DRAM in Safety Critical Automotive Systems

This white paper discusses the evolution of functional safety and the approved approaches to achieve the requisite Automotive Safety Integrity Level (ASIL) as determined by system level exposure, controllability, and severity. Based on quality managed (QM) products, the ISO 26262 standard recognizes several approaches to achieve the requisite ASIL. This paper provides a detailed comparison and discussion of the significant advantages of LPDDR memory with ASIL D certified ISO 26262 compliance. Micron leads the industry with the introduction of an LPDDR5 SDRAM product family with ISO 26262 certified compliance to the most stringent ASIL standard, D.

The Evolution of Functional Safety and ISO 26262

To address the growing trend of safety-critical electronic control units (ECU) in automobiles, the International Organization for Standardization (ISO) published its first international standard for the functional safety of electronic systems installed in road vehicles in 2011: ISO 26262 titled “Road vehicles - Functional Safety.” The second edition was published in December 2018. It included a major addition relevant for semiconductor components: a new “Part 11 – Guidelines on application of ISO 26262 to semiconductors”.

According to leading safety experts contributing to ISO 26262, one of the intents of the second edition was to help guide the rigorous implementation of the ISO 26262 standards for semiconductors used in safety-critical automotive systems while providing a path for existing non-ASIL rated semiconductors to have a transitional phase. This is reinforced by the recommendation given in ISO 26262-2:2018, clause 6.4.12.2 which explicitly refers to current state-of-the-art solutions and domain knowledge:

> *A functional safety assessment may be based on a judgement of whether the objectives of the ISO 26262 series of standards are achieved. NOTE: The achievement of an objective of the ISO 26262 series of standards is judged considering the corresponding requirements of these standards, the state-of-the-art regarding technical solutions and the applicable engineering domain knowledge, at the time of the development.*[1]

Safety Approach

Automotive functional safety compliance is essentially achieved by demonstrating that the system is free from unacceptable risk: Functional Safety is the “absence of unreasonable risk ... due to hazards … caused by malfunctioning behavior … of E/E systems …”[1]. Although it is acknowledged that not all risks can be eliminated from an electrical and electronic (E/E) system, following the implementation guidelines of the ISO 26262 standard should lead to a lower residual risk level. The more rigorously an original equipment manufacturer (OEM) or a tier one supplier implements its E/E systems following the ISO 26262 standards, the better it can demonstrate that the residual risk to harm people is minimized.

Two major failure categories are characterized by the standard as part of the functional safety assessment of semiconductors in general and dynamic random access memory (DRAM) specifically:

Systematic failures – which the ISO 26262 defines as a *failure related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.*[1]

Random hardware failures – which are *failures that can occur unpredictably during the lifetime of a hardware element, and that follow a probability distribution.*[1]

The next sections of this paper will look at systematic failures first, followed by random hardware failures.

Part 1: Systematic Failures

Risk mitigation for systematic failures is performed by implementing additional steps in the development process of semiconductors. These steps are described in ISO 26262 and consist of:

- educational (train staff on ISO 26262)
- organizational measures (e.g., dedicated safety office, external or internal safety certification)
- additional documentation and review requirements.

Each additional safety level requires additional steps in the product development process. ASIL D is currently the highest, the most comprehensive, and the most stringent level of certification for functional safety. While a fully ISO 26262 certified component enables the most stringent safety level for the integrator, the ISO 26262 standard offers three alternative approaches to argue for a significantly reduced risk level for systematic failures:

- Evaluation of Quality Management Hardware (QM HW) elements (ISO 26262-8:2018, clause 13)
- Proven-in-Use of QM HW elements (ISO 26262-8:2018, clause 14)
- ASIL decomposition - DRAM: QM(x) Host: ASIL x(x) (ISO 26262-9:2018, clause 5)

These alternative approaches enable products not originally developed expressly for safety critical automotive systems to achieve the requisite ASIL. In ISO 26262 nomenclature, such components are called QM components. QM stands for quality management and indicate that these products have been developed following standard automotive quality management processes such as IATF 16949, PPAP, AEC Q100/104.

