White Paper

Functional Safety of Industrial Machinery

Yasushi Nakagawa, Sr. Manager, IoT Infrastructure Business Unit, Renesas Electronics Corp.

September 2020

Abstract

In recent years, the concept of "functional safety" has become widespread in the industrial machinery sector as a method for ensuring system safety. Functional safety, long emphasized in the automobile field, is now being prioritized for industrial machinery to avoid negative impacts on factory operations (due to equipment failures/accidents) and society (through injury/workplace health issues), along with overall economic loss. Manufacturers of assembled products are increasingly offering new functional safety devices in response to end user demands, as well as to boost product competitiveness.

This white paper elucidates the basics of functional safety, including its emerging role, actual system configurations, development issues, and functional safety solutions offered by Renesas.

What is Functional Safety?

Functional safety aims to use “functions” to ensure that risk of damage to humans, property, or society caused by equipment malfunction or operational error remains below the permissible limit. For example (as shown in Fig. 1), a person entering a factory area where a robot operates risks injury through collision with the robot arm. The most common prevention is to surround the robot with a fence-like guard, as shown in Step 1 (pg. 2); however, an individual could enter through a door carelessly left ajar, or by climbing over the guard, thereby allowing an accident to occur. An additional protective method, as shown in Step 2, uses a sensor detecting intrusion, which then triggers the robot to terminate operations, further reducing risk. This method then adds safety devices, such as a sensor detecting a hazard or an apparatus halting the robot, to avoid danger. These safety devices are the equipment that provide functional safety.

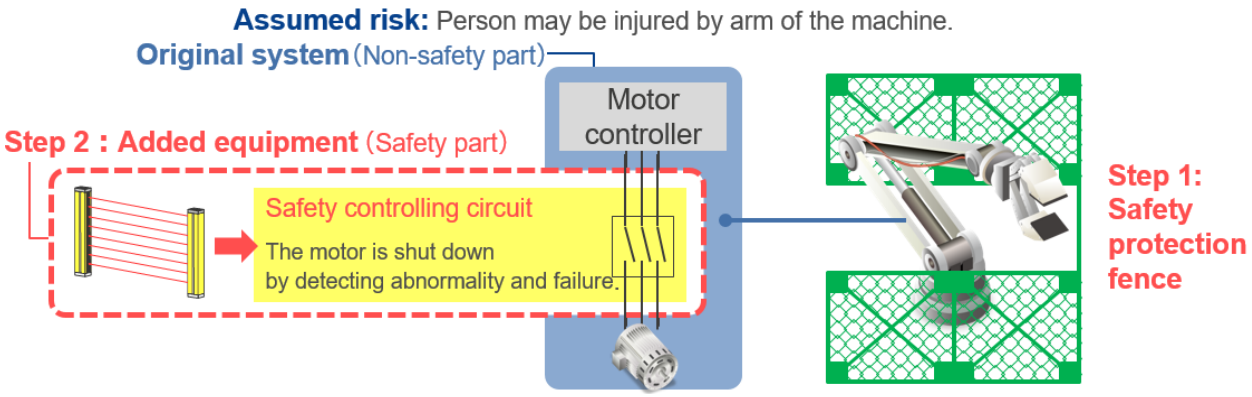


Figure 1: Functional Safety Concept

For further insight, let us examine the configuration of a motor control device which stops a robot motor for hazard avoidance. Fig. 2 shows an example of functional safety in which a system controls the rotation of the motor with an MCU. To realize functional safety, we first analyze the equipment-related risk, then consider countermeasures. This process is called risk assessment. The resulting safety measures are implemented as functional safety devices (or simply “safety devices”) using electronic circuits, etc. At this stage, the key difference between conventional and functional safety devices is that the latter are developed to realize objective and quantitative methods that meet safety device specifications defined by IEC 61508 and other international standards.

