COURSE 5

ASIL - Automotive Safety Integrity Level

Overview

Automotive Safety Integrity Level (ASIL) is a risk classification scheme defined by the ISO 26262 Functional Safety for Road Vehicles standard. This is an adaptation of the Safety Integrity Level used in IEC 61508 for the automotive industry. This classification helps defining the safety requirements necessary to be in line with the ISO 26262 standard. The ASIL is established by performing a risk analysis of a potential hazard by looking at the Severity, Exposure and Controllability of the vehicle operating scenario. The safety goal for that hazard in turn carries the ASIL requirements [10].

There are four ASILs identified by the standard: ASIL A, ASIL B, ASIL C, ASIL D. ASIL D dictates the highest integrity requirements on the product and ASIL A the lowest. Hazards that are identified as QM do not dictate any safety requirements.

1. Hazard Analysis and Risk Assessment

Because of the reference to SIL and because the ASIL incorporate 4 levels of hazard with a 5th non-hazardous level, it is common in descriptions of ASIL to compare its levels to the SIL levels and DO178C Design Assurance Levels, respectively [10].

The determination of ASIL is the result of *hazard analysis and risk assessment*. In the context of ISO 26262, a hazard is assessed based on the relative impact of hazardous effects related to a system, as adjusted for relative likelihoods of the hazard manifesting those effects. That is, each hazard is assessed in terms of severity of possible injuries within the context how much of the time a vehicle is exposed to the possibility of the hazard happening as well as the relative likelihood that a typical driver can act to prevent the injury.

In short, ASIL refers both to risk and to risk-dependent requirements (standard minimal risk treatment for a given risk). Whereas risk may be generally expressed as:

$$\text{Risk} = (\text{expected loss in case of the accident}) \times (\text{probability of the accident occurring})$$

or

$$\text{Risk} = \text{Severity} \times (\text{Exposure} \times \text{Likelihood})$$

ASIL may be similarly expressed as

$$\text{ASIL} = \text{Severity} \times (\text{Exposure} \times \text{Controllability})$$

illustrating the role of Exposure and Controllability in establishing relative probability, which is combined with Severity to form an expression of risk [10].

2. Levels

The ASIL range from ASIL D, representing the highest degree of automotive hazard and highest degree of rigor applied in the assurance the resultant safety requirements, to QM, representing application with no automotive hazards and, therefore, no safety requirements to manage under the ISO 26262 safety processes. The intervening levels are simply a range of intermediate degrees of hazard and degrees of assurance required [10].

ASIL D

ASIL D, an abbreviation of *Automotive Safety Integrity Level D*, refers to the highest classification of initial hazard (injury risk) defined within ISO 26262 and to that standard's most stringent level of safety measures to apply for avoiding an unreasonable residual risk. In particular, ASIL D represents likely potential for severely life-threatening or fatal injury in the event of a malfunction and requires the highest level of assurance that the dependent safety goals are sufficient and have been achieved.

ASIL D is noteworthy, not only because of the elevated risk it represents, and the exceptional rigor required in development, but because automotive electrical, electronic, and software suppliers make claims that their products have been certified or otherwise accredited to ASIL D, ease development to ASIL D or are otherwise suitable to or supportive of development of items to ASIL D. Any product able to comply with ASIL D requirements would also comply with any lower level.

