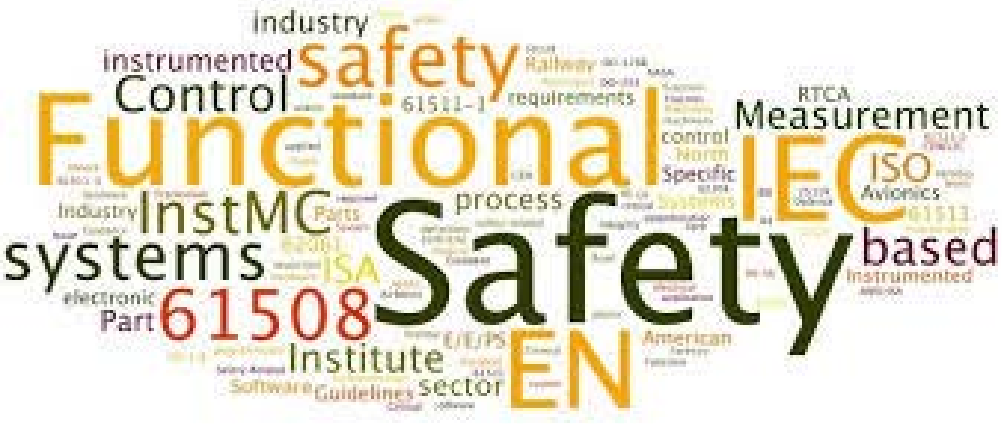
RENESAS FUNCTIONAL SAFETY SOLUTION INTRODUCTION
(IEC61508 COMPLIANCE)

SEP, 28TH, 2022,
JOHNSON TAN
RECN MCU BIZ DEV
RENESAS ELECTRONICS (CHINA) CO., LTD



AGENDA

- IEC61508 COMPLIANCE FUNCTIONAL SAFETY INTRODUCTION
- MARKET TREND & TARGETS APPLICATION
- CHALLENGES OF DESIGNING FUNCTIONAL SAFETY
- RENESAS SOLUTIONS TO ADDRESS CHALLENGES
- WORKING WITH RENESAS
- KEY TAKEAWAYS

TODAY'S FOCUS
IEC61508 FUNCTIONAL SAFETY

Segment Example	Safety standard (Safety level)	Renesas Safety Activity			
		Renesas MCU	Certify body	Safety level	Notes
Automotive	ISO 26262 (ASIL A-D)	RH850	NA	ASIL D	Self certification by Renesas (certificate from 3rd party body is not required in ISO26262)
Industry	IEC 61508 (SIL 1-4) SIL1-3: FA/PA SIL4: train, infrastructure	RXv1, RXv2, RXv3, RA CM4 RA CM23/33 ('22)	TUV	SIL3 (FA/PA)	EU directive forces certification to be done by certified body.
Home Appliance	IEC 60730 (Class A/B/C) A: Lighting B: Washing machine C: Burner	RL78 RX Synergy	VDE	Class B (appliance)	

Today's Focus

WHY FUNCTIONAL SAFETY MATTERS ?

People make mistakes and Machines break down

- In industrial automation, mission of functional safety is to equip products with safety measures to deal with possible failures before releasing products to the market.
- With more Industrial applications been automated, there is an increased need to incorporate measures into the equipment to prevent or minimize human life and social loss.
- IEC61508 is the representative safety standard in the industry having Safety Integrity Level (SIL) ranging from SIL 1 to SIL 4. Today, SIL3 has become the standard for industrial equipment.

Third-party certification is always required

No self-declaration

Why IEC61508 matters for us ?

1. This matters for both our customer and Renesas since the target covers safety systems using electrical/electronic/programmable electronic devices a.k.a. MCUs, MPUs, ASICs, and FPGAs.
2. IEC61508 specifies hazards that occur when safety functions fail and defines reducing the failure risk to a tolerable level.

Renesas offers functional safety solutions under the IEC61508 SIL3 standard since 2014.
Renesas solutions are already certified by TUV Rheinland.

WHAT IS IEC61508?

1. The standard covers safety-related systems incorporating electrical/electronic/programmable electronic devices such as MCUs, MPUs, ASICs, and FPGAs.

2. The standard specifically covers hazards that occur when safety functions fail.

3. The main goal of the safety standard is to reduce the failure risk to a tolerable level. However, to develop a solid safety system can be a very complex process.

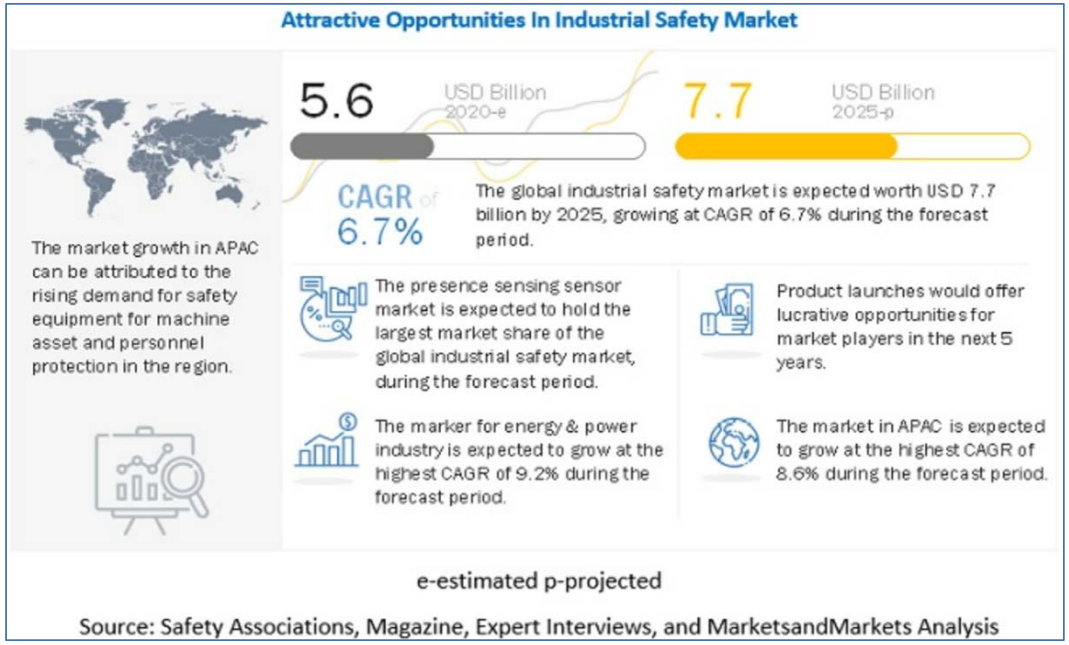
Renesas has offered functional safety solutions under the IEC61508 standard since 2014. The solutions from Renesas are certified by TUV Rheinland.

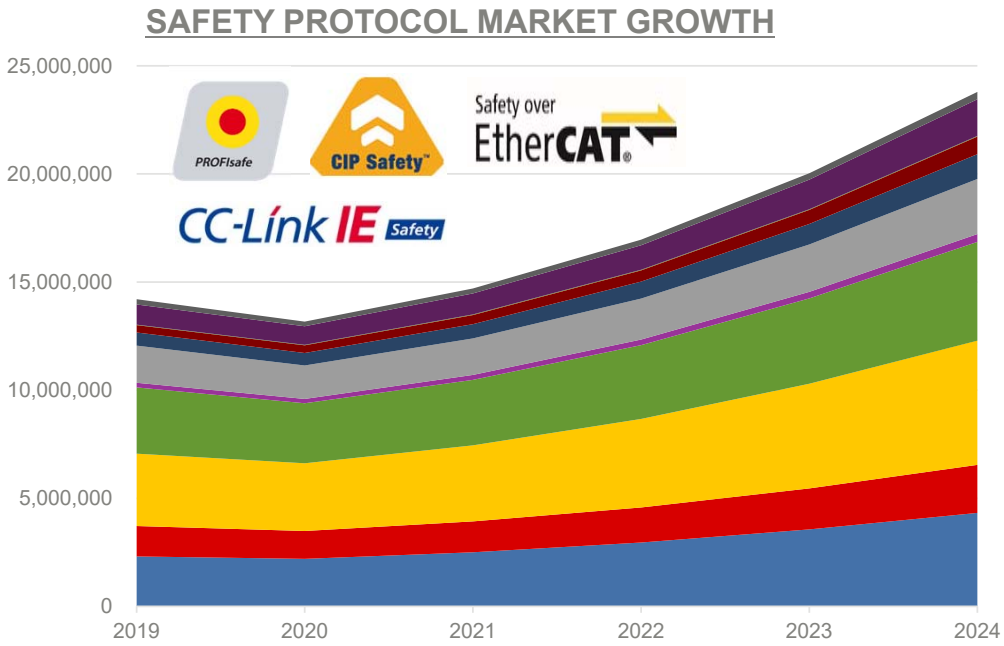
MARKET TREND & TARGET APPLICATION

FUNCTIONAL SAFETY TREND

	Safety application market
Past	• Safety system been implemented by simple (discrete / mechanical) system. • The market were limited in EU and been occupied by EU suppliers (over 50%) of the safety market share.
Today	• Industrie 4.0 & IIoT trend pushed systems to be controlled by MCU/SOC for smarter control & communication, as well in the functional safety system. • Functional Safety been installed globally since this been a fundamental system for smarter factory. Today, Japan, Taiwan, and China suppliers are increasing their share by releasing Safety integrated system in the market.
Tomorrow	• The industrial safety market is expected to grow globally at CAGR of 6.7% (’20-’25)*1, especially in APAC with CAGR of 8.6% (’20-’25)*1. • In addition, Safety network protocol installation are growing from 14M Nodes to 24M Nodes (‘20-’24*2) since the machines are connected via network.

