SURFACE VEHICLE RECOMMENDED PRACTICE

J2980™ APR2018

Issued 2015-05
Revised 2018-04

Superseding J2980 MAY2015

(R) Considerations for ISO 26262 ASIL Hazard Classification

RATIONALE

This SAE Recommended Practice is intended to provide guidance for identifying and classifying hazardous events, which are per ISO 26262:2011 [1], defined at the vehicle level utilizing the ISO 26262:2011 [1] hazard analysis and risk assessment (HARA) method.

TABLE OF CONTENTS

TO PLACE A DOCUMENT ORDER: **Tel: 877-606-7323 (inside USA and Canada)**
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

SAE values your input. To provide feedback on this Technical Report, please visit
http://standards.sae.org/J2980_201804

1. SCOPE

This SAE Recommended Practice presents a method and example results for determining the Automotive Safety Integrity Level (ASIL) for automotive motion control electrical and electronic (E/E) systems. The ASIL determination activity is required by ISO 26262-3:2011 [1], and it is intended that the process and results herein are consistent with ISO 26262:2011 [1]. The technical focus of this document is on vehicle motion control systems. It is limited to passenger cars weighing up to 3.5 metric tons. Furthermore, the scope of this recommended practice is limited to collision-related hazards associated with motion control systems. The recommended practice focused on motion control systems since the hazards they can create generally have higher ASIL ratings, as compared to the hazards non-motion control systems can create. Because of this, the Functional Safety Committee decided to give motion control systems a higher priority and focus exclusively on them in the SAE J2980 recommended practice. ISO 26262:2011 [1] has a wider scope than SAE J2980, covering other functions and accidents (not just motion control or collisions as in SAE J2980).

1.1 Purpose

This SAE Recommended Practice is intended to provide guidance for identifying and classifying hazardous events, which are per ISO 26262:2011 [1], defined at the vehicle level utilizing the ISO 26262:2011 [1] hazard analysis and risk assessment (HARA) method. This SAE Recommended Practice is intended as a guide toward standard practice and is subject to change to keep pace with experience and technical advances. It is not intended to be a substitute for the concept phase activities of ISO 26262:2011 [1]. All the examples and samples contained in this document are intended to aid the reader in understanding the guidance provided in this document, and are not intended to be exhaustive or complete references. Therefore, they do not substitute for a corresponding analysis of the specific item to which the reader is attempting to apply ISO 26262:2011 [1].

1.2 Background

ASIL classification is a result of the HARA which is initiated during the concept phase of the item development. The HARA is conducted to identify item hazards and evaluate the ASIL of each hazard. The ASIL classification is determined by assessing the parameters Severity (S), Exposure (E), and Controllability (C) associated with each hazardous event. Guidelines for determining the hazards and, once determined, the Exposure, Severity and Controllability for a given hazardous event in accordance with ISO 26262:2011 [1] are provided in this document. In case of conflicts between SAE J2980 and ISO 26262:2011 [1], ISO 26262:2011 [1] has precedence. This Recommended Practice uses terminology consistent with ISO 26262:2011 [1] when discussing vehicle level hazards and HARA development.

The intended user of this “Recommended Practice is a functional safety analyst complying with requirements in ISO 26262-2:2011, 5.4.3. Therefore this Recommended Practice does not intend to provide further necessary knowledge or guidelines in related fields including, but not limited to, item specific knowledge, user and road profiling, medicine, statistics, accident research and human factors. Instead it is intended to be related to the field of functional safety with the focus on the HARA method only.

In the examples and Appendices, the values shown are for reference only. Any new HARA can use the latest relevant data and analyses. The values shown in this document were created based on some, but not all segments of information expected within an item description (ISO 26262-3:2011, 5.4), and thus should not be considered as an item definition. ISO 26262:2011 [1] requires that a HARA be based on a specific item definition. This document is not to be construed to suggest that creating a HARA without a specific item definition is acceptable – such a practice is not recommended. ISO 26262:2011 [1] scope is limited to functional safety which is one aspect of the overall system safety assessment in safety risk management.

1.3 Limitations

As for any risk assessment method, the methods mentioned in this document have inherent limitations. The HARA describes a simplified model of the real world, which is neither complete nor fully accurate. Although each assessment is based on available or applicable data as well as on expert judgment, the interpretation of such data can vary among analyses. For these reasons, the user of this document should bear in mind these limitations and judge the applicability of SAE J2980 in any particular case.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE publications shall apply.

1. ISO 26262:2011, Road Vehicles - Functional Safety
2. Ministry of Defence, “Defence Standard 00-58 HAZOP Studies on Items Containing Programmable Electronics”, Issue 2, 19 May 2000
3. Code of Practice for the design and evaluation of ADAS, EU Project RESPONSE 3: Oct. 2006 http://www.acea.be/publications/article/code-of-practice-for-the-design-and-evaluation-of-adas
4. GIDAS, http://www.vufo.de/forschung-und-entwicklung/gidas/?L=1
5. ITARDA, http://www.itarda.or.jp/english/e_outline1.php
6. NASS/CDS, http://www.nhtsa.gov/NASS

3. DEFINITIONS AND ACRONYMS

3.1 Definitions

3.1.1 AUTOMOTIVE SAFETY INTEGRITY LEVEL

One of four levels to specify the item's or element’s necessary requirements of ISO 26262:2011 [1] and safety measures to apply for avoiding an unreasonable residual risk, with D representing the most stringent and A the least stringent level.

3.1.2 CONTROLLABILITY

Ability to avoid a specified harm or damage through the timely reactions of the persons involved, possibly with support from external measures.

3.1.3 EXPOSURE

State of being in an operational situation that can be hazardous if coincident with the failure mode under analysis.

3.1.4 EXTERNAL MEASURES

Measure that is separate and distinct from the item, which reduces or mitigates the risks resulting from the item.

3.1.5 HARM

Physical injury or damage to the health of persons.

3.1.6 HAZARD

Potential source of harm caused by the malfunctioning behavior of the item.

3.1.7 HAZARDOUS EVENT

Combination of a hazard and an operational situation.

3.1.8 ITEM

System or array of systems to implement a function at the vehicle level, to which ISO 26262 is applied.

3.1.9 MALFUNCTIONING BEHAVIOR

Failure or unintended behavior of an item with respect to its design intent.

3.1.10 SAFE STATE

Operating mode of an item without an unreasonable level of risk.

3.1.11 SEVERITY

Estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation.

3.1.12 SYSTEM

Set of elements that relate at least a sensor, a controller and an actuator with one another.

NOTE: All uses of Severity, Exposure, and Controllability are capitalized in this document where such uses are intended to denote the meaning above.

3.2 ACRONYMS

3.2.1 ABS

Anti-lock Braking System

3.2.2 AIS

Abbreviated Injury Scale

3.2.3 ASIL

Automotive Safety Integrity Level

3.2.4 C

Controllability

3.2.5 E

Exposure

3.2.6 EPS

Electric Power Steering

3.2.7 ESC

Electronic Stability Control

3.2.8 GIDAS

German In-Depth Accident Study

3.2.9 MAIS

Maximum Abbreviated Injury Scale

3.2.10 S

Severity

3.2.11 HARA

Hazard Analysis and Risk Assessment

3.2.12 HAZOP

Hazard and Operability Analysis

3.2.13 ISO

International Standards Organization

3.2.14 ITARDA

Institute for Traffic Accident Research and Data Analysis

3.2.15 NASS/CDS

National Automotive Sampling System Crashworthiness Data System

4. HAZARD ANALYSIS AND RISK ASSESSMENT (HARA)

4.1 Identification of Hazards

HARA is an analysis procedure that identifies potential hazards, develops a set of specific hazardous events, and assesses the risk of each hazardous event to determine the ASIL and the safety goal. Functional safety requirements are derived from the safety goals.

The item definition is a prerequisite for the HARA. Hazard identification can be accomplished through various hazard analysis techniques. A functional hazard and operability analysis (HAZOP) is used in this recommended practice as an example [2, 4]. HAZOP is an explorative type of analysis where applicable guidewords are applied to each of the functions of an item to postulate malfunctioning behaviors. HAZOP facilitates a structured and systematic examination of the operation of the item within the vehicle. It may be used to identify and evaluate malfunctioning behaviors of an item that could lead to hazards that create the potential for harm to the occupants of the subject vehicle, to other vehicles and their occupants, or other persons at risk such as pedestrians, pedalcyclists in the vicinity of the subject vehicle or maintenance personnel.

There are also other valid methods that are equally suitable for identifying relevant hazards. SAE does not recommend or endorse a particular method for identifying hazards as part of generating a HARA.

Explained below is a simplified example application of a HAZOP approach that is used to identify potential malfunctioning item behaviors that could lead to hazards. For example, start with the functions described in the item definition, consider the authority of the actuators of the item, and postulate the following malfunctioning behaviors of the item:

1. Loss of Function - function not provided when intended
2. Function provided incorrectly when intended
    a. Incorrect Function-More than intended
    b. Incorrect Function-Less than intended
    c. Incorrect Function-Wrong direction
3. Unintended Activation of Function - Function provided when not intended

4. Output Stuck at a Value - Failure of the function to update as intended

NOTE 1: Maintenance personnel may be considered for tasks that are not related to the repair of an item that is malfunctioning. However, for items that are assumed to be malfunctioning, damaged or disassembled as a prerequisite to performing repairs, a HARA is not applicable. For example, consider an electric power steering system that includes a safety mechanism to switch “off" assist for a malfunction of oscillations. When a system with this malfunction is presented for maintenance, the maintenance personnel may force assist “on” in order to identify the cause of the malfunction. Such a case cannot be analyzed in a HARA, since it is intentionally caused in order to perform a repair.

NOTE 2: According to ISO 26262 the hazard and risk assessment is to be based on malfunctioning behavior of the item.

NOTE 3: Not all HAZOP guidewords [2] are applicable to all analyses uniformly and as such guidewords are to be tailored according to the scope and context of the analysis. The reader may adopt a particular set of HAZOP guidewords that is applicable to the analysis.

Table 1 provides an example of the HAZOP approach to identify malfunctioning behaviors for two vehicle functions: Steering Assist and Brake Control.

