Functional Safety in Industrial Automation

Yasushi Nakagawa, Principal Specialist, IoT Infrastructure Business Headquarters, Renesas Electronics Corporation

March 2022

Abstract

As technology advances and continues to improve, functional safety demands critical consideration across most industrial automation equipment and is now starting to become increasingly important in numerous other applications including service robotics, medical, and building automation in order to prevent adverse effects due to equipment failure in addition to preventing accidents. Set manufacturers are increasingly supporting new functional safety equipment to meet both the demand from the market as well as improve product competitiveness.

In this White Paper, we will outline what functional safety is, why it is necessary, the structure of an actual system, address the challenges in development, and how Renesas' functional safety solutions can alleviate those challenges.

What is Functional Safety?

The goal of functional safety is to use functions to reduce the risk of equipment causing harm to people, damage to property or society due to malfunction or incorrect operation.

An example of a functional safety feature is using motor control devices on robots to avoid hazards by automatically stopping the motor.

Figure 1 shows an example of a system with functional safety support in which the motor rotation is controlled by an MCU. To achieve functional safety, the first step is to analyze the risks associated with the equipment, and then consider countermeasures. This is called a Risk Assessment (RA), and safety measures derived from RA results are implemented as functional safety devices in electronic circuits. Functional safety differs from conventional safety due to the safety measures being defined by international standards such as the IEC61508. This functional safety standard is applicable across all industries and requires certification by impartial third body certification bodies.

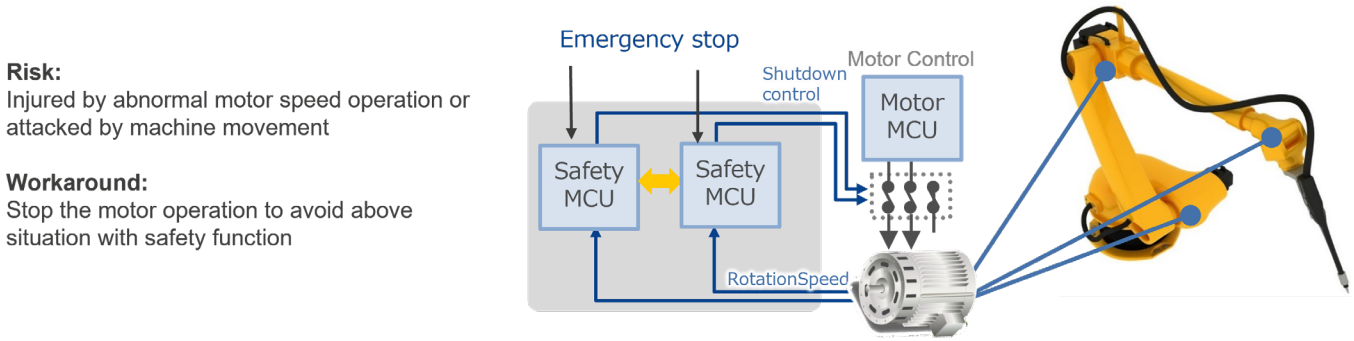


Figure 1: Example of a Motor Drive System with Functional Safety

Functional safety standards require an analysis of how safety device failure influences malfunctions and the use of diagnostics to develop countermeasures that can maintain safety in the event a failure occurs. There are specified design methods and processes to prevent malfunctions due to software and hardware bugs that may occur in the design stage, as well. This means that it is possible to objectively evaluate safety specifications and certainty (reliability) of safety equipment operation. In such FA systems, a redundant MCU configuration, as shown in Figure 1, is also required so that even if one MCU malfunctions, all other functioning MCUs can ensure safe operation.

Example of functional safety system in industrial equipment

Let's take a look at an FA system as an example of a real application of functional safety systems.

Figure 2 shows an example of a system configuration supporting functional safety. This FA system includes input devices like safety sensors that detect human entry into dangerous areas, control devices like safety PLCs that control the whole safety system, drive devices that actually operate machinery, and a network connecting them all. Its internal structure includes a redundant MCU system consisting of two MCUs, as shown in the lower half of Figure 2. This structure ensures safe equipment operation as it allows the MCU on the normal functioning side to reliably avoid danger if a failure occurs somewhere within the safety function.