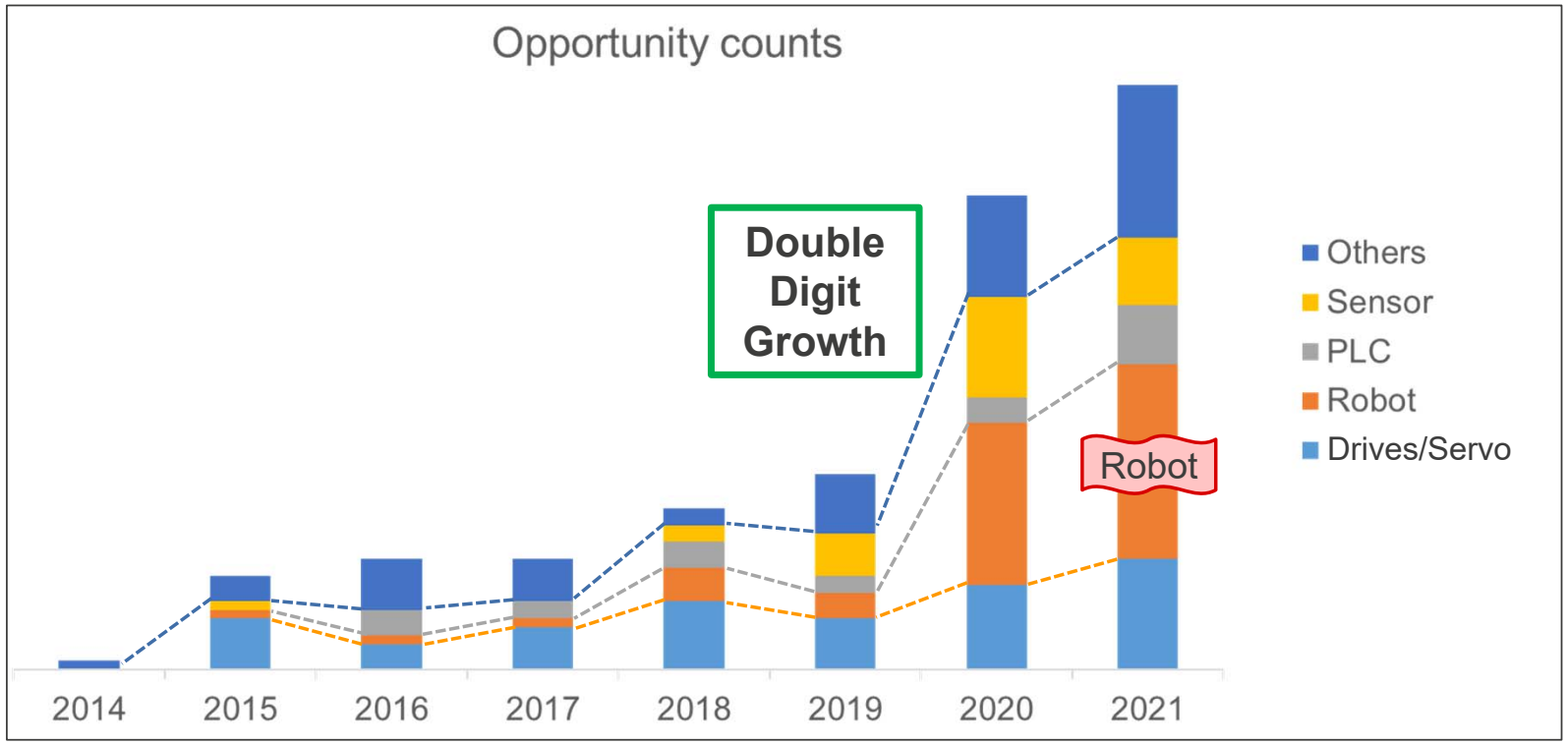
FUNCTIONAL SAFETY MARKET FUTURE





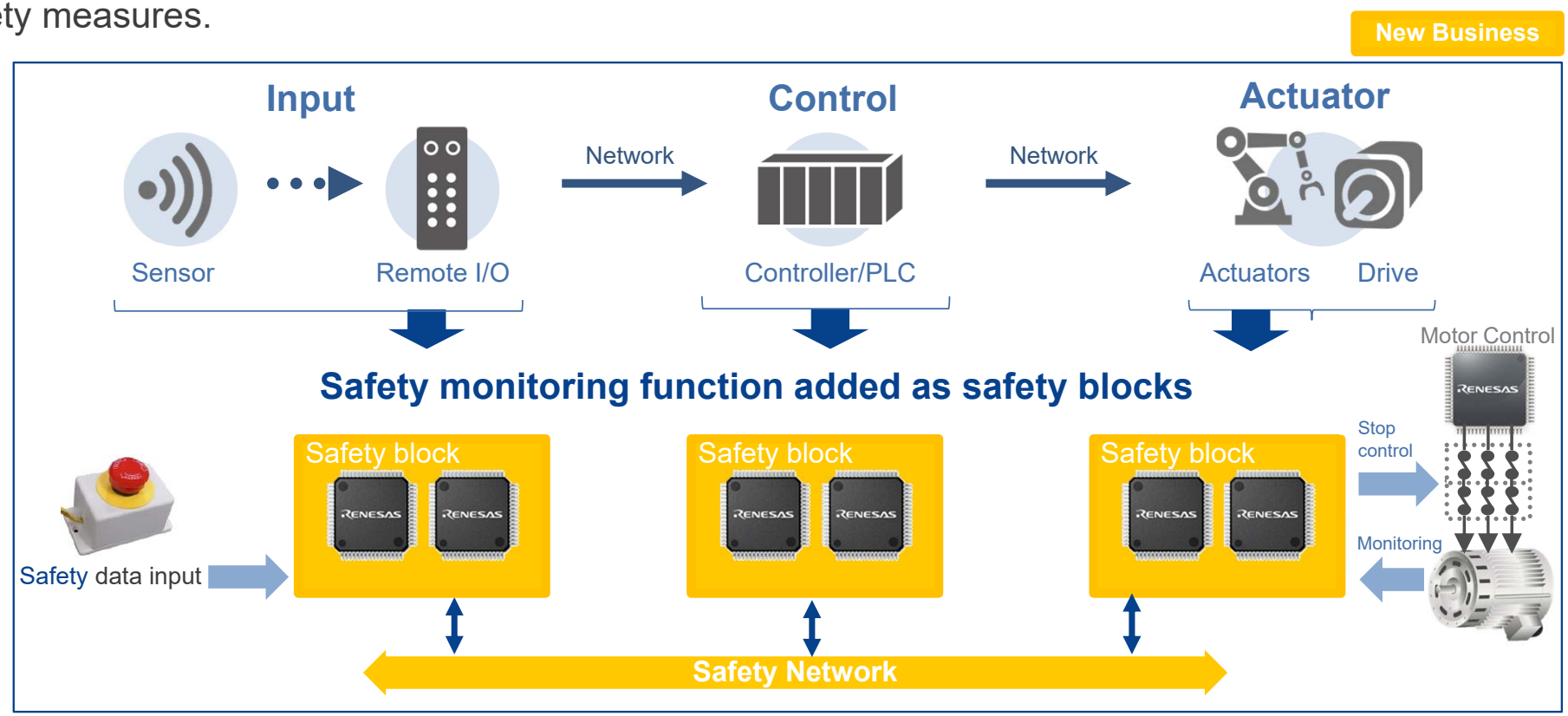
SAFETY APPLICATION TREND

- ✔ Renesas safety business is mainly applied to all major applications such as Robot, Drives/Servo, PLC, and Sensor.
- ✔ Recently, the needs in Robot application is increasing.



TARGET : SAFETY APPLICATION FOR INDUSTRIAL AUTOMATION

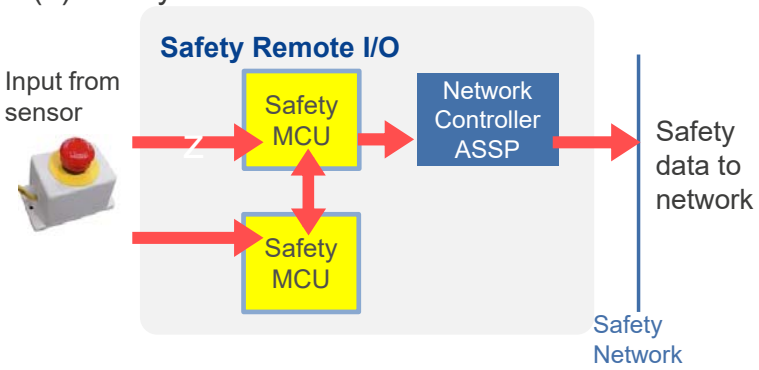
- Functional safety is applied to each machine in Factory Automation & Process Automation system for safety measures.



