ROHM SEMICONDUCTOR

ISO 26262: Functional Safety Standard for Modern Road Vehicles

White Paper

1. Introduction

In recent years, the increasing advancement and proliferation of automated driving have brought about a need for standards such as ISO 26262 that defines functional safety along with functions that contribute to the prevention of accidents in the event of an emergency. Especially in China, where the level of technical innovation is considerable, ISO 26262 has been enacted as a recommended national standard (with a prefix of 'GB/T'). A Chinese translation of the 1st Edition of ISO 26262 was published in October 2017 as GB/T 34590, before going into effect in May 2018.

Amid this backdrop, a growing number of companies are promoting functional safety not only among automotive manufacturers (OEMs), but Tier 1 electronics equipment suppliers as well, making it an increasingly important requirement worldwide.

In this paper, as interest in functional safety and ISO 26262 grows and initiatives and responses are needed, we will introduce these concepts from a semiconductor manufacturer's perspective, including how they affect the automotive sector.

2. What is Functional Safety?

First, let's consider the meaning of functional safety.

2-1. The definition of 'Safe'

If suddenly asked what the meaning of 'safe' is, most people would have a hard time answering right away. In the 1st edition of the international basic safety standard ISO/IEC Guide 51 (which is an introductory guideline on safety), the word 'safe' is defined as having 'no unacceptable risk'. This double negative may be difficult to immediately grasp, so perhaps saying, 'freedom from risk which is not tolerable' is easier to understand. However, in any case it is not easy to define 'safe' in one sentence, so let's go over the definition again.

The opposite of 'safe' is 'dangerous'. So, what is 'dangerous'? 'Dangerous' conditions can be referred to as ones that are 'at risk'. In general, risk can be large or small. Therefore, by taking measures against large risk that is 'dangerous' and reducing it to an acceptable range, this 'dangerous' state then becomes a 'safe' state. Or to put it another way, a 'state without an unacceptably large risk'. So now we see that 'safe=no unacceptable risk' as mentioned in the beginning.

2-2. Comparison between intrinsic safety and functional safety

Now, let's go over the meaning of **functional safety**. The phrase **intrinsic safety** is often cited when describing functional safety. Here we would like to explain functional safety by comparing it to intrinsic safety.

Intrinsic safety is a method for ensuring safety by removing the causes of danger. Functional safety, on the other hand, is a method of reducing risks to an acceptable level to ensure safety by devising functions.

As an example, let's consider what measures to take to prevent a train and car from colliding when a road and railway intersect.

Achieving intrinsic safety involves eliminating the inherent dangers of intersecting railways and roads by using overhead crossings to avoid accidents altogether. In accordance with this concept, an overhead crossing physically prevents collisions between cars and trains.

In contrast, functional safety considers methods such as establishing a railway crossing to reduce the likelihood of a collision. It entails installing a barrier and alarm at the intersection of the railway and road and mounting a sensor on the railway, then sounding the alarm and lowering the barrier when an approaching train is detected. Another sensor is used to detect that the train has passed, after which the alarm is stopped and the barrier is raised. Although in this method railways and roads still physically intersect, railroad crossings are installed to reduce the risk of collisions to an acceptable level. This embodies the concept of 'functional safety'.

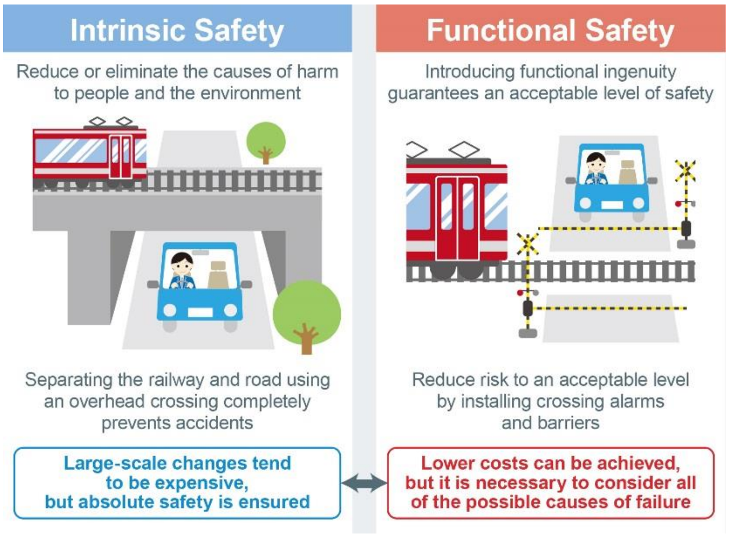

Intrinsic Safety
Reduce or eliminate the causes of harm to people and the environment
Separating the railway and road using an overhead crossing completely prevents accidents
Large-scale changes tend to be expensive, but absolute safety is ensured
Functional Safety
Introducing functional ingenuity guarantees an acceptable level of safety
Reduce risk to an acceptable level by installing crossing alarms and barriers
Lower costs can be achieved, but it is necessary to consider all of the possible causes of failure

Figure 1. Concepts of Intrinsic and Functional Safety

As in the previous example, intrinsic safety guarantees absolute safety, but generally tends to be very expensive. Although functional safety can often be achieved at a lower cost, when designing it is necessary to consider how to ensure safety when additional functions fail.

In the above example of functional safety, if the sensor is broken neither the alarm nor barrier will operate when a train approaches. And because this poses an immediate danger, a design mechanism is required that prevents this dangerous condition from occurring if the sensor fails. For example, by attaching a self-diagnostic circuit to the sensor that automatically lowers the barrier if the sensor breaks. This type of design, in which the direction moves towards safety in the event of failure, is referred to as **fail-safe**. Alternatively, implementing a redundant design by adding a second sensor that acts when the first sensor breaks (and operates until the broken sensor can be repaired), is often used.

Other examples of redundancy include using multiple red lamps in railroad crossing alarms and head/tail lights on cars. These are duplicated not only for design reasons, but also to ensure a minimum level of safety even if one lamp goes out.