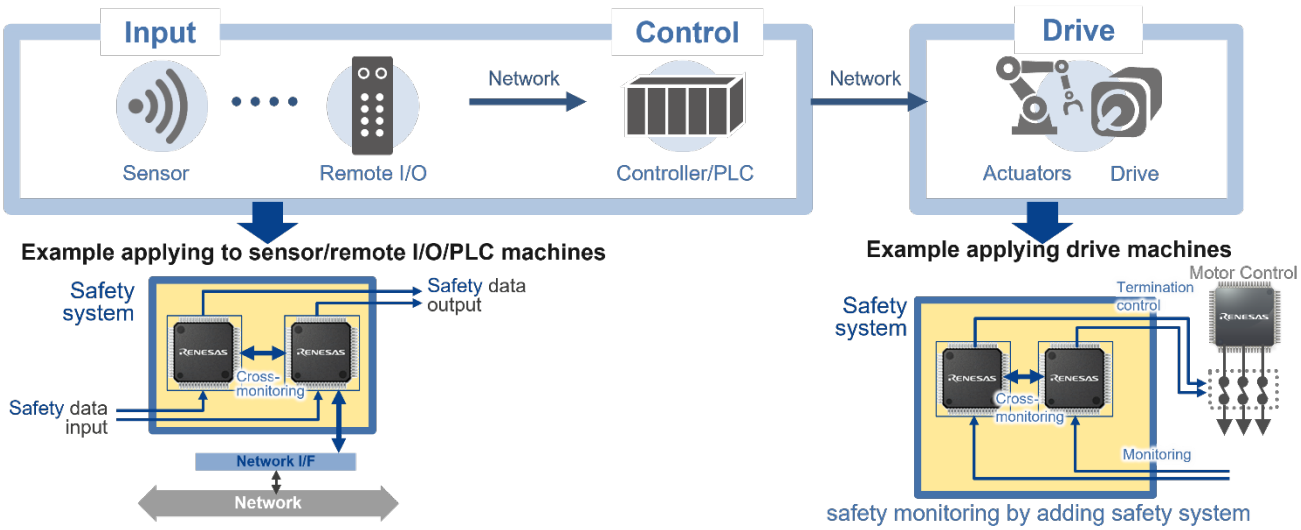
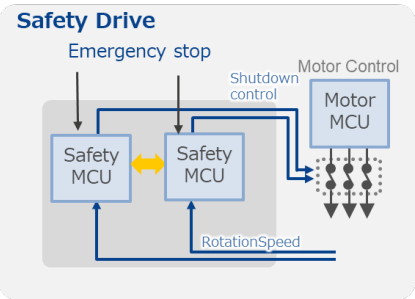


Figure 2: FA System Structure Example

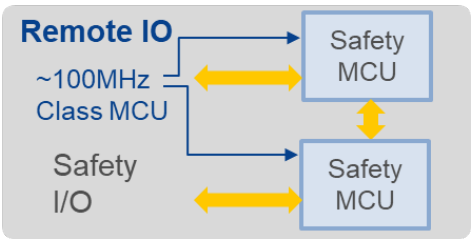
Next, we will discuss the individual devices that make up this FA system: safety drive devices, safety I/O devices, and safety network devices.

Safety Drives



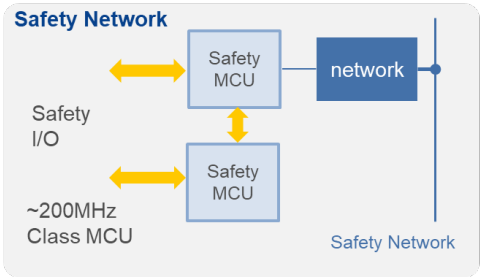
The basic safety specifications of drive devices are to monitor whether the motor is being safely controlled. As discussed with Figure 1 above, typically the structure consists of a monitoring unit attached to the side of any equipment with a rotating motor to monitor its safe operation. This unit has a redundant Safety MCU setup that monitors the rotation speed and any emergency stop signal. The motor control side can send an emergency stop signal if any of these conditions are considered to be dangerous. These operations are redundant, so that even if there is a failure in the monitoring unit, whichever Safety MCU is operating normally can switch to handle safety operations. There are several different methods of monitoring and stopping motors depending on FA system application, and their specifications are defined in IEC 61800-5-2, the international safety standards for electric drives.

