International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

FUNCTIONAL SAFETY IN AUTOMOTIVE SEMICONDUCTORS: A COMPREHENSIVE REVIEW OF ISO 26262 PRACTICES

Sujan Rao

sujangopalrao@gmail.com

Independent Researcher USA

Abstract

The rapid evolution of modern vehicles toward electrification, advanced driver assistance systems (ADAS), and autonomous driving has dramatically increased the reliance on high-performance semiconductor devices for safety-critical operations. Ensuring that these devices operate reliably under all conditions has made functional safety an indispensable engineering requirement. ISO 26262, the automotive functional safety standard, provides a structured framework for identifying hazards, defining safety goals, allocating hardware and software safety requirements, and validating safety mechanisms across the vehicle lifecycle. This review presents a comprehensive examination of ISO 26262 practices as applied to automotive semiconductor components, with emphasis on the unique architectural, diagnostic, and verification challenges present in microcontrollers, mixed-signal ICs, power devices, sensor interfaces, and heterogeneous ADAS SoCs. Key topics include safety requirement allocation, Safety Element out of Context (SEooC) development, FMEDA and FTA-based safety analyses, quantitative hardware metrics, and design patterns that enhance fault tolerance and diagnostic coverage. Industrial case studies illustrate practical implementation strategies and highlight the growing importance of redundancy, safety islands, ECC-protected memories, and in-field diagnostics. The paper also identifies emerging challenges related to advanced semiconductor nodes, AI accelerators, cybersecurity interactions, chiplet-based architectures, and mixed-criticality workloads. Future research directions emphasize the need for integrated safety–security co-engineering, scalable EDA tools, formal verification methodologies, and new diagnostic mechanisms for AI-enabled automotive compute platforms. Overall, this review provides a consolidated perspective on how ISO 26262 principles guide the safe design and deployment of semiconductor devices that underpin next-generation intelligent and autonomous vehicles.

Keywords. Functional Safety, ISO 26262, Automotive Semiconductors, ASIL, SEooC, FMEDA, FTA, Hardware Safety Metrics, Diagnostic Coverage, Soft Errors, Automotive MCUs, ADAS SoCs, Mixed-Signal Safety, Safety Mechanisms, Chiplet Architecture, SOTIF, Cybersecurity Integration.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1. Introduction

The rapid transformation of the automotive industry toward highly automated, electrified, and software-defined vehicles has dramatically increased the reliance on semiconductor devices for safety-critical operations. Modern vehicles integrate hundreds of semiconductor components—including microcontrollers, system-on-chips (SoCs), power devices, sensor interfaces, memory subsystems, and specialized accelerators—each performing complex real-time functions essential for safe vehicle operation. As automotive systems evolve toward Level 3–Level 5 autonomy, semiconductor reliability and functional correctness have become central to preventing hazardous events [1]. This trend has repositioned functional safety as a mandatory engineering discipline, with ISO 26262 emerging as the definitive international standard governing safety-related electrical and electronic systems in road vehicles.

Semiconductors now control or influence nearly every aspect of vehicle behavior, ranging from powertrain control, braking, and steering to advanced driver assistance systems (ADAS) and domain controllers. The enormous increase in computational complexity and integration density introduces new safety risks such as systematic design faults, random hardware failures, transient soft errors, thermal aging, and interactions between heterogeneous IP blocks. Unlike traditional automotive components that degrade gradually, semiconductor failures can occur abruptly and propagate rapidly, necessitating robust safety architectures, diagnostic mechanisms, and compliance-driven development workflows. ISO 26262 mandates a structured safety lifecycle to mitigate such risks, ensuring that semiconductor components deliver predictable and fail-safe behavior across their operational lifetime [2].

The importance of ISO 26262 compliance is amplified by the emergence of semiconductor-focused safety requirements in Part 11 (for semiconductors) and the widespread adoption of the Safety Element out of Context (SEooC) development approach. These frameworks help semiconductor manufacturers develop reusable safety components, define safety mechanisms, quantify risk using architectural metrics such as SPFM, LFM, and PMHF, and implement comprehensive failure-mode analyses like FMEA and FMEDA [3][4]. As automotive OEMs increasingly outsource complex silicon development to semiconductor suppliers, compliance evidence, safety manuals, and well-structured safety cases have become essential deliverables embedded into the supply chain.

