# FUNCTIONAL SAFETY PROCESSOR FOR AUTOMOTIVE APPLICATIONS - A GUIDE TO ISO 26262 COMPLIANCE

***Mrs.Korudu Surekha*[1]*., Chintala Shreya*[2]**

*1 Assistant Professor, Department of ECE, Malla Reddy College of Engineering for Women.,*
*Maisammaguda., Medchal., TS, India*
*2, B.Tech ECE (21RG1A0474),*
*Malla Reddy College of Engineering for Women., Maisammaguda., Medchal., TS, India*

## ABSTRACT

In keeping with the hardware requirements of ISO 26262, this study provides a detailed methodology for assessing the safety of an automotive microprocessor. Section 5 of ISO 26262- During the first stage of building hardware for automobiles, the safety standards are outlined in the domain of hardware development. Here, based on the results of ISO 26262 parts 3 and 4, the hardware safety design is created. Put into action, integrated, and tested. Thorough assessments of the hardware are essential for ensuring compliance with the ISO 26262 standards throughout the development phase. In November 2011, ISO 26262 was presented to the automobile industry as a set of rules and methods meant to meet the need for safety risk management from sensors to actuators. Electronic Controller Units (ECUs), electronic sensors, signals, bus systems, and code are all part of the embedded electronic systems found in most contemporary vehicles. Detailed safety evaluations focusing on the possible risk of failure are necessary for automotive systems due to the complicated use in electrical, electronics, and programmable electronics.

**Keywords:** Safety processor, ISO 26262, Automotive, functional safety.

## INTRODUCTION

The International Organisation for Standardisation (ISO) 26262 is a set of rules for the security of an automobile's electrical and electronic systems. It covers potential dangers that can arise from the interplay or failure of various systems. A variation of IEC 61508 is ISO 26262. The field of system safety engineering is seeing an influx of new features, such propulsion, driver assistance, active and passive safety systems, and vehicle dynamics control. The likelihood of both planned and unplanned hardware failures is growing in tandem with the trend towards ever-increasing levels of technical complexity, software content, and mechatronic implementation. By outlining suitable criteria and procedures, ISO 26262 helps to mitigate these dangers. At each stage of development, several safety measures are employed to ensure the system is safe. These measures are included into different technologies, such as mechanical, hydraulic, pneumatic, electrical, electronic, and programmable electronic ones. While ISO 26262 primarily addresses the functional safety of E/E systems, it also provide a framework for evaluating safety-related systems that rely on other technologies. a) The automotive safety lifecycle is defined by ISO 26262 and helps with customising the required tasks at each stage of the lifecycle (management, development, manufacturing, operation, service, decommissioning);

b) Offers a risk-based method for determining integrity levels that is unique to the automotive industry; c) Uses ASILs to specify relevant requirements of ISO 26262 in order to prevent unreasonable residual risk; d) Outlines validation and confirmation procedures to guarantee an adequate level of safety is being met; e) Outlines requirements for working with suppliers.

## WHAT IS ISO 26262?

When it comes to functional safety in automobiles, the world has agreed upon ISO 26262. All vehicle electrical and electronic systems, including their software and hardware components, are required to comply with the standard. Both the system's safety-relevant function and the development procedures, methodologies, and tools must adhere to the standards laid forth by ISO 26262. All the way through a vehicle's lifespan, the ISO 26262 standard checks to make sure enough safety measures are in place.

ISSN: 1832-5505
Vol-12 Issue-04 Nov 2024

## WHY IS ISO 26262 AUTOMOTIVE INDUSTRY SAFETY STANDARD IMPORTANT?

There are many advantages for automotive original equipment manufacturers (OEMs) and suppliers when they use ISO 26262 to assess the safety of electrical and electronic components in vehicles:

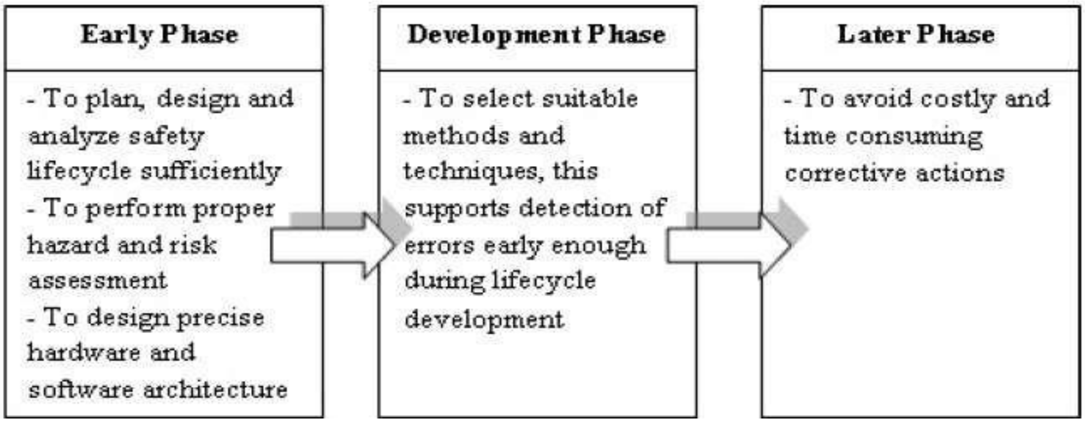
- In accordance with ISO 26262, show that you've done your homework and made sure that the vehicle and/or related systems are safe.
- Keep your edge over the competition by accurately comprehending and applying the criteria of ISO 26262.
- Prevent injury to individuals and market rejection of your items to the greatest extent possible. Inadequate safety assurance may lead to expensive product recalls and harm to a company's image.
- Streamlined entry into foreign markets by guaranteeing adherence to applicable international rules

## IMPLEMENTATION OF ISO 26262

The risks and action plans including systematic documenting, planned training, and appropriate handling of all concerns and problems must be known by all staff and management who worked with this system throughout the implementation of ISO 26262. This will guarantee that everything is under control. As seen in Figure 2, the car manufacturer is guaranteed to benefit from the standard's successful implementation. In the first stage, the item specified in the system is used to conduct risk assessments and hazard analyses. The next step is to identify all categorised dangers and assign an ASIL after establishing safety objectives (SF). To further refine into software and hardware level, technical safety standards are defined throughout the development process. In reality, it is rather difficult to alter operating processes while developing. As a result, components are assigned functional safety criteria according to the items' initial design assumptions. Therefore, in order to begin implementing ISO 26262, pilot projects are chosen. When developing new models, it's important to think forward to any problems with future systems and fix them as soon as possible. During development and the stages that follow, all of the related safety criteria are planned and executed. There are four levels of ASIL, each corresponding to a particular combination of severity, exposure likelihood, and controllability; level D

is the most basic degree of security, while level A is the most advanced. In most cases, ASIL

A–C is used. Table 2 displays a few instances of ASIL classification.



Early Phase

- To plan, design and analyze safety lifecycle sufficiently
- To perform proper hazard and risk assessment
- To design precise hardware and software architecture

Development Phase

- To select suitable methods and techniques, this supports detection of errors early enough during lifecycle development

Later Phase

- To avoid costly and time consuming corrective actions

**Figure: ISO 26262 Implementation in phases**

The development, production, and service phases, as well as the management and oversight phases, all have an impact on functional safety. This includes tasks like requirements definition, design, implementation, integration, verification, validation, and configuration. The development process and its outcomes, whether focused on functionality or quality, are inextricably linked with concerns about safety. When it comes to development processes and final products, ISO 26262 is all about safety.

Some of the words used in ISO 26262 are as follows:

**ASIL**: Automobile Safety Integrity Level (ASIL) - D is the most rigorous level and A is the least stringent level; these levels outline the item's or element's (1.69) or safety measure's (1.110) requirements of ISO 26262 and the actions to be taken to prevent an excessive residual risk (1.97). ISO 26262 9 provides a detailed description of ASIL analysis. (standard ISO 26262-1:1.6/ISO 26262-9).