Table 1 - Example of HAZOP application

Function Versus Guidewords	Loss of Function	Function provided incorrectly when intended			Unintended Activation of Function (Function provided when not intended)	Output Stuck at a Value (Failure of function to update as intended)
		Incorrect Function (More than intended)	Incorrect Function (Less than intended)	Incorrect Function (Wrong direction)		
Steering Assist Function	*Loss of Steering Assist*	*Excessive Steering Assist*	*Reduced Steering Assist*	*Steering in the Opposite Direction*	*Unintended Steering Assist*	*Locked Steering (Steering Output Stuck at Value)*
Brake Control Function (conventional brake control)	*Loss of Braking*	*Excessive Braking*	*Insufficient Braking*	-	*Unintended Braking*	*Locked Braking (Brake Output Stuck at Value)*

NOTE 4: Potential interactions between different functions in a vehicle should be considered. This can be done either during compilation of an item’s safety concept or later during its validation. For example, loss of an item function can be a specified degraded mode in isolation, but when considering the interactions and dependencies between items, it may not be a safe state at a vehicle level.

Once the potential malfunctioning behaviors for a function are identified, the hazard analysis activity is continued to understand and analyze the vehicle hazards that are manifested by each malfunctioning behavior. During this step of the analysis, the operating situations of the vehicle are considered including the life cycle phases of the item (i.e., operation, service, and disposal phase).

It should be noted that the same malfunctioning behavior could produce more than one vehicle hazard depending upon the resultant vehicle behavior under different vehicle operating scenarios. For example, unintended or excessive brake apply could produce both unintended vehicle deceleration and unintended lateral motion depending upon the driving condition.

Additionally, multiple malfunctioning behaviors of an item could produce the same vehicle hazard. HARA is an iterative process. Considering the different vehicle operating scenarios and item life cycle phases, it is possible that additional malfunctioning behaviors of an item and associated vehicle hazards are identified as the HARA progresses.

As an example, the malfunctioning behaviors identified for the vehicle function in Table 1 are mapped to vehicle hazards in Tables 2, and 3 respectively. The mapping varies with the considered driving situations for the various malfunctioning behaviors (e.g., loss of brakes could lead to loss of deceleration, vehicle roll away).

Table 2 - Sample mapping of malfunctioning behaviors of steering assist function to vehicle hazards

Malfunctioning Behaviors	Vehicle Hazards
Unintended Steering Assist	*Unintended vehicle lateral motion/Unintended yaw*
Excessive Steering Assist	
Steering in the opposite Direction	
Locked Steering (Steering output stuck at value)	*Loss of vehicle lateral motion control*
Reduced Steering Assist	*Increased Manual Effort to Steer*
Loss of Steering Assist	

Table 3 - Sample mapping of malfunctioning behaviors of brake control function to vehicle hazards

Malfunctioning Behaviors	Vehicle Hazards
Unintended Braking	*Unintended vehicle longitudinal deceleration*
Excessive Braking	
Locked braking (Brake output stuck at value)	
Loss of Braking	*Unintended reduction in vehicle deceleration*
Insufficient Braking	
Unintended Braking	*Unintended vehicle lateral motion*
Excessive Braking	
Locked braking (Brake output stuck at value)	

4.2 Risk Assessment

In the risk assessment process, it is assumed that a malfunctioning behavior of an item is causing a hazard. A hazard is per definition a potential source of harm which is highly dependent on the driving situation at the time that the malfunction occurs. Therefore, the first step can be to postulate a vehicle driving or operating scenario in order to specify the harm. Based on the operating scenario, the likelihood of Exposure to that scenario is determined following guidelines provided in 4.2.1 of this document. For the hazardous event, the Severity and the Controllability are each assigned following the guidelines provided in 4.2.2 and 4.2.3 respectively. For a given hazardous event, this procedure is repeated for reasonable and foreseeable operating scenarios of the vehicle containing the item.

The results of the risk assessment are dependent upon the item, the vehicle and the availability of data. Functional design of an item and vehicle characteristics will affect the specification of the resulting harm scenarios, as well as the class and rationale for the E, S, and C parameters. The analyst takes these factors into account and bases the rationale in the analysis on the specific characteristics of the system that is to be developed.

For each of the analyzed hazardous events the highest ASIL along with the rationale for the assigned Exposure, Severity, and Controllability should be documented (for example in a HARA template).

NOTE 1: The order of determining Exposure, Severity and Controllability can be permuted (i.e., reordered). This document presumes that Exposure, Severity and Controllability are determined in the order as given in Figure 1.

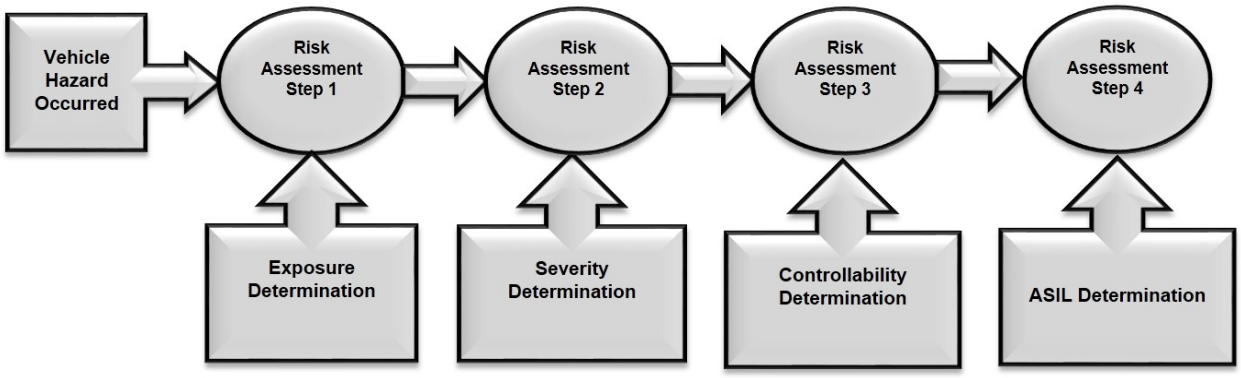


Figure 1 - Example of risk assessment process

4.2.1 Step 1 - Exposure Determination

4.2.1.1 General Information

In accordance with ISO 26262-3:2011 [1], the Exposure to a vehicle operational situation is assigned to one of five levels as shown in Table 4. Table 4 summarizes examples from Tables 2, B.2, and B.3 of ISO 26262-3:2011 [1] for the various Exposure classes both in terms of frequency of exposure and duration of exposure to the vehicle operational situation. Per Figure 1, the first step in the risk assessment is to evaluate the probability of Exposure to a specific vehicle operational situation. This can involve several conditions being required simultaneously. The objective in the Exposure determination is to comprehend realistic situations including normal driving conditions and adverse driving conditions. However, it should be noted that different traffic rules, environmental conditions, etc. influence the situations under consideration and may lead to a different Exposure.

Table 4 - Exposure class description per ISO 26262:2011 [1]

Class	Description	Informative criteria for Exposure based on frequency (see [1], part 3 Table B.3)	Informative criteria for Exposure based on duration (see [1] part 3 Table B.2)
E0*	Incredible	Not specified	Not specified
E1	Very low probability	Occurs less often than once a year for the great majority of drivers	Not specified
E2	Low probability	Occurs a few times a year for the great majority of drivers	<1% of average operating time
E3	Medium probability	Occurs once a month or more often for an average driver	1% to 10% of average operating time
E4	High probability	Occurs during almost every drive on average	>10% of average operating time

* No ASIL is assigned for E0.

4.2.1.2 Exposure based on Duration

An Exposure class is selected based on the duration of a vehicle operational situation for cases where the malfunctioning behavior directly causes the hazardous event.

EXAMPLE: Consider an erroneously applied steering torque by an electric power steering assist system. While the vehicle is at a standstill this may be of minor consequence to the driver, but if the vehicle is driving along a highway it is likely that the driver will leave the intended path. For driving along a highway E4 is specified based on duration for this vehicle operational situation as it occurs >10% of the overall operation time.

NOTE: The potential for harm associated with the hazard may subsequently arise depending on the actions of those people at risk or events in the environment.

4.2.1.3 Exposure based on Frequency

An Exposure class is specified not only for vehicle operational situations in which a considered malfunctioning behavior can directly cause the hazardous event (duration of the situation is relevant), but also for those situations where the situation or condition can initiate the hazardous event, as a result of a fault in the system that has already occurred at an earlier point of time and remained latent. Thus, the occurrence of such a situation will directly initiate the hazardous event because of its combination with the pre-existing fault regardless of its duration

EXAMPLE: Frequency of Exposure may be selected for the activation of the reverse lights at the back of the vehicle. For this example, the vehicle operational situation “vehicle in reverse” can be expected to occur often, so E4 is selected. Frequency is selected because no matter when the fault in the lights occurred, the hazard is likely to be triggered once the gears are shifted to reverse.

4.2.1.4 Vehicle Operational Situation

Figure 2 provides a list of vehicle operational situations that can be used as a starting reference. This example list should not be considered exhaustive and in many cases the situations can and should be combined to reduce and simplify the list of situations considered in the HARA (refer to ISO 26262-3:2011, 7.4.4.2).