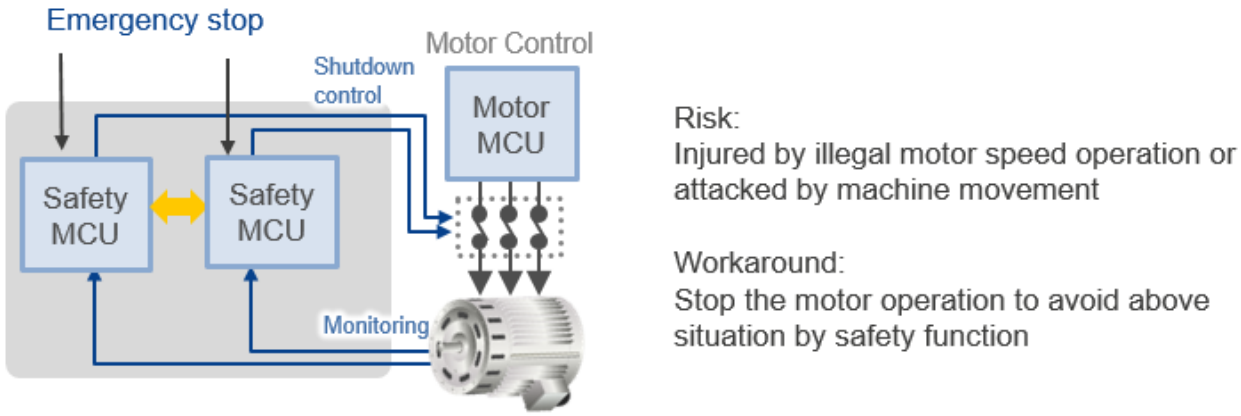


Figure 2: Example of Safety Motor Drive System

Specifically, malfunctions from safety device failure are analyzed and measures implemented based on the diagnostic function that ensure a safe state even when failure occurs. In addition, design methods and processes are stipulated to avoid malfunction due to bugs created during the software or hardware design stage. This makes it possible to judge safety specifications and safety device operational reliability more objectively. In addition, a redundant MCU configuration ensures that even if one MCU malfunctions, the other will sustain normal functions, ensuring reliable and safe operations.

Industrial Sector Functional Safety System: Example

Three key components in FA systems - safety drive, safety I/O, and safety network systems - help clarify system configurations in specific applications.

Fig. 3 shows a sample system configuration for functional safety in which the motor drive is stopped when a safety sensor detects intrusion. This FA system is comprised of a safety sensor or other input device, a safety PLC (programmable logic controller) device for overall control, a safety drive to run the actual equipment, and a safety network that connects all the components. The internal configuration, as shown in Fig. 2, features a redundant MCU structure consisting of two MCUs. This mechanism is required to ensure the safe operation of the machinery. Even if a failure occurs somewhere within the system, the MCU on the side operating normally will implement a process to avoid a dangerous outcome. These are common configurations used for functional safety devices in FA.