**ASIL Decomposition**: "ASIL Tailoring" is another name for ASIL Decomposition, which stands for Automotive Safety Integrity Level Decomposition. Attempting to decrease the ASIL (1.6) of the related elements by assigning redundant safety criteria to adequately independent ones (1.32). (Standards ISO 26262-9 5.4.10/ISO 26262-1 1.7/ISO 26262-9 5 provide a process flow diagram).

**AUTOSAR**: "AUTomotive Open System Architecture" (AUTOSAR) - Disregarding ISO 26262, this is a freely available and standardised software architecture for the automotive industry that was created in collaboration with tool makers, suppliers, and car manufacturers. (“Autosar” in English and “AUTOSAR” in Spanish) are two online resources.

ISSN: 1832-5505
Vol-12 Issue-04 Nov 2024

**CCF**: CCF stands for "common cause failures," which are defined as the failure of two or more item components due to a single event or root cause. Dependent failures (DF) (1.22) that do not constitute cascade failures (CF) (1.13), are known as common cause failures. (Reference 26,262-1.14 from ISO 2626).

**CF**: Cascading Failure - When one component of an item fails, it might cause other components to fail as well. Dependent failures (DF) (1.22) that are not CCFs (1.14), are known as cascading failures. 11.3 according to ISO 26262-1.

**CMF**: When several components fail in the same way, it's called a common mode failure (CMF). Make use of fault tree analysis (FTA) to examine it. 3.2 of ISO 26262-10.

**DC**: Diagnostic Coverage - The percentage of hardware elements that are detected or regulated by the installed safety measures out of the total failure rate of 1.41 (1.32) and 1.41 (1.41). (1.25 according to ISO 26262-1 and 26262-5 D).

**DF**: Dependent Failure - Failures (1.39), where the sum of their unconditional probabilities cannot be used to indicate the likelihood of their simultaneous or subsequent occurrence. For example, CCFs (1.14), which are dependent failures, and CFs, which are cascading failures (1.13), are also among them. Dependent failure analysis (DFA) is described in ISO 26262-9 7 and in ISO 26262-1.22 and 26262-9 7.

**DFA**: In order to ensure that no safety-related requirements or objectives are compromised, Dependent Failure Analysis (DFA) seeks to isolate the specific events or causes that might compromise the necessary independence or freedom from interference among the provided parts. (Reference: ISO 26262-9 7).

**DIA**: DIA stands for "Development Interface Agreement," and it's a contract between a client and a vendor outlining who is responsible for what in terms of actions, evidence, and final deliverables. To illustrate, consider ISO 26262-5 B (ISO 26262 1.24/ISO 26262-8 5).

**E/E/PE**: The term "E/E/PE" refers to electrical, electronic, and programmable electronic technology, as defined in Section 3.2.6 of IEC 615084-4 (see to examples for clarification). as stated in IEC 61508-3.2.6.

**EMI**: The term "electromagnetic interference" (EMI) describes any disruption to a power circuit caused by outside sources of electromagnetic radiation or electromagnetic induction.From Wikipedia: [Wikipedia] (ISO 26262-2/http://en.wikipedia.org/wiki/Electromagn etic_interference).

**EOS**: When it comes to electrical overstress, there are a few different ways in which failures might manifest: thermally, by electromigration, or as a result of an electric field. Could lead to a latchup short circuit. (From Wikipedia) The ISO 26262-10 A.3.4.2.4 provides an example of the failure rate that may be attributed to EOS.Methods for calculations may be found in the "Reliability data handbook - Universal" (IEC TR 62380).

(ISO 26262-10 A.3.4.2.4/IEC TR 62380/http://en.wikipedia.org/wiki/Failure_ modes_of_electronics) is a model for predicting the dependability of electronic components, printed circuit boards, and machinery.

## Details of ISO 26262

Following several modifications, the 2nd Edition of ISO 26262 was issued in December 2018 following the 1st Edition's November 2011 publication. While the first edition focused on mass-produced passenger vehicles under 3,500 kg, the second edition widened the scope to include trucks, buses, and motorbikes. The updated contents of the 2nd Edition will be the primary subject of this discussion on ISO 26262.

