ISABELLENHÜTTE

Innovation by Tradition

THE ADVANTAGES OF INTEGRATING ASIL-RATED COMPONENTS IN AUTOMOTIVE HARDWARE DESIGN

By // Aalyia Shaukat

The Automotive Safety Integrity Level (ASIL) rating classifies the level of safety required for automotive components based upon the potential hazardous outcomes that might occur in the event of the component failing. Functional safety for hardware components such as sensors, microcontrollers and memory devices have become a growing requirement for OEMs, simplifying the process of integrating these components for a safety-critical system. ASIL-rated products ensure the hardware in question has already met regulatory compliance —a time consuming and costly process —and is therefore ready to be implemented in a safety-critical system than other automotive-grade hardware that may have met standards such as AEC-Q100 or AEC-Q200.

What is ISO 26262?

The ISO 26262 standard was developed with the help of the automotive industry to replace the old IEC 61508 functional safety standard for street vehicles (less than 3,500 kg), although this standard still applies to commercial vehicles. There is an entire functional safety process for ensuring the reliability of safety critical systems. This process is often known as the V-model and can be seen in Figure 1.

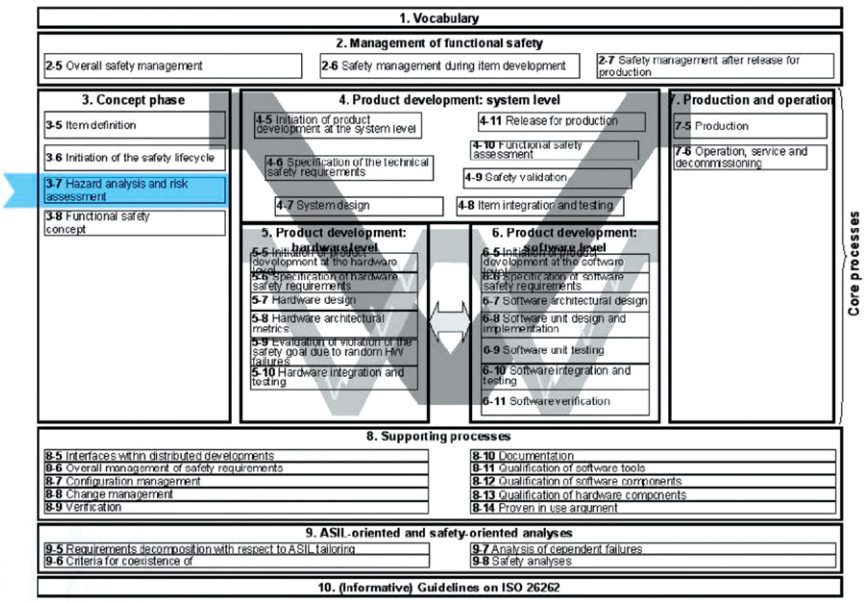

Figure 1. The ISO26262 design processes in a cyclic V-shape from concept to production.
Source: Isabellenhuette

What are ASIL ratings?

Generally, a hazard analysis and risk assessment (HARA) is performed to identify all possible hazards associated with an electronic or electrical (E/E) automotive system such as advanced driver assistance systems (ADAS), airbag controllers, anti-lock braking systems, engine control units (ECUs),and high voltage (HV) battery systems. ASIL ratings are determined according to the parameter's exposure (E), controllability (C) and severity (S).

Based on these parameters, each hazard is assigned an ASIL rating ranging from ASIL A for the least stringent safety requirements, to ASIL D for the most stringent safety requirements (see Table 1). Naturally, an ASIL D rating would be assigned to a hazard that could result in a catastrophic event, such as the loss of life. If the hazard is not deemed a major risk, it can be classified under an ASIL QM rating where quality management measures are enough to ensure the safety of the system.

Severity	Exposure	Controllability		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Table 1. ASIL rating system based upon S, E and C factors.
Data source: Isabellenhuette

Characterizing an automotive part with an ASIL-rating

This can be applied, for instance, with smart sensing in HV battery systems. Table 2 is a high-level overview of what might be seen during the HARA sub-phase in the early "concept phase" (See Figure 1).