Safety Remote I/O Devices



These are devices used to transmit signals, including emergency stop signal outputs in response to safety sensor inputs. The MCU internal configuration here is also redundant, so that even if one safety device fails, safety operation can still be reliably executed. Also, safety control programs run on both Safety MCUs, so the same configuration can implement Safety PLC (primarily low-end types).

Safety Network Devices



Safety network devices are any that transmit safety data over an industrial network. Again, two Safety MCUs are used to process safety I/O as well as safety data transmitted in accordance with the safety network standards. The network devices on the right side are known as the Black Channel, and that section is treated as unsafe. Although the meaning of Black Channel is an unsafe area, the safety protocols standardized on the safety network include a method to verify that data coming through the Black Channel is being sent correctly, which is implemented by using two Safety MCUs.

Issues in Functional Safety Systems Development

Functional safety system development proceeds in three development verification phases: the introduction/concept phase, which includes specification review; the detailed design/trial phase which includes functional evaluation; and the main certification phase, which includes third-party inspection and verification. The whole process has technical requirements and processes that are absent in conventional development.

Figure 3 shows a standard flow for functional safety system development. The top-level Introduction & Concept Phase begins with gaining a fundamental understanding of the functional safety standards and MCU specifications, and then sets up a concept review that includes a safety analysis to identify hazards, sets methods to avoid hazards, and examines specific safety system specifications. It also requires documentation creation for concept review by the certification body. The safety specifications set in this phase must be feasible for the subsequent phases of detailed design and trial/functional evaluation, and certification. After passing the initial certifying organization inspection, the project moves into the middle stage of detailed design and trial evaluation, where detailed hardware and software designs based on the specifications fixed in the concept phase are drawn up for evaluation.

This series of design processes must proceed in accordance with the development process required by the IEC61508 functional safety standards. The design process requires an accurate grasp of the functional safety standards and requires developers to analyze hardware failures, consider diagnostic methods, and implement appropriate development processes to avoid software failures. There are tasks not needed in the traditional development process, such as documenting each design process and calculating safety level achieved based on the systems failure and diagnosis rates.

Once detailed design and evaluation are complete, the contents that have passed through design and evaluation are submitted to the certifying organization in the main inspection and certification phase, as shown at the bottom of the figure.

