COURSE 6

ASIL - Automotive Safety Integrity Level

The ASIL levels – ASIL A, B, C and D are assigned based on an allocation table defined by the ISO 26262 standard [13].

		Probability class	Controllability class		
			C1	C2	C3
Severity class	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

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 is 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).

Severity (S): Defines the seriousness or intensity of the damage or consequences to the life of people (passengers and road users) and property due to safety goal infringement. The order of severity is: S1 for light and moderate injuries; S2 for severe and life-threatening injuries, and S3 for life-threatening incidences.

Let us try to understand the determination of ASIL values for various components based on the E, C and S parameters [13].

Few observations from the ASIL allocation table, a combination of S3, E4 and C3 (the extremes of the 3 parameters) refers to a highly hazardous situation. Hence the component being evaluated is identified to be ASIL D, which means it is prone to severely life-threatening events in case of a malfunction and calls for the most stringent levels of safety measures.

On the contrary, a combination of S1, E1 and C1 (the lowest levels of the 3 parameters in terms of safety-criticality) calls for QM levels, which means the component is not hazardous and does not emphasize safety requirements to be managed under the ISO 26262.

Similarly, combination of the medium levels – S2, E4 and C3 or S2, E3 and C2 defines either an ASIL C or an ASIL A.

The intensity of the hazard thus depends on the ASIL levels of the components, under consideration. Allocation of ASIL helps in identifying how much threat the malfunctioning of a particular component can cause under various situations [13].

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.

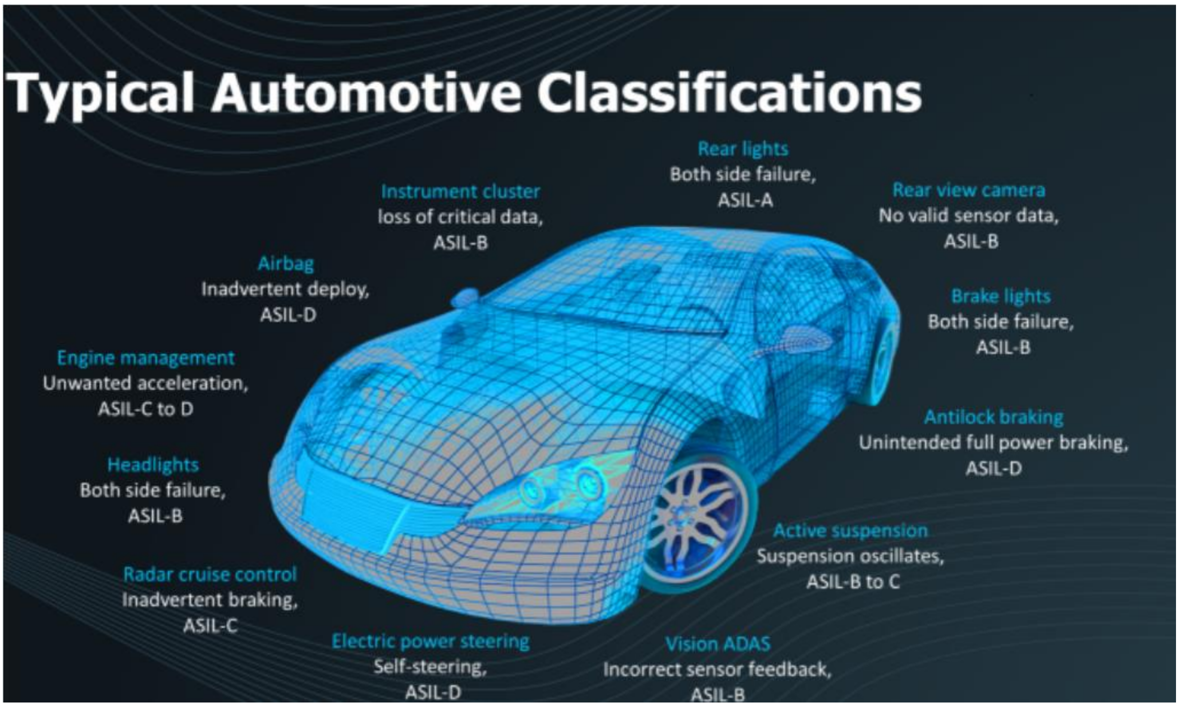
The safety goals associated with a battery is a more critical consideration to be evaluated as per ASIL, more than the battery itself as shown in the table below. The overcharging of battery at a speed below 10 km/hour is not as serious a situation as overcharging at very high speeds, where the possibilities 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 [13].

