白皮书

工业设备的功能安全

中川 靖，高级经理，物联网及基础设施事业本部，瑞萨电子有限公司

2020 年 9 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。因此，越来越多的设备制造商以满足终端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。

在本白皮书中，我们将对功能安全的定义和必要性、实际系统结构、开发中遇到的问题以及用于解决这些问题的瑞萨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”将因装置误动作、误操作而导致装置对人员造成危害、对财产或社会造成损害等风险控制在容许限度以内。例如，如图 1 所示，人员进入机器人工作的工厂区域，与机器人的机械臂发生碰撞而受伤。为了防止这种情况，一般作为第一步，会采取在机器人周围围上栅栏的措施。但是即便如此，也可能会有人员不小心打开栅栏门或跨过栅栏进入，导致事故发生。为了避免此类风险，作为第二步，会用传感器检测打开栅栏、跨越栅栏的行为。一旦检测到，就使机器人停止工作。通过这种方法，可以进一步降低风险。换句话说，这种方法通过加装某种“安全装置”来避开危险。能够检测到这种危险的传感器以及在有危险时令机器人停止工作的“安全装置”，就是用于功能安全的设备。

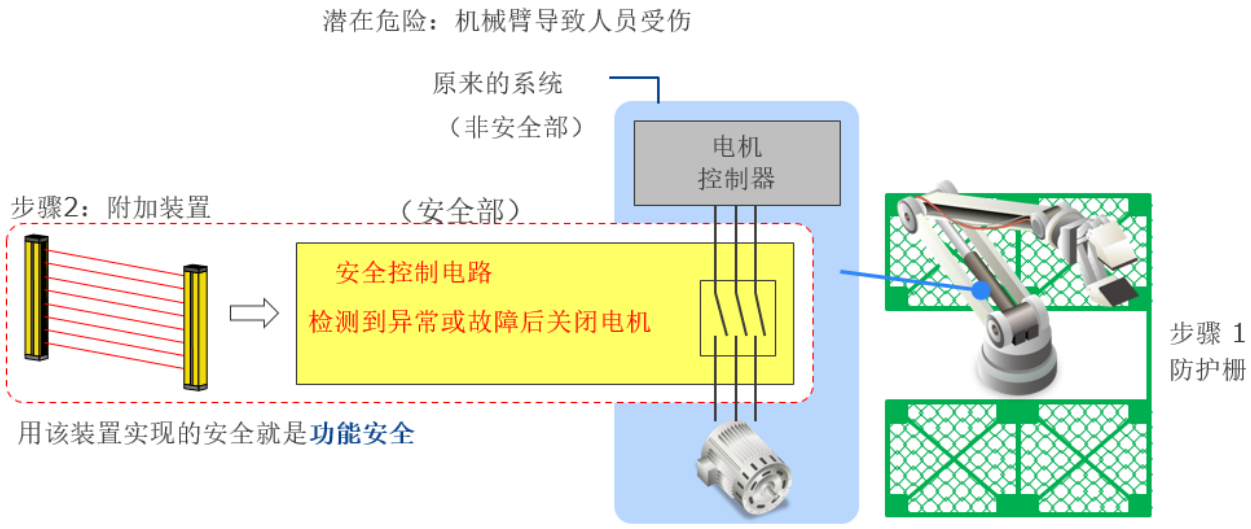


图 1 功能安全系统的概念

为了进一步详细说明，我们将以机器人等电机控制装置中为避免危险情况而停止电机工作的结构为例进行说明。图 2 的例子是在通过 MCU 控制电机旋转的系统中采取功能安全措施。想要实现功能安全，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，按照该标准的定义，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。

图 2 安全驱动装置的结构示例

具体而言，通过以下措施，可以更加客观地判断安全规格和安全装置动作的可靠性（信赖度）：分析因安全装置故障造成误动作的影响，通过诊断功能采取即使发生故障也能引导至安全状态的措施，为避免因软硬件设计缺陷导致误动作，做出设计方法和设计流程的相关规定等。另外，此处由于采用了双配置 MCU 结构，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，这也是该结构的一大特征。

工业领域功能安全系统的具体示例

关于具体应用中的系统结构，我们将说明 FA 系统中的主要构成设备 – 安全驱动系统、安全 IO 系统以及安全网络系统。

图 3 是在人员进入等情况下，通过能够检测此类行为的安全传感器，使电机驱动装置停止工作的功能安全系统结构示例。该 FA 系统由安全传感器等输入设备、用于整体控制的安全 PLC 设备、驱动实际设备的安全驱动装置以及连接它们的安全网络构成。其内部结构如图 2 所示，是由 2 个 MCU 构成的双配置 MCU 结构。这种机构是为了确保设备执行安全动作，即使在某处发生故障，也能通过正常动作的 MCU 可靠地执行用于避免危险的动作。FA 领域的功能安全设备普遍采用这种结构。