Despite significant advancements, functional safety for automotive semiconductors remains challenging due to the rapidly evolving nature of semiconductor technologies. Shrinking process nodes introduce increased susceptibility to radiation-induced faults; AI and machine-learning accelerators introduce non-deterministic behavior; and chiplet-based architectures create new safety interaction boundaries [5]. In addition, the convergence of safety with cybersecurity (ISO 21434) and safety-of-the-intended-functionality (SOTIF, ISO 21448) creates new cross-domain requirements that semiconductor suppliers must address. These complexities underline the need for a comprehensive review of ISO 26262 practices specific to semiconductor development.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1.1 Background and Motivation

Functional safety has always been a critical component of automotive engineering, but the transition to electrically driven, connected, and autonomous vehicles has magnified its importance. Semiconductor content per vehicle has increased exponentially, and their malfunction now directly affects safety goals such as avoiding collisions, maintaining vehicle stability, and ensuring accurate environment perception. This motivates a detailed review of ISO 26262 practices tailored specifically for semiconductor technologies.

1.2 Role of Semiconductors in Modern Vehicles

From ADAS perception pipelines to battery management systems, semiconductors perform the sensing, computation, actuation, and communication that govern vehicle safety. Their failure modes and lifetimes differ fundamentally from mechanical parts, making them central to functional safety engineering.

1.3 Need for ISO 26262–Compliant Semiconductor Development

ISO 26262 provides a structured approach to identifying hazards, deriving safety goals, allocating safety requirements, and validating compliance. Semiconductor companies must meet stringent ASIL targets and safety metrics to ensure their components integrate safely into vehicle architectures.

1.4 Objectives and Scope of the Review

The purpose of this review is to comprehensively analyze ISO 26262 requirements applicable to semiconductor components, examine industry practices, evaluate safety analysis techniques, and outline emerging challenges in safety-compliant semiconductor development.

2. Fundamentals of Functional Safety and ISO 26262

Functional safety represents the discipline of ensuring that systems operate correctly in response to their inputs—including foreseeable failures—such that hazards leading to unsafe conditions are avoided or mitigated. In the context of automotive systems, functional safety addresses the risks arising from malfunctioning electrical and electronic (E/E) components, including semiconductors that underpin the control logic of modern vehicles [6]. As vehicles become more autonomous, connected, and computation-intensive, functional safety processes must rigorously manage both systematic and random hardware failures across increasingly complex semiconductor architectures. ISO 26262 serves as the primary automotive functional safety standard, providing a structured safety lifecycle, risk classification frameworks, and work products required to demonstrate that E/E systems contribute to acceptable levels of risk throughout the vehicle's lifetime [7].

ISO 26262 is derived from the generic functional safety standard IEC 61508, but adapted for the specific needs of road vehicles. It encompasses a set of ten primary parts covering management, concept, system-level design, hardware and software development, production, operation, and supporting processes [8]. ISO 26262 introduces the Automotive Safety Integrity

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Level (ASIL) as its central risk-classification mechanism, guiding the rigor of analysis, verification, and validation activities. Semiconductors, which experience random faults (such as single-event upsets, aging-induced degradation, and transient electrical disturbances) and systematic faults (design, specification, and integration errors), must comply with specific ISO 26262 requirements to ensure safe vehicle operation [9]. The standard mandates robust safety analyses—such as FMEA, FMEDA, FTA, and CCA—to quantify and manage risk, and prescribes architectural metrics like SPFM, LFM, and PMHF to evaluate hardware robustness [10].

With the publication of ISO 26262:2018, Part 11 provides dedicated guidance for semiconductor development, acknowledging their unique failure behaviors, architectural complexities, and diagnostic needs. This section provides a foundational understanding of functional safety principles and the role ISO 26262 plays in guiding semiconductor design, verification, and validation [11].