2-3 Achieving functional safety

The concept of functional safety has emerged because it is necessary to make things based on the premise that *people make mistakes* and *things break* in order to avoid serious accidents. To achieve functional safety, designers need to consider both **systematic failure** and **random failure** to prevent harm from being caused by the movement or actions of the object in question.

Systematic failures are failures created during design, commonly referred to as bugs. To prevent systematic failures, it is necessary to construct a design flow that does not cause design errors. Specifically, it starts with the creation of specifications based on requirements, and each process including design, verification, prototyping, and evaluation are clarified, with reviews performed at each stage. It is also necessary to manage the documents created at each stage and be able to refer to and retrieve them at any time.

In contrast, random failures are failures that occur after manufacturing. Since random failures cannot be completely prevented, a safety mechanism must be in place to prevent harm even if failure occurs.

2-4 Functional safety with semiconductors

As technological innovations progress, primarily in the automotive and industrial equipment sectors, and electronic systems become more sophisticated and complex, the role of semiconductors increases and functional safety measures for semiconductors are required.

Semiconductor products typically consist of circuits formed on a silicon substrate, enveloped by a hardened black resin called a mold that protects the circuit but also prevents the interior from being seen. As many as hundreds of thousands or even millions of semiconductor elements such as transistors and resistors can be encapsulated in the mold resin, making the circuit and block configurations quite complex Therefore, in order to handle failures in semiconductor products, it is necessary to introduce an appropriate concept of functional safety from the specification stage before entering the design phase. As such, semiconductors need to respond to functional safety by considering *both* systematic *and* random failures.

3. ISO 26262 and Related Standards

Now that we understand the concept of functional safety, let us give an overview of the functional safety standard ISO 26262. Also, keep in mind that there are numerous other functional safety standards not limited to the automotive field.

3-1 Regarding the major standards

Before we go into detail about ISO 26262, we would like to explain the key standards.

Foremost are international standards (IS) published by ISO, which stands for International Organization for Standardization, is a non-governmental organization headquartered in Geneva, Switzerland. You may have heard of some of the more well-known standards such as ISO 9001: Quality Management System, and ISO 14001: Environmental Management System.

Next is IATF 16949, a global technical specification and quality management standard for the automotive industry. IATF is short for the International Automotive Task Force. IATF 16949 is designed to be used in conjunction with ISO 9001:2015 and contains supplemental requirements specific to the automotive industry.

IATF 16949 supersedes and replaces the current ISO 26262 standard that defines the requirements of a Quality Management System.

3-2 Origins of ISO 26262 and other functional safety standards

As mentioned above, ISO 26262 is a functional safety standard for electrical and electronic systems in road vehicles based on IEC 61508, considered the parent standard for functional safety.

IEC 61508 is an international standard published by IEC (International Electrotechnical Commission) for the functional safety of Electrical/Electronic/Programmable Electronic Safety-related Systems in all types of industry, including power plants, factories, machinery, railways, medical equipment, and home appliances. Following the basic concept and framework of IEC 61508, ISO 26262 was created as an adaptation for automotive electric/electronic systems.

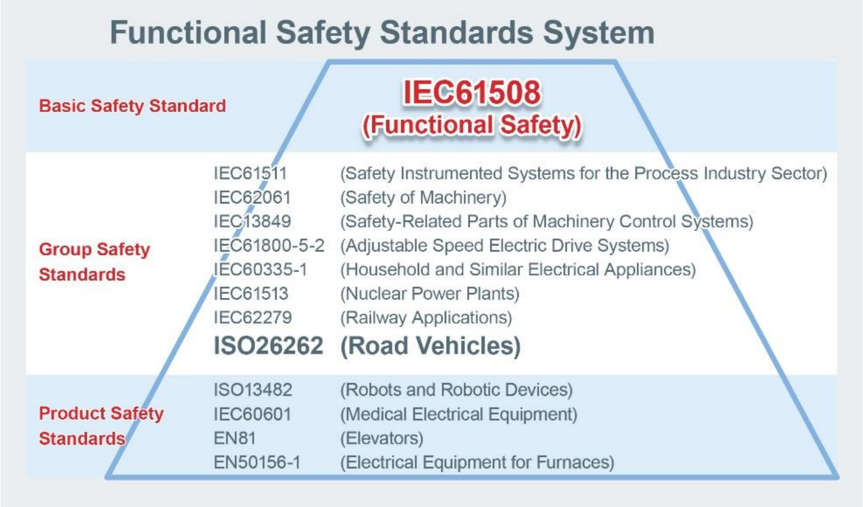

Functional Safety Standards System
Basic Safety Standard
IEC61508
(Functional Safety)
Group Safety Standards
IEC61511 (Safety Instrumented Systems for the Process Industry Sector)
IEC62061 (Safety of Machinery)
IEC13849 (Safety-Related Parts of Machinery Control Systems)
IEC61800-5-2 (Adjustable Speed Electric Drive Systems)
IEC60335-1 (Household and Similar Electrical Appliances)
IEC61513 (Nuclear Power Plants)
IEC62279 (Railway Applications)
ISO26262 (Road Vehicles)
Product Safety Standards
ISO13482 (Robots and Robotic Devices)
IEC60601 (Medical Electrical Equipment)
EN81 (Elevators)
EN50156-1 (Electrical Equipment for Furnaces)

Figure 2. Functional Safety Standards System

In fact, numerous functional safety standards based on IEC 61508 have been published for other industries. For example, there is IEC 61511 (Safety Instrumented Systems for the Process Industry Sector), IEC 62061 (Safety of Machinery), IEC 13849 (Safety-Related Parts of Machinery Control Systems), IEC61800-5-2 (Adjustable Speed Electric Drive Systems), IEC 60335-1 (Household and Similar Electrical Appliances), IEC 61513 (Nuclear Power Plants), IEC 62278 (Railway Applications), ISO 13482 (Robots and Robotic Devices), IEC 60601 (Medical Electrical Equipment), EN 81 (Elevators), EN 50156-1 (Electrical Equipment for Furnaces).