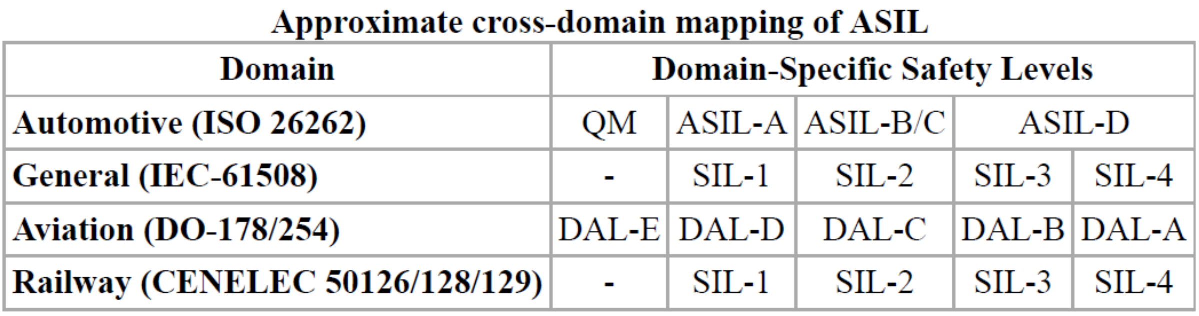
QM

Referring to "Quality Management", the level QM means that risk associated with a hazardous event is not unreasonable and does not therefore require safety measures in accordance with ISO 26262.

3. Comparison with Other Hazard Level Standards

Given ASIL is a relatively recent development, discussions of ASIL often compare its levels to levels defined in other well-established safety or quality management systems. In particular, the ASIL are compared to the SIL risk reduction levels defined in IEC 61508 and the Design Assurance Levels used in the context of DO178C and DO254 [10].

While there are some similarities, it is important to also understand the differences.



Approximate cross-domain mapping of ASIL

Domain	**Domain-Specific Safety Levels**				
Automotive (ISO 26262)	QM	ASIL-A	ASIL-B/C	ASIL-D	
General (IEC-61508)	-	SIL-1	SIL-2	SIL-3	SIL-4
Aviation (DO-178/254)	DAL-E	DAL-D	DAL-C	DAL-B	DAL-A
Railway (CENELEC 50126/128/129)	-	SIL-1	SIL-2	SIL-3	SIL-4

IEC 61508 (SIL)

ISO 26262 is an extension of IEC 61508. IEC 61508 defines a widely referenced Safety Integrity Level (SIL) classification. Unlike other functional safety standards ISO 26262 does not provide normative nor informative mapping of ASIL to SIL. While the two standards have similar processes for hazard assessment, ASIL and SIL are computed from different points. Where ASIL is a qualitative measurement of risk, SIL is quantitatively defined as probability or frequency of dangerous failures depending on the type of safety function. In the context of IEC 61508, higher risk applications require greater robustness to dangerous failures.

$$\text{probability of failure} < \frac{\text{Tolerable Risk}}{\text{Risk}}$$

That is, for a given Tolerable Risk, greater Risk requires more risk reduction, i.e., smaller value for probability of dangerous failure. For a safety function operating in high demand or continuous mode of operation, SIL 1 is associated with a probability of dangerous failure limit of 10^{-5} per hour while SIL 4 is associated with a probability of dangerous failure rate limit of 10^{-9}.

In commercial publications, ASIL D has been shown aligned to SIL 3 and ASIL A is comparable to SIL 1.

SAE ARP4761 and SAE ARP4754A (DAL)

While it its more common to compare the ISO 26262 Levels D though QM to the Design Assurance Levels (DAL) A through E and ascribe those levels to DO178C; these DALS are actually defined and applied through the definitions of SAE ARP4761 and SAE ARP4754. Especially in terms of the management of vehicular hazards through a Safety Life Cycle, the scope of ISO 26262 is more comparable to the combined scope of SAE ARP4761 and SAE ARP4754. Functional Hazard Assessment (FHA) is defined in ARP4761 and the DAL are defined in ARP4754. DO178C and DO254 define the design assurance objectives that must be accomplished for given DAL [10].

Unlike SIL, it is the case that both ASIL and DAL are statements measuring degree of hazard. DAL E is the ARP4754 equivalent of ASIL QM; in both classifications hazards are negligible and safety management is not required. At the other end, DAL A and ASIL D represent the highest levels of risk addressed by the respective standards, but they do not address the same level of hazard. While ASIL D encompasses at most the hazards of a loaded passenger van, DAL A includes the greater hazards of large aircraft loaded with fuel and passengers.