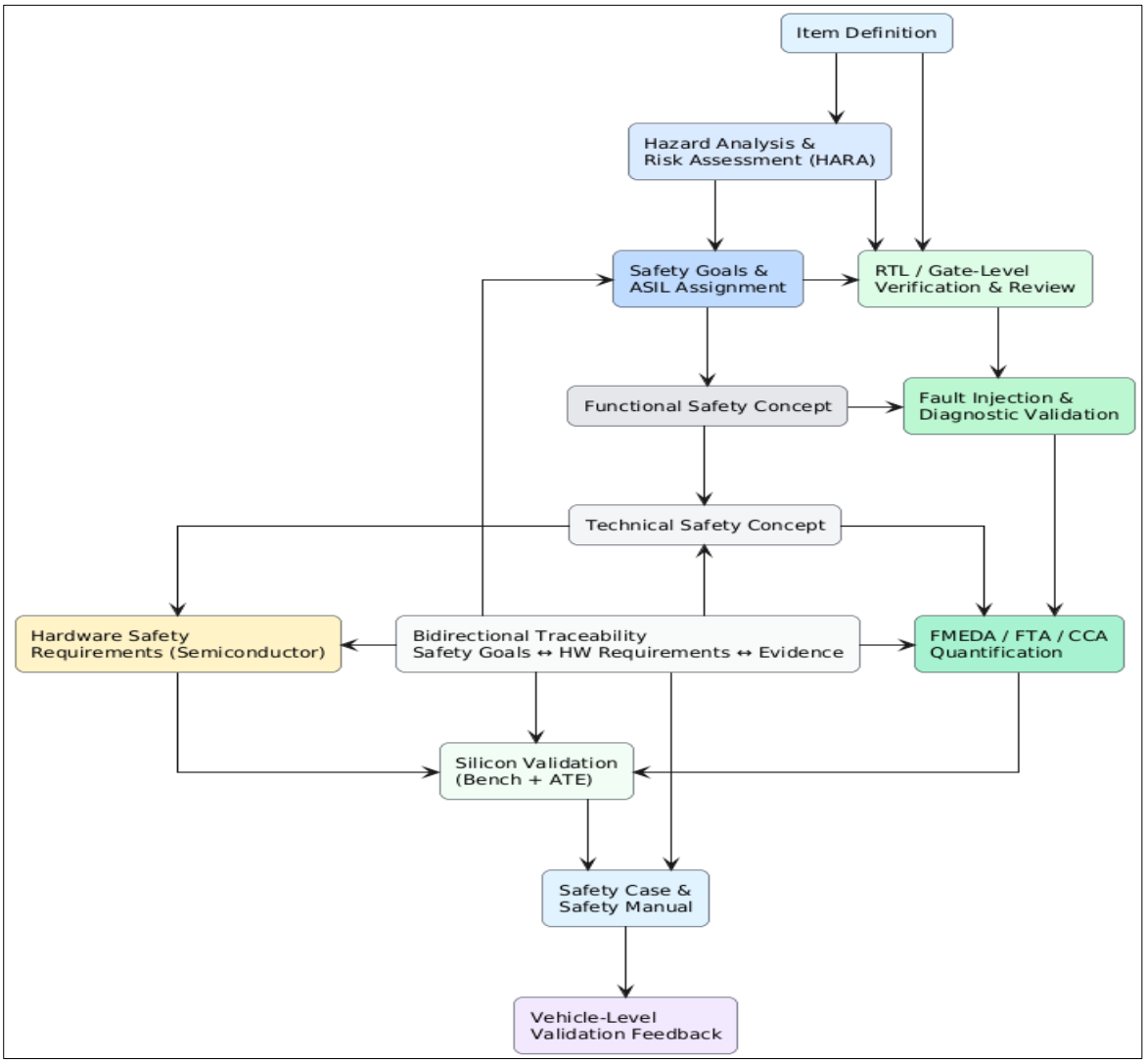

Figure 1. ISO 26262 Functional Safety V-Model for Semiconductors

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2.1 Basic Concepts: Hazard, Risk, Faults, Failures, and Safety Goals

A *hazard* is a potential source of harm, while *risk* is determined by the severity, exposure, and controllability of that harm. Semiconductors contribute to hazards when they malfunction, either due to systematic design defects or random physical events. ISO 26262 defines a *fault* as an abnormal condition and a *failure* as the termination of the ability to perform a required function. Safety goals represent high-level safety requirements derived to prevent hazardous events [12]. For semiconductor devices, safety goals often involve preventing incorrect actuation, loss of control, or undetected errors in sensing or computation. Understanding these concepts forms the foundation of safety engineering.

2.2 Evolution from IEC 61508 to ISO 26262

IEC 61508 introduced a generic functional safety framework for E/E/PE systems across industries. ISO 26262 extends these principles to the automotive sector, incorporating vehicle-specific risk factors, transient operational environments, and lifecycle processes. Over its major revisions—2011 and 2018—the scope expanded from traditional systems to semiconductors, trucks/buses, motorcycles, and highly automated functions. ISO 26262:2018 Part 11 specifically addresses semiconductor safety considerations, marking a major milestone for chip manufacturers supplying the automotive market [13].