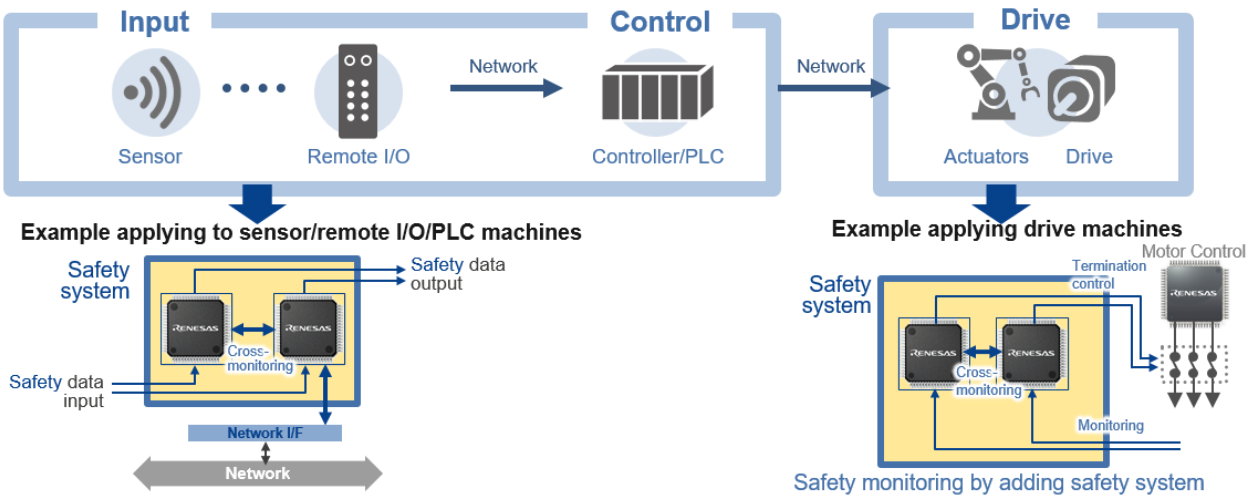


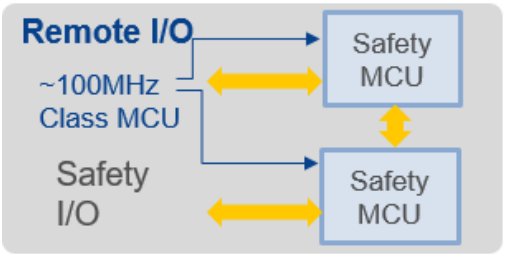
Figure 3: Example of Safety FA System

Next, we describe each device comprising these safety FA systems.

Safety Drive Devices

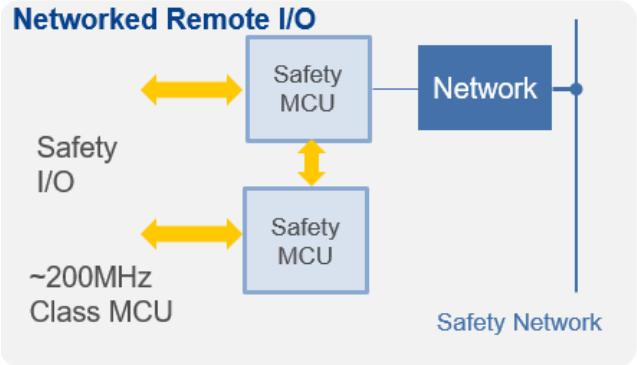
The basic safety specifications of the drive component are achieved by monitoring whether the motor is safely controlled. As shown in Fig. 2, in general, a unit for monitoring safe motor operation is externally attached to the mechanism rotating the motor. This monitoring unit checks the motor speed and other potential hazards that might require the "emergency stop" signal to be activated to stop the machinery. If a state is judged to be dangerous, an emergency stop signal is sent to the motor control side. In this example, the redundant safety MCUs are used to monitor information about the Emergency Stop and motor speed. In the event of a failure, the safety unit outputs a Termination Control command to cut off power to the motor. That signal is transmitted to the motor stop circuit, power is terminated, and safety is ensured. Moreover, because this is a redundant configuration, even if the monitoring unit itself fails, one of the safety MCUs should be operating normally and can shift to safe operation mode. There are several types of motor monitoring and motor termination methods to meet the varying needs of FA systems. Their specifications are defined in IEC61800-5-2, the safety standard for motor drive equipment.

Safety Remote I/O Devices



Safety-related remote I/O devices control safety operations via signal output to components that implement emergency stops in response to input signals from safety sensors and other trigger devices. Basically, the alarm signal from the safety sensor is sent to the input section of the safety remote I/O device, and after performing a simple logical calculation, the signal is emitted from the output side and input to the emergency stop signal section of the motor drive device. Safety remote I/O internal configurations also utilize the redundant MCU mechanism, ensuring safe operations even if safety devices fail. Also, by running the safety function program on both MCUs, the same configuration can realize a safety PLC (mainly low-end type) as well.