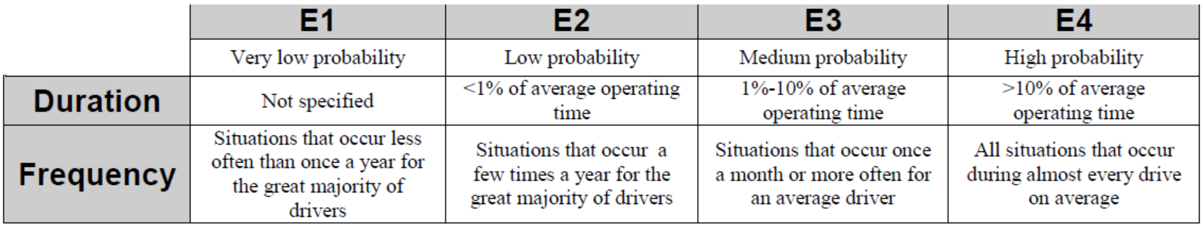
Publications might illustrate ASIL D as equivalent to either DAL B, to DAL A, or as an intermediate level.

4. Hazard Classification for ASIL

Exposure

This is an estimation of how often the customer is exposed to a situation that is hazardous if a certain failure occurs, shown in Table 1 [11, 12]. It is based on the item, not on the user. It doesn't judge how likely a failure is to happen. When choosing a lower grade, a motivation is needed to argument for the choose of low exposure.