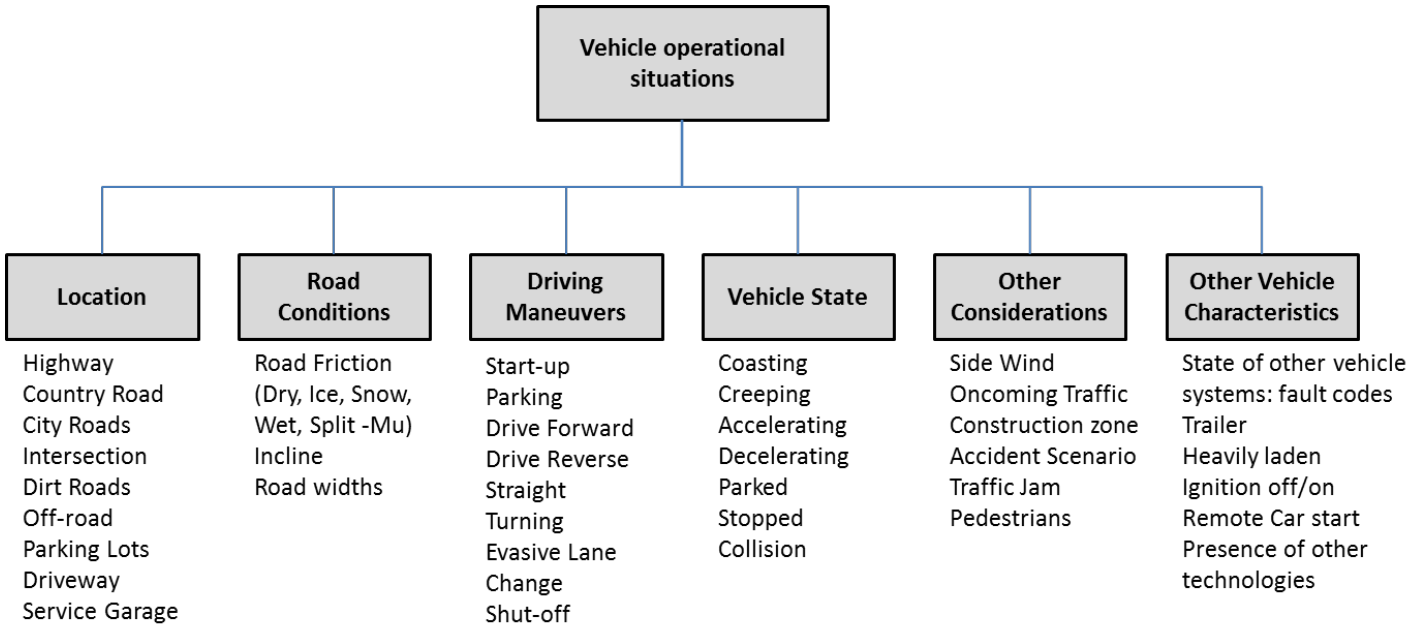


Figure 2 - Potential vehicle operational situations (example)

4.2.1.5 Guidelines for Exposure Class Assignment

1. Exposure assignment in risk assessment is based on expert evaluation of applicable and available data and information considering the traffic profiles, cultures, road conditions and driving styles in different geographical locations or target markets. When in doubt an estimate may be used.

2. Assignment of Exposure can consider either frequency of exposure to the vehicle operational situation or the probability of overall duration of exposure to the vehicle operational situation. In some cases, both exposure criteria may apply, in which case each criterion must be evaluated separately leading to separate ASIL designations.

EXAMPLE: Exposure to a ‘car wash’ scenario can yield E3 based on frequency of Exposure and E2 based on duration of Exposure.

3. The assessment of the Exposure can be done by considering situations occurring in real-world usage of a certain vehicle. If appropriate, target market-specific exposure can be taken into account. However, this should not be used to artificially increase or decrease the Exposure factor.

4. Examples of vehicle operational situations for exposure that are provided in ISO 26262-3:2011 [1] can be used as a reference for Exposure assignment.

5. When evaluating certain vehicle operational situations, multiple contributing factors may be required for the hazard to progress to the point which results in a specified harm. In addition to several factors potentially contributing to a vehicle operational situation, some of the factors may be closely correlated. The correct Exposure factor for any combination of factors prerequisite to a hazardous event is calculated recognizing the correlation between factors.

EXAMPLE: If snow and ice are present, there is a high correlation with reduced friction on the roadway. If the presence of snow/ice and reduced roadway friction are each individually considered an E2 class of Exposure, then requiring two E2 rated Exposure factors should not be expected to result in the equivalent of an Exposure that is less than E2. Indeed, erroneously treating these contributing factors as independent would result in an understated class of Exposure.

6. Hazards that are covered by common workplace safety obligations as well as all hazards caused by an item under repair are not to be evaluated for maintenance personnel in a HARA (see 4.1, NOTE 1).

7. The defined hazardous event must be specific enough to allow for the harm to be specified and the Controllability to be determined consistently.

- A situation may be divided into additional specific situations (which could result in different S and/or C classes).
- Multiple situations related to the same hazard should be combined if their outcomes are similar or the same.
- The above guidance is not to be used to artificially increase or decrease the Exposure factor.
- This is not intended to require an exhaustive examination of all possible combinations; it is enough to consider vehicle operational situations that are representative and include those that lead to the highest ASIL.

4.2.2 Step 2 - Severity Determination

4.2.2.1 General Information

In accordance with ISO 26262:2011 [1], the Severity class of the potential harm caused by a particular hazardous event is assigned to one of four levels as shown in Table 5. These Severity classes are general categories presented for guidance in assigning the ASIL for a given hazardous event.

A Severity class cannot in general be assigned deterministically because the severity of outcome for any actual collision is dependent on a number of factors, many of which cannot be determined in advance. Factors affecting severity may include:

1. Type of collision – such as planar (for example head on, rear end, side impacts)

2. Relative speed between collision participants or at the time of single vehicle events

3. Relative size, height, and structural integrity of the vehicle(s) involved (i.e., crash compatibility)

4. Health and age of vehicle occupants and non-occupants exposed to collision forces

5. Use or not by vehicle occupants of safety protection equipment (e.g., seat belts, child restraints)

6. Availability and response of qualified, rapid emergency assistance (first aid teams)

Of these factors, it may be possible to project some collision characteristics and, in some cases, to project an estimated relative speed of collision. Most of the other factors that may influence the severity of injury outcome cannot be reasonably predicted in advance for a postulated hazardous event. The factors above are considered to the extent practical as a part of determining the Exposure and the Controllability factors used during risk assessment.

In all but the most negligible collisions, the possibility of injury, including fatality, is never equal to zero. The characteristics that may influence injury potential are extremely diverse for all road users, which include both motorists (motorized vehicle drivers and passengers) and non-motorists (e.g., pedestrians and pedalcyclists). Persons involved in traffic collisions range from young, healthy individuals that may be able to tolerate considerable collision force without sustaining significant injuries to elderly, infirm individuals who may be susceptible to major injuries even in minor, low speed collisions. As a result, the outcome of almost any collision type consists of a distribution of outcome likelihoods ranging from property damage without injuries to fatalities.

Table 5 provides the ISO 26262:2011 [1] description of the S0-S3 Severity classes.

Table 5 - Severity class description per ISO 26262:2011 [1]

Severity Class	Description
S0*	No Injuries
S1	Light & Moderate Injuries
S2	Severe and Life-threatening Injuries, Survival Probable
S3	Life Threatening Injuries (Survival Uncertain), Fatal Injuries

* No ASIL is assigned for S0.
NOTE: The reader is referred to ISO 26262-3:2011, Table B1 for examples of Severity classification.

The Severity class will be assigned to a given hazardous event based on a representative hazardous event scenario. Developing this hypothetical scenario will involve drawing from multiple sources of information including, but not required or limited to, expert analysis and judgment, technical reports analyzing specifically-relevant crashes or tests, simulation experiments, and historical crash data. Appendix B provides some general information that may be used to assign the appropriate Severity class for a given vehicle-level motion control hazard.

4.2.2.2 Guidelines for Severity Class Assignment for Collision-Related Hazards

1. Severity class assignment in the HARA necessitates expert evaluation and consideration of a representative sample of relevant traffic profiles, vehicle speeds and road conditions. Analysis of historical accident data tends to overestimate future measures of injury risk due to continuous improvements over time in roadway and vehicle technology (both crashworthiness and crash avoidance), as well as education and law enforcement efforts to improve road user behaviors, but also may not include data appropriate for a different scenario relevant to a new capability. In such cases a model may be used to insert new scenarios into the context of the historical data in order to better project the outcomes.

2. In general, road user injury risk increases as collision speeds increase. For planar collisions, post-crash estimates of delta velocity (delta v) available in some historic accident databases may aid in accident severity assessment. Other post-crash estimates may be considered in place of delta v (e.g., energy-equivalent speed, relative speed between vehicles/objects), and other crash characteristics such as vehicle overlap and crush/intrusion may be considered. Appendix B provides some general guidance that may aid in Severity classification. For non-planar collisions, such as a vehicle rollover, other available criteria depending upon the hazard scenario may be considered for Severity estimation. Examples for Severity that are provided in ISO 26262-3:2011 [1] can also be considered as a reference for Severity assignment.

3. When determining a likely Severity classification of collision outcome from historic data, the relevance of available data should be considered with respect to the system being developed. For example, as new active safety features are introduced that automatically intervene to control vehicle dynamics under certain crash-imminent circumstances, the balance between driver and vehicle control is changing. As a result, current data may not always reflect likely outcomes with the application of new functionality. The vehicle or system manufacturer should consider all technologies being applied to its specific vehicle when determining Severity and ASILs for that product.

4. The Severity class of the representative scenarios that are being considered is documented in the HARA.

NOTE 1: The assignment of the Severity class should also be considered relative to the Exposure. If the Severity is chosen higher than indicated by the traffic data for the general driving situation, then the Exposure should be chosen to be consistent with the probability of being in that driving situation and being exposed to situations where a failure would lead to a hazardous event resulting in harm at that higher severity.

NOTE 2: Historical crash data do not necessarily predict injury outcomes for future crash types. Due to the fact that vehicles, roadways and road user behavior undergo continuous changes intended to improve traffic safety over time, historical crash data tend to overestimate future crash risk and injury severity. For this reason, simplistic application of historical crash data to project injury outcomes and assign a Severity class to a particular vehicle-level hazard is not recommended.

4.2.3 Step 3 – Controllability Determination

4.2.3.1 General Information

In accordance with ISO 26262-3:2011[1], the Controllability of a hazardous event is assigned to one of four levels as shown in Table 6.

Table 6 - Controllability class description per ISO 26262:2011 [1]

Controllability Class	Title	Description
C0*	Controllable in general	If dedicated regulations exist for a particular hazard, Controllability may be rated C0 when it is consistent with the corresponding existing experience concerning sufficient Controllability. For use of C0 refer ISO 26262-3:2011, 7.4.3.8.
C1	Simply controllable	99% or more of all drivers or other traffic participants are usually able to avoid the specified harm.
C2	Normally controllable	90% or more of all drivers or other traffic participants are usually able to avoid the specified harm
C3	Difficult to control or uncontrollable	Less than 90% of all drivers or other traffic participants are usually able to avoid the specified harm

* No ASIL is assigned for C0.
NOTE: Description has used the “specified harm” based on ISO 26262-3:2011, 7.4.3.7, Note 2.

4.2.3.2 Guidelines for Controllability Class Assignment

1. The Controllability class can be determined by using available data, by performing tests in a simulator or a vehicle or by consulting a team of interdisciplinary experts (e.g., human factors).

2. Examples for ‘Controllability’ that are provided in ISO 26262-3:2011, Annex B.4, can also be considered as a reference for ‘Controllability’ assignment.