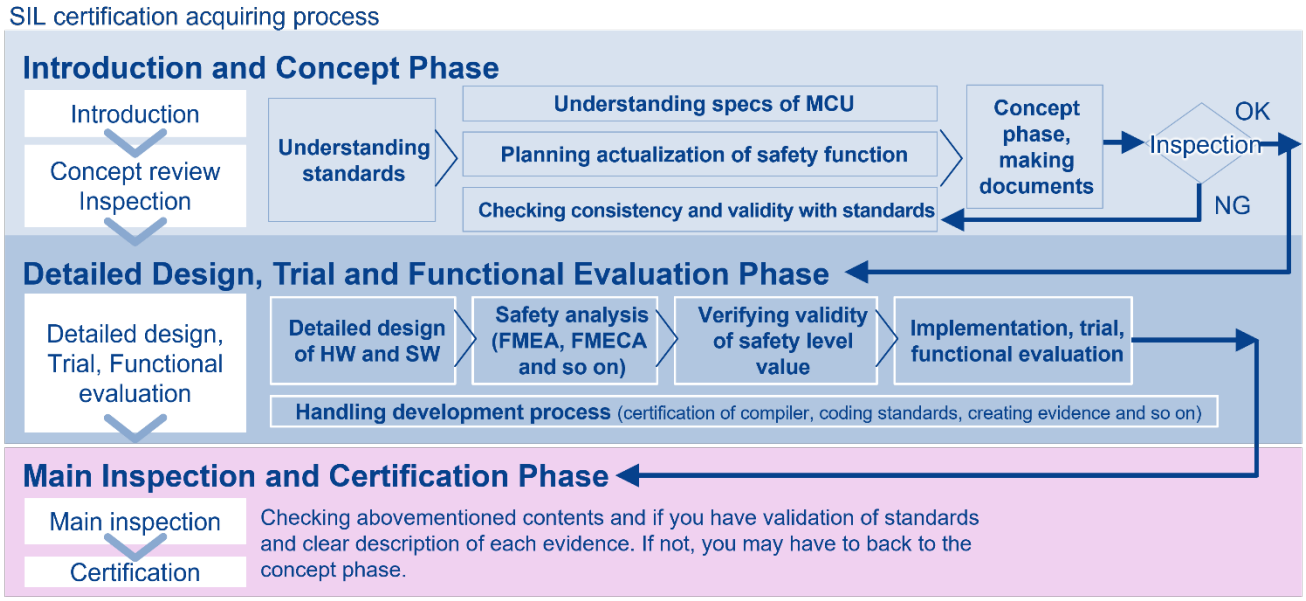


Figure 3: Functional Safety System Development Process

Renesas' Proposals for Functional Safety Development

The following are some of the technical issues developers face when moving through the process of attaining functional safety standards certification.

1. Methods of creating the various documents needed to get certification, system failure mode and effects analysis (FMEA), calculation methods for various parameters to achieve SIL levels
2. Implementing fault diagnosis software like MCU self-diagnosis and mutual monitoring in a redundant system configuration consisting of two Safety MCUs
3. Hardware structure for redundant Safety MCU systems (mutual monitoring transmission, input/output circuit diagnosis, power system diagnosis configuration, etc.)
4. Implementing application-specific functional safety equipment (motor shutdown equipment, motor speed detection encoders, safety network implementation, etc.)

Renesas' functional safety solutions offer a variety of ways to address these challenges in implementing functional safety systems. This section introduces solutions that address the issues developers face.

Figure 4 lists seven solutions offered to support functional safety system development, followed by a description of how they help address the issues.

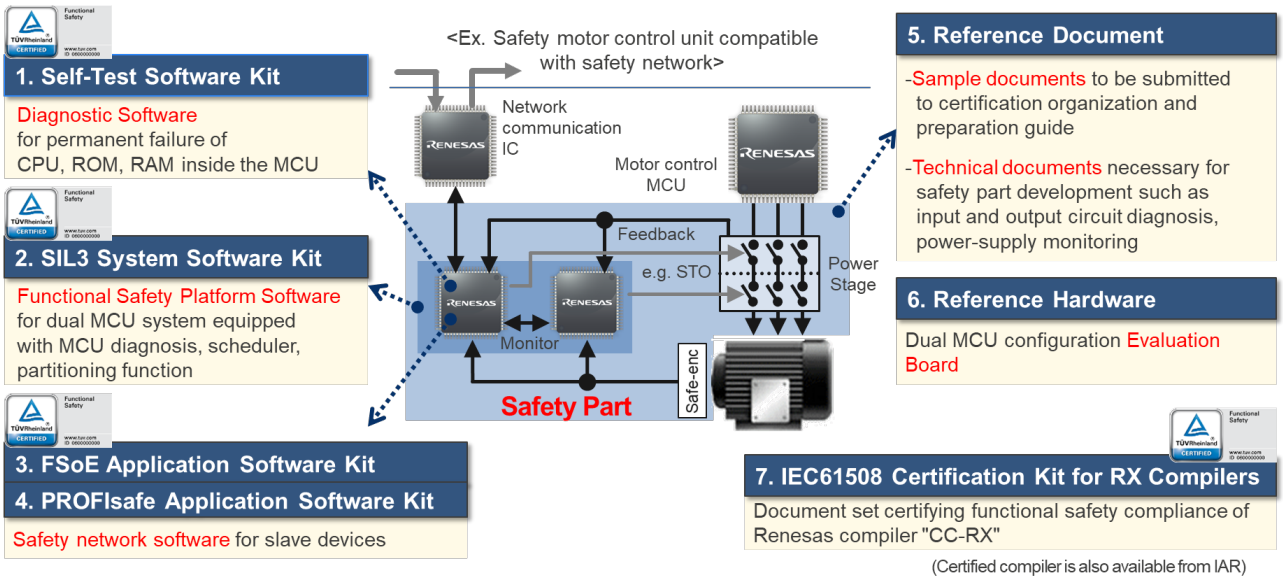


Figure 4: Renesas Functional Safety Solutions

Methods of Creating Various Documents Required for Certification: Reference Documents

The first step in developing a functional safety system is the concept phase, when specifications are reviewed, which also requires a variety of documentation, like SRS, SC, SP, or V&V. Developers without any certification experience will have to go through the process of filling out each entry and description, which can greatly affect time and cost. Solution 5: Reference Documents include specific examples of the documents required in the concept phase based on the example of implementing a safety system for a motor drive. Using them as templates, the developer can modify each entry as needed to fit use specifications, so that only the necessary information is included.