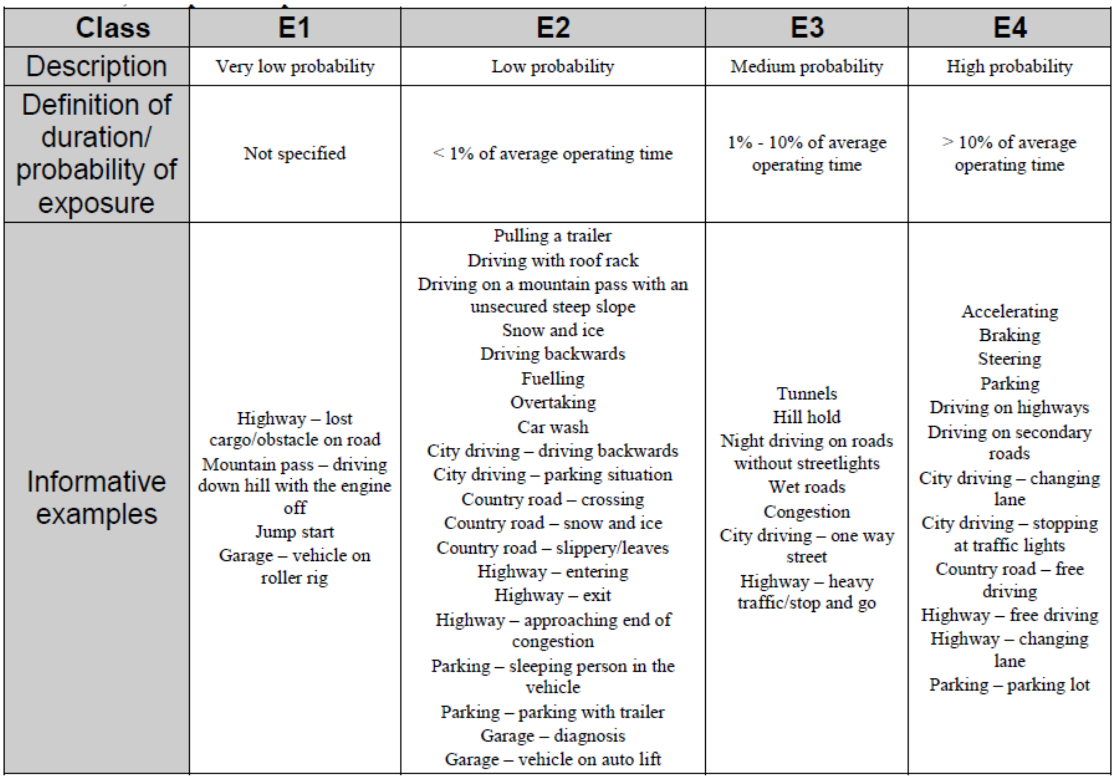
Table 1. Description of exposure



	E1	E2	E3	E4
	Very low probability	Low probability	Medium probability	High probability
Duration	Not specified	<1% of average operating time	1%-10% of average operating time	>10% of average operating time
Frequency	Situations that occur less often than once a year for the great majority of drivers	Situations that occur a few times a year for the great majority of drivers	Situations that occur once a month or more often for an average driver	All situations that occur during almost every drive on average

Examples of different exposures are shown below, in Table 2 [11, 12]:

Table 2. Examples of exposures



Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability
Definition of duration/ probability of exposure	Not specified	< 1% of average operating time	1% - 10% of average operating time	> 10% of average operating time
Informative examples	Highway – lost cargo/obstacle on road Mountain pass – driving down hill with the engine off Jump start Garage – vehicle on roller rig	Pulling a trailer Driving with roof rack Driving on a mountain pass with an unsecured steep slope Snow and ice Driving backwards Fuelling Overtaking Car wash City driving – driving backwards City driving – parking situation Country road – crossing Country road – snow and ice Country road – slippery/leaves Highway – entering Highway – exit Highway – approaching end of congestion Parking – sleeping person in the vehicle Parking – parking with trailer Garage – diagnosis Garage – vehicle on auto lift	Tunnels Hill hold Night driving on roads without streetlights Wet roads Congestion City driving – one way street Highway – heavy traffic/stop and go	Accelerating Braking Steering Parking Driving on highways Driving on secondary roads City driving – changing lane City driving – stopping at traffic lights Country road – free driving Highway – free driving Highway – changing lane Parking – parking lot

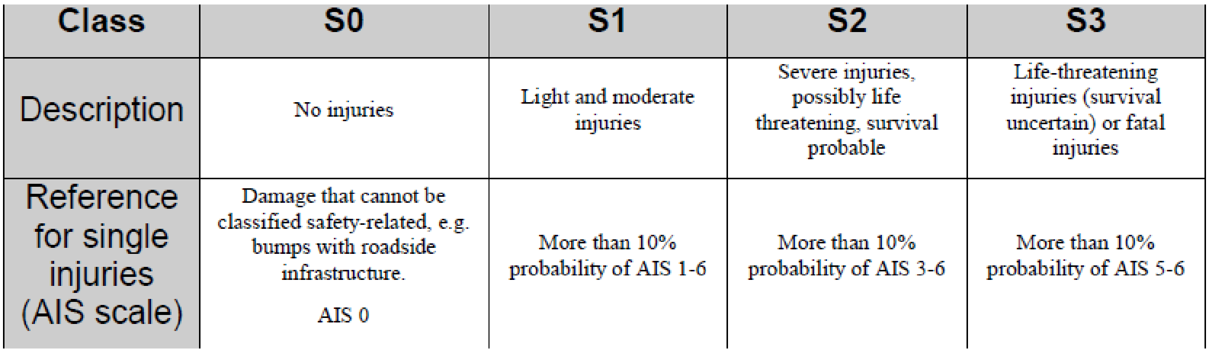
Severity

The severity shall be considered for all involved parties. It can be for instance:

- Unprotected road users
- Driver
- Passenger
- Other drivers/persons travelling along the road
- Service workers

Severity shall also be considered depending on vehicle type and situation. Table 3 shows the description of the levels of severities [11, 12]. It is very important to make it clear for who the severity level is chosen for, is it driver or pedestrian? Sometimes it is possible that it requires a severity for all the considered parts and then pick the one with the highest ASIL.