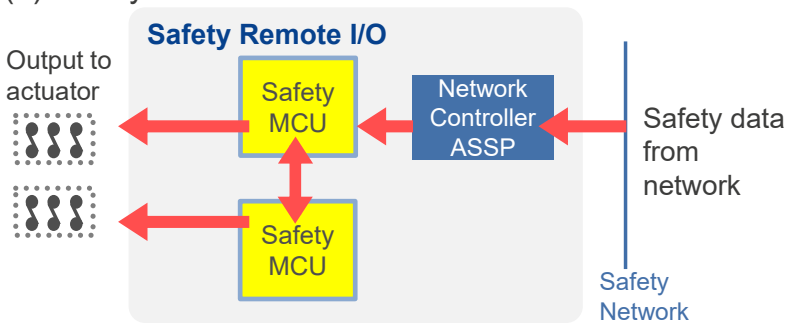
APPLICATION EXAMPLE

Safety Remote I/O

(1) Safety data from sensor to network



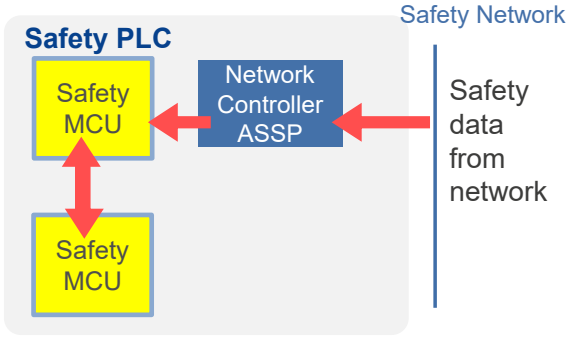
(2) Safety data from network to actuator



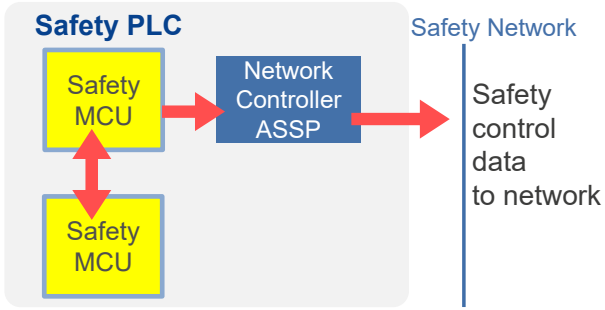
: Data flow

Safety PLC

(1) Input safety data from network

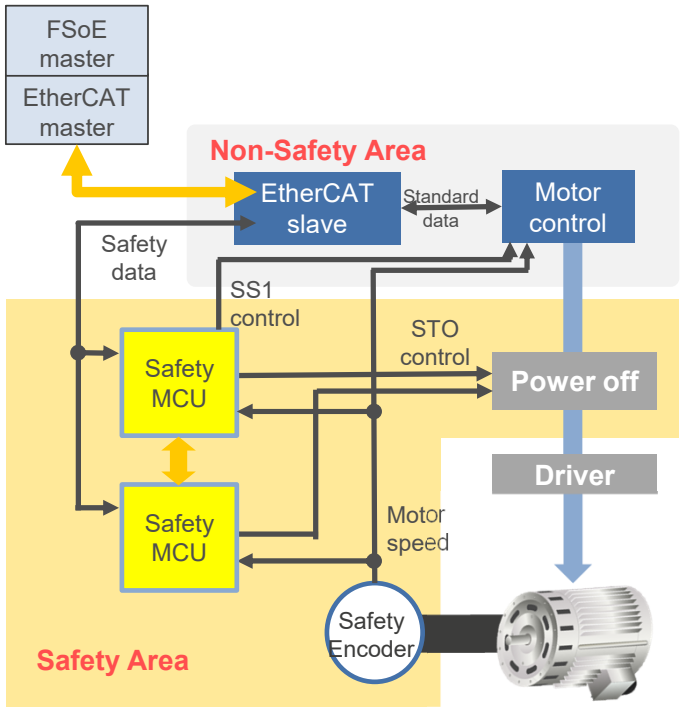


(2) Output safety control data to network



: Data flow

Safety Servo drive with Safety Network (FSoE)



OTHER SAFETY APPLICATIONS

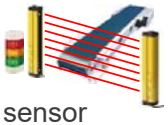
FA and PA (IEC61508, others)

PLC(controller)

AC servo/Inverter
Robot, PressMachine

DCS(plant controller)

Remote I/O



FA sensor

PA sensor

Service Robot (ISO13482)

Bed equipment

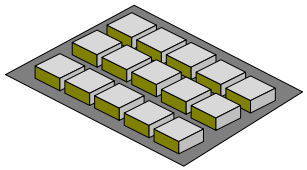
Electric cart

Transport robot

Automatic Door (EN16005)

Battery System (IEC62133, others)

Household fuel cell



Indoor storage battery

Motor assist cycle (EN15194)

BA

Alarm machine

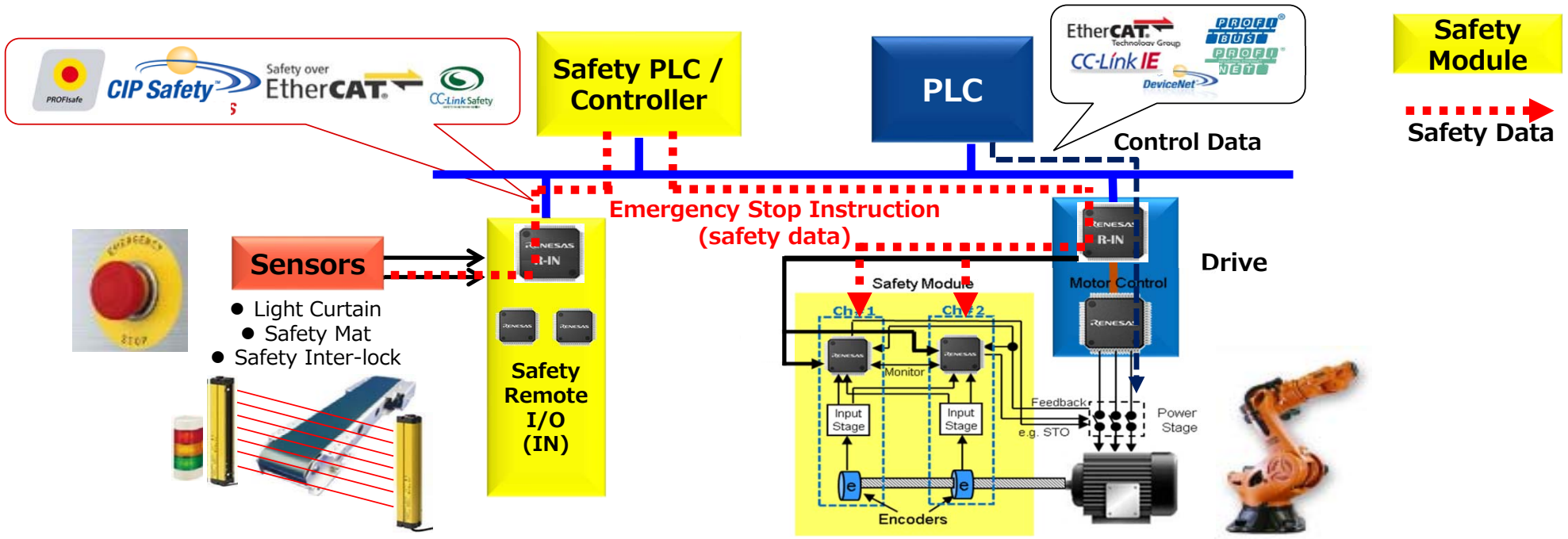
Printer

Office printer

Production printer

SAFETY SYSTEM OVERVIEW

- Today, machines are connected via industrial ethernet between sensors, PLC, and/or drives.
- Because each system is controlled and monitored over the network, both the system and the network protocol itself must have safety controls.



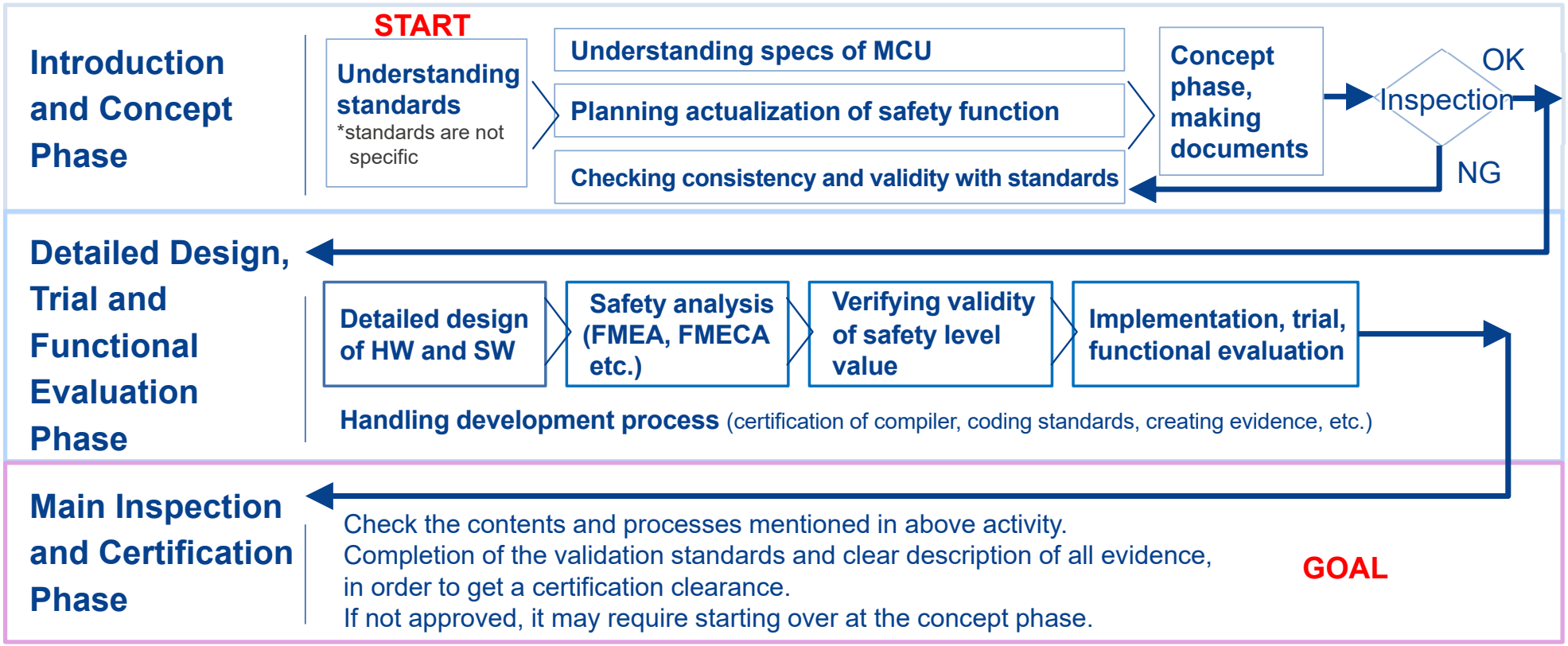
CHALLENGES OF DESIGNING FUNCTIONAL SAFETY