At this point we want to clarify that ISO 26262 is not an actual law. For this reason, noncompliance with ISO 26262 is not illegal. However, automakers will not purchase products that do not comply with this standard, as they must prove that vehicles are made safe by designing electronic and electrical systems in accordance with ISO 26262. This ensures that even if electrical/electronic systems fail, no persons (not only the driver and passengers, but pedestrians as well) will be harmed as a result.

3-3 Compliance with ISO 26262

To comply with ISO 26262, it is necessary to respond to both processes and products. Processes refer to a set of inputs, processes, and outputs, while process response is the response to the development flow that summarizes the development procedures, etc. Maintaining internal regulations and development standards requires that the development process for documents and reviews necessary for development be established.

At the same time, product response is a response to product functions, so if a failure occurs somewhere in a target product, that failure is detected and some type of safety mechanism is in place that performs some type of processing to avoid danger.

Now let’s delve a little deeper into both types of responses.

From the viewpoint of *people make mistakes*, failures created at the time of design (bugs) are described as systematic failures, and process response is required as a countermeasure to avoid such failures. In order to prevent bugs from being created during the design phase, the necessary documents and reviews must be specified during development, to be kept and used as evidence. All software failures are systematic failures.

In addition, from the viewpoint of *things break*, failures that occur in the market (and factory), are described as random failures (or random hardware failures), requiring product response as a countermeasure. It is necessary to implement design in consideration of various margins to prevent damage, but from a functional safety point of view, it is also important to carry out design to prevent injury even in the event of failure. For this reason, designers must establish safety measures to detect failures and take appropriate actions. During initial specifications review in the design stage the various types of failures need to be considered for each function along with their corresponding safety measures. Product response entails adding a safety mechanism to accommodate for random failures.

3-4 Product responsibility for designers

Perhaps you have heard of **product liability**. This means that manufacturers and/or other entities can be held liable in the event a defect in a product causes damages to human life, body, or property. As designers need to prove that there are no design flaws (bugs) in the design of their products by leaving evidence (i.e. their design rationale and design assumptions), dealing with product reliability can be considered a type of process response.

4. Details of ISO 26262

The 1st Edition of ISO 26262 was published in November 2011, then after several revisions the 2nd Edition was released in December 2018. The 1st Edition targeted mass-produced passenger cars weighing less than 3,500kg, while the 2nd Edition expanded the scope to include trucks, buses and motorcycles. Here we would like to go over the details of ISO 26262, focusing on the revised contents of the 2nd Edition.

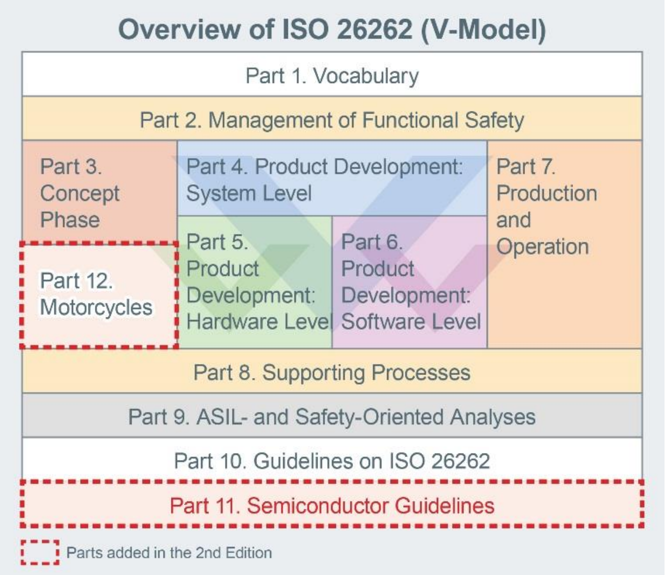

Overview of ISO 26262 (V-Model)
Part 1. Vocabulary
Part 2. Management of Functional Safety
Part 3. Concept Phase
Part 4. Product Development: System Level
Part 7. Production and Operation
Part 12. Motorcycles
Part 5. Product Development: Hardware Level
Part 6. Product Development: Software Level
Part 8. Supporting Processes
Part 9. ASIL- and Safety-Oriented Analyses
Part 10. Guidelines on ISO 26262
Part 11. Semiconductor Guidelines
Parts added in the 2nd Edition

Figure 3. Overview of ISO 26262

4-1 Trucks and buses (T&B) added

The first major change in the 2nd Edition are the types of vehicles subject to the standard. The 1st Edition targeted mass-produced passenger cars weighing less than 3,500kg, but the 2nd Edition removed the frame restriction and expanded the scope to include trucks, buses and motorcycles. However, it seemed that when the 1st Edition was enacted buses and trucks were also planned to be covered under the standard, but this took time to consider, and there was precedent for limiting vehicles to under 3,500kg.

Generally, trucks are produced by automotive manufacturers using base models (i.e. cabin, engine, chassis) while installers (body builders) add specialized body parts (e.g. containers, dumps, mixers). For this reason, it is conceivable that a base vehicle designed and manufactured in accordance with ISO 26262 may be equipped with body parts designed and manufactured without complying with this standard. Apparently, discussing how to deal with such a situation took a considerable amount of time. Terms and abbreviations for trucks and buses (T&B) have been added to the glossary in Part 1 of Figure 3.

4-2 Motorcycles added

Motorcycles as shown in Fig. 3 are newly defined in Part 12. The target here is defined as 2- or 3-wheeled drive vehicles not weighing more than 800kg without load, excluding mopeds as defined in ISO 3833. Mopeds refer to anything less than 50cc designed with a top speed less than 50km/hr. As a result, although the legal speed of motorized bicycles (mopeds) in Japan is 30km/hr, they are not considered mopeds since they are designed to go up to 60km/hr.

Let's classify Motorcycles that are a part of Part 12 in an easier to understand way.

- Mopeds and electrically assisted bicycles: Not applicable
- Japanese mopeds, motorcycles, and 3-wheeled vehicles weighing less than 800kg: Target
- 3-wheeled vehicles weighing more than 800kv and vehicles with 4 or more wheels: Not applicable (these are subject to the standard Part, not Part 12).