Table 3. Description of severity



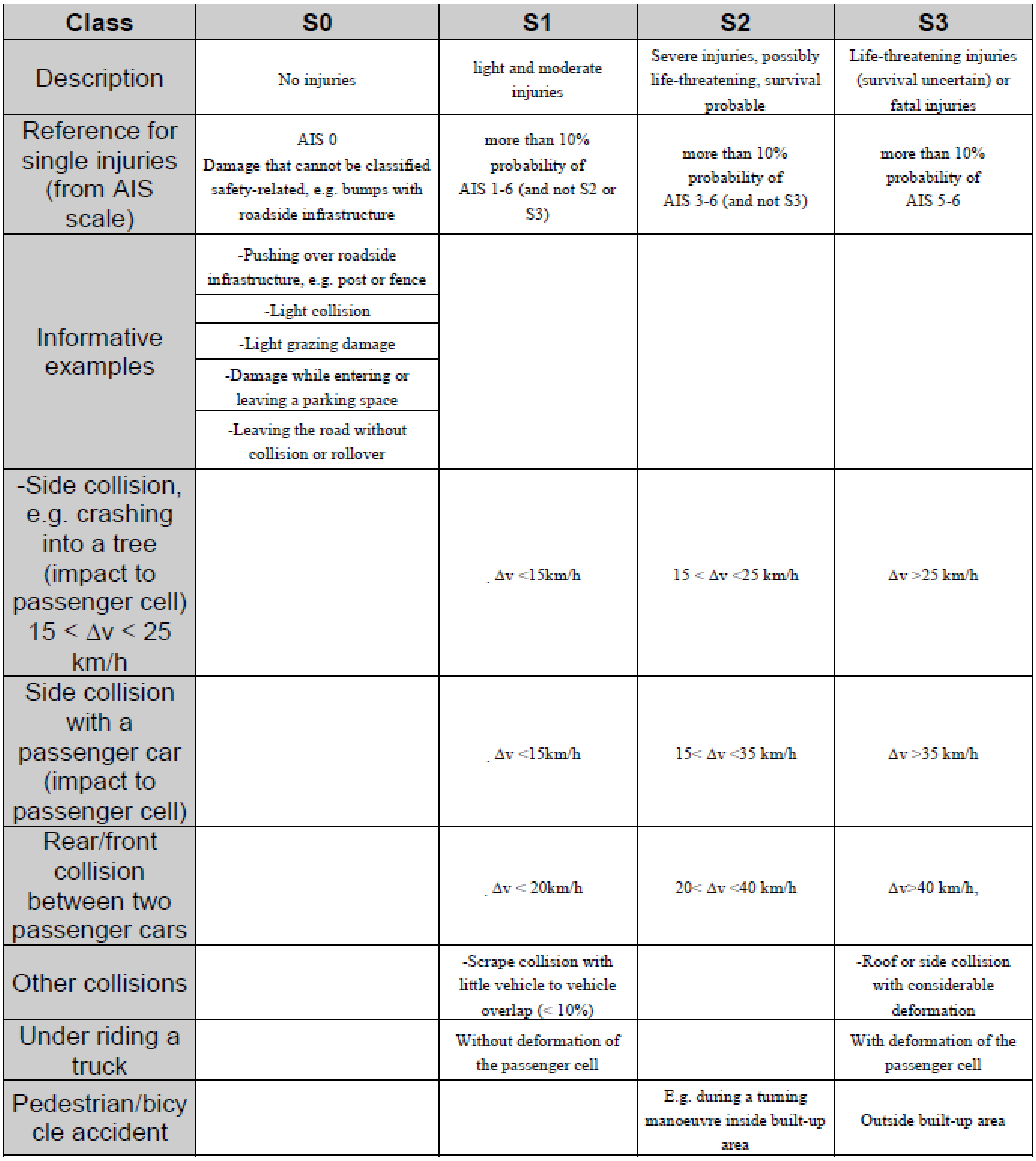
Class	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe injuries, possibly life threatening, survival probable	Life-threatening injuries (survival uncertain) or fatal injuries
Reference for single injuries (AIS scale)	Damage that cannot be classified safety-related, e.g. bumps with roadside infrastructure. AIS 0	More than 10% probability of AIS 1-6	More than 10% probability of AIS 3-6	More than 10% probability of AIS 5-6