Page 14

IEC61508 CERTIFICATION PROCESS

Long process/High cost from Development **Start** to Certification

SIL certification process : Long Process / High cost from development start to certification.



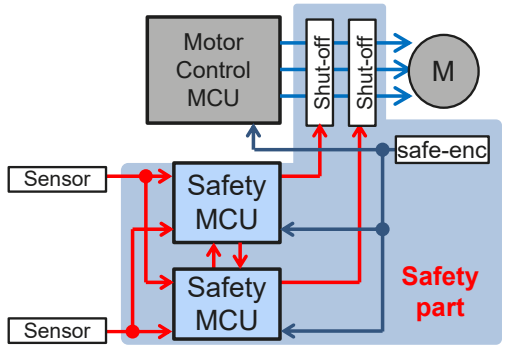
ISSUES ON FUNCTIONAL SAFETY SYSTEM DEVELOPMENT

Starting development from scratch leads to significant cost increase

Increased certification cost

- Attend functional safety seminar
- Negotiation with the certification body
- Concept inspection
- Safety software inspection
- Safety hardware inspection
- Documents inspection
- Development process inspection
- Recertification when changing software/hardware

Increased parts cost



Additional safety circuit

Increased development time

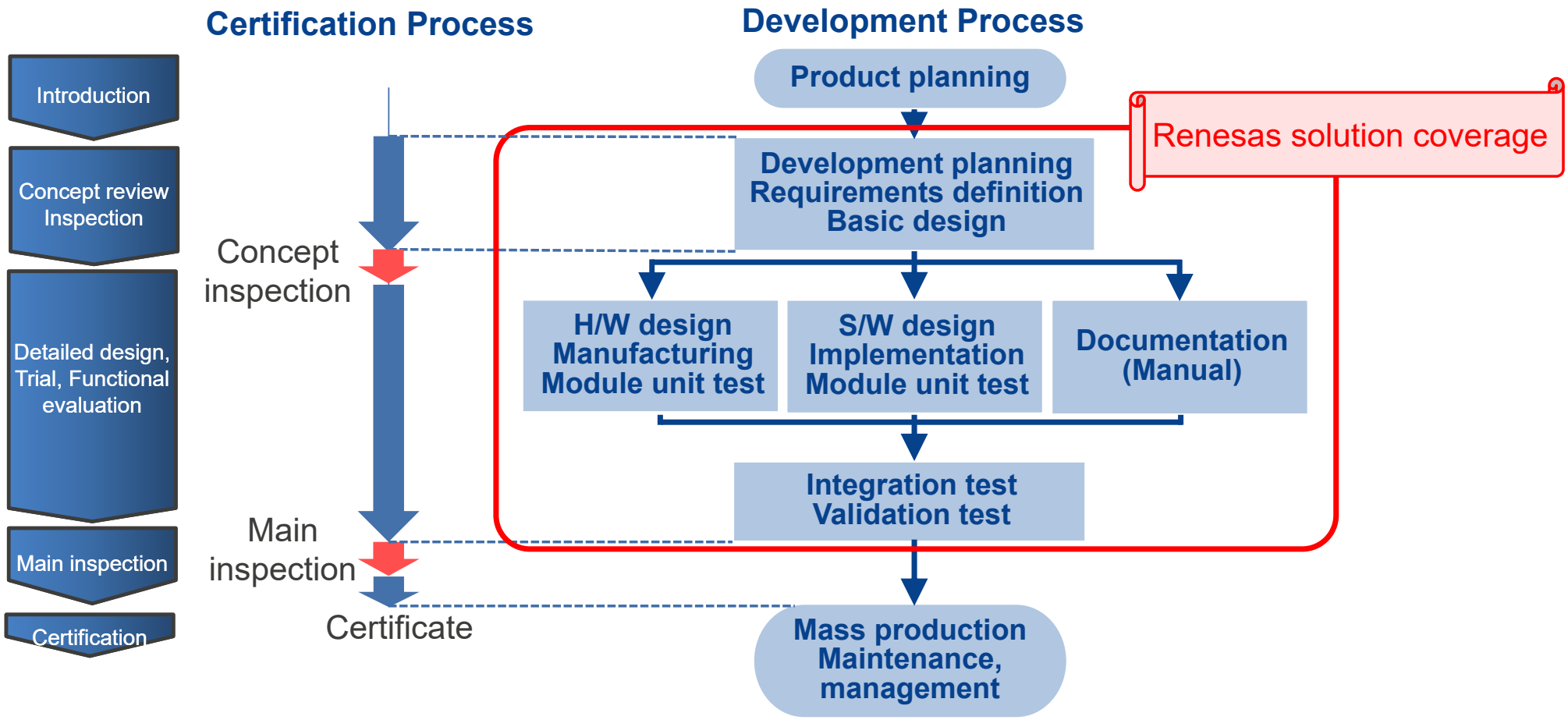
- Understanding functional safety standards
- Understanding MCU specifications
- Examination of MCU diagnosis method
- Examination of peripheral function diagnosis method
- Writing documents for certification
- Design, development and evaluation of safety software/hardware
- Repeated trial production

RENESAS SOLUTIONS TO ADDRESS SAFETY SYSTEM CHALLENGES

HARDWARE (HW) AND SOFTWARE (SW)

Page 17

PROCESS FOR FUNCTIONAL SAFETY SYSTEM DEVELOPMENT



HARDWARE PROPOSAL
MCU SAFETY SYSTEM ARCHITECTURE

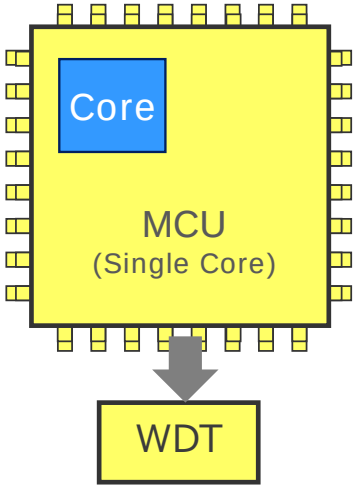
Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode or continuous mode)	1
4 (any mode)	2

IEC61511-2016

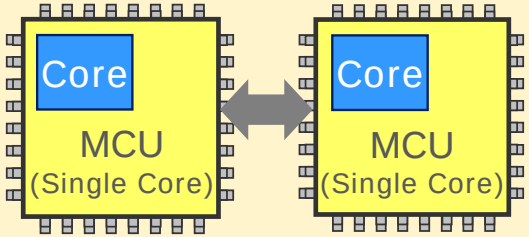
- SIL3 can be achieved by using an MCU dual configuration using general purpose MCUs.