Table 1 compares the ISO 26262 standard approaches with a detailed discussion of each method below.

	ASIL Rated ISO 26262:2018	**HW-Evaluated QM** ISO 26262-8:2018, clause 13	**Proven in Use QM** ISO 26262-8:2018, clause 14	**ASIL Decomposition** QM(x)/ASIL x(x) with x=A,B,C,D ISO 26262-9:2018, clause 5
Effectiveness of safety solution	++++	++	+ Valid – with mitigation strategy. Need to manage risk in the case of excursion	++
System Availability	Aims for fault avoidance	Aims for fault avoidance	Aims for fault avoidance	Aims for fault detection
Effort memory supplier	High	Low	Medium	Low
Effort Memory Integrator	Low	High According to ISO 26262 integrator ownership	Low	Medium-range Additional measures in other parts of the system and to prove independence
Solution Cost				Possibly increased Because of redundancy, included in other parts of the system
Sustainability	Yes	**No**	No Mostly intended for legacy products	Yes

Table 1: Comparison of options for systematic capability argumentation

- Table definition:
  - Effectiveness of Safety Solution – Summarizes the rigor of the safety assessment.
  - System Availability – Compares if the safety argumentation is to avoid systematic failures or simply to detect them when they occur
  - Effort of Memory Supplier – the level of effort required by the memory supplier to support ISO 26262 safety standard
  - Effort of Memory Integrator – the level of resources needed ~~to be spent~~ by the integrator to demonstrate compliance
  - Solution Cost – evaluates if the approach leads to additional cost, for example through duplicated resources – which may include memory.
  - Sustainability – evaluates if the same safety approach can be carried forward to the next generation of products

Hardware Evaluated QM

In the process of "*evaluation of hardware elements,*" an already developed QM component is assessed for its suitability in a safety application. Specifically, "*an argument that the risk of a violation of a safety goal or the risk of a violation of a safety requirement due to systematic faults is sufficiently low*"[1] needs to be provided. The hardware evaluation needs to be done thoroughly and in-depth. First, an evaluation plan is developed. After this, the evaluation is executed by analyzing existing documentation such as verification and qualification reports, field return data, existing FMEAs and by executing additional new tests to verify the robustness of the hardware element. All of these steps are documented in an evaluation report.

Additionally, initiating the hardware evaluation process includes ensuring the hardware element is classified as one of three complexity classes: class I, class II, or class III. ISO 26262-8, clause 13.4.1.1 provides examples for different components:

A) Class I: Resistor, capacitor, transistor, diode, quartz, resonator

B) Class II: Fuel pressure sensor, temperature sensor, stand-alone analog digital converter (ADC)

C) Class III: Microprocessor, microcontroller, digital signal processor (DSP)

Because DRAM is not explicitly mentioned in the examples given above, further review of the classification criteria provided in ISO 26262 is needed. Table 2 lists the criteria and the assessment of each criterion for LPDDR5/5X DRAM.

Classification criteria	Class I		Class II		Class III		Comment
How many internal states (i.e. registers, operating modes, state machine states, etc.) does the HW element have?	☐	Very few (e.g. ≤4)	☐	Few	☒	Many	Many mode and pipeline registers, complex state machines to for internal data and control flows.
Can all internal states be tested and analyzed without knowledge of implementation details?	☐	Yes			☒	No	Not possible to analyze internal states/flows w/o implementation knowledge.
Can all failure modes be identified, understood and analyzed without knowledge of the design, implementation and production process?	☐	Yes	☐	Yes (with available documentation and confirmed assumptions)	☒	No	Internal failure modes cannot be identified w/o knowledge of the design. Even TLFM is difficult.
Does the HW element have internal safety mechanisms which are relevant for the safety concept?	☐	No			☒	Yes	On-die ECC is relevant for the safety concept and shall be treated as a safety measure.