3. The adverse effects of the hazard on involved persons (refer to ISO 26262-3:2011, 8.4.2.6) may be taken into account during the Controllability determination whenever such driver reactions are likely to be caused by the failure of the E/E system. In order to assess such potential adverse effects, the methodology of the “Code of Practice for the Design and Evaluation of Advanced Driver Assistance Systems [3]” may be employed. This was drafted by the Response 3 project and has been endorsed by the European Automobile Manufacturers’ Association (ACEA).

4. Extended response times caused by driver impairment (i.e., driver use of drugs, alcohol or sleep deprivation) or by driver inattention or distraction are excluded from Controllability consideration (see ISO 26262-3:2011, 7.4.3.7, Note 2).

5. Reasonably foreseeable misuse should be taken into consideration when applicable to a particular analysis.

6. Relevant environmental features (for example guard rails on roads), and driver experience/behavior/training may be taken into account. Relevant in-vehicle systems can be considered in the HARA if they are able to mitigate the hazard during the hazardous event, given sufficient independence exists between the item and the other in-vehicle systems (ISO 26262-3:2011, 7.4.1.2, Note 1).

7. Safety or driver assistance systems, which are optional (e.g., lane keeping assistance systems) should not be considered as risk reduction measures when a Controllability class needs to be set for a specific vehicle platform.

4.2.4 Step 4 - ASIL Determination

4.2.4.1 Combining S, E, and C to Determine ASIL

In accordance with ISO 26262-3:2011, 7.4.4.1, an ASIL is determined for each hazardous event using the parameters "Severity", "probability of Exposure" and "Controllability" in accordance with Table 4 of ISO 26262-3:2011 [1]. ASIL determination is based on relevant scenarios where S, E and C are consistent.

NOTE: If a resultant ASIL for a new system is inconsistent with the hazard experience of similar, existing systems with extensive field history, it may indicate that the field and traffic data used to derive S, E, and C classes for the new system need to be re-examined. This is also consistent with the fact that the HARA process can be iterative in nature.

Table 7 - Criteria for determining ASIL per ISO 26262-3:2011 [1]

ASIL Determination		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

When determining an ASIL for a new system, the Severity and occurrence of accidents of that Severity that may result from malfunctioning behavior of the new system can be compared, when appropriate, to existing relevant accident data. The hazard response behavior of test subjects can then be evaluated to derive an initial Controllability class.

The evaluator should avoid overestimating the Severity, Exposure, and Controllability classes and resultant ASIL, which could otherwise result in reduced functionality, or even cancellation, of a beneficial feature that may improve the overall safety of the vehicle. Similarly, the evaluator should also avoid underestimating the Severity, Exposure, and Controllability classes and resultant ASIL, which may otherwise lead to insufficient safety requirements.

4.3 Relationship between Safety Goals and Safe States

In performing the HARA, the output is a set of safety goals to assure safe operation. These are derived from potential hazards that may result from malfunctioning behaviors of the item. Safe states and related safety measures are specified in the functional or technical safety concept, as appropriate, to achieve the safety goals in case of faults within the item. A HARA is not always required for safe states, although a hazard referring to a safe state condition may result from a HARA as a matter of course in cases where a safe state is identical to a particular failure at the item level. Therefore, because both safety goals and safe states result from consideration of malfunctioning behaviors at different points in the safety lifecycle, inconsistency may result. For consistency of the safety case, it is recommended that care be taken that the safe state does not violate a safety goal. This recommendation can be achieved by different formulations of the safety goal and safe states. For example, the safety goal may be to “avoid loss of crash imminent braking functionality without warning” and the safe state may be to “disable the function and notify the driver that the function is unavailable”. In this safe state the warning mitigates the results of a loss of function as the driver gets aware of the fact that he cannot rely on it. The safety concept and HARA must be consistent otherwise this adversely affects the safety case. If the safe state for a safety goal leads to the violation of a different, less critical, safety goal, care must be taken that their respective safety requirements stay consistent. A rationale supporting this strategy is recommended.

EXAMPLE: Consider a system where avoiding a malfunction is specified as a safety goal with a high, vehicle dependent ASIL. Then the analyst also mistakenly specifies this malfunction as the “safe state” during the concept phase of the development as had been done in previous applications where the malfunction was assigned a lower ASIL. Then later, in the hardware design phase, when the effect of component failures are analyzed in the determination of the single point failure metric, measures such as safety mechanisms are specified that lead to the malfunction. However, this violates a safety goal requiring a safety mechanism to lead to a safe state. The technical safety concept now has a contradiction. To resolve this, a different safe state could be specified, or the malfunction condition could be redesigned, and the HARA can be repeated.

5. NOTES

5.1 Revision Indicator

A change bar (I) located in the left margin is for the convenience of the user in locating areas where technical revisions, not editorial changes, have been made to the previous issue of this document. An (R) symbol to the left of the document title indicates a complete revision of the document, including technical revisions. Change bars and (R) are not used in original publications, nor in documents that contain editorial changes only.

PREPARED BY THE SAE FUNCTIONAL SAFETY COMMITTEE OF
THE ELECTRICAL DISTRIBUTION STEERING COMMITTEE

APPENDIX A - VEHICLE LEVEL MOTIONS

This Appendix briefly discusses the possible vehicle level motions along the different vehicle axes. Figure A1 illustrates the vehicle axis item with 6 degrees of freedom. The three linear motions are the longitudinal, lateral and the vertical motions and the rotational moments along these axes are roll, pitch and yaw respectively. Unintended item behaviors could potentially impact vehicle motion along one or more axes.

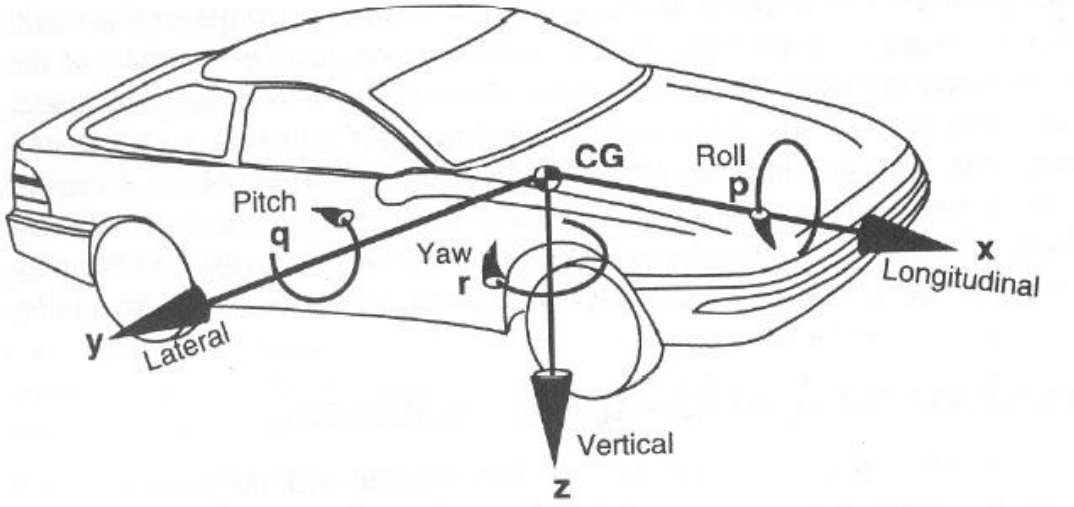


Figure A1 - Vehicle motion axes

Source: SAE Vehicle Axis Reference

Table A1 provides guidelines for systematic consideration of item malfunctions that potentially cause motions along or around the vehicle axes. Table A1 is intended to be used during the item HARA to map item hazard states to vehicle level hazardous events.

Table A1 - Example list of potential malfunctioning behaviors along the vehicle axes

Vehicle motion	Potential Malfunctioning Vehicle Behaviors
Longitudinal Motion (Linear)	Unintended Acceleration
	Unintended Loss of Acceleration
	Unintended Deceleration
	Unintended Loss of Deceleration
	Unintended Longitudinal Motion
	Unintended Loss of Longitudinal Motion
	Unintended Longitudinal Motion In The Incorrect Direction
Lateral Motion (Linear)	Unintended Lateral Motion
	Unintended Loss of Lateral Motion
Vertical Motion (Linear)	Unintended Vertical Motion
Pitch (Rotational)	Unintended Rotational Motion (Lateral axis)
Roll (Rotational)	Unintended Rotational Motion (Longitudinal axis)
Yaw (Rotational)	Unintended Rotational Motion (Vertical axis)
	Unintended Loss of Rotational Motion (Vertical axis)

APPENDIX B - SEVERITY CLASSIFICATION GUIDANCE

This Informative Appendix contains general information for assigning a Severity class to a given vehicle-level motion control hazard as part of generating a HARA. However, it is neither exhaustive nor definitive, and should therefore be applied with caution.

The development of a Severity classification assignment may involve multiple sources of information including, but not required or limited to, expert analysis and judgment, technical reports analyzing specifically-relevant crashes or crash tests, simulation experiments, or historical crash data. Crash, laboratory, track and other testing data may provide objective, reliable, and repeatable results. Simulation experiments may provide direction on the relative contributions of some of the many factors and interactions typically present in pre-crash scenarios and crash events. Analysis of historic accident data may provide general direction on the relative frequency and historic injury potential for various crash circumstances; however, inherent limitations preclude precise projections relevant to future experience.

For vehicle crash-based scenarios, ISO 26262-3:2011 [1] conceptualized a severity classification based on injuries to crash-involved persons (see Table B1). The Abbreviated Injury Scale (AIS), which assigns a severity score from 1-6 to an individual injury, is referenced and a “probability of injury” at certain AIS levels was conceptualized (in Annex B of ISO 26262:2011) as an illustration for assigning the S0-S3 Severity classes in ISO 26262-3:2011 [1]. The AIS for injuries sustained by some or all road users involved in traffic crashes within a defined geographic location is available in some historic accident databases. These collections of accident data are typically small samples with case selection criteria that vary by location.

Appropriate use of injury rates from available accident database(s) must account for the inherent limitations of the data source; use of accident data to support a Severity class assignment requires an adequate understanding of the collection practices and limitations of the available data to ensure that suitable methodologies are employed and that the results are appropriately interpreted.