Networked Safety Remote I/O Devices



As the term infers, networked safety remote I/O devices are simply safety remote I/O devices that include a network function. In addition to using two safety MCUs and safety I/O processing, this method also processes transmitted safety data according to safety network standards. The network device is called a “Black Channel” and is included in the non-safety-related part of the system. Although Black Channel indicates an unreliable communication path, the safety protocol standardized by the safety network has a method for confirming that data sent via the Black Channel was transmitted correctly. This method is realized by confirmation using the two safety MCUs.

Issues in Functional Safety System Development

Functional safety system development embodies three phases: Introduction and Concept; Detailed Design, Trial and Function Evaluation; and Main Inspection and Certification (by a 3rd party). It also involves technical requirements and processes not found in conventional development.

The basic development flow for creating a functional safety system is shown in Fig. 4. In the Introduction and Concept Phase (upper section), once basic knowledge of functional safety standards and MCU specifications are secured, a “safety analysis” is conducted to examine risks, determine hazard avoidance methods, and formulate a concept for examining detailed safety system specifications. Also, required documents need to be generated and submitted for review by the appropriate certification authority. Preliminary discussion of safety system specifications at this point will enable their realization in the subsequent detailed design and trial evaluation phase. Following review by certification authorities, the flow proceeds to the detailed Design and Trial Production Evaluation Phase, where detailed hardware and software designs are evaluated based on the specifications defined in the concept phase. This series of design processes must follow the development process required by the international standard IEC 61508 for functional safety. When designing a system, an accurate grasp of the meaning of the functional safety standard must be obtained before proceeding to development. This stage includes analyses of hardware failures and related diagnostic methods, and incorporation of an appropriate development process to avoid potential software defects. All tasks require documentation for each design process, as well as calculation of the achieved safety level based on the failure rate and diagnostic rate of the system, along with other requirements not found in the conventional development process.

Once the Detailed Design and Trial Production Evaluation Phase is completed, the flow proceeds to the Main Inspection & Certification Phase. The contents of design evaluations are submitted to the certification authority and, if necessary, a witness test is conducted. If the content is approved, the system will be certified.