Table 2: LPDDR5/5X DRAM classification according to the criteria of ISO 26262-8, clause 13.4.1.1 – Source: exida

As defined by ISO 26262, there is a specific set of criteria that are used to establish the classification of a hardware element. The classification typically is a reflection of the complexity of the given device. As an example, a very complex semiconductor device – such as a system on a chip (SOC) – is rated as a class III hardware element, whereas a more simplistic device, such as a resistor, would be rated as a class I hardware element. As shown in the table above, as the complexity of the device increases, there is corresponding increasing challenge to identify possible failure modes due to limited observability of hidden or buried nodes. When reviewing this criterion for a memory device, the identified items in the table above that are checked reflect challenges that directly apply to memory, and hence, memory, which has historically been characterized as a class II hardware element, should be treated as class III hardware element. As such, appropriate considerations must be made when designing safety solutions.

ISO 26262 discourages hardware evaluation of class III components: *Class III hardware elements should be developed in compliance with ISO 2626* and only permits it as an exceptional case for a transitional period: *… the "evaluation of class III elements" is not the preferred approach and therefore the next version of the hardware element is planned to be developed in compliance with ISO 26262.*[1]

Hardware evaluation provides a lower level of safety assurance for DRAM versus a fully ISO 26262 ASIL D compliant component. Based upon customer and partner feedback, it can take up to 12 months of multiple individuals' time and effort on the system integrator side for a hardware evaluation to be executed with the appropriate rigor. This assumes a close interaction between component supplier and integrator: while the integrator knows the details of its system, only the supplier has the in-depth knowledge about functionality and failure modes of the component and the documentation of the verification and review steps performed during its development.

In addition, class III hardware evaluation is, per ISO 26262 requirements, not a sustainable solution for successive generations of products.

Proven-In-Use of QM Hardware

The proven-in-use argumentation can be applied for products that are in the field already in adjacent non-safety applications with similar use conditions. The idea is to show that the product is in use in high quantities without

any issues. ISO 26262:2018-8, clause 14 provides the key performance indicators (KPIs) for incidence rates and required evaluation periods for the different ASIL. This method may present an issue in terms of the accuracy of the evaluation:

> Requires a high level of market saturation. This approach requires about five million components being in the field and could take 4-6 years to achieve an ASIL D certification through proven in use.

Considering possible delays of the supply chain, shipped volumes and operating hours, the proven in use approach provides a lower level of safety assurance and is not recommended as a sustainable approach. It should be applied only in exceptional cases for legacy products.

ASIL Decomposition

The third approach to argue for systematic capability of a system using QM-grade DRAM is ASIL decomposition. ASIL decomposition is described in ISO26262-9:2018, clause 5 and is widely used on system level components and for software — for example — to decompose between intended functionality and a checker[4] (i.e., additional hardware that validates proper operation of the device and overall system). Its principles can, however, also be applied to components. In simple terms, ASIL decomposition is a structured way of adding redundancy to the system with the goal of reducing the required ASIL for parts of the system. Possible systematic issues of the reduced-ASIL parts of the system will still be detected through the added redundancy. ISO 26262 specifies which combinations are feasible. In the case of a QM DRAM component in an ASIL D system the following decomposition concept can be applied:

ASIL D = ASIL D(D) + QM(D)

A practical implementation could be that a checker is added to an ASIL D host system on a chip (SoC) that can detect all possible systematic issues that the QM DRAM component (QM(D)) could have. Special efforts are required as part of the ASIL decomposition process to prove the so-called *freedom from interference* between the decomposed elements. They should a) not be affected by the same systematic issue at the same time and b) common cause failures (e.g., failures in common power supplies and clocks) should not impact the capability of detecting faults.

The drawback to this approach is that the QM DRAM component can fail because of a safety critical systematic issue. In this case, the host checker would detect this failure and take the necessary actions to go to a safe state. A vehicle with ADAS features would disengage those features and hand control back to the driver; whereas an autonomous driving vehicle would mostly likely cripple the vehicle taking it off to the side of the road or some defined safe state. The failure of the QM component with a systematic failure can directly impact system availability. The availability of a component with ASIL systematic compliance is typically very high to begin with, even more so if the component supports ASIL D systematic compliance. Moreover, the added redundancy on the host side, associated with a solution that is used to cope with possible systematic issues of the QM component can typically lead to additional system cost.