Generally, literature reviews and analyses of various global real-world crash databases illustrate the principle that crash severity generally increases as delta v increases. As such, higher travel speeds might increase the likelihood for collisions at higher delta v resulting in an elevated injury potential. However, there may be a wide variation in any consideration of speed ranges for the S0-S3 assignment based on different historic accident data sources and the specific crash selection criteria. These variations may be attributed to regional differences in the traffic environment, variations in the accident sampling criteria for the historic data, as well as consideration of available collision characteristics, collision partner, occupant restraint fitted or used, and other factors.

Technical and practical considerations for the use of historic accident data, available through literature reviews or specifically developed analyses, to support Severity class assignment include:

- Case sampling criteria and data collected vary globally for in-depth accident databases. Differences in analytic findings from different databases may be attributed, in part, to variations in the sampling criteria.
- Sample sizes should be considered to better understand the uncertainty based on the accident sampling process, which varies for each available database. In particular, the low frequency of the highest injury severity crashes in available in-depth accident databases may constrain any injury classification developed to support a Severity assignment.
- Selection of the population of interest (level of analysis). For a given set of crashes, injury rates based on the highest recorded injury severity for the crashes, for the involved vehicles, for the involved road users, and for the involved vehicle occupants will likely be different. That is injury rates of a particular severity computed at the crash, vehicle, or occupant level typically are different for any specific set of crashes.
- Per ISO 26262-3:2011, 7.4.3.2 Note 1, the Severity classification should consider the injuries potentially sustained by all involved participants in an accident.

- Many data elements collected post-crash that may correlate with injury risk are not available pre-crash, so the applicability of these elements in a pre-crash environment is limited. Examples include occupant characteristics (e.g., the oldest occupants will generally have higher injury risk than younger occupants in similar crashes) and collision partner characteristics (e.g., crash energy potential will vary for an un-laden, large commercial vehicle compared with the same vehicle with maximum load).

- Post-crash estimates of crash energy (e.g., delta v, barrier-equivalent speed) are:

  - Not necessarily computed for every vehicle (e.g., no delta v estimate is available in the current sample of US tow away crashes if the collision partner is a medium/heavy truck);
  - Not necessarily the same as occupant crash pulse, which may be affected by specific collision characteristics, vehicle structure and interior, occupant kinematics, the restraint system, etc.;
  - Not necessarily the same as or even close to, the pre-crash travel speeds.

If a user of this Recommended Practice has access to specific data or information (for example, data/information that is vehicle-specific or specifically relevant to a future application), perhaps derived from simulation or testing or another method of estimating severity associated with a particular hazard, such data/information could be used. In addition, the presence of another safety system(s) on a vehicle (i.e., in addition to the system that is the subject of the HARA in question) can reduce the potential for harm, and thus may also be factored into a particular Severity class assignment, as well as the related Controllability class. Therefore, the general guidance provided in this informative Appendix is intended to support the user to understand the complexity of the topic and make an appropriate decision where further expert analysis is needed. SAE J2980 does not recommend or endorse a specific method for assigning a Severity class as part of generating a HARA.

In the absence of specific, implementable direction from ISO 26262:2011 [1], literature reviews and analyses of historic accident databases that include post-crash reconstructed delta v and injury coded to the AIS were conducted. For Table B1, information such as the following was taken into account: plane of damage, Maximum Abbreviated Injury Scale (MAIS) of injured participants, direction of the impact force, collision partners, and use of occupant restraints.

General guidance for review of the injury rates was interpreted from ISO 26262-3:2011, Annex B Table B.1 – Examples of Severity classification. A summary of the speed ranges based on post-crash delta v estimates from these various analyses and reviews are provided in Table B1. Although injury rates generally increase as impact speed increases, there is a wide variation in the speed ranges for the S0-S3 assignment depending on the data source and crashes considered. Although the speed ranges from these analyses were based on delta v from post-crash reconstruction, these ranges may provide some general initial guidance for S0-S3 assignment; however, use of the following Table B1 is not required as part of the SAE J2980 Recommended Practice.

To obtain a set of discrete ranges, the analyst may select only one source of data, and apply interpretation including appropriate selection criteria and Severity criteria. Following this procedure, the resulting speed ranges to assign the Severity classes will not overlap.

Table B1 - Minimum and maximum speed ranges (delta v) from various analyses of global accident databases

Collision Type	*Range For*	S0	S1	S2	S3
Front	Minimum speed		> 4-10 kph and	> 20-50 kph and	> 40-65 kph
	Maximum speed	< 4-10 kph*	< 20-50 kph	<= 40-65 kph	
Back	Minimum speed		> 4-10 kph and	> 20-50 kph and	> 40-60 kph
	Maximum speed	< 4-10 kph*	< 20-50 kph	<= 40-60 kph	
Side	Minimum speed		> 2-10 kph and	>= 8-30 kph and	>16-40 kph
	Maximum speed	< 2-3 kph*	< 8-30 kph	<16-40 kph	

* Not specified in some analyses
kph = kilometer per hour
NOTE: The above list is not exhaustive. When determining the Severity classification of a hazardous event, the participants potentially at risk should be considered. This includes pedestrians, pedal cyclists, and occupants of other vehicles whether on or off public roads.

B.1 BACKGROUND FOR TABLE B1: GENERAL METHODOLOGY

Table B1 is based on results from analyses of in-depth traffic accident data bases from France, Germany, Japan, and the U.S. To derive a specific result for a selected scenario within a HARA, appropriate filtering criteria should be carefully chosen taking into account the scope of the analysis and adjustments that might be necessary depending on the nature of the hazard. For those analyses that contributed to Table B1 the following elements were applied:

- Selection of an appropriate population for analysis (e.g., accidents, vehicles in accidents, or accident-involved persons).
- Various factors were considered, such as collision type, overlap, use of restraints, age of occupants
- Severity classification based on the following concept from ISO 26262-3:2011 [1]:
  - S0: Damage that cannot be classified safety-related, e.g., bumps with roadside infrastructure (and not S1, S2 or S3)
  - S1: > 10% probability of AIS 1-6 (and not S2 or S3)
  - S2: > 10% probability of AIS 3-6 (and not S3)
  - S3: > 10% probability of AIS 5-6

B.2 EXAMPLE OF ANALYSIS USED FOR TABLE B1: GIDAS DATABASE

GIDAS (German In-Depth Accident Study) [4] is a project started in 1999 to gather accident data involving personal injury in two of Germany's metropolitan regions (Hannover and Dresden). Each year approximately 2000 accidents are recorded and added to the database. The in-depth study includes on-the-scene documentation, interviews with involved persons, and data gathered from police, hospitals and rescue teams. In addition, each accident is reconstructed to determine additional parameters. Up to 3000 parameters are determined for each accident (further information is available at [4]).

Use of these data as a basis for Severity classifications in a HARA requires attention to several points of caution:

- Although the accidents are sampled according to a well-defined method there is some bias compared to national statistics, which can be compensated for by standardized and published weighting methods.

- The database contains data starting from 1999. The use of these data to determine accident severity for a car that is still under development therefore needs to consider advances in active and passive safety and improvements in road infrastructure that have occurred in the meantime. One possible way to factor in such advances may be to consider only recent model years or cars fitted with certain systems (e.g., ABS, ESC, curtain airbag, pedestrian protection).

- A given hazardous situation could lead to a range of possible accident scenarios. The analyst should refrain from detailed analysis that is only possible a posteriori but cannot be predicted in a HARA.

Table B1 incorporates analysis of GIDAS data consistent with the general methodology described above.

NOTE: The GIDAS data has been normalized before use to extrapolate the personal injury statistics to match the statistics expected on a national basis.

B.3 VARIATION IN TABLE B1

In addition to GIDAS, the entries in Table B1 were compiled from proprietary analysis conducted using available accident databases from France, Japan, and the U.S.

The French data was from Laboratoire d'Accidentologie et de Biomécanique. The data was collected based on crashes occurring on cars built in 1990 or later, for which an AIS determination was available. Every injured person was considered in this analysis, whether they were adequately restrained or not, since it is representative of the actual usage of the vehicle. The considered accidents were classified according to the crash direction (front, side, rear). The French data analysis was complemented with expert judgment for some situations (e.g., pedestrian crashes).

The Japan data was from the Institute for Traffic Accident Research and Data Analysis (ITARDA) [5]. The data are a census of police investigations of all fatal and injury crashes, as well as driver licenses and vehicle registration data. For a subset of the accidents, ITARDA also includes in-depth investigations. Further information is available at [5].

The U.S. data was from the National Automotive Sampling System Crashworthiness Data System (NASS/CDS), which includes retrospective in-depth investigations of a multi-stage stratified sample of police-reported crashes with at least one towed light vehicle (GVWR ≤ 4,536 kgs). The NASS/CDS limitations include: injury information is available only for light vehicle occupants (and only for vehicles 10 years old and newer since 2009), and delta v is not available for all collision partners (e.g., medium/heavy truck). Further information is available at [6].

Each individual analysis based on the above data sources produced a set of discrete speed ranges for the S0-S3 Severity classes. The aggregate results of the individual analyses are shown in Table B1 as a range for the minimum speed and a range for maximum speed for each of the S0-S3 Severity classes. Those resulting ranges shown in Table B1 reflect the overlap for the discrete speed ranges produced by each analysis, which may be attributed to a variety of differences in the available data sources and analytic methods that were used. Those differences may include:

- Regional travel patterns and environments
- Crash selection criteria for the in-depth accident databases
- Extrapolation from the in-depth accident database to a broader population
- Region vehicle fleet composition
- Vehicle selection criteria (e.g., vehicle age, fitment of specific vehicle technologies such as airbags)
- Definition of collision type - front, side, back (e.g., plane of damage, direction of force)
- Categorization of collision types (e.g., by amount of overlap)
- Inclusion and categorization of collision partners

- Occupant inclusion (e.g., seat position, restraint use)
- Occupant characteristics (e.g., age)
- Inclusion of non-occupant injury outcomes (e.g., pedestrians, occupants of other vehicles)

It is recommended that the user ensures that the data source and interpretation is appropriate for the hazardous event being analyzed.

APPENDIX C - EXAMPLES AND GUIDANCE FOR STEERING FUNCTION HARA

C.1 INTRODUCTION

This Appendix provides an example of the HARA for the Electric Power Steering (EPS) assist function. Section C3 provides a HAZOP analysis to identify the malfunction behaviors of the EPS function which are mapped to vehicle level hazards. Some of the EPS malfunctions, the resulting vehicle level hazards and the associated ASIL are provided as examples in Section C4. It must be noted that this Appendix does not represent a complete HARA for the steering function but a subset of functional safety hazards for the EPS function for guidance.