4-3 Semiconductor guidelines

New semiconductor guidelines have been established as Part 11. Please note that as Part 11 is simply a guideline, there are no requirements or work deliverables necessary, but it does give a clearer understanding of the contents specified in Part 5 (Hardware Design) and Part 6 (Software Design) when designing with semiconductors. Unlike the 1st Edition which does not illustrate how to respond when designing using semiconductors, the 2nd Edition contains many examples that facilitate semiconductor designs in accordance with ISO 26262.

4-4 Detailed objectives

As you can see from comparing the 1st and 2nd Editions of ISO 26262, the description of the target items has significantly increased in the 2nd Edition. The main reason is the addition of specific examples that clarify the purpose of each section. The principles that should be followed are described in detail, allowing users to ensure safety using other methods without being limited to the items listed in the requirements.

4-5 Remarks and examples added

Numerous remarks and examples have been added to make the requirements and recommendations easier to understand.

5. Obtaining Certification

Thus far, we have provided an overview and details of ISO 26262, but how exactly does one acquire certification? In this section, we will introduce the certification method along with ROHM's activities.

5-1 Certification by 3rd party certification organization

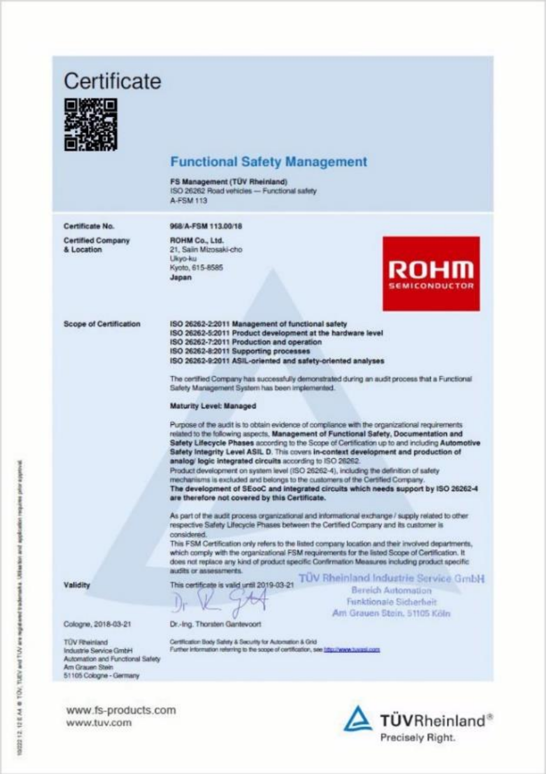
It is common to obtain ISO 26262 certification by undergoing an audit from a 3rd party certification body, such as TÜV Rheinland, TÜV SUD, SGS TÜV, DNV-GL, or TUV Saarland. TÜV (Technischer Überwachungs-Verein) refers to a private inspection organization authorized by the German Technical Inspection Association to perform inspections and certifications. All processes (including internal regulations, development standards, and procedures) in accordance with ISO 26262 are audited and certified.

5-2 Self-certification is also permitted

Companies do not necessarily need to obtain certification from a 3rd part certification body if they can demonstrate compliance with ISO 26262. It is not a problem if a work product is created that includes the necessary requirements and can be shown that it was developed in accordance with the standard even if certification was not obtained. However, understanding and implementing the standard requires a great deal of time and effort, and proving that all requirements have been met can be a daunting task. For this reason, it is much more efficient to undergo an audit and receive certification from a 3rd party organization rather than explain and show compliance to individual clients.

5-3 ROHM has received process certification

ROHM began building an ISO 26262 process in 2015 and was able to receive ISO 26262 Process Certification from third-party certification authority TÜV Rheinland in Germany two and a half years later, in March of 2018 (Fig. 4). In other words, ROHM’s ISO 26262 process is recognized to be compliant with the ISO 26262 standard. And while it is common to build a process by receiving advice from consultants, ROHM attended a number of workshops to better understand and study the standard and successfully achieve a compliant process.



Certificate

Functional Safety Management

FS Management (TÜV Rheinland)
ISO 26262 Road vehicles — Functional safety
A-FSM 113

Certificate No. **968/A-FSM 113.00/18**

Certified Company & Location
ROHM Co., Ltd.
21, Saiin Mizosaki-cho
Ukyo-ku
Kyoto, 615-8585
Japan

Scope of Certification
ISO 26262-2:2011 Management of functional safety
ISO 26262-5:2011 Product development at the hardware level
ISO 26262-7:2011 Production and operation
ISO 26262-8:2011 Supporting processes
ISO 26262-9:2011 ASIL-oriented and safety-oriented analyses

The certified Company has successfully demonstrated during an audit process that a Functional Safety Management System has been implemented.

Maturity Level: Managed

Purpose of the audit is to obtain evidence of compliance with the organizational requirements related to the following aspects, **Management of Functional Safety, Documentation and Safety Lifecycle Phases** according to the Scope of Certification up to and including **Automotive Safety Integrity Level ASIL D**. This covers **in-context development and production of analog/ logic integrated circuits** according to ISO 26262.
Product development on system level (ISO 26262-4), including the definition of safety mechanisms is excluded and belongs to the customers of the Certified Company.
The development of SEooC and integrated circuits which needs support by ISO 26262-4 are therefore not covered by this Certificate.

As part of the audit process organizational and informational exchange / supply related to other respective Safety Lifecycle Phases between the Certified Company and its customer is considered.
This FSM Certification only refers to the listed company location and their involved departments, which comply with the organizational FSM requirements for the listed Scope of Certification. It does not replace any kind of product specific Confirmation Measures including product specific audits or assessments.