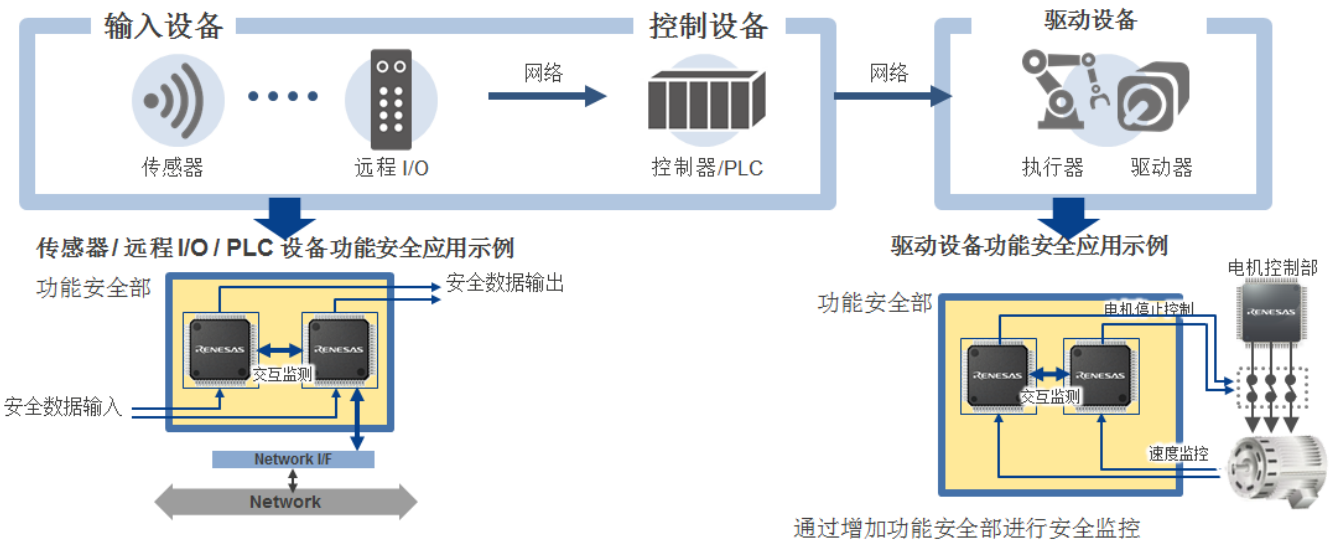


图 3 FA 系统的结构示例

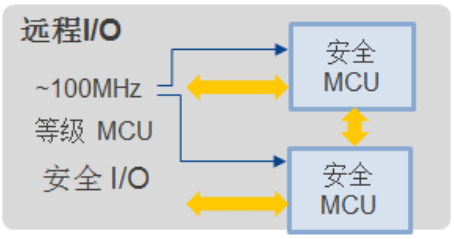
接下来，对构成这些安全 FA 系统的各设备进行说明。

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 2 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。该监控单元监控电机转速和在紧急情况下紧急停止装置的“Emergency Stop”信号。当它们的状态被判断为危险状态时，在电机控制侧执行发出紧急停止信号的动作。在这个例子中，通过双配置安全 MCU 监控“Emergency Stop”信号和转速信息，当发生某种故障时，输出 Termination Control 作为切断电机动力的指令，并将该信号传送到电机停止电路，切断动力以确保安全。而且，因为这是双配置结构，所以可以认为即使监控单元本身发生故障，也能通过正常动作的某个安全 MCU 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。

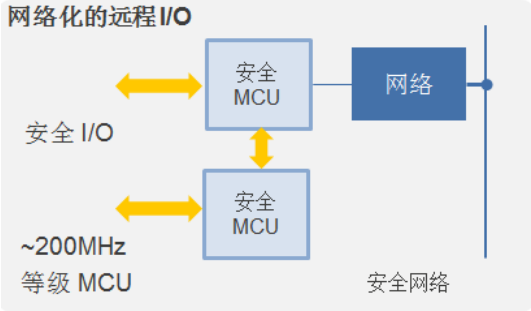
安全远程 IO 设备

这种设备根据安全传感器等的输入信号，对安全动作进行控制，例如向需要紧急停止的设备发出信号等。它的工作方式是，将来自安全传感器的报警信号输入到安全远程 IO 设备的输入部，在执行了简单的逻辑计算之后，从输出侧输出信号，再输入到电机驱动装置的紧急停止信号部等。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 MCU 执行用于安全控制的程序，也能以同样结构实现安全 PLC（主要是低端型）。