Implementing Diagnostic SW for Redundant Systems: SIL 3 System Software Kit, Self-Test Software Kit

Functional safety systems require fault diagnosis to avoid hardware failures that can prevent the safety functions from working properly. In addition to detecting individual device failures, fault diagnosis must also detect soft-error malfunctions caused by radiation, noise, and so on during operation, and immediately shift to safe operation, such as stopping motors if abnormality occurs. Fault diagnosis for individual devices requires analysis of each one's failure mode, an examination of fault detection methods to detect those modes, and defining the fault detection rate (diagnostic rate) based on that detection method. It is also necessary to detect soft-errors using systematic functions such as monitoring program execution sequences, or inter-comparison using redundant Safety MCUs.

However, with complex devices like Safety MCU, finding fault detection methods and defining their diagnostic rate pose a considerable workload for equipment developers. Furthermore, communication methods between Safety MCUs used in program sequence monitoring and inter-comparison must also be run in a way appropriate to the functional safety standards, which is another major burden for developers.

Solution 1: Self-Test Software Kit offers a self-diagnostic program to detect errors in Safety MCUs which achieves a diagnostic rate of 90%, satisfying the SIL 3 level required for IEC61508 standards.

Solution 2: SIL 3 System Software Kit comes preloaded with software for mutual monitoring, program sequence monitoring, and other functions needed to implement redundant systems. The solution can be used as-is by developers since it already has the

primary software needed for Safety MCU diagnostics, program sequence monitoring, and redundant Safety MCU mutual monitoring, and since it is already SIL3 certified based on IEC61508.

Using these solutions means developers can build a functional safety system by simply configuring the Self-Test Software and SIL3 System Software Kit, freeing them from tedious Safety MCU diagnostics and control section development for redundant Safety MCU.

In addition, the compilers used for this software must be proven to be usable in developing functional safety systems. Renesas also offers #7 CC-RX, an IEC61508 SIL3 pre-certified compiler. IAR Systems also provides SIL 3 certified compilers.

Implementing Redundant System Hardware: Reference Documents, Reference Hardware

Specific hardware is required to implement redundant structure, such as communication means for mutual monitoring between two Safety MCUs, power supply isolation and monitoring, and input/output circuit diagnostics.

Solution 6: Reference Hardware offers reference data, including power circuits for redundant Safety MCU. Another advantage of using redundant configuration is that by exchanging processing data between each side, it is possible to confirm normal operation without using any special diagnostic hardware. These hardware configurations and diagnostic techniques series are described in Solution 5: Reference Documents.

Determining whether the hardware/software being designed has reached the target safety level requires defining the hardware failure rate, diagnosis methods and the diagnosis rate, calculating various parameters using complex formulas based on reliability theory, and showing whether they meet standard values for the target safety level. Reference Documents contain completed samples of all the verification documents, with detailed explanations of calculation methods for all the parameters and the formulas offered in Excel format. With these tools, even first-time developers can proceed with assurance by simply entering in data like failure and diagnostic rates. As methods related to peripheral Safety MCU functions vary depending on the use case, the reference documents describe different diagnosis methods according to different use cases.

Implementing Application-Specific Functional Safety Equipment: Reference Documents, FSoE Application Software Kit, PROFIsafe Application Software Kit

In addition to MCU diagnostic solutions, we also provide application-level solutions that are effective for safety drive devices, safety I/O devices, and safety network devices. Reference Documents include sample documents describing hardware configurations, safety control methods, and their safety concepts as required to comply with IEC 61800-5-2, the international safety standards for electric drives. Here, we use an example of functional safety for drivers as an example. The structure is a typical functional safety device control block, of "safety input-safety control-safety output," and can serve as a reference for developing safety sensors and safety remote I/O devices with the same configuration. The Reference Documents also discuss the process of making networks safe.