Validity This certificate is valid until 2019-03-21

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Dr R GA

Cologne, 2018-03-21 Dr.-Ing. Thorsten Gantevoort

TÜV Rheinland
Industrie Service GmbH
Automation and Functional Safety
Am Grauen Stein
51105 Cologne - Germany

Certification Body Safety & Security for Automation & Grid
Further information referring to the scope of certification, see http://www.tuvasi.com

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

Figure 4. ROHM's ISO 26262 Process Certificate

5-4 Functional Safety Engineers (FSE) and Functional Safety Managers (FSM)

ROHM employs 24 Functional Safety Engineers along with 3 Functional Safety Managers possessing even higher qualifications (current as of Feb. 2020). Both are licensed through TÜV Rheinland. Functional Safety Engineers, who belong to departments that develop automotive

ICs, fulfill their duties by promoting development that conforms to ISO 26262 processes while with handling FIT and FMEDA submission requests from users. At the same time, Functional Safety Managers belong to departments separate from IC development and carry out verification measures, including verification review, functional safety audits, and functional safety assessments, in a manner that ensures independence required by the standard.

6. Circuit Configuration of Automotive Applications that Supports Functional Safety

Finally, we will introduce how semiconductors are contributing to functional safety in recent automotive applications, together with ROHM’s initiatives and solutions.

6-1 Safety design for modern automotive applications

Speaking of display devices in the car, in addition to the instrument cluster such as speedometer, tachometer, water temperature/fuel gauges, and other indicators, newer vehicles now typically include a navigation system. And some higher end cars are seeing the instrument cluster being replaced with an LCD and electronic mirrors replacing side/rear view mirrors (Fig. 5).

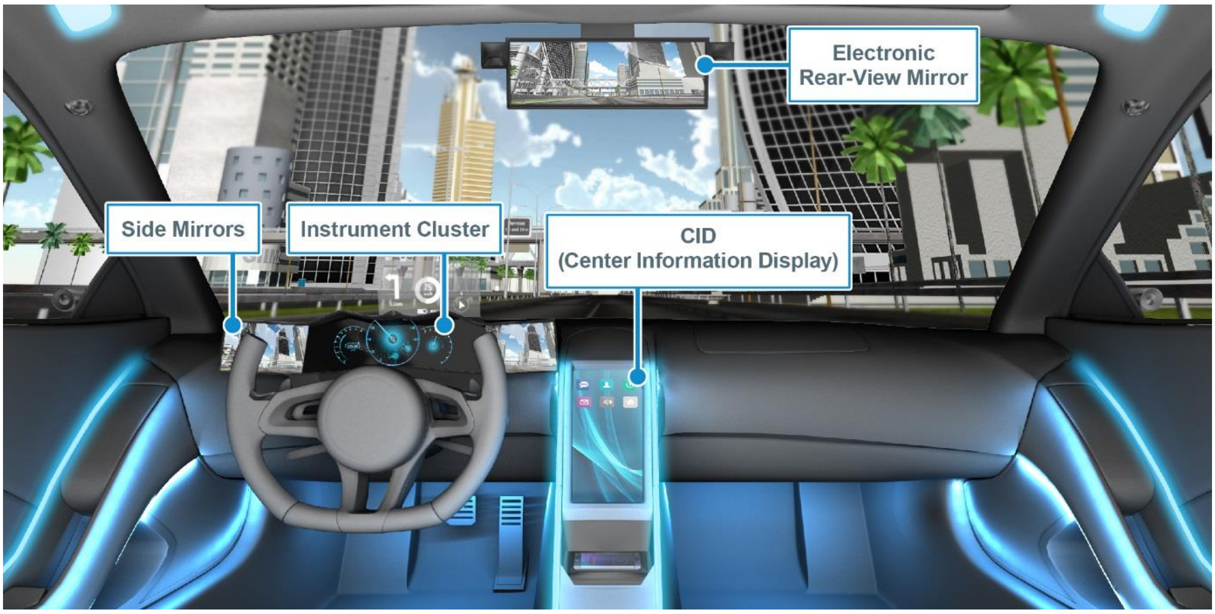


Figure 5. Examples of Vehicle Display Devices

These display devices fulfill an important role by conveying various information to the driver, so major problems can occur if the display fails and/or the screen goes dark. However, it can be even more dangerous if the instrument cluster and electronic mirrors display erroneous information.

This is because a black screen automatically tells the driver a malfunction has occurred, but if the display freezes or is delayed, since the driver is not constantly staring at the screen, he/she may not notice the failure until it is too late. For example, if the speedometer shows lower than the actual speed, the driver may not realize it and exceed the speed limit. And in the case of electronic mirrors, displaying a delayed image that fails to show a vehicle approaching from the side may lead the driver to believe it is ok to change lanes, possibly causing an accident. To prevent these types of failures, instrument clusters and electronic mirrors must integrate fail-safe designs – even when dealing with high reliability electronic devices – since as mentioned above there is always a possibility that the system will break due to some type of failure.

So, what kind of design should be carried out? One possibility is a design that constantly monitors the data to be displayed and shows a black or warning screen indicating abnormality, notifying the driver of a malfunction if the display freezes or erroneous display is likely to occur. In this way, functional safety is achieved that prevents accidents even in the event of failure.

6-2 Circuit configuration of instrument clusters and electronic mirrors

When implementing such a design, let’s take a detailed look at the actual circuit configurations of the instrument cluster and electronic mirror.

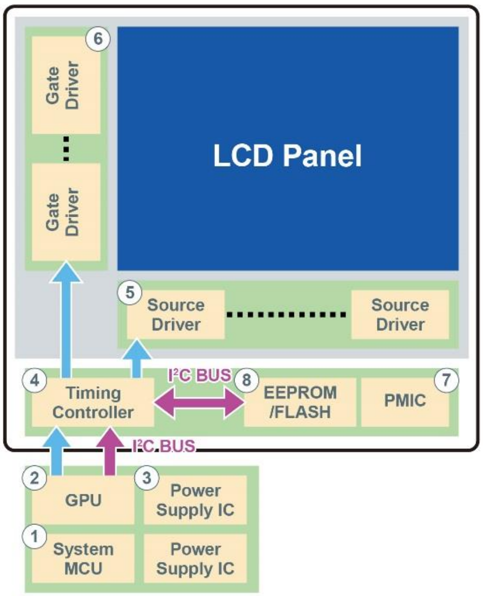


Figure 6. Block Diagram of a Typical Vehicle Display System

Fig. 6 shows an example of a circuit configuration for a display device in a vehicle. Let’s go over each function according to the numbers in the figure.