Hence, determination of ASIL forms the very first phase of the automotive system development. Here, basically all potential scenarios of hazards and dangers are evaluated for a particular automotive component, the occurrence of which can be critical for vehicle safety.

For example, an unexpected inflation of airbag or failures of brakes are potential safety hazards that should be assessed and managed in advance. This step is followed by identifying the ***safety goals*** for each component, which are then classified according to either the QM or ASIL levels, under the ISO 26262 standard [13].

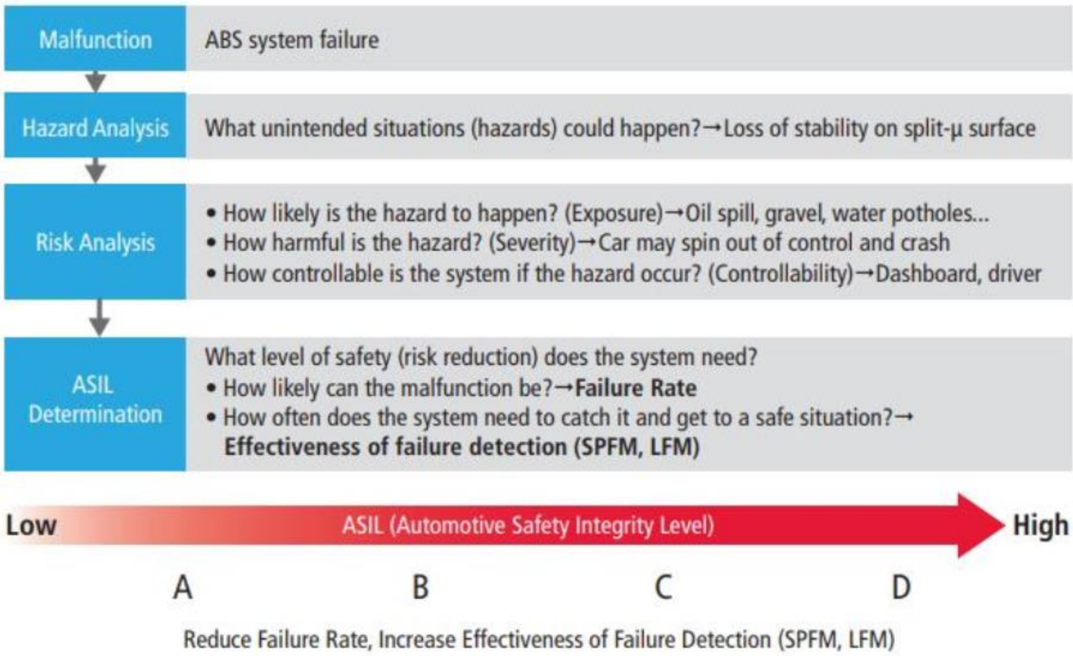


Determining the ISO 26262 ASIL for an Automotive Application

There are four ASILs identified by the ISO 26262 standard: ASIL A, ASIL B, ASIL C, ASIL D.

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).



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 [13].

What is the financial impact of higher ASIL?

It is generally accepted that each increase in ASIL level causes a ten-fold increase in cost. If an ASIL A requirement costs 1, setting it to ASIL B costs 10, to ASIL C 100 and to ASILD 1000.

ASIL determination for motorbike's Electronics Throttle Control System (ETCS) malfunction [14]

In this study, Hazard Analysis and Risk Assessment (HARA) has been applied on motorbike's ETCS to determine the required ASIL level for two types of hazard namely, unintended acceleration and deceleration. Hazardous events that comprise of hazards and operational scenarios (i.e. riding situation) have been derived. Finally, the combination of three parameters that are controllability, severity, and exposure for each hazardous event is analysed to determine the required level of Automotive Safety ASIL level.

