。这些工作要求各设计流程中实现文档化以及基于系统故障率和诊断率的达成安全等级的计算等，并需要加入传统开发过程中没有的工作。

详细设计和评估完成后，在第三阶段——主检和认证阶段，向认证机构提交至今为止的设计和评估内容，视需要安排现场测试，如果这些内容得到批准就能获得认证。



3: 功能安全系统的开发流程

瑞萨对功能安全系统开发的提案

在推进系统功能安全标准认证获取流程时，开发者面临的技术问题列举如下。

1） 获得认证时的各种文档的记述方法，用于系统安全分析（FMEA），SIL 等级达成的各种参数计算方法

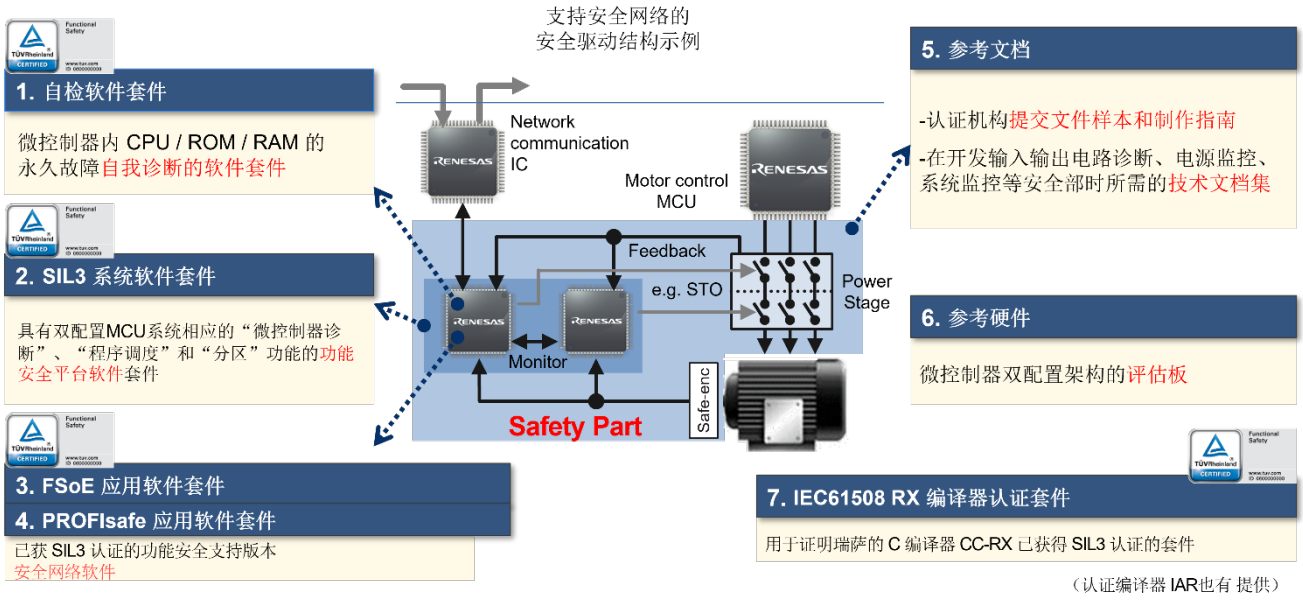
2） 在由 2 个 SafetyMCU 构成的双配置系统结构中实现 MCU 自我诊断，交互监测等用于故障诊断的软件

3） 双配置 SafetyMCU 系统的硬件结构（交互监测的通信，输入输出电路诊断，电源诊断的结构等）

4） 实现符合应用的功能安全机构（实现电机关闭机构，用于检测电机转速的编码器，安全网络等）

针对这些实现功能安全系统的过程中遇到的课题，瑞萨的功能安全解决方案提供了各种解决方案，以解决这些课题。下面我们将介绍与这些开发者面对的课题相对应的解决方案。

瑞萨准备了图 4 所示的 1.~7. 的解决方案，用来支持功能安全系统的开发。接下来说明这些解决方案将如何解决课题。



4: 瑞萨的功能安全解决方案

获得认证时的各种文档记述方法：参考文档

开发功能安全系统时，在首要工作即研究规格的概念阶段中，会制作 SRS，SC，SP，V&V 等必要文档，但是在没有认证获取经验的情况下，这些文档的记载事项和记述方法不得不需要工作人员自行摸索，对时间和成本造成严重的浪费。5.的参考文档以实现电机驱动装置安全系统为例，具体记述了概念阶段中所需要的文档。将这些文档作为模板，根据每位用户的规格进行修改，可以恰当地记录必要的信息。