2.3 ISO 26262 Structure: Parts, Clauses, and Life Cycle Phases

ISO 26262 consists of ten core parts:

- **Part 1** – Vocabulary
- **Part 2** – Management of functional safety
- **Part 3** – Concept phase
- **Part 4** – System-level development
- **Part 5** – Hardware development
- **Part 6** – Software development
- **Part 7** – Production, operation, service
- **Part 8** – Supporting processes
- **Part 9** – ASIL-oriented analyses
- **Part 10** – Guidelines
- **Part 11** – Semiconductor development

The lifecycle follows a V-model structure, beginning with hazard analysis and culminating in verification, validation, and safety case development. Semiconductor development aligns primarily with Parts 5, 8, 9, and 11, with deliverables such as hardware requirements, FMEDA, safety mechanisms definition, and architectural metrics.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2.4 Automotive Safety Integrity Levels (ASILs) and Risk Classification

ASILs classify risk into four levels: **ASIL A** (lowest) to **ASIL D** (highest). Classification depends on:

- **Severity (S)** – Impact of failure on the occupants/road users
- **Exposure (E)** – Probability of operating conditions where the hazard may occur
- **Controllability (C)** – Driver's ability to avoid harm

Semiconductor components inherit ASIL requirements from system-level safety goals. Higher ASILs demand more robust diagnostic coverage, stricter design rules, redundancy, rigorous verification, and compliance evidence. Components may contain ASIL-mixed or decomposed elements requiring safety partitioning and independence.

2.5 Functional Safety Lifecycle and V-Model Overview

The functional safety lifecycle spans concept, development, production, operation, and decommissioning. The V-model organizes these activities into two symmetric halves: definition (left side) and verification/validation (right side). For semiconductors, key lifecycle activities include:

- safety requirements allocation,
- hardware architecture specification,
- selection of safety mechanisms,
- FMEDA-driven design optimization,
- fault injection and coverage analysis,
- safety case creation and release documentation.

The lifecycle ensures traceability from safety goals through implementation to verification evidence, forming the backbone of ISO 26262 compliance.

3. Automotive Semiconductor Landscape and Safety Context

Semiconductors form the computational backbone of modern vehicles, enabling functions ranging from low-level sensing and actuation to high-performance automated driving systems. As vehicles evolve into complex cyber-physical systems with interconnected control units and domain controllers, semiconductor devices must deliver deterministic, fault-tolerant, and real-time processing under harsh environmental conditions. The operational landscape places unique demands on semiconductor reliability: extreme temperatures, voltage variations, mechanical vibrations, electromagnetic interference (EMI), and prolonged lifetime requirements exceeding 15 years. With the rapid increase of electronics per vehicle—from legacy ECUs to centralized compute platforms—semiconductors have become critical contributors to functional safety, making their design, analysis, and verification essential components of ISO 26262–compliant development [12].

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Automotive semiconductors serve diverse safety-critical applications such as ADAS perception, powertrain management, braking, steering control, airbag deployment, and battery management. Failures in any of these domains can lead to hazardous events, especially in autonomous and electric vehicles where decision-making heavily depends on reliable sensor processing and computational integrity. The complexity of semiconductor architectures further increases safety risks: a single SoC may integrate CPUs, GPUs, DSPs, NPU/AI accelerators, real-time islands, memory subsystems, bus interconnects, sensor interfaces, and power regulators. Interactions among these subsystems can produce subtle failure modes that require rigorous safety mechanisms and quantitative analysis. ISO 26262:2018 Part 11 recognizes this complexity and provides semiconductor-specific guidance addressing diagnostic coverage, architectural metrics, and failure-mode modeling tailored to chip-level designs [14].

This section provides a structured overview of the automotive semiconductor ecosystem, the safety-critical applications they support, and the operational challenges that influence functional safety requirements.

3.1 Types of Automotive Semiconductors

Automotive electronics rely on a broad spectrum of semiconductor devices, each serving a unique safety role:

- **Microcontrollers (MCUs)** – Host safety-critical control loops (e.g., braking, steering, powertrain) and often incorporate dual-core lockstep, ECC-protected memories, and watchdog mechanisms.
- **System-on-Chips (SoCs)** – Used in domain controllers, ADAS compute units, infotainment, and autonomous driving platforms, integrating CPUs, GPUs, NPUs, and accelerators.
- **Sensors & Sensor Interfaces** – LiDAR, radar, cameras, IMUs, and pressure sensors require safe signal processing and interface components with diagnostic self-tests.
- **Power Devices** – IGBTs, MOSFETs, gate drivers, and PMICs in EVs demand robust thermal and electrical protection to avoid catastrophic failures.
- **Memory Devices** – DRAM, SRAM, Flash, and EEPROM require ECC, wear-leveling, and redundancy due to high fault susceptibility.
- **Analog & Mixed-Signal ICs** – ADCs, DACs, comparators, and sensor front-ends are crucial for accurate perception and control-loop feedback.
- **AI/ML Accelerators** – Used in ADAS and autonomous vehicles; they pose new challenges due to non-determinism and high computational density.

The diversity of semiconductor devices necessitates tailored functional-safety strategies, as no single safety mechanism fits all architectures.