Sample analysis on smart sensor including current sensor, voltage, and insulation monitor						
Component Failure	Situation	Hazard scenario	Severity (S)	Controllability (C)	Exposure (E)	ASIL rating
Current sensor (causes overcharging)	Charging	Smoke and fire from HV battery system due to overvoltage	Fatal injury (S3)	Possible to control (C1)	Medium probability (E3)	A
	Stop (ignition on)					A
	Driving			Difficult to control (C3)		C
Insulation monitor (causes loss of info on isolation status)	Charging	Electric shock due to contact to exposed HV parts. (IM failure does not directly cause iso failure.)	Fatal injury (S3)	C2	E3	B
	Driving					B
Voltage sensor						

Table 2. The possible scenarios that would result in the event of current sensor or insulation monitor failure as well as the S, C and E evaluation.
Data source: Isabellenhuette

The failure of a current sensor would, for instance, cause the overcharging of the battery; a situation that can occur during charging while the vehicle is in stop with the ignition on, and while driving in recuperation mode. The resulting hazard is smoke and fire from the HV battery
system due to the overvoltage.

The severity of the hazard is a potential fatality (S3 rating), controllability of this hazard easily possible (C1 rating) during charging and stopping and has an exposure level of medium probability (E3), resulting in an ASIL A level for these situations. However, there is far less controllability of an overcharging scenario while the vehicle is moving (C3) resulting in a ASIL C level for this situation. Using a current sensor such as the
IVT 3 series (Figure 2) can simplify the design process as it has been developed according to ISO 26262. The IVT 3 has recently been the first current sensor on the market to receive certification for compliance to ISO 26262 ASIL C functional safety level by an independent institute (TÜV Rheinland/KUGLER MAAG CIE).

Figure 2. The IVT 3 Pro is qualified with an ASIL C rating for current measurements, ASIL B for voltage measurements and ASIL B for insulation monitoring. Source: Isabellenhuette

The advantages of incorporating an ASIL-rated product

At the system level, OEMs need to be aware of ASIL ratings for safety-critical automotive systems. Functional safety is intrinsic to the design process and cannot be considered as an afterthought, contrary to components where a certain degree of “quality assurance” is sufficient.

Safe, future-proofed and easy to integrate

While most manufacturers produce components that are used within these safety-critical systems without being certain of its end-application (e.g., microcontrollers or smart sensors), an ASIL-rating necessitates a thorough understanding of the circuits and systems the component will be integrated into. And, while this is a large endeavor for manufacturers of E/E components (companies often have to build an entire functional safety department to comply with the ISO26262 standard) it builds in-house expertise and infuses the company with an understanding of the OEM’s larger system. This also allows for a market advantage where consumers and vehicle manufacturers are more likely to trust and adopt components that have undergone rigorous safety assessments.

The ISO 26262 standard is intentionally quite abstract in order to address the range of automotive systems. This can make it difficult to apply to specific systems such as a battery management system. For this reason, every OEM will have their own ASIL letter ratings for different aspects of their system. The complexity also naturally increases with larger systems, where the process of decomposition is used to break down the specific ASIL requirements of independent parts of the system. Automotive systems typically have long life cycles where the ASIL rating of various parts or systems can change based upon the demands of the larger development program and the requirements of evolving safety standards.

Investing in components with higher ASIL ratings ensures that the system is better prepared for future safety requirements and changes in regulation. Components with defined ASIL ratings have well-documented safety requirements and assumptions, making them easy to integrate into complex automotive systems. This clarity facilitates system-level safety analysis and helps ensure that the entire system achieves the desired level of safety.

Mitigating risk and global relevance

By assigning ASIL ratings, automotive engineers and manufacturers can prioritize safety-critical components and allocate resources accordingly. Components with a higher ASIL rating may require additional redundancy, fault tolerance and testing, helping to mitigate potential risks in case of failure. Using suppliers that provide ASIL-rated components simplifies the system-level design and product curation process.

This also helps with any potential audit. These systems follow stringent functional safety requirements due to their hazards and potential for loss of life. Larger government and third-party agencies such as TÜV NORD, the U.S. National Highway Traffic Safety Administration (NHTSA) and the U.S. Environmental Protection Agency (EPA) have the ability to investigate vehicle manufacturers. Products that are already ASIL-rated are already scrutinized with the independent confirmation reviews, safety audits and safety assessments required for various ASIL ratings.

Different regions around the globe have their own specific regulatory requirements for automotive safety. The ISO 26262 standard is widely recognized and adopted in the industry so having an ASIL rating ensures that the component complies with safety standards used globally.

Summary

When functional safety is woven into the very fabric of the automotive development process, it is crucial that each component used within the safety-critical system is ASIL-rated and incorporates ASIL-rated components. These ratings provide a standardized approach for evaluating safety performance and contribute to the development of safer and more advanced vehicles.