Single MCU Configuration
(SIL2 on HFT=0)



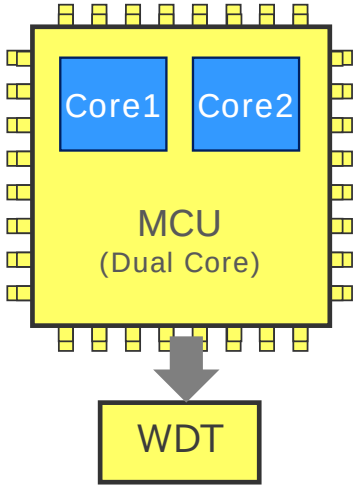
Dual MCU Configuration
(SIL3 on HFT=1)

Best Architecture



The dual configuration enables:
1. Simple safety verification
2. Decreased diagnostic frequency
3. Improved system performance

Dual Core & Single MCU Configuration
(SIL3 on HFT=0)

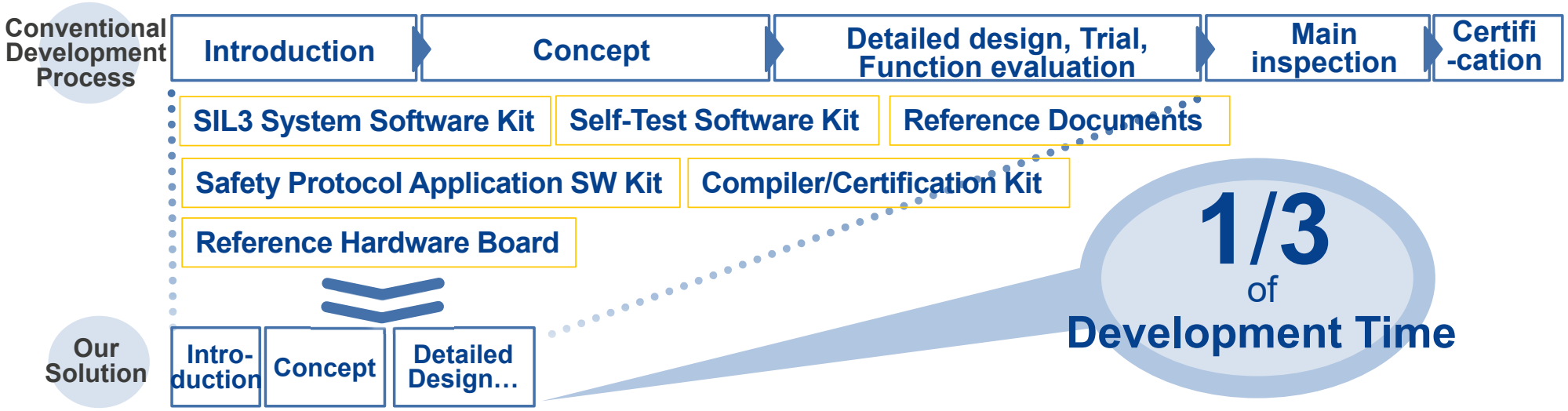


HFT : Hardware Fault Tolerance ["HFT=1" means that the safety function is not lost even if the system on one side fails]

SOFTWARE PROPOSAL

SAFETY SOLUTION TO SHORTEN DEVELOPMENT AND CERTIFICATION PROCESS

- Renesas certified functional safety solutions will shorten safety system development with Renesas MCU.
- This means customer can focus on the application development.



RENESAS FUNCTIONAL SAFETY SOLUTION

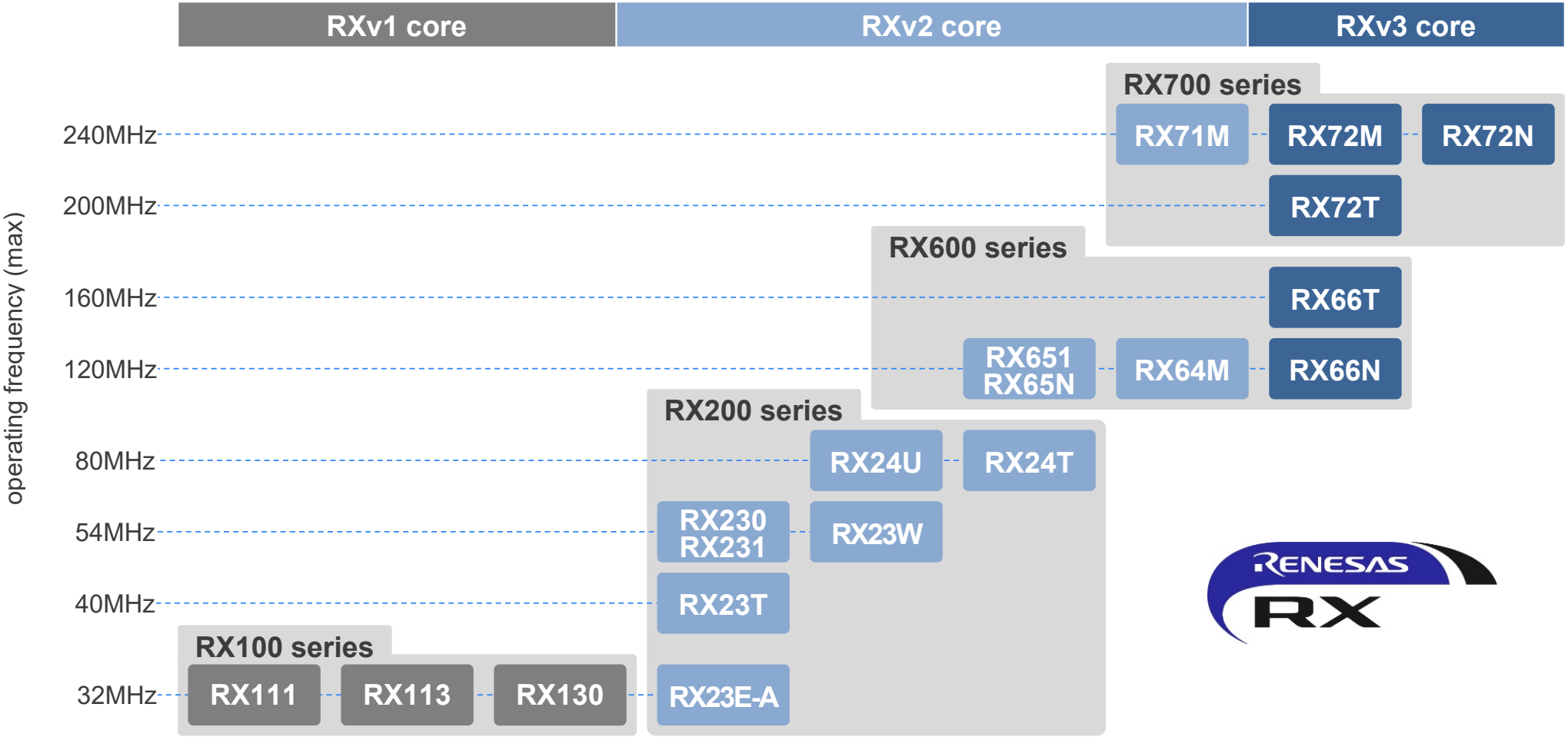
SOLUTION VALUE

1. Shorter TTM : Eliminate certification cost related to MCU for faster TTM.
   - Shortens the time for safety SW development for MCU
   - Shortens the time to preparing the certification process document to Certifier
   - Support the process of the certification phase

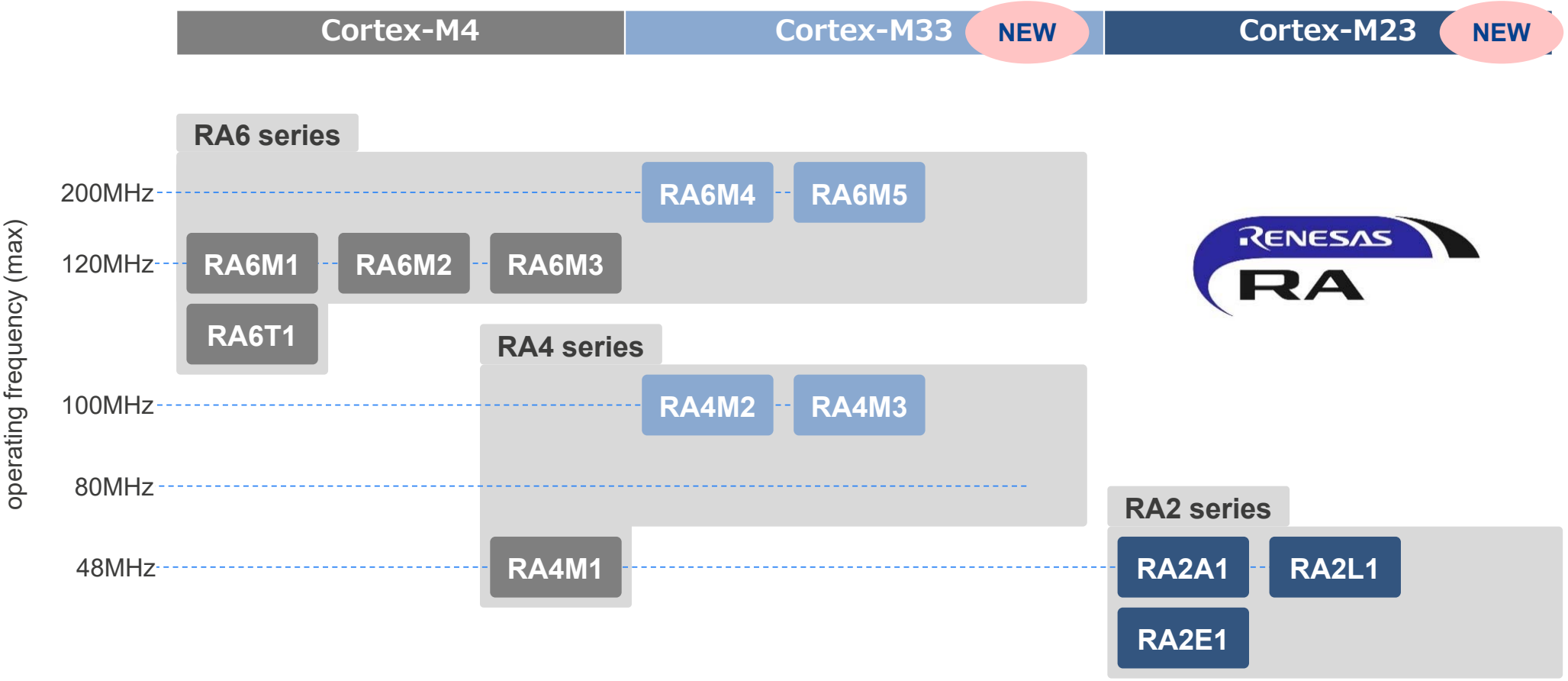
2. Simplify communication & system development : One stop shop from Renesas of MCU plus Certified SW combination.
   - gives all size (big, medium to small size) customer to develop safety system at lower cost compared to conventional system development involving IDHs.