Part 2: Random Hardware Failure Analysis

In the previous paragraphs, we discussed the value of an ISO 26262 certified DRAM component versus the alternative approaches for a systematic fault safety argumentation based on QM components. This section will now look at the random hardware failure analysis in more detail. As stated earlier in this paper, random hardware failures occur unpredictably over the useful lifetime of the product and are of a probabilistic nature. These failures can happen in hardware even if there have been no flaws in the development and production of the component and potentially as a result of various reasons that are entirely beyond the control of the developer and manufacturer. Figure 3 shows the component failure rate over time — the so-called bathtub curve.

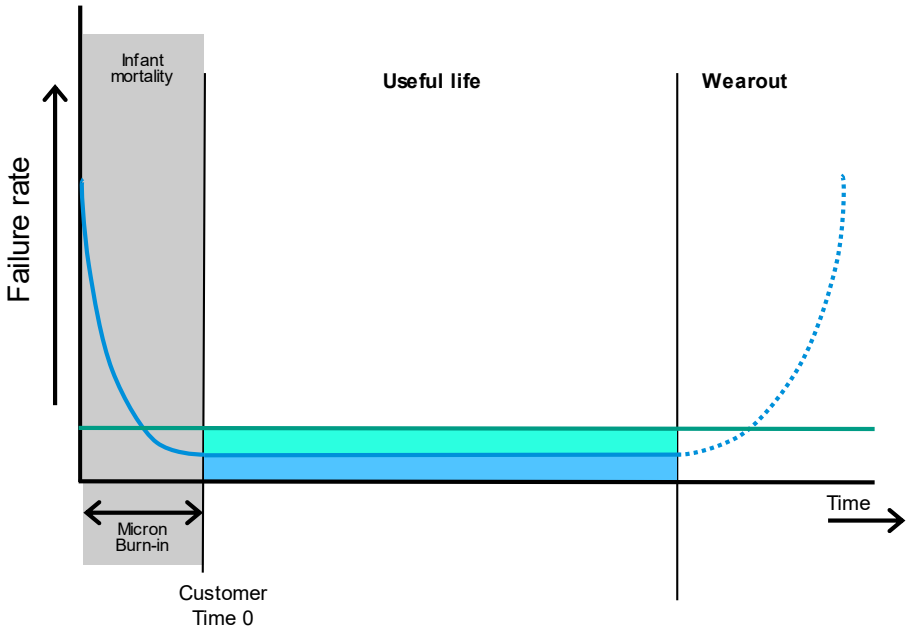

Figure 3: Component failure rate over time

The analysis of random hardware failures of DRAM components encompasses failures of the die and the package during the useful life of the product (solid) area under blue line of the bathtub chart above), as well as those induced by particle hits (solid area under green line). Particle hits are caused by neutron strikes from cosmic radiation or alpha particles from the package material. Random hardware failures are measured in failures in time (FIT). One FIT is defined as one failure in 10^9 hours.

As part of the safety analysis of the ASIL D LPDDR5/5X DRAM, a thorough analysis of both types of random hardware failures identified the effects of failures across parts of the DRAM component and developed technical safety concepts that address avoiding or detecting random hardware failures so that ASIL D hardware metrics can be achieved. Table 3 lists the hardware metrics required by ISO 26262 for the different ASIL:

ASIL	PMHF	SPFM	LFM
A	N/A	N/A	N/A
B	< 100 FIT	≥ 90%	≥ 60%
C	< 100 FIT	≥ 97%	≥ 80%
D	< 10 FIT	≥ 99%	≥ 90%

Table 3: ISO 26262 metrics for random hardware failures

- PMHF - Probabilistic metric for random hardware failures
- SPFM – Single-point fault metric
- LFM – Latent fault metric

More detailed definitions of these metrics can be found in ISO 26262:2018-8, clause 8 (Evaluation of the hardware architectural metrics). It should be noted that the target hardware KPIs are specified for the whole system — for example, a complete electronic control unit (ECU). SPFM and LFM are relative metrics so that the target values can be directly assigned to the DRAM component. PMHF is an absolute metric. Only a small portion of the overall FIT budget can be allocated to the DRAM with the assumption that a low single digit percent of the overall budget — which corresponds to an equally low FIT in ASIL D systems — can be allocated to the DRAM.