General Disclaimer

This informative Appendix contains example ASILs for select hazard case. Unless otherwise noted, these ASILs were the result of consensus of vehicle manufacturers and suppliers prior to the publication and use of SAE J2980, and is a reference for these existing systems only. While the ASILs provided represent the consensus of the taskforce members, it must be noted that the ASILs could be lower or higher depending upon the vehicle, function authority and tuning.

C.2 ITEM DEFINITION: FUNCTIONAL CONCEPT SUMMARY

EPS function assists the driver to provide vehicle directional control to the steered wheels while reducing the effort required by the driver to steer the vehicle. It measures the driver's intention at the steering wheel and processes with other vehicle inputs to provide steering torque assistance. For the scope of this analysis, the EPS system is assumed to have a mechanical steering connection which would aid the operator to steer the vehicle in the absence of the electric power steering assist function.

C.3 HAZOP ANALYSIS

Table C1 shows the HAZOP analysis to identify the malfunction behaviors of the EPS assist function. Table C2 shows the mapping of the EPS malfunctions to vehicle hazards.

Table C1 - HAZOP analysis for electric power steering assist function

System Function versus HAZOP Guidewords	Loss of Function	Incorrect Activation (More than Requested)			Unintended Activation (When None was Requested)	Output Stuck at a Value (Failure of Function to Update as Intended)
		Incorrect Activation (More than Requested)	Incorrect Activation (Less than Requested)	Incorrect Activation (Activation in Opposite Direction)		
Steering Assist	Loss of Steering Assist	Excessive Steering Assist	Reduced Steering Assist	Reverse Steering Assist (Steering in the opposite direction than requested)	Unintended Steering Assist	Locked Steering

Table C2 - Mapping of EPS malfunction behaviors to vehicle hazards

Malfunction Behaviors	Vehicle Hazards
Loss of Steering Assist	Increased Manual Effort to Steer
Reduced Steering Assist	
Excessive Steering Assist	Unintended Vehicle Lateral Motion/Unintended Yaw
Reverse Steering Assist	
Unintended Steering Assist	
Locked Steering	Loss of Vehicle Lateral Motion Control

C.4 HARA

Table C3 shows some examples of the HARA for EPS assist function. The example HARA provided in this Appendix contains a sample of vehicle motion control hazards related to the steering assist function that are functional safety relevant.

Table C3 - Example HARA analysis for electric power steering assist function

Hazard ID	Function	Malfunctioning Behavior(s)	Vehicle Level Hazard	Assumption	Hazard Detailed Description	Potential accident scenario(s)- considering worst case mishap potential	ASIL Assessment							Comments or Considerations (if applicable)
							S	**Rationale**	**E**	**Rationale**	**C**	**Rationale**	**ASIL**	
Steering Hazard #1	Steering Assist	**Unintended Steering Assist**	**Unintended Vehicle Lateral Motion/ Unintended Yaw**	None	The steering system provides torque actuation unexpectedly when there is no driver request.	Potential for vehicle to depart the intended path/lane and collide with oncoming traffic or neighboring traffic or roadside objects before driver is able to control the situation. If steering produced unintended yaw moment, could cause loss of control of the vehicle.	3	Highway speed vehicle collision or collision with objects	4	Every day Exposure to city roads, highway, freeways	3	Most drivers are unable to control the situation	**D**	This hazard would be applicable to steering torque or angle control functions. ASIL can be lower depending upon vehicle and calibrations, and the magnitude of the control disturbance.
		Reverse Steering Assist			The steering system provides torque actuation in the opposite direction to the driver request.									
Steering Hazard #2	Steering Assist	**Excessive Steering Assist**	**Unintended Vehicle Lateral Motion/ Unintended Yaw**	None	The steering system provides steering assistance more than the design intent; The steering system feels lighter than normal, but the response is in the same direction as the driver request.	During a highway lane change at higher vehicle speeds, the increased assistance could cause a steering overshoot by the driver. Potential for vehicle to depart the intended path/lane and collide with oncoming traffic or neighboring traffic or roadside objects before driver is able to control the situation.	3	Highway speed vehicle collision or collision with objects	4	Every day Exposure to city roads, highway, freeways	1	Simply Controllable	**B**	This hazard is only applicable to steering assist control function. ASIL can be lower depending upon vehicle and calibrations, and the magnitude of the control disturbance.

Steering Hazard #3	Steering Assist	**Locked Steering Control**	**Unintended Loss of Vehicle Lateral Motion Control**	Electrical Resistance in the Steering System	The steering system is electrically locked or stuck in a specific position and does not respond to the driver request when the vehicle is moving. Malfunction prevents manual steering of the vehicle.	The vehicle continues motion in the last position of the steering system and the road wheels. Driver unable to turn or steer the vehicle. Potential for vehicle to depart the intended path/lane and collide with oncoming traffic or neighboring traffic or roadside objects before driver is able to control the situation.	3	Highway speed vehicle collision or collision with objects	4	Every day Exposure to city roads, highway, freeways	3	Most drivers are unable to control the situation	**D**	This hazard would be applicable to steering torque or angle control functions.
Steering Hazard #4	Steering Assist	**Loss of Steering Assist**	**Increased Manual Effort to Steer**	There is a mechanical steering connection; Steering System meets ECE R79 regulation;	There is sudden loss of steering assistance when the vehicle is moving. Increased driver manual steering effort may be required depending upon the vehicle and the steering system compliance.	Only a small portion of steering assistance is needed to turn the vehicle when vehicle is moving at higher speeds. At low speeds, some drivers may be challenged to steer sufficiently enough in time when needed. Potential for collision with vehicle or pedestrian in traffic.	Vehicle Dependent							ASIL determination for sudden loss of assist is dependent upon the vehicle design and configuration. Following are a few guidelines for the classification of Severity, Exposure and Controllability: Severity could be based on -Vehicle collision speed -Potential collision of vehicles/road side objects/pedestrians -SAE J2980 Appendix B Severity Table B1 Exposure could be based on -The duration spent at different lateral accelerations at specific vehicle speed ranges -Probability of being exposed to a threat Controllability during Loss of Assist could depend on multiple factors related to steering system design and vehicle characteristics -An important measure for Controllability among others is the steering wheel rim force* *150 N was proposed as an indicator for C1 upper limit based on ECE R79 (value for fully functional EPS system) and MIL-STD-1472 Additional considerations: The current Loss of Steering Assist behavior and history of steering systems in the field is accepted. Loss of assist behavior and history in the field can be used as a baseline design criteria for future systems It is common industry practice for steering systems to meet ECE-R79 globally. Within Europe it is mandatory.

APPENDIX D - EXAMPLES AND GUIDANCE FOR PROPULSION AND DRIVELINE FUNCTIONS HARA

D.1 INTRODUCTION

This Appendix provides examples, guidance and arguments for the HARA to determine the ASIL, in accordance with ISO 26262:2011 [1] for the most relevant malfunctioning behavior and vehicle level hazards regarding propulsion and driveline functions.

It must be noted that this Appendix does not represent a complete HARA for the propulsion and driveline functions but rather a subset of significant and instructive evaluation examples. These examples do not necessarily define the minimum or maximum ASIL for any specific vehicle system. The Appendix only provides examples, where enough valid data or a clear common expert judgment was available to allow a common evaluation and justify a publication as a guiding example. In a real HARA, additional situations have to be evaluated to find out which one gives the highest ASIL.

General Disclaimer

This informative Appendix contains example ASILs for select hazard case. Unless otherwise noted, these ASILs were the result of consensus of vehicle manufacturers and suppliers prior to the publication and use of SAE J2980, and is a reference for these existing systems only. While the ASILs provided represent the consensus of the taskforce members, it must be noted that the ASILs could be lower or higher depending upon the vehicle, function authority and tuning.

D.2 ITEM DEFINITION: FUNCTIONAL CONCEPT SUMMARY

As the objective of the workgroup is, to give general recommendations and not system specific evaluation, the item definition has to remain as generic as possible. Thus, only the basic propulsion and driveline functions have been listed and additional comments have been added, whenever they proved to be relevant for the exemplary risk evaluations.

Table D1 provides an overview of the basic functions for propulsion and driveline systems.

Remark:

When using the provided examples, take care that some parameters are strongly dependent on the vehicles/systems and can lead to different risk evaluation for different vehicles. These parameters have to be taken into account to retain an appropriate outcome of the specific HARA.

Table D1 - List of functions

ID	Function	Details and Comments
F1	Provide powertrain start/stop option	Provide powertrain start/stop option can mean: start/stop conventional engine start/stop electric engine start/stop with creeping mode start/stop without creeping mode start/stop by key start start/stop by automatic stop/start system start/stop for other reasons (like automatic cooling/heating)
F2	Provide selectable driving direction	Provide selectable driving direction can mean: forward (D) backward (R) neutral (N) Comments: Basic function is "moving the vehicle" (moving forward / moving backward / not moving). An automatic transmission or Shift-by-wire system is considered to provide driving direction.
F3	Provide requested drive torque	Provide requested drive torque by conventional powertrain by electric powertrain by hybrid powertrain
F4	Provide braking torque	Provide braking torque by (electric) regeneration by (conventional) drag torque by automatic transmission mechanisms Comments: Regarding automatic transmission mechanisms, it could be necessary to differentiate gearbox modes (automatic, sports, economy) Regarding regeneration, there are two options to differentiate: (1) Regeneration, not related to the main brake → Release of gas pedal results in regenerative deceleration that might be higher than conventional drag torque (vehicle dependent) (2) Regeneration, related to the service brake → Pressing the brake pedal might lead to regenerative deceleration (combined with brake system deceleration) Option (2) is not within the scope of this Appendix.
F5	Provide selectable / automatic rollaway prevention	Provide selectable/automatic rollaway prevention: by automatic parking lock (Auto-P) by manually activated parking lock (P) Function also includes automatic unlock and manually activated unlock Comments: An E/E-related system is considered to prevent rollaway

D.3 HAZOP ANALYSIS

For each analyzed function, the relevant vehicle level hazards have been derived from potential unintended system states. Table D2 gives an overview. The last column indicates, whether a certain malfunction effectively leads to the same risk evaluation as another one. In these cases, no additional examples will be provided for these malfunctions within the Appendix.

