Understanding How ISO 26262 ASIL is Determined for Automotive Applications

According to the Motor vehicle safety data, by the BTS (Bureau of Transportation Statistics), more than 6 million crashes involving motor vehicles are reported every year on an average.

As per the U.S. Transportation Department data, United States automakers had to make a record safety recall of 53.2 million vehicles in 2016. This increase in auto safety recalls was caused by the rise in road traffic deaths/road traffic fatalities in U.S.

An auto recall, according to National Highway Traffic Safety Administration (NHTSA, US), is said to be issued when a manufacturer or NHTSA determines that a vehicle, equipment, car seat, or tire can create an unreasonable safety risk or fails to meet minimum safety standards".

These statistics clearly lead us to one common conclusion – how even after technical advancements along the breadths and depths of the industry, an automobile is still a major reason for road accidents.

Hence safety, becomes the fundamental requirement of an automotive application development. For an automotive vehicle, in specific, the functional safety is a very crucial paradigm at every stage of production and decommission.

The Functional Safety Paradigm in Automotive

Within the automobile industry, the functional safety as a process is based on the guidelines specified by ISO 26262 , an international safety standard for automotive.

ISO 26262 standard defines functional safety as the "absence of unreasonable risk due to hazards caused by malfunctioning behavior of electrical/electronic systems".

For ISO 26262 compliance; a functional safety consultant identifies and assesses hazards (safety risks). These hazards are then categorized based on their criticality factor under the Automotive Safety Integrity Level (ASIL) under ISO 26262. Such a clear classification of hazards helps to :

- Establish various safety requirements to mitigate the risks to acceptable levels
- Smoothly manage and track these safety requirements
- Ensure that standardized safety procedures have been followed in the delivered product.

Automotive Safety Integrity Level (ASIL) , specified under the ISO 26262 is a risk classification scheme for defining the safety requirements. Under the ISO 26262, ASILs are assigned by performing a risk analysis of a potential hazard by looking at various risk parameters (Severity, Exposure and Controllability) of the vehicle operating scenario.

ASIL and Safety Criticality of Automotive Components:

The safety lifecycle of any automotive component, within the ISO 26262 standard starts with the definition of the system and its safety-criticality at the vehicular level.

ASIL D represents the highest degree of automotive hazard and ASIL A the lowest. There is another level called QM (for Quality Management level) that represents hazards that do not dictate any safety requirements.

The following figure demonstrates the steps involved in the determination of ASIL for an Anti-Breaking System (ABS).