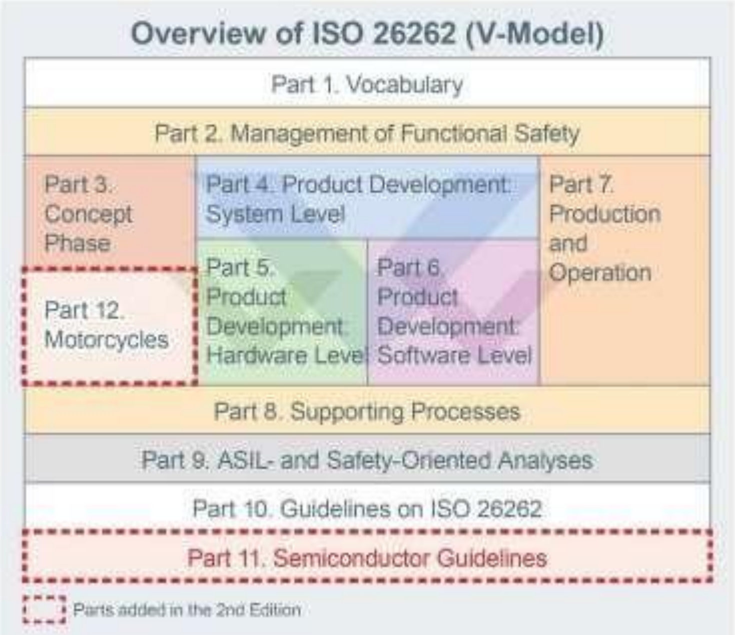

Overview of ISO 26262 (V-Model)
Part 1. Vocabulary
Part 2. Management of Functional Safety
Part 3. Concept Phase
Part 4. Product Development: System Level
Part 7. Production and Operation
Part 12. Motorcycles
Part 5. Product Development: Hardware Level
Part 6. Product Development: Software Level
Part 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: Overview of ISO 26262**

## Functional security

The concept of functional safety arose out of the need to build goods and services in a way that people can't possibly anticipate or prevent potentially harmful occurrences. Designers should think about both systematic and random failures while making safety equipment for the workplace. The former helps make sure that the product isn't accidentally hurting anybody. Systematic failures, sometimes known as bugs, are the outcome of issues with the design. The first step in preventing systemic failures is to develop a reliable design approach that is impervious to design mistakes. The process begins with requirements gathering and then moves on to developing specifications. Along the way, we explain and examine each stage in detail; this includes creating design prototypes, verifying them, and evaluating them. Maintaining documentation of all manufacturing-related paperwork is essential, as is the records are accessible whenever needed. Following production, the most prevalent types of failures occur. Given that random errors are impossible to totally prevent Even if everything goes wrong, there should still be a security mechanism to keep you secure.

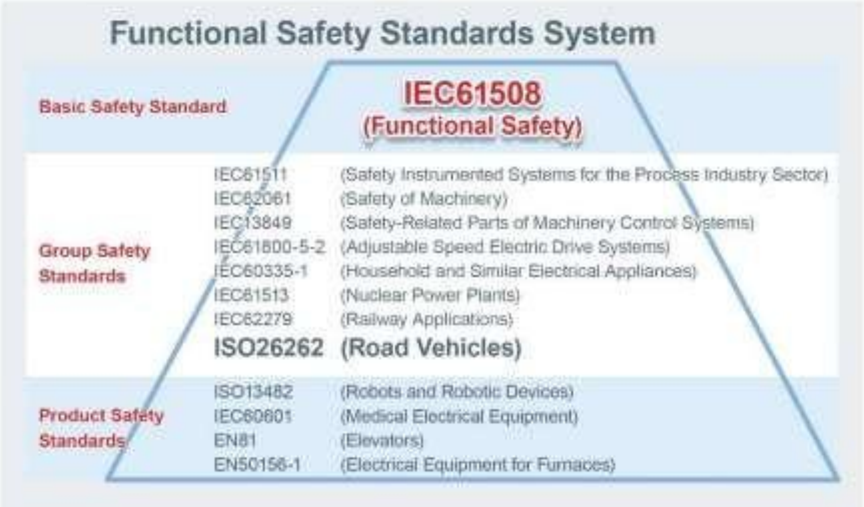

Functional Safety Standards System
Basic Safety Standard
IEC61508
(Functional Safety)
Group Safety Standards
IEC61511 (Safety Instrumented Systems for the Process Industry Sector)
IEC62061 (Safety of Machinery)
IEC13849 (Safety-Related Parts of Machinery Control Systems)
IEC61800-5-2 (Adjustable Speed 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: Functional Safety Standards System**