① The system is controlled by the system MCU (Micro Controller Unit), which acts as the ‘brains’ and performs processing for the entire system.

② The block that performs the same functions as the MCU but for the display is called the GPU (Graphics Processing Unit). Unlike CPUs (Central Processing Units), which are the brains of PCs and excels at performing processing for the entire computer, GPUs are often ICs that specialize in graphics processing.

③ Power supply ICs provide the necessary power for the entire system.

④ The timing controller sends image data sent from the GPU to the source driver for displaying on the LCD panel and controls the gate driver based on the display.

⑤ The source driver determines the brightness of one pixel by adjusting the current to the source amplifier circuit according to the image data to be shown on the LCD.

⑥ The gate driver displays one line at a time based on the display data from the source driver.

⑦ The panel PMIC (Power Management IC) generates the voltage required by the LCD panel for display.

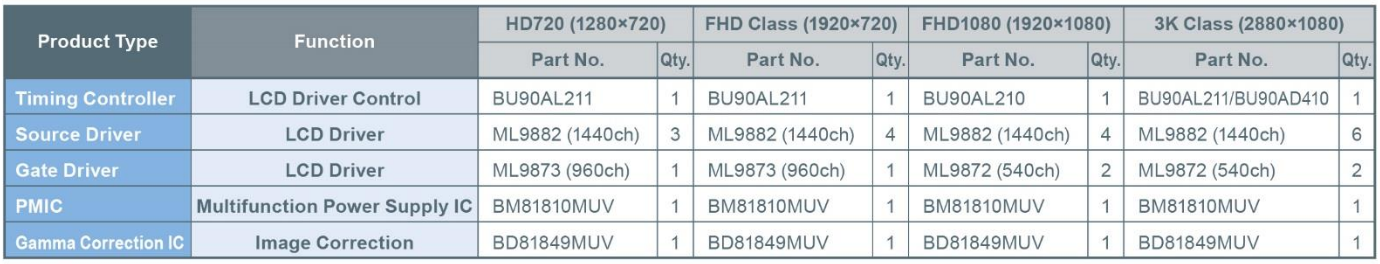
⑧ The EEPROM/Flash stores the initialization data of the timing controller, lookup tables, indicator image, and other information and can overwrite the image sent from the GPU with the indicator image.

6-3 ROHM’s LCD panel chipset

In the application block diagram shown in Fig. 6, if the timing controller controls the two drivers and simply displays the image data sent from the GPU on the LCD panel as-is, nothing can be done if a display error occurs, possibly resulting in an accident.

In response, ROHM solves this problem by providing functions that notify the driver in the event of malfunction, such as by sending a signal to the MCU and displaying an error warning screen, or monitoring the onboard timing controller for the images sent from the GPU and displaying a black screen when either data or input signal abnormalities occur.

ROHM offers a chipset for LCDs that supports complete functional safety for LCD panels, consisting of timing controllers for controlling each LCD driver (BU90AL210 / BU90AL211 / BU90AD410), source/gate drivers for driving LCD panels (ML988 / ML9873 / ML9872), a multifunction power supply IC (BM81810MUV), and gamma correction IC for image correction (BD81849MUV).



Product Type	Function	HD720 (1280×720)		FHD Class (1920×720)		FHD1080 (1920×1080)		3K Class (2880×1080)	
		Part No.	Qty.	Part No.	Qty.	Part No.	Qty.	Part No.	Qty.
Timing Controller	LCD Driver Control	BU90AL211	1	BU90AL211	1	BU90AL210	1	BU90AL211/BU90AD410	1
Source Driver	LCD Driver	ML9882 (1440ch)	3	ML9882 (1440ch)	4	ML9882 (1440ch)	4	ML9882 (1440ch)	6
Gate Driver	LCD Driver	ML9873 (960ch)	1	ML9873 (960ch)	1	ML9872 (540ch)	2	ML9872 (540ch)	2
PMIC	Multifunction Power Supply IC	BM81810MUV	1	BM81810MUV	1	BM81810MUV	1	BM81810MUV	1
Gamma Correction IC	Image Correction	BD81849MUV	1	BD81849MUV	1	BD81849MUV	1	BD81849MUV	1

Figure 7. Examples of Functional Safety Chipsets

This LCD panel chipset can detect a variety of problems as shown in Fig. 8 and includes the necessary safety functions for vehicle displays.

Each IC included in the chipset incorporates a function for mutual detecting possible failure modes, and in addition to a timing controller function mentioned above, information such as source/gate driver driver/separation and input signals to the LCD are verified and fed back as needed to enable complementary failure detection. Integrating functional safety makes it possible to prevent serious accidents caused by the malfunction of monitors used for the speedometer, side mirrors, and other systems.

Panel PMICs continuously monitor whether the voltage required for LCD panel display can be supplied, and in the event a voltage abnormality occurs, a function is included that automatically shuts down operation, along with redundant registers for detecting abnormalities and an auto-refresh function that enables recovery during abnormal operation, ensuring high reliability against unexpected influences such as noise.