3. Lower entry barrier : educational content ready.
   - Reference solution and certified SW best-fit to customers who will start functional safety design.

EXPANDING LINEUP OF RX FOR FUNCTIONAL SAFETY



EXPANDING LINEUP OF RA FOR FUNCTIONAL SAFETY

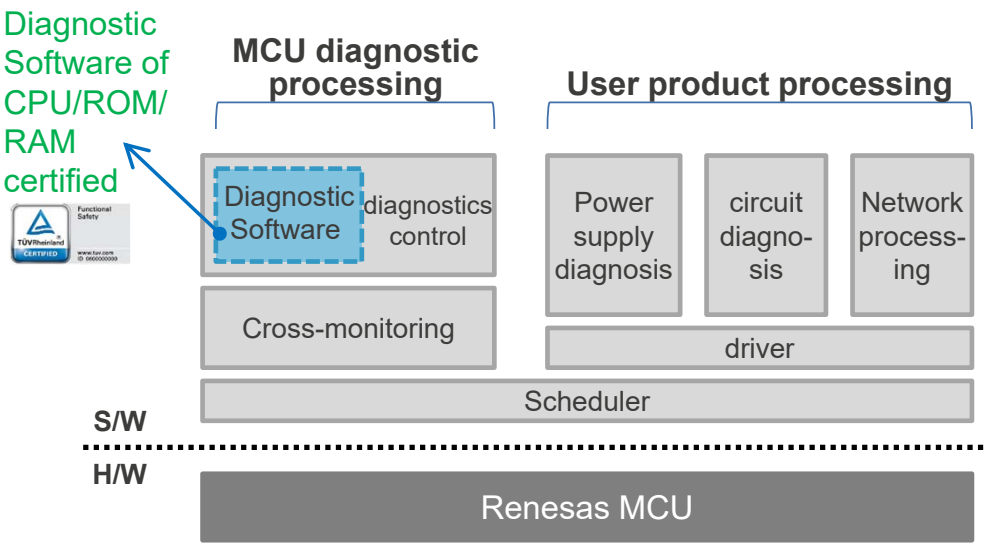


Shorten Certification Process

FUNCTIONAL SAFETY SW DEPENDING ON CUSTOMER NEEDS

Diagnostic Software

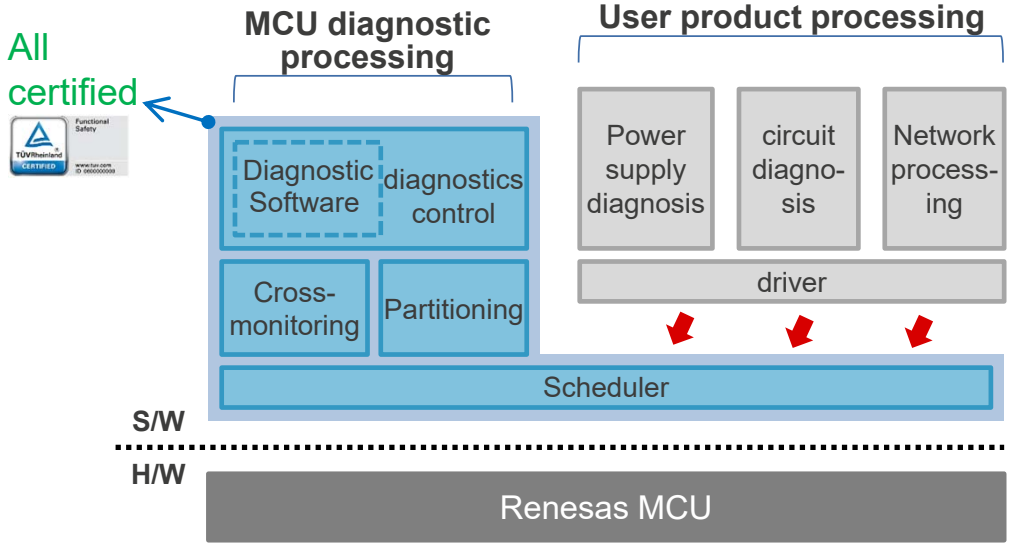
- All Software development and certification work is required except for Diagnostic Software



Product name : Self-Test Software Kit

Function Safety Platform Software

- Functional safety platform S/W carries out all diagnostic processing required for safety MCUs such as self-diagnosis and cross-monitoring, etc.
- User only need to develop user product processing software

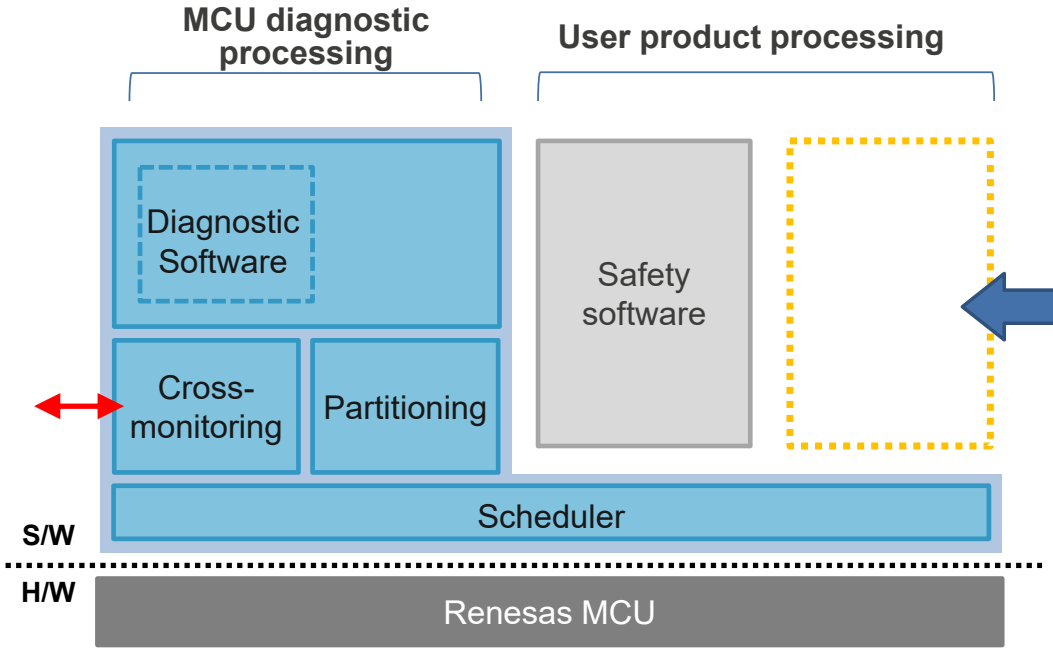


Product name : SIL3 System Software Kit

Shorten Certification Process

SAFETY NETWORK SOFTWARE

Multi-protocol using Functional Safety Platform Software

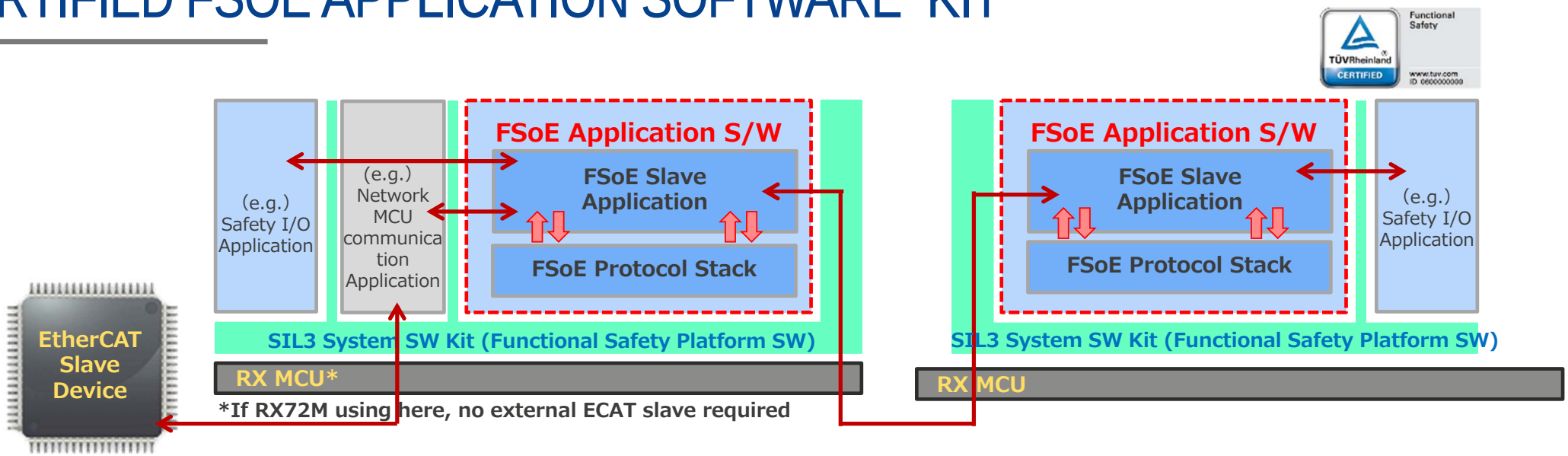


Easy protocol changes by exchanging stack applications*

*: under planning

CERTIFIED FSOE APPLICATION SOFTWARE KIT

Shorten Certification Process



Basic	• **ETG.5100 S (R) V1.2.0 compliant** Safety over EtherCAT(FSoE) Slave application S/W • **IEC61508 SC3/SIL3 Certified** • Supporting MCU : Runs on Renesas RXv3 core and RXv2 core MCUs • Supporting Compiler : Renesas CC-RX and IAR EWRX version.
Feature	• **Safety data process function of FSoE slave can be easily realized** by using SIL3 System SW kits together. • Comprehensive application SW to **support all functions required for safe data processing e.g.** FSoE Slave network state management, safety data exchange process between dual MCUs, diagnostic processes, and FSoE stack processes • Includes **dedicated setting file to easily set different safety data and parameters** per product.