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3.2 Safety-Critical Applications of Automotive Semiconductors

Semiconductors contribute directly to safety-critical functions across the vehicle's electronic architecture:

- **ADAS & Autonomous Driving:** Perception (sensor fusion), decision-making, and path-planning rely on high-performance SoCs.
- **Powertrain Control:** ICs manage ignition timing, fuel injection, and torque distribution with real-time constraints.
- **Braking and Steering:** MCUs and sensor ICs ensure ABS, ESC, EPS, and brake-by-wire reliability.
- **Battery Management Systems (BMS):** Power-electronics devices monitor voltage, current, and thermal behavior in EV batteries.
- **Chassis and Body Control:** Airbags, seatbelt tensioners, lighting, and HVAC all depend on safe semiconductor operation.
- **Vehicle Communication Networks:** Transceivers for CAN, LIN, FlexRay, and Ethernet support safe data transmission between ECUs.

Failures in these domains can directly cause hazardous events; thus, semiconductor integrity is vital for preventing unintentional acceleration, loss of braking, steering failure, or misinterpretation of environmental conditions.

3.3 Failure Modes in Semiconductor Devices (Random vs Systematic)

Automotive semiconductors experience two broad categories of failures:

Random Hardware Failures

Caused by physical phenomena such as:

- thermal noise,
- electromigration,
- radiation-induced soft errors (SEUs/MBUs),
- hot-carrier injection,
- dielectric breakdown,
- aging and wear-out.

These failures must be quantified using **FIT rates**, and mitigated using redundancy, ECC, CRC, and real-time diagnostics.

Systematic Failures

Occur due to:

- design defects,

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- specification errors,
- toolchain bugs,
- integration mistakes,
- incorrect safety assumptions.

ISO 26262 requires rigorous processes, documentation, verification, and validation to prevent systematic failures from escaping into production.

Both failure types influence architectures, safety mechanisms, and verification strategies.

3.4 Environmental and Operational Stresses in Automotive Domains

Automotive environments are significantly harsher than consumer electronics. Semiconductors must withstand:

- **Wide temperature ranges:** –40°C to +150°C
- **Voltage transients:** load dumps, ESD, EMI
- **Mechanical vibration and shock** in powertrain and chassis ECUs
- **Long operational lifetime:** 15–20 years
- **High humidity, chemical exposure, and thermal cycling**

Such conditions accelerate aging, promote random failures, and challenge diagnostic reliability. Therefore, environmental robustness is inseparable from functional safety.

3.5 Interaction with Related Standards (ISO 21434, ISO 21448, AEC-Q100)

Semiconductor safety compliance intersects with multiple automotive standards:

- **ISO 21434 — Cybersecurity**
  Ensures secure boot, protected communication, and resistance to cyberattacks that could compromise safety functions.
- **ISO 21448 — Safety of the Intended Functionality (SOTIF)**
  Addresses performance limitations of perception systems (e.g., camera misdetections), especially for AI-based accelerators.
- **AEC-Q100/Q200**
  Qualification standards for reliability and stress testing of ICs in harsh automotive environments.
- **SAE J3016**
  Defines autonomy levels and drives high-performance computing requirements.

Together, these standards ensure that semiconductor components meet holistic safety, reliability, and cybersecurity criteria.

4. ISO 26262 Requirements for Semiconductor Components

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Automotive semiconductor development must comply with ISO 26262 to ensure that hardware devices contribute to the safe operation of electrical and electronic (E/E) systems throughout the vehicle lifecycle. Unlike typical consumer-grade semiconductors, automotive chips must withstand long-term field conditions, include robust diagnostic capabilities, support traceable safety requirements, and demonstrate predictable behavior under both normal and faulty conditions. ISO 26262:2018 introduced **Part 11**, dedicated entirely to semiconductors, reflecting their increasing importance in safety-critical automotive architectures. Part 11 provides guidance for developing semiconductor Safety Elements out of Context (SEooCs), defining safety mechanisms, conducting hardware safety analyses, and ensuring adequate diagnostic coverage for random and systematic failures.

ISO 26262 imposes rigorous requirements across the entire semiconductor development lifecycle, beginning from safety goal derivation, allocation of hardware safety requirements, definition of the hardware architecture, identification of safety mechanisms, and quantitative assessment of architectural metrics. Semiconductor suppliers must provide comprehensive documentation—including safety manuals, safety analyses (FMEDA, FTA, CCA), verification reports, and safety cases—to enable automotive OEMs and Tier-1 suppliers to integrate these devices into higher-level systems. This section explains key ISO 26262 requirements tailored specifically to semiconductor components and provides an overview of how compliance is achieved at the silicon, IP, and SoC levels.