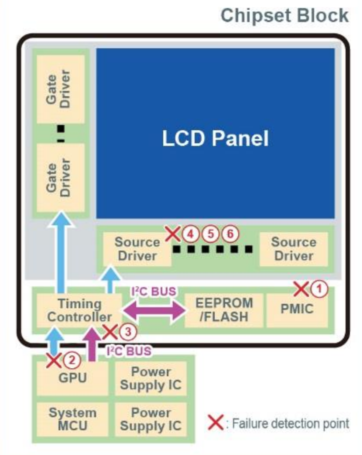
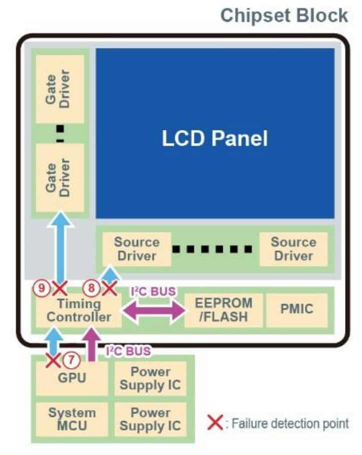
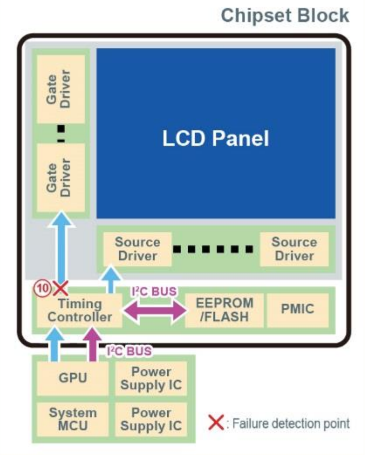
LCD Failure Modes		Black Screen	Freeze/Burn-In	Display Delay
Abnormality Occurrence Location		 Chipset Block Gate Driver Gate Driver LCD Panel Source Driver Source Driver ④⑤⑥ ① Timing Controller I²C BUS EEPROM /FLASH PMIC ② ③ I²C BUS GPU Power Supply IC System MCU Power Supply IC ✕: Failure detection point	 Chipset Block Gate Driver Gate Driver LCD Panel Source Driver Source Driver ⑨ ⑧ Timing Controller I²C BUS EEPROM /FLASH PMIC ⑦ I²C BUS GPU Power Supply IC System MCU Power Supply IC ✕: Failure detection point	 Chipset Block Gate Driver Gate Driver LCD Panel Source Driver Source Driver ⑩ Timing Controller I²C BUS EEPROM /FLASH PMIC I²C BUS GPU Power Supply IC System MCU Power Supply IC ✕: Failure detection point
Expected IC Error Based on Abnormality Occurrence	PMIC	①Shutdown	—	—
	Timing Controller (T-CON)	②LVDS signal error ③Internal register fault	⑦LVDS signal error	—
	Source Driver	④Input voltage error ← PMIC detected ⑤No input signal ← T-CON detected ⑥Fixed output Low	⑧Indeterminate input signal	—
	Gate Driver	—	⑨Input signal error ← T-CON detected	⑩Input voltage error ← PMIC detected

Figure 8. Detectable Failure Examples

6-4 Power supply circuit configuration in a standard ECU

At the same time, automotive ECUs (Engine Control Units) typically require multiple power supplies. Various voltages and currents are demanded by the MCU (which may need separate power supplies for the core and I/O), sensors, motor drivers, CAN (Controller Area Network – a serial communication protocol used in vehicles), and other systems. Inside the car, power supply ICs generate the necessary voltages and currents from the 12V battery. These power supply systems may be comprised of multiple power supply ICs or multichannel PMICs, but especially in the case of vehicle ECUs, abnormalities that occur in these power supplies can lead to accidents.

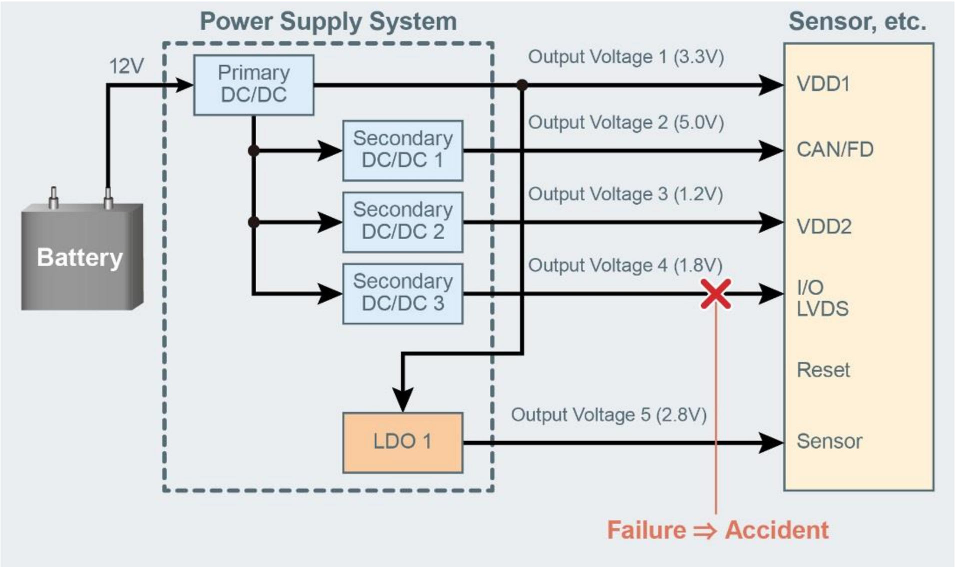


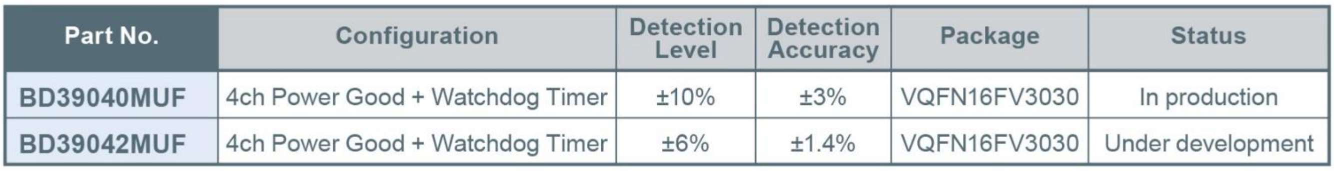
Figure 9. Power Supply Configuration Example

Therefore, it is necessary to monitor the multiple power supplies within the ECUs and perform processing in the event of abnormalities to prevent accidents from occurring based on the location. The power supply monitoring IC also plays a role by monitoring these voltages and notifying the MCU when an abnormality occurs, prompting the user to take appropriate action.