## RESULTS AND DISCUSSION

## SIMULATION RESULTS

There are several benefits of using LED lights instead of traditional light bulbs: The results of the simulations run by the 16-bit CPU are shown in the figures below. The test bench receives an alarm signal from the clock generator, which is used to test the functioning. Using a test case to execute programmes inside memory cells, the simulator mimics CPUs.

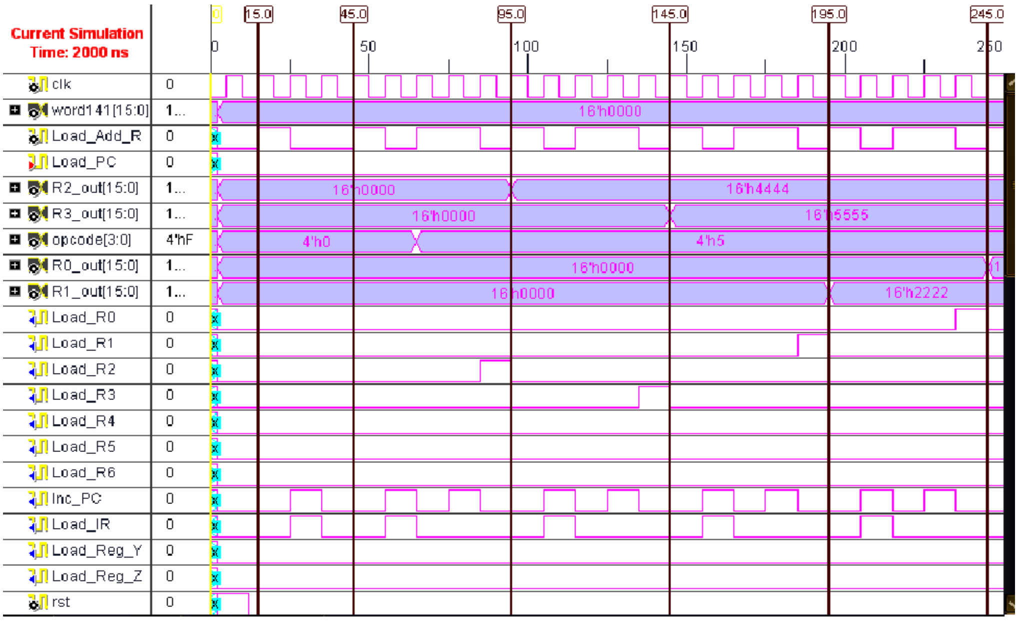


**Figure: Simulation results for NOP Instructions window 1 for RD**

Figures 15 and 245 show the outcomes of the simulations, respectively. Within 15 to 45 nanoseconds, NOP's instructions are carried out. It takes merely three clock cycles as it doesn't need a cycle to be executed. There are four Read operations, and each one takes between 45 and 245 nanoseconds, or five clock cycles.