4.1 Allocation of Safety Requirements to Hardware Elements

Once system-level safety goals are defined during hazard analysis, the next step involves decomposing these goals into hardware safety requirements. For semiconductors, requirements may include:

- detection of transient and permanent faults,
- implementation of error-correction mechanisms,
- ensuring redundant computation or safe-state feedback,
- bounded reaction times to detected faults,
- maintaining safe outputs under erroneous inputs,
- avoiding unintended actuation due to hardware failures.

These requirements are allocated at the IP, subsystem, or SoC level based on failure impact, propagation paths, and architectural constraints. ISO 26262 mandates traceability from safety goals → technical safety requirements → hardware requirements → verification evidence, ensuring complete coverage through the V-model lifecycle.

4.2 Safety Element out of Context (SEooC) for Semiconductors

Semiconductor suppliers often develop chips without knowledge of the final vehicle environment. ISO 26262 Part 11 introduces the concept of **SEooC (Safety Element out of**

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Context) to enable the development of reusable, safety-compliant semiconductor components. A semiconductor SEooC must:

- define its assumed safety requirements and operating conditions,
- specify integration assumptions (voltage, frequency, timing constraints),
- describe intended diagnostic interactions with the system,
- outline limitations and boundaries of safe operation,
- provide a detailed *safety manual* for integrators.

SEooCs enable semiconductor companies to achieve ISO 26262 compliance even when the final system-level safety goals are unknown.

4.3 Hardware Safety Requirements and Safety Mechanism Specifications

ISO 26262 requires semiconductor designs to implement safety mechanisms that detect, control, or mitigate hardware faults. Typical safety mechanisms include:

- **ECC-protected memories**, supporting SEC-DED or advanced multi-bit detection,
- **CPU lockstep architectures** for redundant instruction execution,
- **Built-In Self Test (BIST)** for digital, analog, and memory subsystems,
- **Clock/power supervisors** to detect glitches or brownouts,
- **Watchdog timers** for control-flow monitoring,
- **End-to-end protection** using CRC, parity, and data path monitoring,
- **Thermal, voltage, and current monitors** in power devices,
- **Redundant comparators and threshold monitors** in mixed-signal IP.

ISO 26262 Part 11 mandates that safety mechanisms must be correctly modeled in safety analyses and included in FMEDA tables for diagnostic coverage estimation.

4.4 Hardware Architectural Metrics: SPFM, LFM, and PMHF

Semiconductor compliance requires quantitative evaluation of three key metrics:

Single-Point Fault Metric (SPFM)

Measures the proportion of faults that are **not single-point faults**, i.e., faults that do not lead to violation of safety goals without detection.

Latent Fault Metric (LFM)

Represents coverage for faults that remain hidden until a second fault occurs (e.g., redundant channel failure).

Probabilistic Metric for Hardware Failure (PMHF)

Specifies the acceptable failure rate (in FIT) for each ASIL level:

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- ASIL D: ≤ 10 FIT
- ASIL C: ≤ 100 FIT
- ASIL B: ≤ 1000 FIT
- ASIL A: qualitative reasoning allowed

Semiconductor suppliers must construct accurate FMEDA models including FIT rates, fault modes, and diagnostic coverage to compute these metrics.

4.5 Diagnostic Coverage and Safe/Fault-Tolerant Behavior

Diagnostic coverage (DC) quantifies the effectiveness of safety mechanisms in detecting faults. For semiconductor devices, DC must account for:

- transient soft errors,
- stuck-at faults,
- bridging faults between signals,
- clock/power domain failures,
- memory bit-cell and row/column failures,
- analog drift or parameter degradation.

ISO 26262 requires documentation of:

- fault detection latencies,
- safe-state transitions,
- minimum reaction times,
- coverage justifications,
- fault-injection validation evidence.

High ASIL levels (ASIL C/D) demand both high detection rates and low response times, especially for safety-critical domains like braking, steering, or ADAS perception.

4.6 Decomposition, Redundancy, and Independence Requirements

To satisfy stringent ASIL requirements, ISO 26262 allows **decomposition**, where a high ASIL safety goal is achieved using multiple lower-ASIL components, provided independence is ensured. For semiconductors, decomposition may involve:

- redundant computing cores (dual-core lockstep, triple modular redundancy),
- replicated sensor interfaces,
- independent voltage/clock domains,
- parallel memory arrays with mutual monitoring,

Received: August 07, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- safety islands architecturally separated from application processors.

Independence must be demonstrated via:

- physical separation,
- diverse implementation,
- separate timing domains,
- isolation mechanisms in interconnects and fabric switches.