Renesas also offers Solution 3: FSoE Application Software Kit, compatible with the safe version of EtherCAT, FSoE (Functional Safety over EtherCAT) as safety network software. We have also begun offering new PROFIsafe Application Software Kits, which support PROFIsafe, the safety version of PROFINET.

Recap

As shown in Figure 5, Renesas' functional safety solutions offer support for 60-70 percent of the functional safety system development, from the specification review of the concept phase to the failure analysis and diagnosis programs needed for functional safety around MCUs, redundant structure and peripheral diagnosis, system-level diagnostic software for networks and documentation for submitting these to certification bodies. This allows developers to complete a safety system independently by designing and developing device-specific parts.

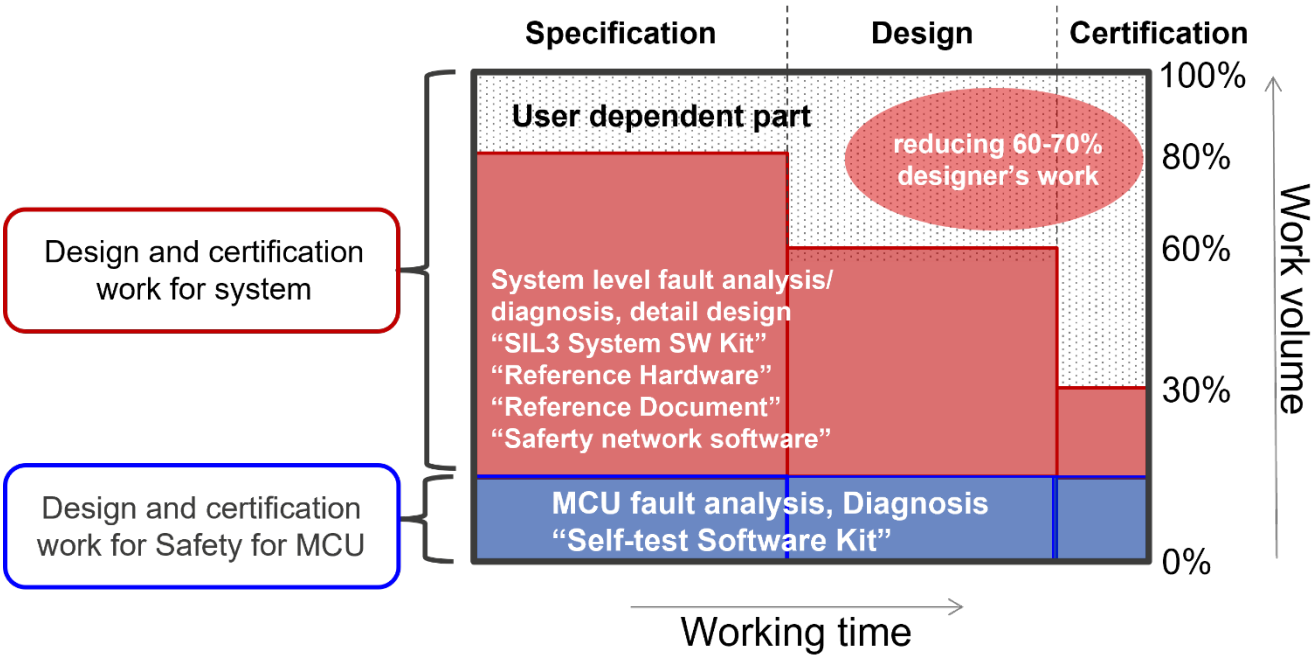


Figure 5: Cover range of Renesas safety solution

Using Renesas functional safety solutions means system developers won't be burdened by device-specific software development and certification tasks such as Safety MCU diagnostics, resulting in more system development time and reduction in overall cost. Renesas' functional safety solutions provides a faster, reliable path through the development and certification process.

Reference Materials

IEC Functional Safety and IEC 61508

Functional Safety for Industrial Automation

RX Family (32-bit MCUs)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu, Koto-ku, Tokyo 135-0061, Japan
https://www.renesas.com

Contact Information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
https://www.renesas.com/contact-us

Trademarks

Doc Number: R30WP0002EG0100