Table D2 - HAZOP results and mapping of function, malfunction behavior and potential vehicle level hazard

Hazard ID	Function	Malfunctioning Behavior	Potential Vehicle Level Hazard	Same As…
F1	Basic function: Provide powertrain start/stop option			
F1-1	activate/deactivate powertrain	Unintended powertrain activation	Unintended acceleration (creeping)	
F1-2	activate/deactivate powertrain	Unintended powertrain deactivation	Loss of acceleration (coasting)	
F1-3	activate/deactivate powertrain	Powertrain activation not possible	none	
F2	Basic function: Provide selectable driving direction			
F2-1	Move in intended direction	Move in unintended direction	Motion in the incorrect direction	
F2-2	Move in intended direction	No movement	none	
F2-3a	Engage "Neutral"	Unintended engagement of D/R instead of N	Unintended acceleration (mostly creeping)	F1-1
F2-3b	Engage "Neutral"	Unintended engagement of P instead of N	Loss of longitudinal motion (low speed)	F2-4b
F2-4a	Engage "Neutral"	Unintended engagement of D/R when vehicle is in N	Unintended acceleration (mostly creeping)	F1-1
F2-4b	Engage "Neutral"	Unintended engagement of P when vehicle is in N	Loss of longitudinal motion (low speed)	
F3	Basic function: Provide requested drive torque			
F3-1a	Provide requested drive torque	provide more drive torque than requested	Unintended acceleration (without destabilization)	
F3-1b	Provide requested drive torque	provide more drive torque than requested	Unintended rotational motion (vertical axis) --> Yaw	
F3-2	Provide requested drive torque	provide less drive torque than requested	Loss of acceleration (coasting)	
F4	Basic function: Provide braking torque			
F4-1a	Provide braking torque	provide more braking torque than requested	Unintended deceleration (without destabilization)	
F4-1b	Provide braking torque	provide more braking torque than requested	Unintended rotational motion (vertical axis) --> Yaw	
F4-2	Provide braking torque	Unintended lack of regenerative deceleration (when gas pedal is released)	Loss of deceleration	
F4-3	Provide braking torque	Unintended lack of drag torque	Loss of deceleration	
F5	Basic function: Provide rollaway prevention			
F5-1a	Provide rollaway prevention	Unintended engagement of rollaway prevention (while stand still)	Loss of longitudinal motion (blocking of axle)	F2-4b
F5-1b	Provide rollaway prevention	Unintended engagement of rollaway prevention (while	Loss of longitudinal motion (blocking of axle)	

Hazard ID	Function	Malfunctioning Behavior	Potential Vehicle Level Hazard	Same As…
		driving)		
F5-1c	Provide rollaway prevention	Unintended engagement of rollaway prevention (while driving)	Unintended rotational motion (vertical axis) --> Yaw	
F5-2	Provide rollaway prevention	Unintended disengagement of rollaway prevention	Unintended longitudinal motion	
F5-3	Provide rollaway prevention	No engagement of rollaway prevention	Unintended longitudinal motion	

D.4 HARA

D.4.1 Vehicle Operating Scenarios / Harm Scenarios

For this Appendix, only some of the most significant operating scenarios are analyzed as examples for the risk evaluation of each hazard. Selection of the scenarios has been performed by the participants of the workgroup, by deriving them from their own HARAs. Each situation is specified in a way that – in combination with the specified malfunction - allows for a logical construction of a specified harm scenario to be evaluated.

D.4.2 Selection of Examples

To find out, which malfunction / hazardous event needs detailed discussion, and for which the evaluation is quite clear, all available results were gathered (maximum ASIL for the specified malfunction) from already executed HARA of participant organizations. In case the results were the same for all of them, in this appendix only one descriptive example for a hazardous event is specified and evaluated, to illustrate the common result. In case the results were different within different HARA, different examples and a more detailed explanations are provided, to explain the reasons for the different results.

NOTE: The examples are not to be understood as an exhaustive list of all hazards. Additional possible malfunctioning behavior or vehicle level hazards might be relevant and needs to be analyzed in a concrete HARA for a real item.

All examples are listed in Table D3.

Table D3 - Example HARA analysis for propulsion and driveline functions

Hazard ID	Function	Mal-functioning Behavior	Vehicle Level Hazard	Assumptions	Hazard Detailed Description	Potential accident scenario(s) (considering worst case mishap potential)	ASIL Assessment							Comments or Considerations (if applicable)
							S	Rationale	E	Rationale	C	Rationale	ASIL	
F1	Basic function: Provide powertrain start/stop option													
F1-3	activate/deactivate powertrain	Powertrain activation not possible	--		Vehicle at stand still with deactivated powertrain. Driver wants to start.	Vehicle will remain in standstill condition. No hazardous effect.	S0	Vehicle will remain in standstill condition. No hazardous effect.	E4	--	--		*none*	
F2	Basic function: Provide selectable driving direction													
F2-2	Move in intended direction	No movement	--	Unwanted movement due to change to "neutral" should be analyzed separately.		Vehicle will remain in standstill condition. No hazardous effect.	S0	Vehicle will remain in standstill condition. No hazardous effect.	E4	--	--		*none*	
F2-4b	Engage "Neutral"	Unintended engagement of P when vehicle is in N	Loss of longitudinal motion (very low speed)	Engaging P when vehicle is in D is discussed separately (see example F5-1).	Vehicle in car wash	Vehicle and car wash can be damaged.	S0	Unwanted engagement of P leads to blocking of the drive axle. Vehicle and car wash can be damaged. No injury to persons.	E2	Vehicle in car wash. *[E2, see ISO 26262-3]*	--		*none*	It may be a system function to activate P after a certain time, when vehicle is left in N.
F3	Basic function: Provide requested drive torque													
F3-1a (1)	Provide requested drive torque	provide more drive torque than requested	Unintended acceleration (without destabilization)	Evaluation is valid for vehicles with typical drive torque dynamics. For high performance propulsion systems with greater torque dynamics the possible combinations of distances, collision speeds and reaction time should be reconsidered to decide whether a higher ASIL evaluation is more appropriate. (see chapter D5.3 for additional guidance). In addition, the risk of destabilization should also be evaluated (see example F3-1b).	Vehicle driving in city or on country roads behind another car.	Front/rear collision with the vehicle in front.	S2	Frontal crash of the vehicle into the rear end of another vehicle at intermediate speed (e.g., 20 km/h speed difference between the two cars).	E4	Driving with another car in front of the own car is a very common situation. This is judged to be more than 10% of operation time.	C2	Situation can be controlled by pressing the brake pedal (intuitive reaction of driver). For most of the situations, the reaction time will be sufficient to avoid the specified harm.	B	

F3-1a (2)	Provide requested drive torque	provide more drive torque than requested	Unintended acceleration (without destabilization)		Vehicle driving at low speed (e.g., first gear) in a location where Pedestrians are in the hazard area.	Frontal collision with pedestrian at a certain speed (no run over assumed)	S2	Collision speed will be relatively low, as initial speed was very low and pedestrian is regarded to be close to the vehicle.	E3	A significant proportion of drive cycles includes areas where pedestrians are present (e.g., crossroads, parking lots). However, it is evaluated that only a certain proportion of the driving time is spent at this locations and pedestrians are not always in the hazardous area.	C3	Some drivers will be startled at the moment of unintended acceleration and the close proximity of vehicle and pedestrian lowers the reaction time; less than 90% of all drivers or all traffic participants are usually able or barely able to avoid harm.	B	
F3-1a (3)	Provide requested drive torque	provide more drive torque than requested	Unintended acceleration (without destabilization)		Vehicle driving at low speed (e.g., first gear) in a location where vulnerable Pedestrians are in the hazard area or conditions for a run over are true. (These conditions depend on the pedestrian but also on the specific vehicle design. (see chapter D5.3 for additional guidance).	Frontal collision with pedestrian with run over	S3	As the situations is focused on accident scenarios where a run over is expected, the evaluated Severity is S3.	E2 to E3	A significant proportion of drive cycles includes areas where pedestrians are present (e.g., crossroads, parking lots). However, it is evaluated that only a certain proportion of the driving time is spent at this locations and pedestrians are not always in the hazardous area. As focus is on the run over scenario, the probability is reduced further to a certain extent. However, there is no conclusive data available to decide the Exposure class as a general result for any vehicle.	C3	Some drivers will be startled at the moment of unintended acceleration and the close proximity of vehicle and pedestrian lowers the reaction time; less than 90% of all drivers or all traffic participants are usually able or barely able to avoid harm.	B to C	

F3-1b	Provide requested drive torque	provide more drive torque than requested	Unintended yaw rate change *[= Unintended rotational motion (vertical axis)]*	(1) Max. ASIL for a system depends on the potential to destabilize the car in certain driving situations, due to malfunction. It typically depends on system properties like: a) Level (Nm) and Gradient (Nm/s) of unwanted torque b) Powertrain concept (front/rear), vehicle mass, load distribution etc.	For evaluation, a set of situations should be analyzed, where the most relevant parameters are selected systematically: - surface friction - vehicle speed - curve speed	Front/side collision with roadside objects or oncoming traffic.	S2 to S3	If the vehicle loses road grip and an unintended yaw rate can't be prevented by the driver: a) Front drive vehicle will go on straight forward (under steering), but might leave the road with some speed and collide with roadside objects like tree etc. (S2). b) Rear drive vehicle will rapidly over steer. (Side) collision with oncoming traffic or roadside objects is possible (S3).	E2 to E4	Most significant situation for ASIL Assessment is driving with typical country road speed and moderate lateral acceleration. Now it depends on the system properties, whether destabilization is possible on a) dry road (E4), b) wet road (E3) or c) only on icy road (E2) → *Typical level and dynamics of torque for conventional cars leads E3 as a maximum in this case. For electric car, this can be different.* *Comment:* *Higher speed and/or higher lateral acceleration would reduce the E-parameter*	C2	Driver's first impulsive reaction is to apply brake pedal. Secondary he might shift to neutral or he can turn the engine off.	QM to C	ASIL is strongly vehicle and system property dependent