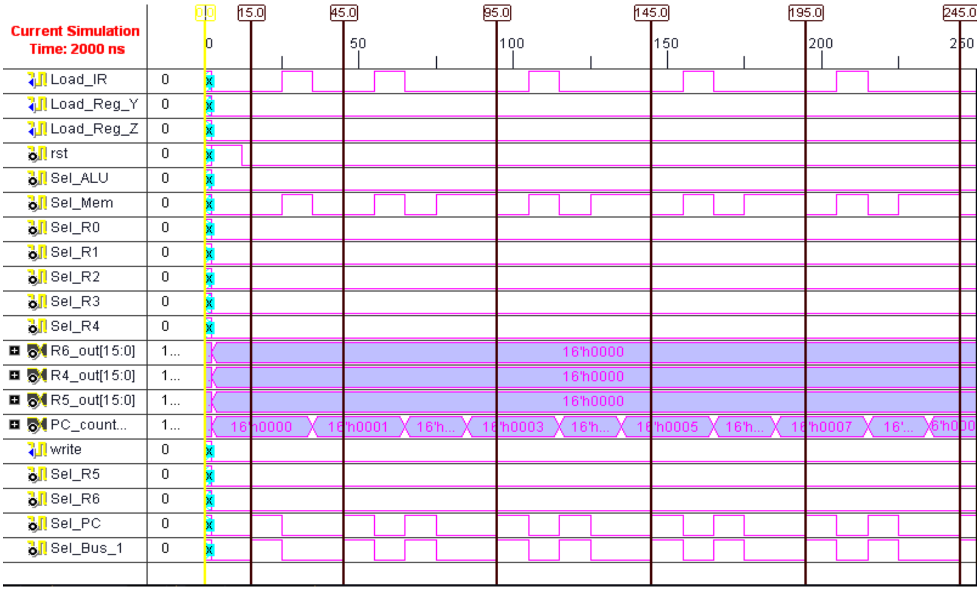


**Figure: Simulation results for NOP Instructions window 2 for RD**

## CONCLUSION

There would be several advantages for the car industry in the long run as a consequence of this implementation's success. Although the complete integration of this standard for current safety-related E/E systems will be a lengthy process, the advantages of its application will increase worldwide competitiveness in the automobile industry. Many avenues for investigation in the field of vehicle safety evaluation remain uncharted as ISO 26262 does not specify in detail how to achieve the stated goals. The automobile industry may need some help adopting this new standard, and a variety of methodologies and techniques could be useful in this regard, including risk and hazard assessment and the creation of systems, software, and hardware. There are several possibilities and difficulties for research that supports the methodologies and procedures now that the standard is about to be implemented by the automobile industry. The automobile industry may look to ISO 26262 for direction on how to keep up the high level of safety they've already attained and how to implement safety systems of the next generation.

## REFERENCES

1. Born, M., Favaro, J., and Kath, O. (2010). Application of ISO DIS 26262 in practice, In Proceedings of the 1st Workshop on Critical Automotive applications Robustness& Safety, 3-6.
2. Dardar, R., Gallina, B., Johnsen, A., Lundqvist, K., and Nyberg, M. (2012). Industrial Experiences of Building a Safety Case in Compliance with ISO 26262, In 2012 IEEE 23rd International Symposium on Software Reliability Engineering Workshops, 349– 354.
3. Habli, I., Ibarra, I., Rivett, R. S., and Kelly, T. (2010). Model-Based Assurance for Justifying Automotive Functional Safety, In SAE 2010 World Congress & Exhibition,2010–01–0209.
4. Hillenbrand, M., Heinz, M., Adler, N., Matheis, J., and Muller-Glaser, K. D. (2010). Failure Mode and Effect Analysis based on Electric and Electronic Architectures of Vehicles to Support the Safety Lifecycle ISO/DIS 26262, In IEEE International Symposium on Rapid System Prototyping (RSP), 1–7.
5. Seo-Hyun, C. Jin-Hee, J. Yangjae, P. Sachoun, and H. Tae-Man, "Automotive hardware development according to ISO 26262," in Advanced Communication Technology (ICACT), 2011 13th International Conference on, 2011, pp. 588-592.
6. R. Mariani, "The impact of functional safety standards in the design and test of reliable and available integrated circuits," in Test Symposium (ETS), 2012 17th IEEE European, 2012, pp. 1-1.
7. M. Born, J. Favaro, and O. Kath, "Application of ISO DIS 26262 in practice," presented at the Proceedings of the 1st Workshop on Critical Automotive applications: Robustness & Safety, Valencia, Spain, 2010.
8. "ISO 26262 Road vehicles - Functional safety - Part 5: Product development at the hardware level," ed: International Organization for Standardization, 2011.