INDUSTRIAL ETHERNET SAFETY PROTOCOL

SUMMARY

Shorten Certification Process

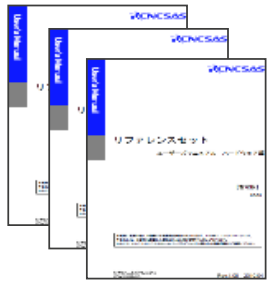
- Renesas also will release CC-Link IE TSN Safety this July by partnership with Zuken ELMIC.
- For FSoE stack, Renesas will support directly under copy license scheme which is same as other of our SW solution.

Safety Protocol Name	Release Status	Supporting Family	Stack Partner
FSoE	Available	RXv3, RXv2	Renesas
CC-Link IE Safety	Available	RXv3, RXv2	eForce
CC-Link IE TSN Safety		RXv3, RXv2	eForce
PROFI-safe	Q1/2022	RXv3, RXv3	Renesas
CIPsafety	Under Market Survey		

Shorten Certification Process

REFERENCE DOCUMENT

- The guide book containing IEC61508 essential requirements and application design examples to reduce the complexity of understanding the standard and certification process



Two product lineup

✓ **Reference document digest** (Overview of the Reference Document)

✓ **Reference documents** (No.1~No.20 : 20 documents ＋ 6 excel files)

What's inside

Safety part specification	1. Motor control system safety part specification (Includes safety part circuit diagram and parts list	
Concept phase documents	2. Creation guide documents for concept phase 3. Safety Plan and Verification & Validation (SP, V&V) 4. Safety Requirements Specification (SRS) 5. Safety Concept (SC)	**EXCEL files** ・Development document, Data management list ・IEC61508 HW fault avoidance adapted technique list ・IEC61508 SW fault avoidance adapted technique list
Safety Validation documents	6. HW-FMEA 7. Safety Integrity Level (SIL) calculation resource 8. SW-FMECA 9. Coding standard 10. Explanation of calculation formula for checking safety level	**EXCEL files** ・Safety part HW FMEA implementation list ・Safety part HW failure rate calculation list ・Safety part SW FMECA implementation list
MCU internal diagnosis documents	11. Partitioning operation technique of MCU self diagnosis 12. Transient failure diagnosis technique 13. Cross monitoring technique 14. Diagnosis of ECC circuit	
MCU peripheral diagnosis documents	15. MCU power-supply voltage monitoring technique 17. Motor diagnosis technique using encoder pulse 19. Safety output circuit diagnosis technique	16. Network communications section diagnosis technique 18. Safety input circuit diagnosis technique 20. Safety control

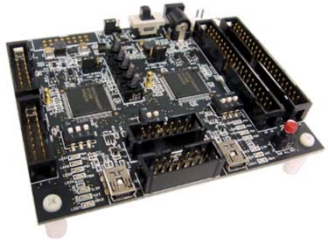
REFERENCE BOARDS

- Evaluation boards verified by the certification body packed with **functional safety design know-how**.
- Designed including the diagnosis and monitoring circuits required by the functional safety standard.
- Let's **immediately start Prototype and Software development** !

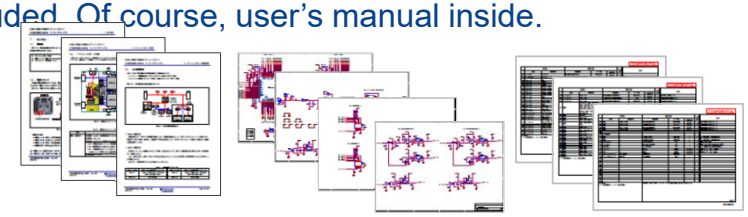
RXv1 core
RX111 - RX111 mounted
Reference board

RXv2 core
RX71M - RX651 mounted
Reference board

RXv3 core
RX72N – RX72N mounted
Reference board



✓ Various circuits required by the standard and parts list included. Of course, user's manual inside.



MCU pins connected to extension connector to ;

✓ Start SW prototype or evaluate Renesas Safety SWs.

✓ Can be connected to your pre-existing system to start prototype development.

Shorten Certification Process

SAFETY COMPILER AND CERTIFICATION KIT FOR COMPILER

- Compiler for functional safety must have a reliability certification (IEC61508-3)

Above process not needed when using RX compiler and certified certification kit

- **CC-RX compiler V2.03.00 & V3.01.00 suitable for development**
- **Certification Kit for CC-RX available for customer's certification process with certifier**
  Certified as IEC61508 SIL3 by TUV-Rheinland
- **Embedded Workbench for RX Functional Safety by IAR (V3.10.5, V4.14.2)**
  Certified as IEC61508 SIL3 by TUV-SUD

Functional Safety TÜVRheinland CERTIFIED www.tuv.com ID 0600000000

FUNCTIONAL SAFETY SOLUTION LINEUP

Various solutions for developing functional safety products

1. Self-Test Software Kit RA/RX

Diagnostic Software for permanent failure of CPU, ROM, RAM inside the MCU

2. SIL3 System Software Kit RX

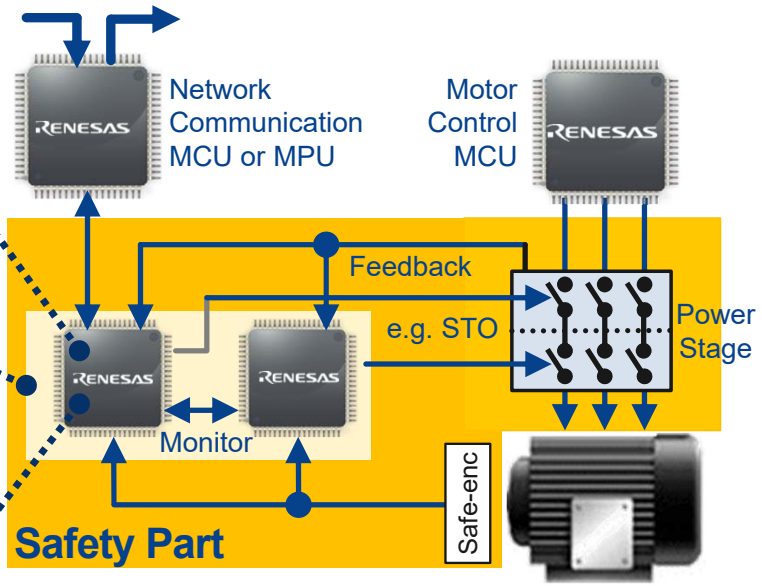
Functional Safety Platform Software for dual MCU system equipped with MCU diagnosis, scheduler, partitioning function

3. FSoE Application Software Kit RX

4. PROFIsafe Application Software Kit RX

Safety network software for slave devices

System example ;
Safety motor control with safety network



5. Reference Document RA/RX

Guideline document to obtain IEC61508 certification
-Sample documents to be submitted to certification body & preparation guide
-Technical documents necessary for safety part development such as input and output circuit diagnosis, power-supply monitoring

6. Reference Hardware RX

Dual MCU configuration Evaluation Board

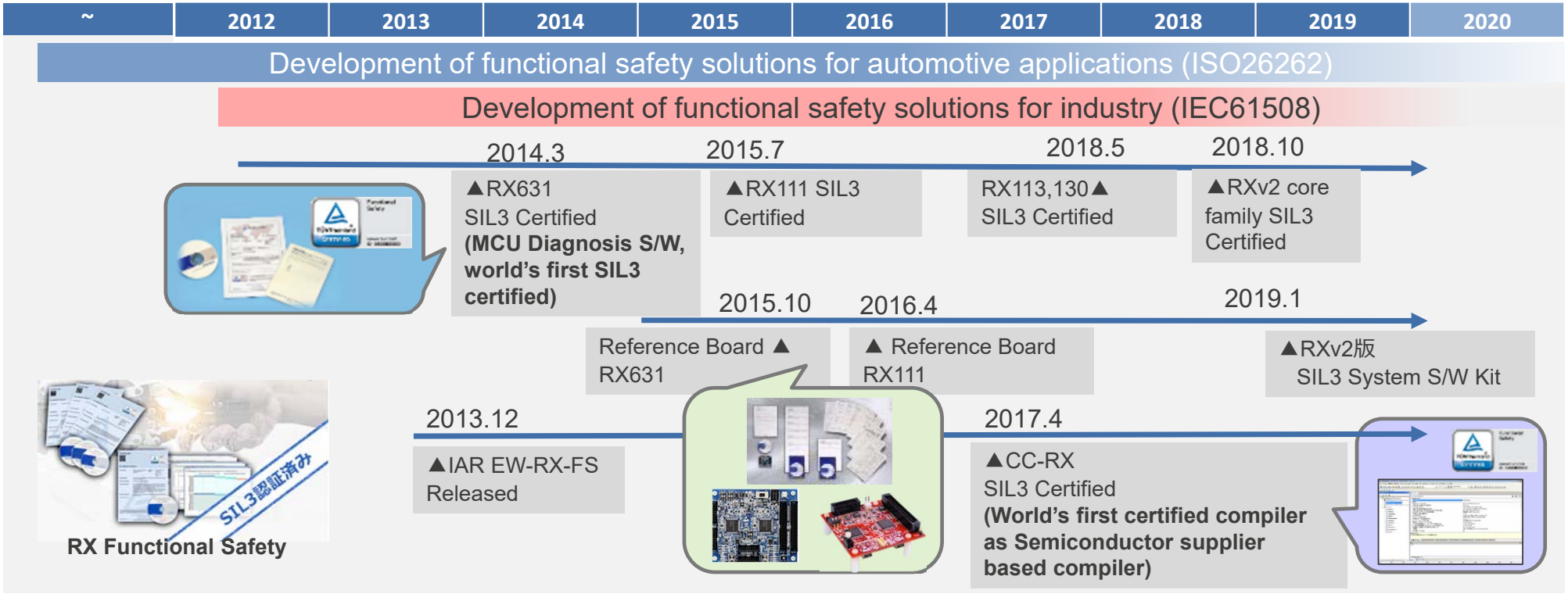
7. IEC61508 Certification Kit for Compilers RA/RX