Random hardware failures require the adoption of so-called “safety measures for risk mitigation” and a quantitative analysis methodology to estimate their effectiveness. Two possible methods that can be used here are quantitative fault tree analysis (FTA) and failure mode, effects and diagnostics analysis (FMEDA). FTA maps the relationship between faults, subsystems, and redundant safety design elements by creating a logic diagram of the overall system. The undesired outcome is taken as the root (top event) of a tree of logic.

FMEDA

FMEDA methodology is an extension of the classical qualitative failure mode effects analysis (FMEA) that quantify and assign FIT rates to failure modes. As the starting point, a base failure rate needs to be calculated for the die and for the package. The handbook approach based on IEC/TR 62380 is used for this. IEC/TR 62380 has been taken over by ISO 26262 (ISO 26262:2018-11, clause 4.6). The alternative would be to determine the base failure rate based on qualification data. It has been found that this leads to unreliable and incomparable results. The base failure rate (BFR) calculator requires several inputs that can directly affect the overall failure rates. In addition, the passenger compartment profile defined in ISO 26262 can be used or it can be changed in case customers require different mission profiles. Transient events are also quantified accordingly. Neutron FIT is typically referenced to New York, sea level altitude in the analysis.

As the next step, the base FIT is distributed to each block in the DRAM architecture by using the respective gate count as a reference. Figure 3 depicts a high-level view of an LPDDR DRAM architecture. A significant portion of the FIT budget is also allocated to the periphery such as global I/O, command and address decode, row and column decode, input and output buffers, the on-chip error correction code (ECC) and so on.

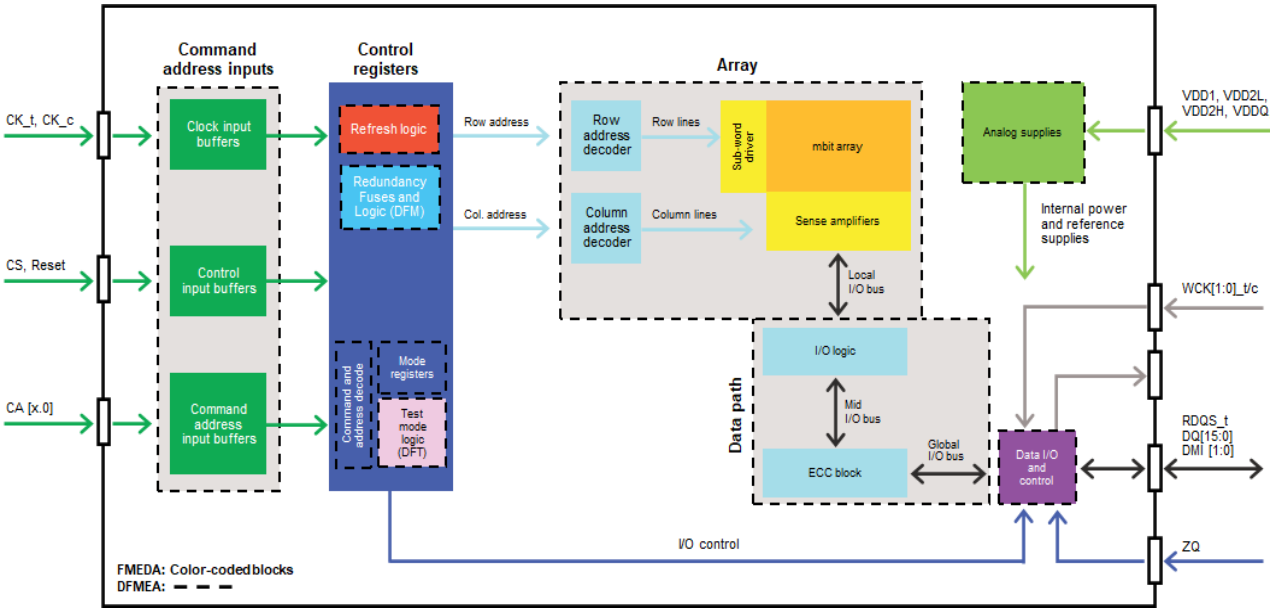

Figure 3: High-level LPDDR DRAM architecture diagram

Each block is then analyzed as to how it can fail, and which failure modes are possible. FIT distribution to the block level failure modes is done by engineering judgement. Eventually, to make it easier for our customers, we aggregate all individual block level failure modes up to a small set of top-level failure modes (TLFM) that the host would see in case a low-level failure occurs. The identified TLFM can be found in Table 4.