实现双配置系统的诊断软件：SIL3 系统软件套件，自检软件套件

在功能安全系统中，为了避免安全功能因硬件故障无法正常工作的状态，必须执行故障诊断。在故障诊断中，除了对每个设备进行故障检测，还必须检测动作期间因放射线，干扰等而发生软件错误继而导致的误动作，并在异常时立即转移到电机停止等安全动作。在对每个设备执行故障诊断时，必须分析各设备的故障模式，研究用于检测故障的故障检测方法，以及定义该检测方法的故障检测率（诊断率）。此外，检测软件错误也需要监控程序执行顺序，并通过用双配置 SafetyMCU 交互比较等方法对系统性动作进行检测。但是，

如果是像 SafetyMCU 这样复杂的设备，故障检测方法及其诊断率定义成为了装置开发者的沉重工作负担。而且，还必须根据功能安全标准的要求采用适当的 SafetyMCU 间通信方法，用于程序顺序监控和交互比较，这同样令开发者感到头疼。1.自测试软件套件提供了用于检测 SafetyMCU 故障的自我诊断程序，满足 IEC61508 标准中 SIL3 所要求的 90% 诊断率。2.的 SIL3 系统软件套件预先安装了实现双配置系统所需的交互监测和程序顺序监控等软件。它提供了主要的 SafetyMCU 诊断，程序顺序监控，双配置 SafetyMCU 间交互监测所需的软件，并取得了 IEC61508 的 SIL3 认证，因此开发者可以直接拿来使用。

通过应用这些解决方案，开发者只需要在自检软件，SIL3 系统软件套件上构建安全系统所需的应用程序，就能开发功能安全系统，从繁琐的 SafetyMCU 诊断和双配置 SafetyMCU 控制部开发中解放出来。

此外，还要求证明这些软件所使用的编译器能够用于功能安全系统的开发。瑞萨提供已取得 IEC61508SIL3 认证的 7.的 CC-RX 编译器。另由 IAR Systems 公司提供已取得 SIL3 认证的编译器。

实现双配置系统的硬件：参考文档 参考硬件评估板

为了实现双配置结构，必须有特定的硬件，比如在 2 个 SafetyMCU 间交互监测的通信手段，电源分离和电源监控，输入输出电路的诊断等。6.的参考硬件提供了包括双配置 SafetyMCU 电源电路在内的参考数据。此外，使用双配置结构的优点，是可以通过相互交换处理数据，在不使用特殊诊断硬件的情况下正常动作。这一系列硬件结构和诊断方法都记载在 5.的参考文档中。

在判断设计的软硬件是否达到目标安全等级时，必须定义硬件故障率，故障诊断方法以及诊断率，使用以可靠性理论为基础的复杂计算公式计算各种参数，并表明是否满足安全等级所对应的基准值。这些认证文档的记述样本，各种参数的计算方法也在参考文档中有详细记载，并以 Excel 格式提供了计算公式。通过这些方法，即使是开发新手，也能在表格中输入故障率，诊断率等数据，切实地开展工作。此外，SafetyMCU 的周边功能因各用例而有不同方法，参考文档中记载了与用例对应的诊断方法。

实现与应用对应的安全功能：参考文档 FSoE 应用软件套件，PROFIsafe 应用软件套件

除 MCU 诊断的解决方案之外，瑞萨还在应用级别为安全驱动设备，安全 IO 设备，安全网络设备提供有效的解决方案。参考文档以样本文档的形式，提供了符合驱动系统安全标准 IEC61800-5-2 所需的硬件结构，安全控制方法以及将这些作为安全概念记述下来的内容。其中用针对驱动装置的功能安全的例子进行了说明，不过该结构由“安全输入-安全控制-安全输出”这种一般功能安全设备的处理块构成，在具有相同结构的安全传感器，安全远程 IO 设备开发中也可以作为参考。参考文档中还记述了网络安全化。关于面向安全网络的软件，为了支持 EtherCAT 的安全版 FSoE（Functional Safety over EtherCAT），瑞萨提供了 3.FSoE 应用软件套件。另外，为了支持 PROFINET 的安全版 PROFIsafe，瑞萨还开始提供全新的 4.PROFIsafe 应用软件套件。

总结

如图 5 所示，瑞萨的功能安全解决方案可提供向认证机构提交资料时的文档记录方法等，这些资料包括概念阶段的规格研究，关于 MCU 的功能安全的相关故障分析和诊断程序，双配置结构和周边诊断，网络等系统级诊断软件。这些解决方案能够支持 60%～70% 的功能安全系统开发工作。由此，开发者就可以通过设计，开发设备固有部分来完成安全系统。