These techniques ensure that a single common-cause event does not compromise all redundant channels.

5. Safety Analysis Techniques for Automotive Semiconductors

Safety analysis forms the backbone of ISO 26262–compliant semiconductor development, ensuring that hardware faults do not lead to violations of safety goals and that implemented safety mechanisms achieve sufficient diagnostic coverage across all failure modes. Automotive semiconductors are subject to both random hardware faults arising from physical degradation or environmental effects, and systematic faults that originate from design defects, specification errors, toolchain issues, or process misalignments. ISO 26262 mandates multiple structured safety analysis methods to identify, classify, and mitigate these faults through modeling, quantitative assessment, and experimental validation.

For semiconductor suppliers, safety analysis is performed at various abstraction levels—IP block, subsystem, and full SoC. At the earliest stage, designers conduct preliminary analyses to understand critical components, operating conditions, and failure propagation. As the design matures, detailed hardware-level analyses such as FMEDA and FTA quantify the impact of faults and determine compliance with architectural metrics (SPFM, LFM, PMHF). In advanced semiconductor designs such as ADAS SoCs, multi-core MCUs, mixed-signal front-ends, and AI accelerators, safety analyses must consider interactions between analog and digital domains, cross-domain dependencies, shared resources, and systemic error propagation.

Table 1: Comparison of Safety Analysis Techniques Used in ISO 26262–Compliant Semiconductor Development

Technique	**Primary Purpose**	**Fault Types Addressed**	**ISO 26262 Relevance**	**Semiconductor Use Cases**
FMEA (Failure Modes & Effects Analysis)	Identify failure modes and assess their local/system effects	Random & systematic (functional faults)	Part 5 (Hardware Development)	Memory bit faults, logic gate faults, ADC offset errors, voltage monitor failures

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

FMEDA (Failure Modes, Effects & Diagnostic Analysis)	Quantify diagnostic coverage, safe vs. dangerous faults, and compute SPFM/LFM/PMHF	Random hardware faults	Part 5, Part 11	Safety mechanism modeling, estimating FIT contributions, evaluating ECC, lockstep, BIST
FTA (Fault Tree Analysis)	Top-down analysis of fault combinations leading to hazards	Multiple-point & latent faults	Part 9 (ASIL-oriented analyses)	Cross-block failure propagation in SoCs, evaluating clock/power tree faults
CCA (Common Cause Analysis)	Identify faults affecting redundant channels simultaneously	CCF, EMI, environmental, shared resources	Part 9	Redundant CPUs, duplicated ADCs, multi-rail PMIC designs
DFA (Dependent Failure Analysis)	Evaluate failures that depend on shared resources or interactions	Interdependent faults across blocks	Part 9	Multicore SoCs with shared buses, interconnect fabrics, caches
Transient Fault Analysis	Model soft errors, SEUs, MBUs, radiation effects	Transient/random	Part 11	SRAM SEU analysis, NPU/AI accelerator transient modeling, DRAM retention
Analog/Mixed-Signal Fault Modeling	Simulate drift, parameter variation, and	Analog, thermal, parametric failures	Part 11	ADC, PLL, sensor front-end drift/stuck faults

Received: August 07, 2025

Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	performance degradation			
Fault Injection (RTL, gate-level, AMS)	Validate safety mechanism detection and system reaction	Digital + analog faults	Part 5, Part 11	Lockstep CPU validation, ECC test, watchdog behavior verification
Reliability & FIT Rate Estimation	Predict lifetime failure rates across process, voltage, and temperature	Aging, thermal cycling, wear-out	Part 11	IGBT/MOSFET degradation, electromigration modeling, SRAM wear
Model-Based Safety Analysis Tools	Automated failure propagation & FMEDA generation	Random + systematic	Part 8 (Tool Qualification)	EDA-assisted safety modeling for billion-gate SoCs

6. Conclusion

Functional safety has emerged as a foundational requirement for modern automotive semiconductors as vehicles transition toward electrification, advanced driver assistance systems, and higher levels of autonomy. ISO 26262 provides the structured safety lifecycle, analytical rigor, and verification discipline needed to ensure that semiconductor devices operate reliably despite increasing architectural complexity, harsh environmental conditions, and long operational lifetimes. This review highlighted the pivotal role of semiconductors in safety-critical automotive functions and discussed how ISO 26262 Part 11 establishes specialized guidance tailored to the unique challenges of IC design, verification, and integration. The evolution of semiconductor technologies—from traditional MCUs and mixed-signal front-ends to heterogeneous ADAS SoCs and domain controllers—has significantly expanded the scope of functional safety engineering. The discussion in this paper covered key elements such as allocation of safety requirements, SEooC development practices, architectural safety mechanisms, diagnostic approaches, and quantitative evaluation through SPFM, LFM, and PMHF. Safety analysis methodologies including FMEDA, FTA, and mixed-signal analysis were shown to be essential for assessing fault behavior, determining diagnostic coverage, and supporting compliance across different ASIL levels. Case studies further illustrated how leading semiconductor companies implement ISO 26262 through redundant architectures, lockstep CPUs, ECC-protected memories, built-in self-tests, and robust analog safety circuits to achieve safe and predictable operation. At the same time, this review identified several emerging challenges that require significant attention. The continuous scaling of semiconductor technologies introduces heightened susceptibility to soft errors, increased