ID	Description	Comment	Critical FIT	Failure type
TLFM-01	Corrupt data: Single-bit error (SBE)	Single corrupted bit in one or multiple words	~70%	SBE
TLFM-02	Corrupt data: Double-bit error (DBE)	Two corrupted bits in one or multiple words		DBE
TLFM-03	Corrupt data: Multiple-bit error (MBE)	Multiple corrupted bits or random data vector		MBE
TLFM-04	Corrupt data: Continuous MBE (CMBE)	Repeated MBE for many/every read access		MBE
TLFM-05	Wrong data	Example: Data from a wrong address	~30%	Address
TLFM-06	Lost / old data	Example: No data written, old data at this address		Address
TLFM-07	No data driven during read operation	Termination pulls data to VSS — all-0 received		MBE
TLFM-08	DQ bus disturbance	Leading to MBE on the shared DQ bus		MBE

Table 4: DRAM top-level failure modes

There are eight distinct TLFM that can be grouped into three main failure mode types:

- single-bit errors (TLFM-01)
- multi-bit errors (TLFM-02, -03, -04, -07, -08)
- addressing errors (TLFM-05, -06)[5, 6]

For LPDDR5/5X DRAM, a significant percentage of the safety critical FIT budget is allocated to single-bit errors that can easily be covered by a standard ECC on DRAM or on the host side, but the remaining percentage of the FIT are more difficult to detect because they are multi-bit and addressing errors.

Note that all failure modes are single-point fault failures which means, for example, that a single fault event causes multiple bits in a read burst to be wrong (MBE failure type). Because of the significant allocation to MBE and addressing failure types, we found that a standard JEDEC LPDDR DRAM with commonly used host inline ECC schemes (e.g., 64+8 single error correction, double error detection (SEC-DED)) is not able to reach the ASIL B hardware KPIs shown in Table 3. This finding has recently also been confirmed independently by a team of researchers from TU Kaiserslautern, Fraunhofer Institute and Mercedes-Benz using a different analysis methodology — fault tree analysis (FTA) instead of FMEDA[7]. The issue is the mediocre detection capability of traditional ECC schemes for multi-bit and addressing errors[8].

Micron ASIL-D ISO 26262 Certified LPDDR5 Memory

Micron achieved ASIL D certification for its LPDDR5/5X[3] memory. The certificates issued by the independent assessor company exida for Micron's "Functional Safety Management Process for SDRAM IC Hardware Development"[9] as well as the industry's first ASIL D product certification "Micron Y4BM LPDDR5 SDRAM"[3] can be downloaded from the exida certificate database. Additional detail is provided in the extensive Assessment Reports of the conducted process as well as product certifications. Micron's ASIL D certificate can be seen in Figure 5.

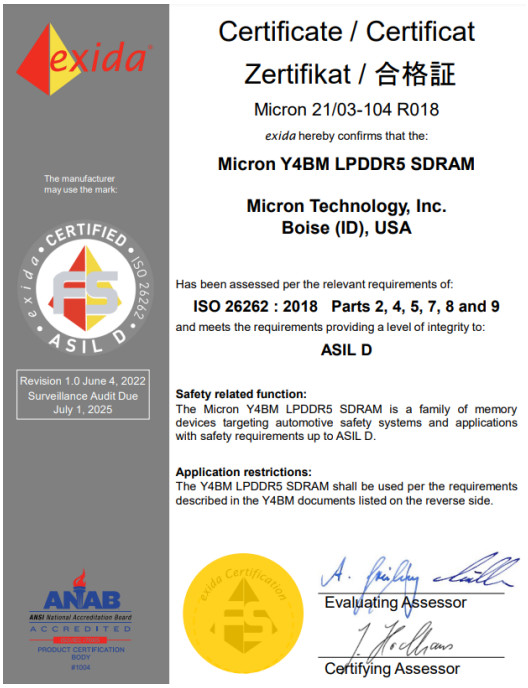

Figure 5: ASIL D Certificate Micron LPDDR5/5X DRAM

There are publicly available documents from exida,and Micron delivers the following safety related documents to its customers:

- Safety Manual – Summarizes the safety concepts and use scenarios
- Safety Analysis Report – Summarizes the results of the FMEDA analysis
- PIN FMEA – Helps our customers to analyze failure modes on the PCB level

Customers might need to use parameters different than the default assumptions in our random hardware failure analysis (FMEDA). This could be related to different use conditions (operating hours, temperature profiles, altitudes) or different safety mechanisms used on the host or system level. In this case, and on a case-by-case basis, we can offer tailored FMEDAs and supply custom Safety Analysis reports based on the concrete requirements of our customers.

Summary

IC vendors are developing solutions to meet the ISO 26262 standard for “Road vehicle – Functional safety.” Based on quality managed (QM) products, there are several recognized approaches by the ISO 26262 standard to achieve the requisite ASIL. Micron reaffirms its commitment to the automotive market by ensuring that state-of-the-art components, processes and methodologies are used in the development of such systems and in our memory components. This commitment requires the mitigation of systematic issues as well as minimizing random hardware failures. Micron leads the industry with the introduction of an LPDDR5 SDRAM product family with ISO 26262 certified compliance to the ASIL D level, the most stringent level.

Acknowledgement

Micron's Product Architecture team recognizes Alexander Griessing of exida for his continuous training and guidance in tailoring functional safety requirements to Micron processes. Special thanks to the Micron DRAM Engineering Group (DEG) development team that made the industry's first fully ISO 26262 ASIL D certified LPDDR5 SDRAM possible.

References

1. International Organization for Standardization (ISO), "*Road vehicles – Functional safety*", *ISO 26262*, 2018
2. Gary Hilson, "*Micron Readies for Level 5 Autonomy with LPDDR5 DRAM*", EE Times, https://www.eetimes.com/micron-readies-for-level-5-autonomy-with-lpddr5-dram/, 2022
3. exida, *"exida CERTIFIED ISO 26262 ASIL D – Micron Y4BM LPDDR5 SDRAM",* https://www.exida.com/SAEL-Safety/Micron-Technology-Inc.-Micron-Y4BM-LPDDR5-SDRAM, 2022
4. Nageswaran Jayaraman, Sowmya Radhakrishnan, Sridharan Subramani, "*The Mumbo-Jumbo called ASIL Decomposition!*", https://www.functionalsafetyfirst.com/2020/06/asil-decomposition.html, 2020
5. Aaron Boehm, "DRAM – More Important Than You Think for Achieving Automotive Functional Safety", Design News, https://www.designnews.com/electronics/dram-more-important-you-think-achieving-automotive-functional-safety, 2021
6. Steffen Buch, "*Questions to Ask Your - Memory Supplier… About Functional Safety for DRAM*", https://www.youtube.com/watch?v=mzcbtXdWDcg, 2020
7. Lukas Steiner, Kira Kraft, Denis Uecker, Matthias Jung, Michael Huonker, Norbert Wehn, "*An LPDDR4 Safety Model for Automotive Applications*", MEMSYS 2021, https://dl.acm.org/doi/abs/10.1145/3488423.3519333, 2021
8. Steffen Buch, "*Error Correcting and Detecting Codes for DRAM Functional Safety*", https://www.youtube.com/watch?v=2lYmtMVn5cI, 2021
9. exida, *"exida CERTIFIED ISO 26262 ASIL D CAPABLE – "Functional Safety Management Process for SDRAM IC Hardware Development",* https://www.exida.com/SAEL-Safety/micron-technology-inc.-fsm-process-for-sdram-ic-hardware-development, 2022

micron.com