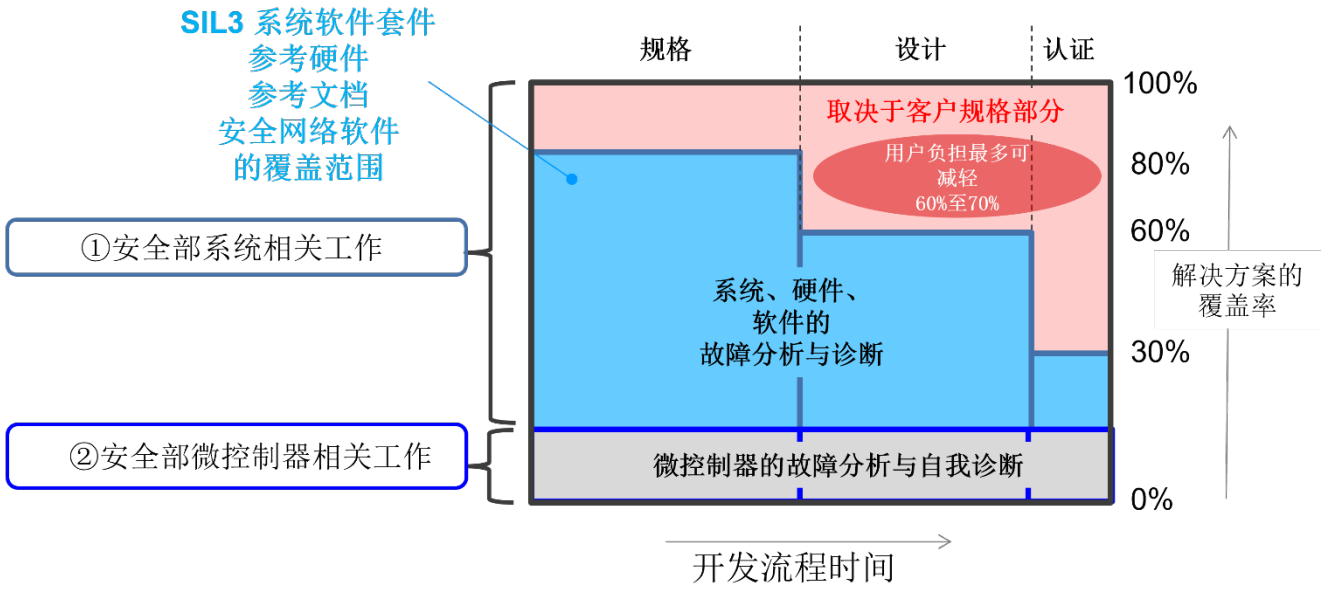


图 5: 瑞萨功能安全解决方案覆盖范围

通过应用瑞萨的功能安全解决方案，系统开发者能够从 SafetyMCU 诊断等设备固有软件开发，认证工作中解放出来，有效利用系统开发所花费的时间和成本。瑞萨的功能安全解决方案为不得不摸索着尝试开发功能安全系统的开发认证工作提供可靠，便捷的路径。

参考资料

IEC 的 Functional Safety and IEC 61508

面向工业设备的功能安全解决方案

RX 系列 （32-bit MCUs）

重要通知和免责声明

瑞萨电子株式会社及其关联公司（以下简称“瑞萨”）的技术规范和可靠性数据（包括数据手册）、设计资源（包括参考设计）、应用或其他设计建议、Web 工具、安全信息以及其他资源“按原样”提供，不保证无瑕疵。瑞萨不做任何明示或暗示保证，包括但不限于产品适销性、特定用途适合性或不侵犯第三方知识产权的保证。

这些资源的适用对象为使用瑞萨产品熟练进行设计的开发人员。以下事宜请自行负责：(1)为您的应用选择合适的产品，(2)设计、验证和测试您的应用，(3)确保您的应用符合适用标准以及安全性等所有其他要求。这些资源如有更改，恕不另行通知。瑞萨仅授权您将这些资源用于开发采用瑞萨产品的应用。严禁复制这些资源或用于其他用途。我们未授予任何其他瑞萨知识产权或任何第三方知识产权的许可。

瑞萨对因使用这些资源而产生的任何索赔、损害、成本、损失或负债概不负责，且瑞萨及其代表的全部损失须由您赔偿。瑞萨的产品仅遵守瑞萨的销售通用条款和条件，或书面签订的其他适用条款。使用瑞萨的任何资源不会扩大或更改这些产品的任何适用保修或保修免责声明。

(Rev.1.0 Mar 2020)

公司总部

135-0061, 日本东京江东区

豊洲 3-2-24, TOYOSU FORESIA

https://www.renesas.com

联系信息

有关产品、技术的更多信息，文档的最新版本，或

离您最近的销售办公室，请访问：

https://www.renesas.com/contact-us

商标

瑞萨电子的名称和徽标是瑞萨电子公司的商标。 所有商

标和注册商标均为其各自合法所有者的财产。

Doc Number: R30WP0002CC0100