Received: August 07, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

variability, and new types of failure interactions—especially in chiplet-based or 3D integrated architectures. The rapid integration of AI accelerators and machine-learning-based perception pipelines introduces non-deterministic behaviors that traditional hardware safety analysis cannot fully capture, necessitating closer alignment with SOTIF (ISO 21448) and new diagnostic paradigms tailored for AI. The growing interdependence of functional safety and cybersecurity further complicates risk assessment, as malicious attacks can now induce safety-critical faults or disable safety mechanisms. Increasing SoC complexity also exposes limitations in existing EDA tools, fault injection methodologies, and mixed-signal safety verification flows. Despite these challenges, the future of functional safety in automotive semiconductors is promising. Emerging trends point toward the development of safety-aware design automation, formal fault-propagation analysis, AI-based runtime safety monitors, and integrated safety-security co-engineering flows. Advancements in fault modeling for advanced process nodes, standardized chiplet safety frameworks, and scalable FMEDA generation will play a critical role in improving the accuracy and efficiency of safety analysis for next-generation automotive ICs. As vehicle architectures become more centralized and software-defined, semiconductor safety will increasingly rely on collaborative ecosystems involving OEMs, Tier-1 suppliers, semiconductor vendors, and EDA tool providers.

References

[1] R. Debouk, “Overview of the Second Edition of ISO 26262: Functional Safety—Road Vehicles,” *Journal of System Safety*, vol. 55, no. 1, pp. 13–21, 2019.

[2] A. Ismail and Q. Liu, “ISO 26262 automotive functional safety: issues and challenges,” *International Journal of Automotive Technology*, vol. 15, no. 4, pp. 597–610, 2014.

[3] M. Paulitsch, D. Hall, T. Vasile, and S. Haid, “ISO 26262 compliant fault analysis and fault injection for automotive safety-critical systems,” in *Proc. SAE World Congress*, 2018, pp. 1–10.

[4] “Fundamentals of Semiconductor ISO 26262 Certification: People, Process and Product,” Design & Reuse, 2018.

[5] Y. Li, Y. Sun, X. Li, and Q. Chen, “Complying with ISO 26262 and ISO/SAE 21434: A safety-and-security approach,” *Sensors*, vol. 24, no. 6, Art. no. 1848, 2024.

[6] J. Rushby, “A safety-case approach for certification of safety-critical automotive systems,” in *Proc. 22nd Int. Symp. Software Reliability Engineering*, 2011, pp. 272–280.

[7] Optima Design Automation, *An ISO 26262 Automotive Semiconductor Safety Primer*, White Paper, Oct. 2019.

[8] I. Pathak, “ISO 26262 Functional Safety—An approach to compliance readiness,” *SAE Technical Paper* 2024-26-0104, 2024.

[9] Siemens EDA, “Understanding automotive reliability and ISO 26262 for safety-critical ICs,” Siemens Technical Report, 2024.

Received: August 07, 2025

Volume 38 No. 11s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[10] Ansys, “Understanding ISO 26262 for Semiconductors,” Ansys Technical Blog, Dec. 2024.

[11] A. Foglia, S. Longo, and A. Colombo, “Safety mechanisms and fault coverage in modern automotive microcontrollers,” *Microelectronics Reliability*, vol. 88–90, pp. 987–994, 2018.

[12] T. Hollstein et al., “Architectural metrics for fault-tolerant multicore systems in ISO 26262 context,” *IEEE Trans. Dependable and Secure Computing*, vol. 17, no. 3, pp. 524–537, 2020.

[13] H. Fujiwara and M. Shimohama, “Functional safety of mixed-signal semiconductor devices,” *IEEE Trans. Device and Materials Reliability*, vol. 22, no. 1, pp. 55–64, 2022.

[14] Infineon Technologies, *AURIX™ TC3xx Microcontroller: Safety Manual*, Munich, Germany, 2023.

Received: August 07, 2025