Below table shows the ASIL determination of malfunction of motorbike's ETCS. Note that, ASIL determination of each hazardous event and type of accident will be based on worst case scenario of the result reported in different papers. Also, we assumed that the rider follows closely behind a car in all hazardous events. The results are divided based on unintended acceleration and deceleration. For unintended acceleration the result are as follows:

i. Riding on expressway give two different ASIL (i.e. C and D) because of the probability of exposure for a driving situation for cruising and overtaking is different.
ii. ASIL C is assigned for two different type of accident (i.e. rear-end and overtaking) of riding on country road due to similar probability of exposure.
iii. The ASIL for rear-end accident is higher than head-on collision for similar operational scenario (i.e. riding on country road) because of higher severity class.
iv. ASIL A is given for all type of accident for riding on town road because of low speed.

Meanwhile, the results of the deceleration hazards will be as follows:

i. Riding on expressway give two different ASIL (i.e. QM and B) because of the probability of exposure to the driving situation for overtaking is higher compared to cruising.
ii. Riding on the country road has similar ASIL A for both rear-end and head-on accident due to similar probability of exposure.
iii. The operational scenario of riding on country road for rear-end and head-on accident is different which is ASIL A and ASIL B, respectively due to different controllability.
iv. Riding on town road is not considered to comply with any ASIL due to lowest risk occurring.

Hazardous event		**Type of accident**	**ID**	**S [21]**	**E [17]**	**C [18]**	**ASIL**	**Justification**
Hazard	**Operational Scenario**							
Unintended acceleration	Riding on: 1. **Straight** road with large bends[1] 2. **Cruising** at speed (> 90km/h)[2]	Rear-end [7]	Hazard_1	S3	E3	C3*	C	S3: Life-threatening injuries (survival uncertain), fatal injuries E3: The probability of exposure that 'rider follow closely behind a car' in expressway during overtaking is low. [17] C3* : Uncontrollability because of high speed as compared to [18]
	Riding on: 1. **Straight** road with large bends 2. **Overtaking** at speed (> 90km/h)	Overtaking [8]	Hazard_2	S3	E4	C3*	D	E4: The probability of exposure that 'rider follow closely behind a car' in expressway during overtaking is high.
	Riding on: 1. **Curve** with medium bend road [3] 2. **Cruising** at speed (>60km/h ≤90km/h)[4]	Rear-end[7]	Hazard_3	S3	E4	C2	C	C2: It is normally controllable respectively due to lower speed.
		Head-on	Hazard_4	S2	E4	C2	B	S2: Severe and life-threatening injuries (survival probable)
	Riding on: 1. **Curve** & medium bend road 2. **Overtaking** at speed (>60km/h ≤90km/h)	Overtaking [8]	Hazard_5	S3	E4	C2	C	Similar as Hazard_3
	Riding on: 1. **Straight** and small bend road [5] 2. **Cruising** at speed (≤60km/h)[6]	Rear end[7] Crossing[9] Turn left[10] Turn right[11]	Hazard_6	S2	E4	C1	A	C1: The controllability during riding in town road is slightly more easier because of lower speed.
Unintended deceleration	Riding on: 1. **Straight** road with large bends[1] 2. **Cruising** at speed (> 90km/h)[2]	Rear end[12]	Hazard_7	S3	E3	C0	QM	C0: Controllable in general
	Riding on: 1. **Straight** road with large bends 2. **Overtaking** at speed (> 90km/h)	Rear end[12]	Hazard_8	S3	E4	C1	B	C1: The controllability during riding in town road is slightly more easier because of lower speed.
	Riding on: 1. **Curve** with medium bend road[3] 2. **Cruising** at speed (>60km/h ≤90km/h)[4]	Rear-end[12]	Hazard_9	S3	E4	C0	A	C0: Controllable in general
		Head-on	Hazard_10	S3	E4	C1	B	Similar as Hazard_8