网络安全远程 IO 设备

在安全远程 IO 设备上添加网络功能后，即成为网络安全远程 IO 设备。这里也采用了 2 个安全 MCU，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。网络设备被称为“黑色通道（BlackChannel）”，是非安全处理的一部分。黑色通道是指没有可靠性的通信路径，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 个安全 MCU 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（Introduction and concept）、详细设计/评估（Detailed Design, Trial and Function Evaluation）、主检和第三方认证（Main inspection and certification）等三个阶段进行，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 4 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，设定用于具体安全系统规格研究的概念。此外，还要创建必要的文档，并接受认证机构的审查。这里的安全系统规格研究应该是接下来的详细设计、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 – 详细设计、试生产评估阶段，根据在概念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 – 主要检测 & 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。

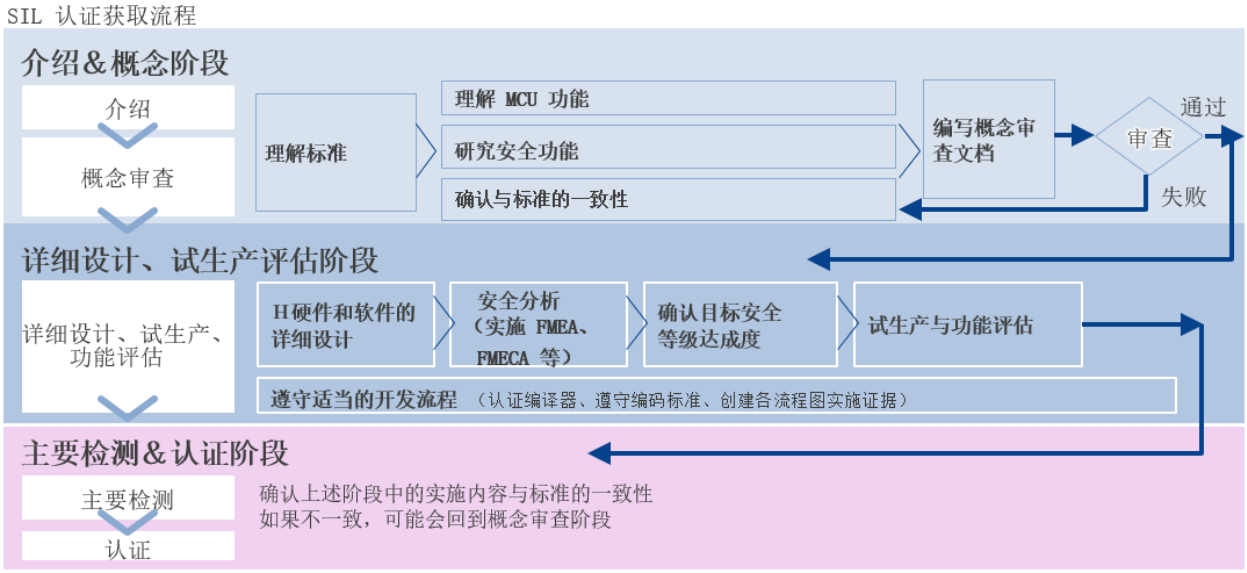


图 4 功能安全系统的开发流程

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 FMEA、SIL 等级达成的各种参数计算方法

2） 在由 2 个 MCU 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 MCU 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（电机关闭机构、用于检测电机转速的编码器、实现安全网络等）