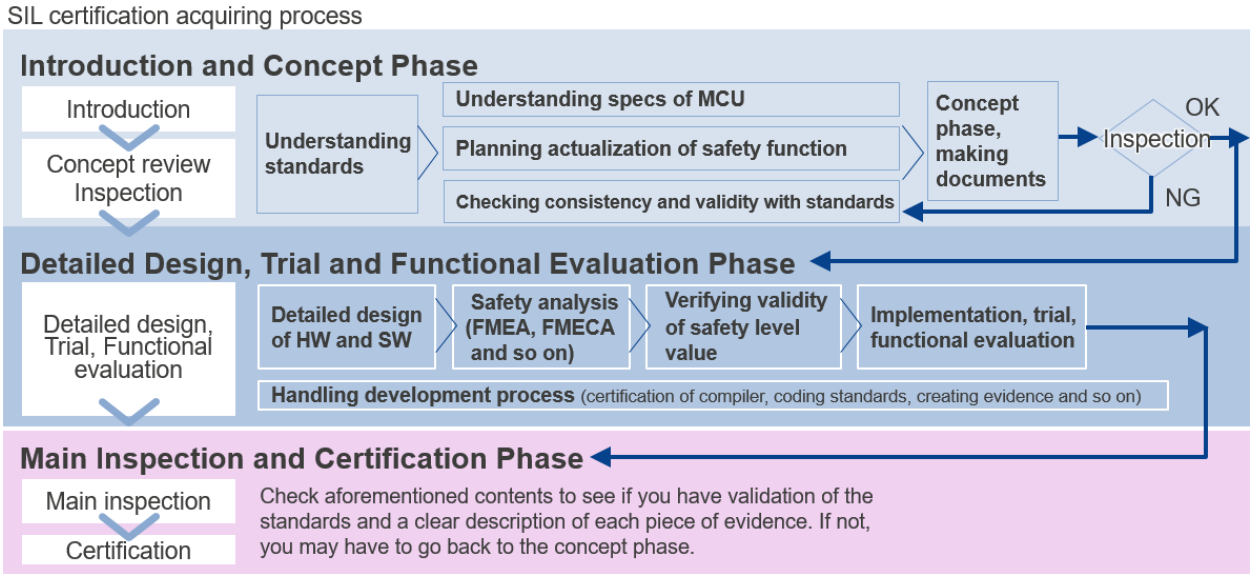


Figure 4: Functional Safety System Development Process

Renesas Proposals for Functional Safety System Development

The technical challenges faced by developers advancing toward functional safety standard certification for these systems include the following:

1） How to generate each document required for certification and how to calculate parameters for verification of system FMEA and SIL targets

2） Generating failure diagnosis software such as MCU self-diagnostics and mutual monitoring for a redundant system configuration consisting of two MCUs

3） Developing the hardware configurations for a redundant, two-MCU system (mutual monitoring communication, I/O circuit diagnosis, power supply diagnosis)

4） Achieving functional safety mechanisms that meet application requirements (motor shutdown mechanism, motor speed detection encoder, safety network, etc.)

Renesas offers functional safety solutions for solving the issues faced by developers when creating functional safely systems, as listed below.

Fig. 5 introduces six solutions offered by Renesas to support functional safety system development, with descriptions of how each issue can be resolved.

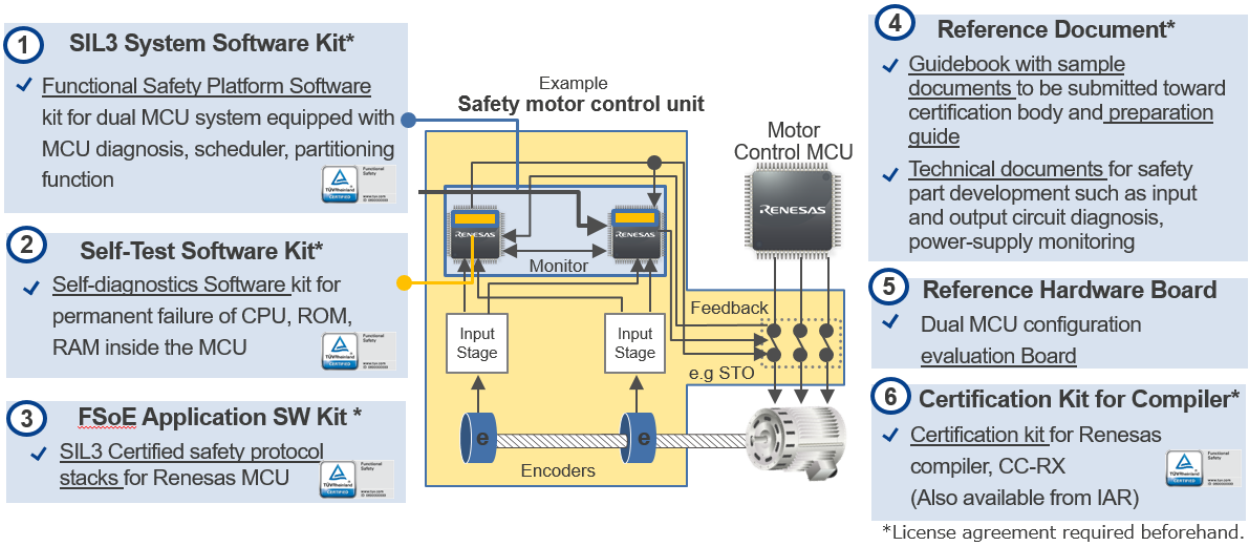


Figure 5: Renesas Functional Safety Solution

✓ How to generate various documents for certification: Reference Documents (4)