AIS – Abbreviated Injury Scale

1. Minor
2. Moderate
3. Serious
4. Severe
5. Critical
6. Maximum

Examples of severities are shown below, Table 4 [11, 12]:

Table 4. Examples of levels of severities

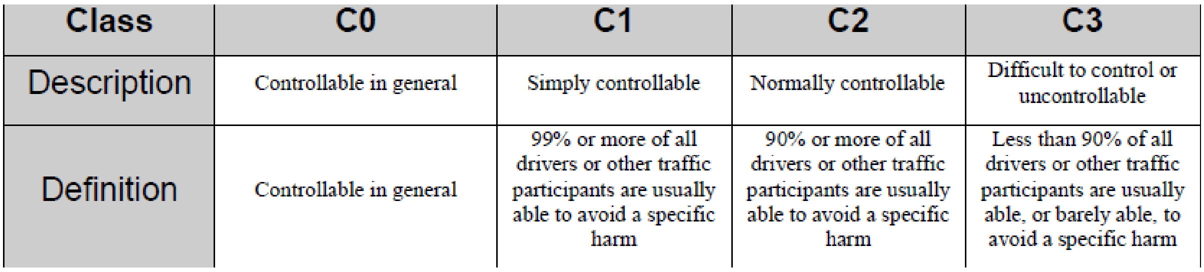


Class	S0	S1	S2	S3
Description	No injuries	light and moderate injuries	Severe injuries, possibly life-threatening, survival probable	Life-threatening injuries (survival uncertain) or fatal injuries
Reference for single injuries (from AIS scale)	AIS 0 Damage that cannot be classified safety-related, e.g. bumps with roadside infrastructure	more than 10% probability of AIS 1-6 (and not S2 or S3)	more than 10% probability of AIS 3-6 (and not S3)	more than 10% probability of AIS 5-6
Informative examples	-Pushing over roadside infrastructure, e.g. post or fence -Light collision -Light grazing damage -Damage while entering or leaving a parking space -Leaving the road without collision or rollover			
-Side collision, e.g. crashing into a tree (impact to passenger cell) $15 < \Delta v < 25$ km/h		$\Delta v <15$km/h	$15 < \Delta v <25$ km/h	$\Delta v >25$ km/h
Side collision with a passenger car (impact to passenger cell)		$\Delta v <15$km/h	$15< \Delta v <35$ km/h	$\Delta v >35$ km/h
Rear/front collision between two passenger cars		$\Delta v < 20$km/h	$20< \Delta v <40$ km/h	$\Delta v>40$ km/h,
Other collisions		-Scrape collision with little vehicle to vehicle overlap (< 10%)		-Roof or side collision with considerable deformation
Under riding a truck		Without deformation of the passenger cell		With deformation of the passenger cell
Pedestrian/bicycle accident			E.g. during a turning manoeuvre inside built-up area	Outside built-up area

Controllability

Controllability is the ability that the driver must avoid an accident or any other harm. This includes e.g. reaction time, i.e. prevention action for an accident. The levels are defined in Table 5 [11, 12].