In this way, vehicle applications monitor not only the main function, but for abnormalities in the main function itself as well, to achieve functional safety a mechanism is required to perform processing in accordance with each function and ensure the safety of both the driver and passengers as well as pedestrians. What's more, a self-diagnostic function is needed to verify whether these safety mechanisms are working properly.

6-5 ROHM power supply monitoring ICs

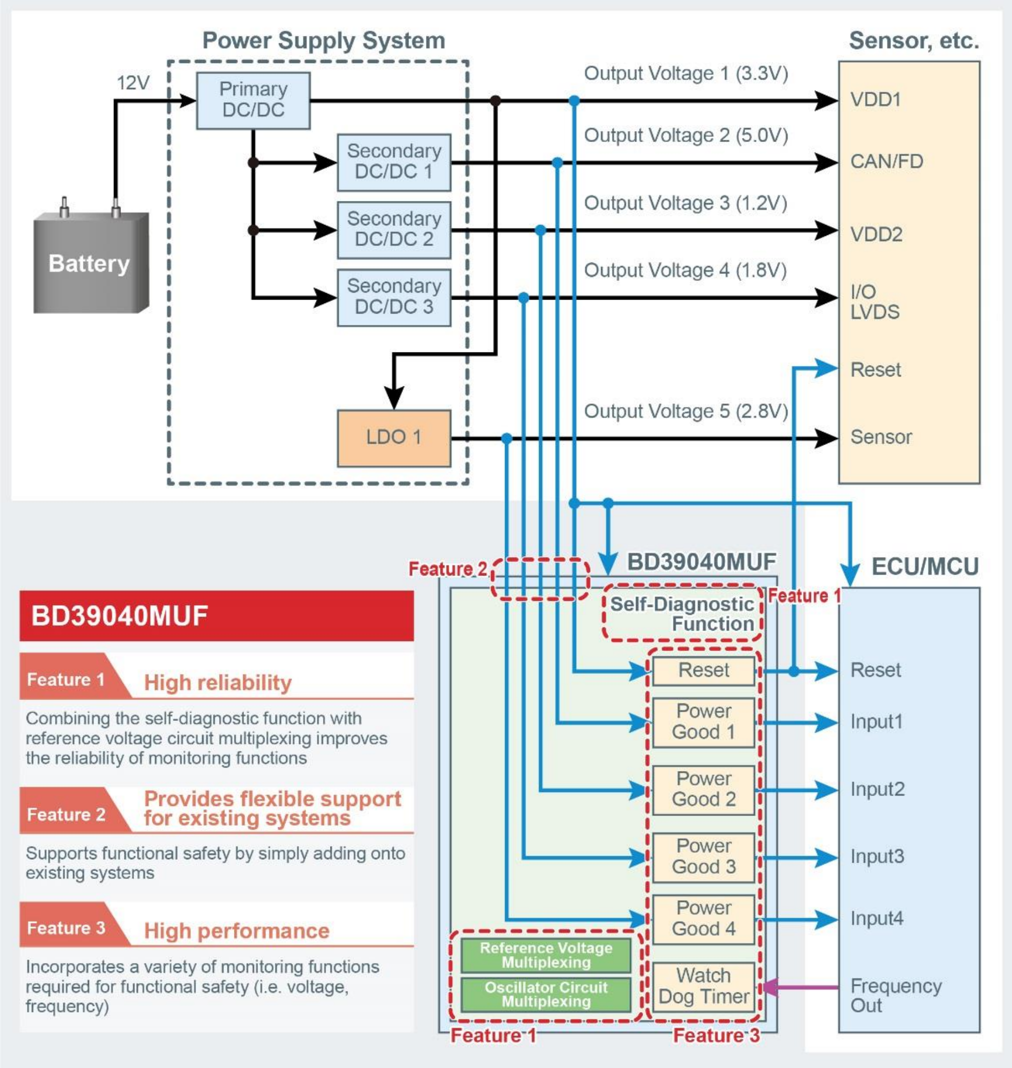
In response, ROHM mass produces power supply monitoring ICs that can easily add functional safety to existing power supplies by incorporating some monitoring functions and the self-diagnostic function in a standalone form factor. The BD39040MUF is a power supply monitoring IC capable of monitoring multiple power supplies, while the BD39042MUF features even higher detection accuracy (currently under development, Fig. 10).



Part No.	Configuration	Detection Level	Detection Accuracy	Package	Status
BD39040MUF	4ch Power Good + Watchdog Timer	±10%	±3%	VQFN16FV3030	In production
BD39042MUF	4ch Power Good + Watchdog Timer	±6%	±1.4%	VQFN16FV3030	Under development

Figure 10. Product Examples of ROHM Power Supply Monitoring ICs

The BD39040MUF integrates a supply voltage VDD monitoring (Reset) function, supports simultaneous monitoring of 4ch power supplies, and is capable of independently detecting power supply abnormalities (under/over voltage). Also a window-type Watchdog Timer (WDT) enables to detect MCU abnormalities within the ECU along with all functions required for the functional safety of ECUs, including a self-monitoring function for redundant reference voltages, a monitoring function for the WDT clock oscillator, and a self-diagnostic function to check whether the detection function in the IC is operating normally at startup.



Combining the self-diagnostic function with reference voltage circuit multiplexing improves the reliability of monitoring functions

Supports functional safety by simply adding onto existing systems

Incorporates a variety of monitoring functions required for functional safety (i.e. voltage, frequency)

Figure 11. Block Diagram of ROHM's BD39040MUF Power Supply Monitoring IC

Simply adding ROHM’s power supply monitoring IC to existing systems makes it possible to achieve the power monitoring capability required for functional safety in a space-saving design.

7. Conclusion

Hopefully this article has provided a sufficient overview of the ISO 26262 functional safety standard. In addition to a broad range of high quality, high reliability products, as introduced here, ROHM offers solutions that deliver greater safety and security. And going forward, ROHM will continue to contribute to technological advancement in the automotive industry by focusing on product development in accordance with ISO 26262.