In the concept phase during which specifications are examined, the first task in the development of a functional safety system is generating the required documentation, including Safety Requirements Specification (SRS), Safety Concept (SC), Safety Plan (SP), and Verification & Validation (V&V). Trying to create these documents successfully can be a lengthy and costly process for those without prior experience in obtaining certification. The Reference Documents solution (4) provides a concrete description using a safety system for motor drive devices as an example, along with all the necessary documents required in the concept phase. Utilizing these templates, the user can revise the specification data to meet each development, thus avoiding the omission of required information.

✓ Creating redundant system diagnostic software: Combining SIL3 System Software Kit (1) and Self-Test Software Kit (2)

To avoid a malfunction due to a hardware failure, the safety function in a functional safety system must perform failure diagnosis. The diagnosis should detect failures in any of the system devices, as well as malfunctions due to soft errors generated by radiation or noise during operations. In the event of an abnormality, the system must immediately shift to safe operation, such as stopping the motor. A failure diagnosis of each device requires the failure mode of each to be analyzed, each failure detection method examined, and the failure detection rate (diagnosis rate) for each method defined. In addition, soft errors must be detected by monitoring the execution sequence of the program and detecting errors using systematic behavior with methods such as mutual comparison using MCU redundancy; however, defining failure detection methods and corresponding diagnostic rates for complicated devices like MCUs can be a considerable burden for device developers. Implementing MCU intercommunication to enable program sequence monitoring and mutual comparison based on functional safety standard requirements adds to that burden.

The Self-Test Software Kit (2) provides a self-diagnostics program that detects MCU failures, realizing the 90% diagnostic rate required to achieve SIL3 as stipulated in the IEC 61508 standard. The SIL3 System Software Kit (1) includes the software required for redundant systems, such as mutual monitoring and program sequence monitoring. As most of the software required for MCU diagnosis, program monitoring and redundant MCU mutual monitoring is already integrated into the two kits and is SIL3 certified based on IEC 61508, ready for developers to use as-is.

Taking advantage of these solutions, developers can develop functional safety systems simply by building application programs required for the safety system on the pre-certified self-test software and SIL3 system software. Eliminating the troublesome step of establishing MCU diagnostics and creating the redundant MCU control section frees up valuable development time.

✓ Realizing redundant system hardware: Reference Documents (4) and Reference Hardware board (5)

The redundant configuration requires a communication method for mutual MCU monitoring, power supply isolation and monitoring, input/output circuit diagnostics and other specialized hardware. The Renesas Reference Hardware Board solution (5) provides reference data that includes a redundant MCU power supply circuit. One merit of using the redundant configuration is that the exchange of processing data eliminates the need for dedicated diagnostic hardware, enabling the confirmation of normal operations. All hardware configurations and diagnostic methods are described in Reference Documents (4).

To determine whether the designed hardware and software have reached target safety levels, one must define the hardware failure rate, and its diagnostic method and rate. Parameters calculated using a complex equation based on reliability theory are necessary to prove whether the system meets the standard values corresponding to the target safety level. Samples of certification documents and the calculation methods of various parameters are detailed in Reference Documents (4), with the equations provided in a usable Excel spreadsheet. These helpful hints and documents enable even a first-time developer to enter the failure and diagnostic rates into the data charts, expediting the certification process. Note that methods for MCU peripheral functions differ according to each usage case. Diagnostic methods for various usage examples are also included in the Reference Documents.