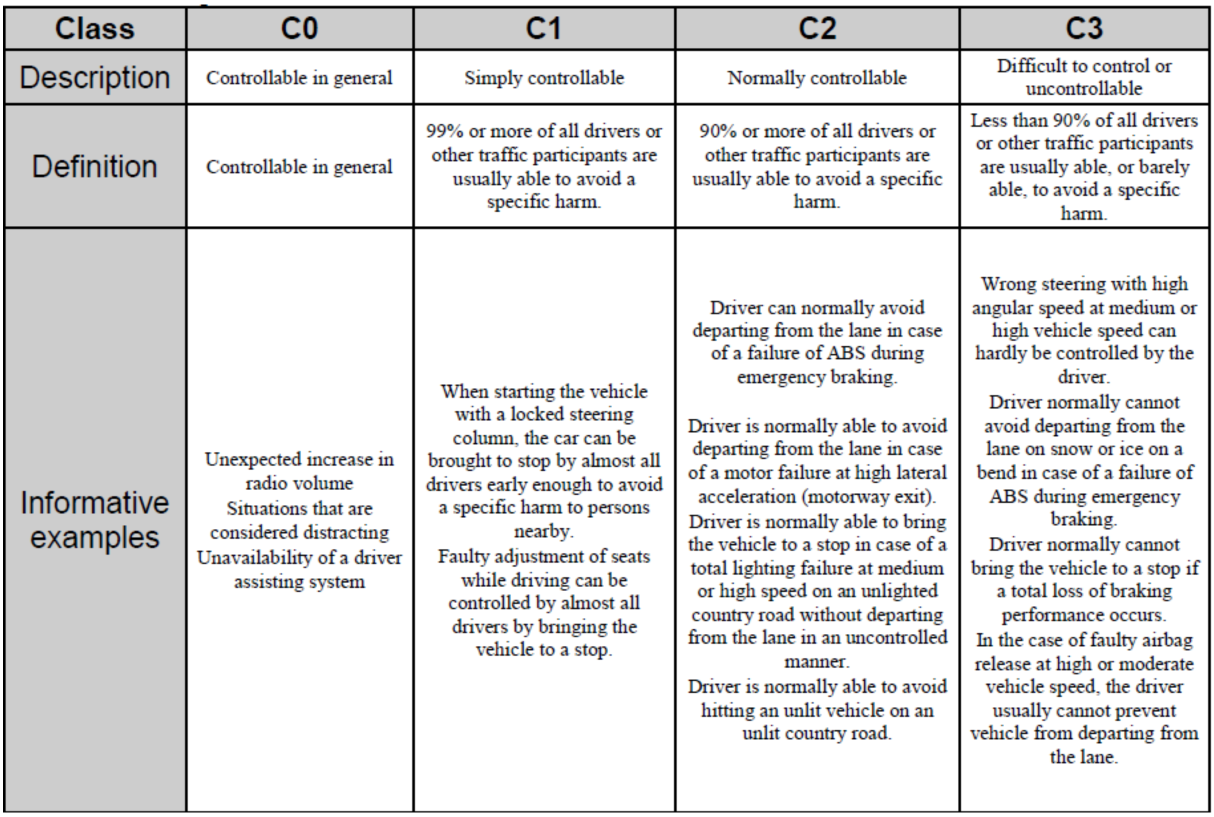
Table 5. Description of levels of classification



Class	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Definition	Controllable in general	99% or more of all drivers or other traffic participants are usually able to avoid a specific harm	90% or more of all drivers or other traffic participants are usually able to avoid a specific harm	Less than 90% of all drivers or other traffic participants are usually able, or barely able, to avoid a specific harm

Examples of controllability's are shown below, Table 6 [11, 12]:

Table 6. Examples of levels of classification

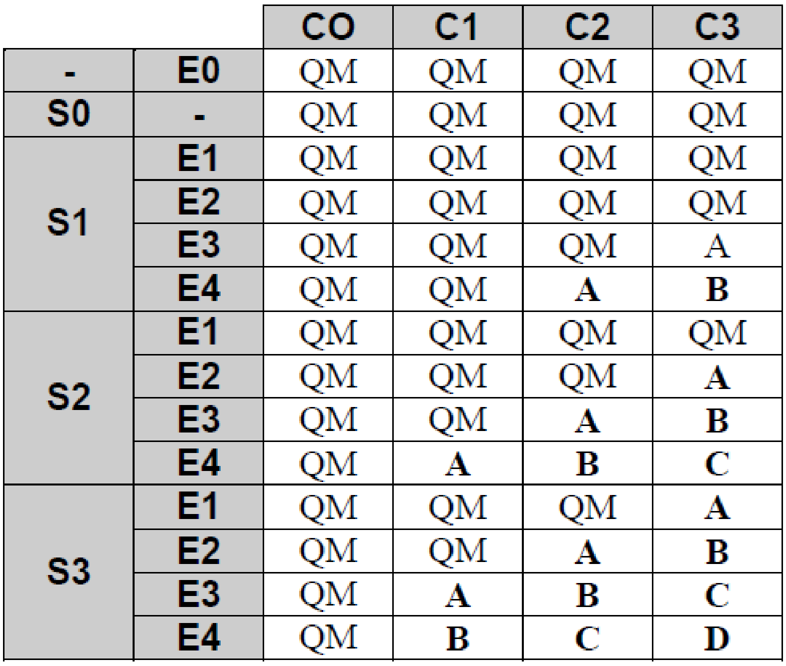


Class	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Definition	Controllable in general	99% or more of all drivers or other traffic participants are usually able to avoid a specific harm.	90% or more of all drivers or other traffic participants are usually able to avoid a specific harm.	Less than 90% of all drivers or other traffic participants are usually able, or barely able, to avoid a specific harm.
Informative examples	Unexpected increase in radio volume Situations that are considered distracting Unavailability of a driver assisting system	When starting the vehicle with a locked steering column, the car can be brought to stop by almost all drivers early enough to avoid a specific harm to persons nearby. Faulty adjustment of seats while driving can be controlled by almost all drivers by bringing the vehicle to a stop.	Driver can normally avoid departing from the lane in case of a failure of ABS during emergency braking. Driver is normally able to avoid departing from the lane in case of a motor failure at high lateral acceleration (motorway exit). Driver is normally able to bring the vehicle to a stop in case of a total lighting failure at medium or high speed on an unlighted country road without departing from the lane in an uncontrolled manner. Driver is normally able to avoid hitting an unlit vehicle on an unlit country road.	Wrong steering with high angular speed at medium or high vehicle speed can hardly be controlled by the driver. Driver normally cannot avoid departing from the lane on snow or ice on a bend in case of a failure of ABS during emergency braking. Driver normally cannot bring the vehicle to a stop if a total loss of braking performance occurs. In the case of faulty airbag release at high or moderate vehicle speed, the driver usually cannot prevent vehicle from departing from the lane.

ASIL

When knowing all these three factors it is now possible to arrange an Automotive Safety Integrity Level classification table to get the ASIL code for every hazard.

Table 7. Definition of ASIL



		CO	C1	C2	C3
-	E0	QM	QM	QM	QM
S0	-	QM	QM	QM	QM
S1	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	A
	E4	QM	QM	A	B
S2	E1	QM	QM	QM	QM
	E2	QM	QM	QM	A
	E3	QM	QM	A	B
	E4	QM	A	B	C
S3	E1	QM	QM	QM	A
	E2	QM	QM	A	B
	E3	QM	A	B	C
	E4	QM	B	C	D

ASIL D – Highest

ASIL C

ASIL B

ASIL A – Lowest

QM – Normal quality management. No safety requirements.

By knowing the level of Exposure (E), Classification (C) and Severity (S), the ASIL can be found by looking in the Table 10 [11, 12].

A hazard with E3, S1 and C2 gives an ASIL A.