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

瑞萨准备了图 5 所示的①~⑥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问题。

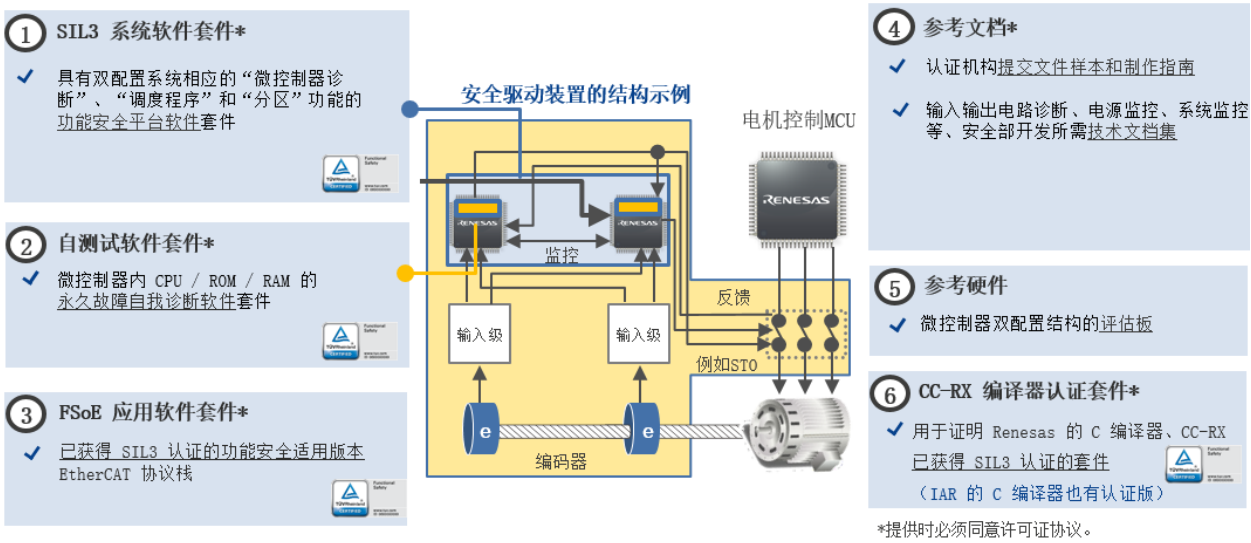


图 5　瑞萨的功能安全解决方案

✓　获得认证时的各种文档记述方法：④参考文档

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，会制作安全需求规格（SRS）、安全概念（SC）、安全计划（SP）、验证和确认(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。④参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：①SIL3 系统软件套件，②自测试软件套件

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 MCU 交互比较等方法对系统性动作进行检测。但是，如果是像 MCU 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 MCU 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。②自测试软件套件提供了用于检测 MCU 故障的自我诊断程序，满足 IEC61508 标准中 SIL3 所要求的 90%诊断率。①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 MCU 诊断、程序顺序监控、双配置 MCU 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，开发者只需要在自测试软件、SIL3 系统软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 MCU 诊断和双配置 MCU 控制部开发中解放出来。

✓　实现双配置系统的硬件：④参考文档 ⑤参考硬件板

为了实现双配置结构，必须有特定的硬件，比如在 2 个 MCU 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。⑤参考硬件板提供了包括双配置 MCU 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④参考文档中。

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④参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，MCU 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：④参考文档 ③FSoE 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电机驱动、安全 IO 系统、安全网络提供有效的解决方案。④参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。其中以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，因此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 EtherCAT 的安全版 FSoE（Functional Safety over EtherCAT），瑞萨还提供了将协议栈和 MCU 诊断部结合起来的解决方案③FSoE 应用软件套件。

总结

如图 6 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、网络等系统等级诊断软件。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。

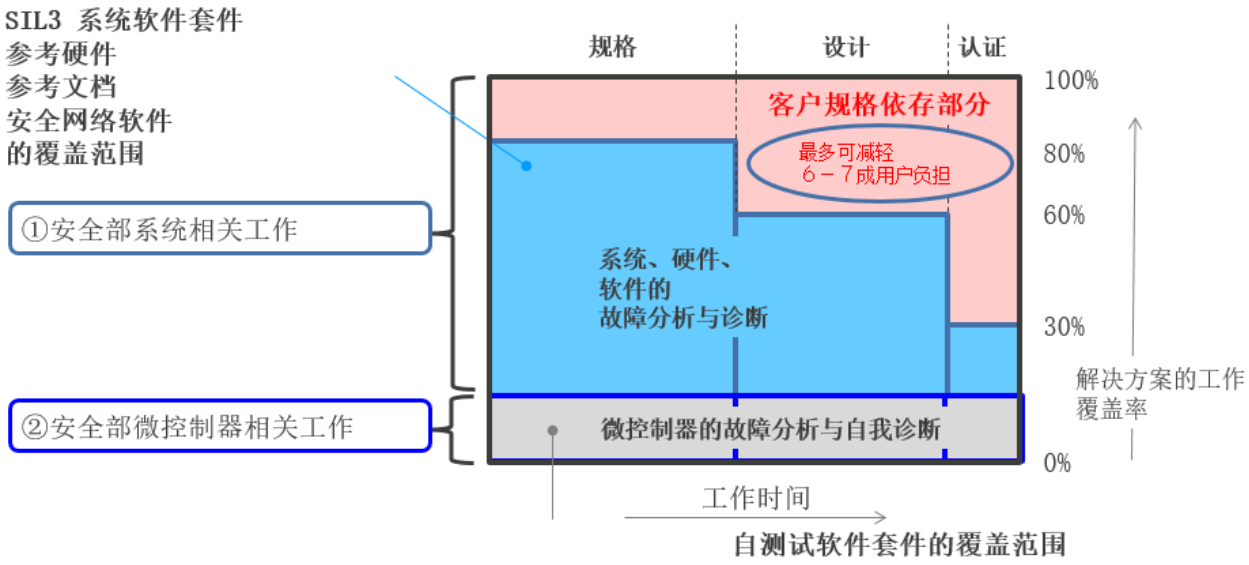


图 6　瑞萨功能安全解决方案的效果

通过应用瑞萨的功能安全解决方案，系统开发者能够从 MCU 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

1. IEC 的 Functional Safety and IEC 61508
2. 面向工业设备的功能安全解决方案
3. RX 系列（32 位 MCU）