✓ Realizing Safety Functions for Specific Applications: FSoE Application Software Kit (3)

Renesas also offers effective solutions for safety motor drives, safety I/O systems, and safety networks at the application level. Reference Documents (4), for example, include sample documents for hardware configurations, safety control methods, and corresponding safety concepts to meet the IEC 61800-5-2 drive system safety standard. Functional safety for drives serves as an example, but the configuration’s processing blocks for general functional safety machinery (safety input - safety control - safety output) also apply to the development of safety sensors and safety remote I/O devices. Reference Documents also describe safety systems for networks. Finally, the FSoE (Functional Safety over EtherCAT) version includes the FSoE Application Software Kit (3) as a solution integrating protocol stack and the MCU diagnostic unit.

Conclusion

Renesas functional safety solutions, as mapped out in Fig. 6, support 60 to70 percent of all functional safety system development aspects. These include specification review in the Concept Phase, failure analysis and diagnostics programs for overall MCU functional safety, redundant configuration and peripheral testing, and system level diagnostic software for networks, etc., as well as guidance for the generation of documentation required by certification authorities. These solutions make it easier for developers to build safety systems for machinery by designing and developing device-specific parts.

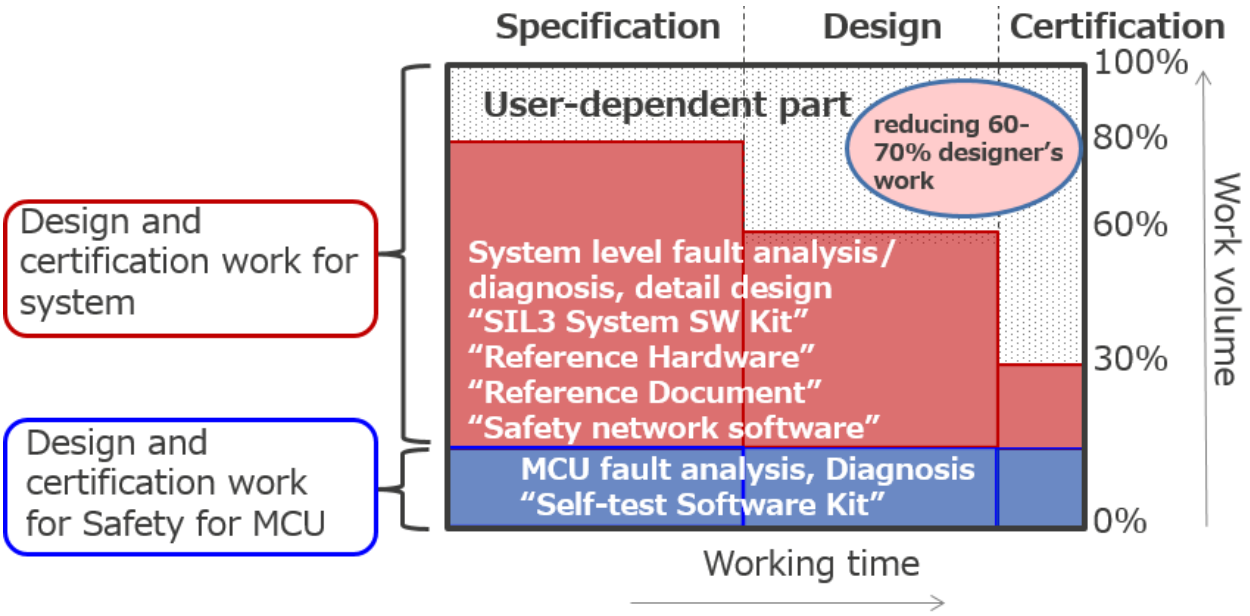


Figure 6: Value of Renesas Safety Solution

Renesas functional safety solutions free the system developer from having to develop and verify device-specific software such as MCU diagnostics, promoting more effective time/cost usage in system development. The solutions also provide a reliable shortcut for completing the cumbersome development certification tasks required in developing functional safety systems.

References

1. IEC's Functional Safety and IEC 61508
2. Functional Safety Solutions for Industrial Machinery
3. RX Family (32-bit MCUs)