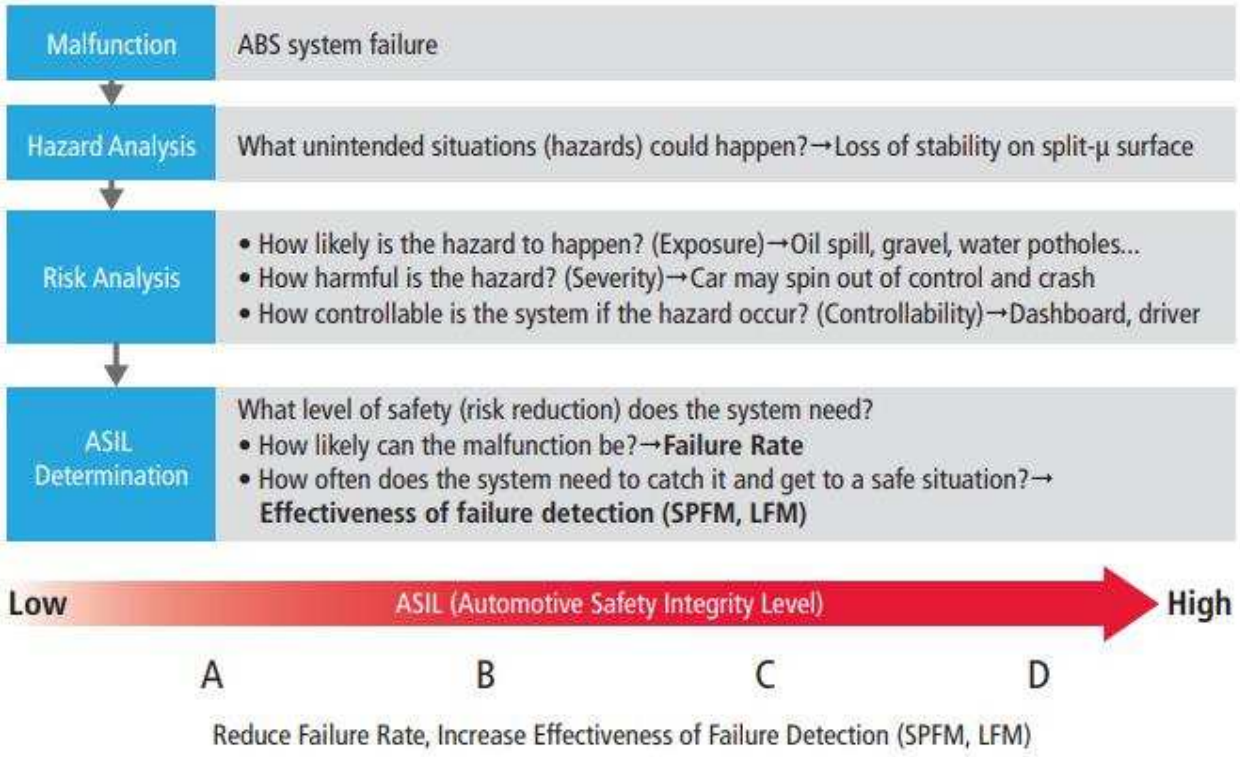

Image credit: Whitepaper by Cadence

For any particular failure of a defined function at the vehicle level, a hazard and risk analysis (HARA) helps to identify the intensity of risk of harm to people and property. Once this classification is completed, it helps in identifying the processes and the level of risk reduction needed to achieve a tolerable risk. Safety goal definition as per ASIL is performed for both hardware and software processes within automotive design to ensure highest levels of functional safety.

These safety levels are determined based on 3 important parameters:

Exposure (E): This is the measure of the possibilities of the vehicle being in a hazardous or risky situation that can cause harm to people and property. Various levels of exposure such as E1: very low probability, E2: low probability, E3: medium probability, E4: high probability are assigned to the automotive component being evaluated.

Controllability (C) : Determines the extent to which the driver of the vehicle can control the vehicle if a safety goal is breached due to failure or malfunctioning of any automotive component being evaluated. The order of controllability is defined as: C1<C2<C3 (C1 for easy to control while C3 for difficult to control).

Under the framework of the ISO 26262 ASIL and functional safety; the safety goals are more critical than the functionality of the automotive component. Let us take the example of charging of a vehicle battery to understand this statement.

The safety goals associated with a battery is a more critical consideration to be evaluated as per ASIL, more than the battery itself as shown in the table below. The overcharging of battery at a speed below 10 km/hour is not as serious a situation as overcharging at very high speeds, where the possibilities of overheating and consequent fire could also be high. :

Vehicle Condition	Cause of malfunction	Possible hazard	ASIL
Running Speed< 10 km/h	Charging of battery pack beyond allowable energy storage	Overcharging may lead to thermal event	A
Running Speed> 10 – 50 km/h	Charging of battery pack beyond allowable energy storage	Overcharging may lead to thermal event	B
Running Speed> 50 km/h	Charging of battery pack beyond allowable energy storage	Overcharging may lead to thermal event	C

Thus, ASIL determination forms a very critical process in the development of highly reliable and functional safe automotive applications. In today's time where the car designs have become increasingly complex with huge number of ECUs, sensors and actuators, the need to ensure functional safety at every stage of product development and commission has become even more important.

This is why modern day automotive manufacturers are very particular about meeting the highest automotive safety standards in accordance to the ISO 26262 standard and ASIL Levels.