- Document set certifying functional safety compliance of Renesas compiler "CC-RX" (RX only)
- Certified compiler Kit supported by IAR (both RX/RA)

WORKING WITH RENESAS

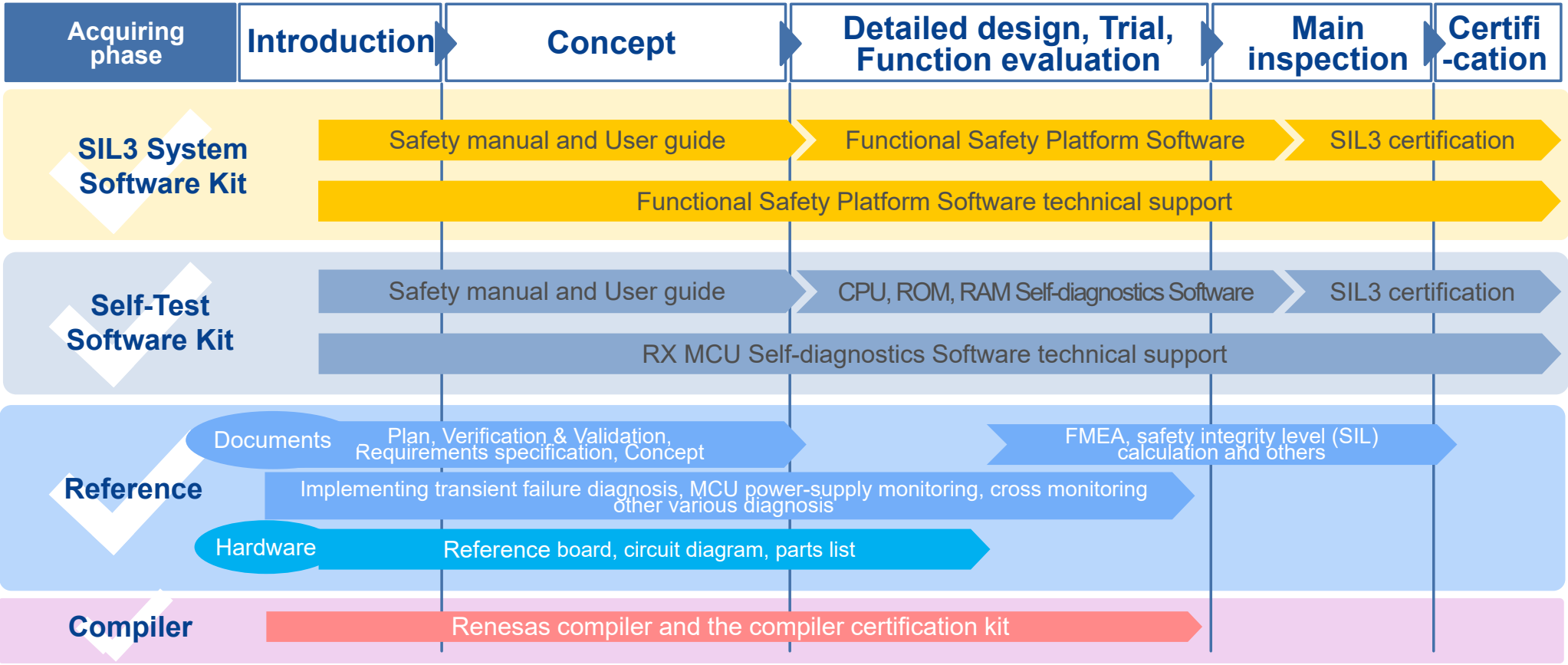
EXPERIENCE IN INDUSTRIAL AUTOMATION FUNCTIONAL SAFETY

- **Renesas has Industrial Segment know-how built up with 20 years of experience in automotive safety and 8 years of experience in industrial functional safety**



RENESAS SOLUTIONS COVER ALL CERTIFICATION PROCESSES

Customers can focus on application development and not be delayed while learning and completing the safety certification process without certified SW kit & Compiler and validated Reference documents and EV board.



FLEXIBLE OFFERINGS FROM RENESAS
KNOWING YOUR NEEDS

- Basic offer - **Free of charge certified Self-test SW kit with certificate**

  ✓Available via web download

  ②Self-Test Software Kit*

- Premium **certified solutions** for easier and faster safety system development.

  ✓ Free **evaluation version available** for your evaluation purpose.

  ①SIL3 System Software Kit* **③Safety Protocol Application SW Kit***

  ④Reference Documents*

  ✓ Board and Compiler + Certification Kit for Compiler ready to purchase.

  ⑤Reference Hardware Board **⑥Compiler, Certification Kit***

  ✓Also, annual support package available as optional

*SW License agreement required beforehand

SUPPORTING TABLE PER PRODUCT FAMILY

- Renesas provides full support coverage of Certified Function Safety Solutions for all three versions of the CPU cores used in the RX Family.
- Renesas will expand it's supporting products on both RX and RA Family.

		RX Family			RA Family	
		RXv1	RXv2	RXv3	RA4M1 RA6M1/M2/M3	CM23 and CM33 (Coming in 2022)
①	SIL3 System Software Kit		✓	✓		
②	Self-Test Software Kit	✓	✓	✓	✓	✓
③	FSoE Application SW Kit		✓	✓		
④	Reference Documents		✓		✓	
⑤	Reference Hardware	✓	✓	✓		
⑥	Safety Compilers	✓	✓	✓	✓	✓
NEW	PROFIsafe Application SW Kit					

FUNCTIONAL SAFETY SOLUTION SUPPORTING MCU

No	Product	Family	RX			RA			
		Core	RXv1	RXv2	RXv3	CM4	CM23	CM33	
		Group	RX111 RX113 RX130	RX71M RX651/N RX64M RX24U RX24T RX230/1 RX23T RX23W RX23E-A	RX72M RX72N RX72T RX66N RX66T	RA6M1 RA6M2 RA6M3 RA6T1 RA4M1	NEW RA2A1 RA2L1 RA2E1	NEW RA6M4 RA6M5 RA4M2 RA4M3	More to come !
1	Self-Test Software Kit		✓	✓	✓	✓	✓	✓	
2	SIL3 System Software Kit			✓	✓				
3	FSoE Application Software Kit			✓	✓				
4	PROFIsafe Application Software Kit NEW			✓	✓				
5	Reference Document		✓	✓	✓	✓*1	✓*1	✓*1	
6	Reference Hardware		✓	✓	✓				
7	IEC61508 Certification Kit for RX Compilers		✓	✓	✓	*2	*2	*2	

*1: Although it is described in the example using RX MCU, it can be used to other MCUs because it is a technical document of functional safety standard itself not related to dedicated MCU Family.
*2: IAR Systems compilers can be used

Functional Safety Web

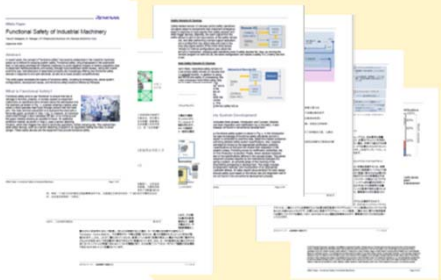
FOR YOUR INVESTIGATION...

Brochure

Flyer

Web Page

White Paper



Blog

Webinar

SUMMARY

Page 40

Functional Safety

for IA

KEY TAKEAWAYS

- Renesas certified functional safety solutions cover both development and certification for easier and faster time to market.
  - ✓Certified safety SW: By using certified safety software and safety protocols, users do not need to develop Safety SW for MCU around and can concentrate on the development of Safety SW for user's application.
  - ✓Reference HW Boards: Dual MCU safety system boards with safety circuits for user reference and to shorten development time.
  - ✓Reference Documents: Complete safety guidebook including design know-how of the IEC61508 standard.
  - ✓Certified Compiler: For smooth and fast development.
- For more information, please visit our Functional Safety Web. Webinar & white paper available.

THANK YOU !