F3-2	Provide requested drive torque	provide less drive torque than requested	Loss of acceleration (coasting)	Comment: If driving situation is almost at limit of stability, the sudden loss of torque possibly can lead to some destabilization. (side force is affected due to change in longitudinal force) → see F4-1b for details.	Malfunction occurs while overtaking another vehicle on country road with oncoming traffic.	frontal collision with oncoming traffic.	S3	If the overtaking maneuver can't be accomplished as quick as anticipated, a frontal collision with the oncoming vehicle is possible. In this case, severe injury due to the high relative speed is probable.	E2	Duration based evaluation: Overtaking with oncoming traffic is a short time maneuver that does not happen very often and will not exceed 1% of total operation time.	C1	Overtaking maneuvers with oncoming traffic demand more driver attention and concentration. He/she can reduce speed / apply brake and get back. In addition, the oncoming vehicle driver can reduce speed and/or execute evasion maneuver.	QM	
F4	Basic function: Provide braking torque													
F4-1a	Provide braking torque	provide more braking torque than requested	Unintended deceleration (without destabilization)	Max. ASIL for a system depends on the level (and gradient) of unwanted deceleration that is possible due to malfunction.			Hazard item is covered under the Brakes Appendix. See Brakes Appendix Section F4.1 (Braking Hazard 1) for details.							
F4-1b (1)	Provide braking torque	provide more braking torque than requested [rear drive]	Unintended yaw rate change *[= Unintended rotational motion (vertical axis)]*	Max. ASIL for a system depends on the potential to destabilize the car in <u>certain driving situations</u>, due to malfunction. It typically depends on system properties like: a) Level (Nm) and Gradient (Nm/s) of unwanted torque b) Powertrain concept (front/rear), vehicle mass, load distribution etc.	For evaluation, a set of situations should be analyzed, where the most relevant parameters are selected systematically: - surface friction - vehicle speed - curve speed	Front/side collision with roadside objects or oncoming traffic.	S3	If the vehicle loses road grip and an unintended yaw rate cannot be prevented by the driver. The rear drive vehicle will rapidly over steer. (Side) collision with oncoming traffic or roadside objects is possible without losing much speed in advance (S3).	E2 to E4	Most significant situation for ASIL Assessment is driving with intermediate speed (e.g., 130 km/h) and limited lateral acceleration (e.g., 2 m/s²). Now it depends on the system properties, whether destabilization is possible on dry road (E4), wet road (E3) or only on icy road (E2). Comment: Higher speed and/or higher lateral acceleration would reduce the E-parameter.	C3	The driver will not be able to regain control, when the vehicle has lost grip and is destabilized on wet or icy road. Oncoming traffic might react and decelerate, but for the collision with roadside objects, there is no Controllability.	B to D	ASIL is strongly vehicle and system property dependent

F4-1b (2)	Provide braking torque	provide more braking torque than requested [front drive]	Unintended yaw rate change *[= Unintended rotational motion (vertical axis)]*	Max. ASIL for a system depends on the potential to destabilize the car in certain driving situations, due to malfunction. it typically depends on system properties like: a) Level (Nm) and Gradient (Nm/s) of unwanted torque b) Powertrain concept (front/rear), vehicle mass, load distribution etc.	For evaluation, a set of situations should be analyzed, where the most relevant parameters are selected systematically: - surface friction - vehicle speed - curve speed	Front/side collision with roadside objects or oncoming traffic.	S2 to S3	If the vehicle loses road grip and an unintended yaw rate cannot be prevented by the driver: The front drive vehicle will go on straight forward (under steering). On dry road, the vehicle will rapidly decelerate but might leave the road with some speed and collide with roadside objects like tree etc. (S2). On wet or icy road, collision is possible without losing much speed in advance (S3).	E2 to E4	Most significant situation for ASIL Assessment is driving with intermediate speed (e.g., 130 km/h) and limited lateral acceleration (e.g., 2 m/s²). Now it depends on the system properties, whether destabilization is possible on dry road (E4) wet road (E3) or only on icy road (E2). *Comments:* *Higher speed and/or higher lateral acceleration would reduce the E-parameter.* *E4-scenario leads to S2, E2/E3 scenario can lead to S3 also.*	C3	The driver will not be able to regain control, when the vehicle has lost grip and is destabilized on wet or icy road. Oncoming traffic might react and decelerate, but for the collision with roadside objects, there is no Controllability.	B to C	ASIL is strongly vehicle and system property dependent
F4-2	Provide braking torque	Lack of regenerative torque (when accelerative pedal is released)	Loss of (regenerative) deceleration	Effect will be like "unwanted vehicle sail-on".	Vehicle at low speed drives up to a cross-walk. Driver wants to stop by regenerative deceleration.	Collision with pedestrian at low speed.	--	Collision with pedestrian at low speed.	--	Vehicle at low speed drives up to a cross-walk. Driver wants to stop by regenerative deceleration.	C0	It is regarded to be controllable for everybody (C0), at least as long as the expected regenerative deceleration the driver is accustomed to, is not too high. (e.g., < 3 m/s^2).	*none*	

F4-3	Provide braking torque	Lack of drag torque	Loss of (drag) deceleration	Effect will be like "unwanted vehicle sail-on". Comment: Vehicles with heavy trailers might require drag torque when going downhill, to avoid brake system overheating. This should be kept in mind if this case is discussed together with brake system requirements (not within this workgroup).	Vehicle at low speed drives up to a cross-walk. Driver wants to stop by drag torque deceleration.	Collision with pedestrian at low speed.	--	Collision with pedestrian at low speed.	--	Vehicle at low speed drives up to a cross-walk. Driver wants to stop by drag torque deceleration.	C0	It is regarded to be controllable for everybody (C0), as long as the brake system is working.	*none*	Vehicles with heavy trailers might require drag torque when going downhill, to avoid brake system overheating. This should be kept in mind if this case is discussed together with brake system requirements (not within this workgroup).
F5	Basic function: Provide selectable/automatic rollaway prevention														
F5-1b	Provide rollaway prevention	Unintended engagement of rollaway prevention (while driving)	Unintended deceleration	System independent evaluation ("Generic rollaway prevention") → see F4-1a											
F5-1c	Provide rollaway prevention	Unintended engagement of rollaway prevention (while driving)	Unintended yaw rate change *[= Unintended rotational motion (vertical axis)]*	System independent evaluation ("Generic rollaway prevention") → see F4-1b											
F5-1d	Provide rollaway prevention	Unintended engagement of rollaway prevention (while driving)	Loss of longitudinal motion (very low speed)	Special case: Typical parking lock system The maximum level of torque depends on parking lock mechanics, because it will break at certain level. It is assumed, that there is a mechanical measure that prevent parking lock from being engaged when drive shaft has a certain minimum speed. In this case, malfunction is only possible when speed is very low or when drive shaft is stopped due to blocking wheels (e.g., braking on low friction without ABS).	Vehicle drives at low speed (<5 km/h) into a crossroad when malfunction is happening. Other vehicle comes from the side.	front-to-side-collision with other vehicle	S2	Final impact of oncoming vehicle is likely to be in the range 25 kph ≤ Δv ≤ 35 kph (16 mph ≤ Δv ≤ 22 mph).	E2	Relevant situations are less than 1% of total operation time, e.g., when vehicle is merging into the far lane of the road, crossing a thoroughfare or turning across traffic which has the right of way.	C2	Driver can avoid exposing vehicle to the risk of collision. By driving correctly there will be enough time for the oncoming vehicle to brake.	QM	See D5.1 for detailed explanation and guidance.

F5-2 / F5-3	Provide rollaway prevention	No engagement or unintended disengagement of rollaway prevention	Unintended longitudinal motion	Evaluation depends on several basic system properties: (1) Malfunction usually is only possible when E/E system is active. For plug-in electric cars this can be much longer than for conventional cars (2) Driver expectation is different when Auto-P function is available.	Vehicle is stopped at a slope (engine off) with enough free space to roll (to pick up hazardous speed). Pedestrian or other road user is in hazard area (downhill).	collision with pedestrian or other road user.	'--	Severity can be derived from the collision speed that mainly depends on distance and slope.	'--	Parking at a slope is a common event, but the probability to have free space to roll and for a pedestrian to be in the hazard area is correlated with the assumed slope and distance.	'--	With no driver in the car, C3 is assumed as the pedestrian might not be aware of the danger or fails to react fast enough. With the driver still in the car, Controllability depends on driver status (distracted, hurry) and reaction time (correlated to slope and distance).	'--	See D5.2 for detailed explanation and guidance.
F5-4	Provide rollaway prevention	Unable to disengage rollaway prevention	--	Not safety relevant. (S0)	Vehicle at stand still with engaged rollaway prevention. Driver wants to start.	Vehicle will remain in standstill condition. No hazardous effect.	S0	Vehicle will remain in standstill condition. No hazardous effect.	E4	Vehicle at stand still with engaged rollaway prevention. Driver wants to start.	--		*none*	

D.5 EXPLANATIONS AND DETAILS TO THE EXAMPLES

In this section, additional detail is provided on how the evaluation has been performed for the examples shown within Table D3.

D.5.1 Estimation and Calculation of Exposure Class

F5-1: Unintended engagement of rollaway prevention

Based on this example, it can be explained how estimation based evaluation of Exposure has been done.

Scenario F5-1d

Detailed situation: Vehicle is stopped at cross road for red signal. The signal changes to green and the first vehicle starts and accelerates. Another vehicle comes from the side and the driver of this vehicle expects that the first one will quickly cross the road. Then unintended engagement occurs in the leading vehicle, while the distance between both vehicles is quite short.

Evaluation / Discussion

1st step: Discussion of relevant aspects of the scenario, to improve understanding

It is assumed, that there is a mechanical measure that prevent parking lock from being engaged when drive shaft has a certain minimum speed (e.g., 5 km/h). Thus, the malfunction has to occur before this speed is reached.

In a common driving situation, the driver of the vehicle coming from the side will recognize that a car is just crossing and will avoid entering the crossroad too quickly.

2nd step: Experience based estimations for required parameters

1. Assumed acceleration time: 2 seconds (until 5 km/h are reached)

2. Assumed number of crossroad situations per drive cycle: 20x

3. Relative number of crossroad situations with a car entering the crossroad from side in a risky way: 1 out of 10

3rd step: calculation of situation duration

Depending on the scenario, the Exposure has to be evaluated duration based (relative to operating time) or frequency based (relative to number of drive cycles). To allow for quantitative Exposure evaluation, for both cases some basic numbers have to be specified.[1] Based on these values, the limits for the E-parameter classes can easily be calculated according to ISO 26262-3:2011 [1] as it is shown in Table D4.

[1] Within this appendix, the following parameters have been used as evaluation basis:

Average operating time	400 h/year
Average number of drive cycles	1000/year

Table D4 - Calculated limits for E-parameter classes

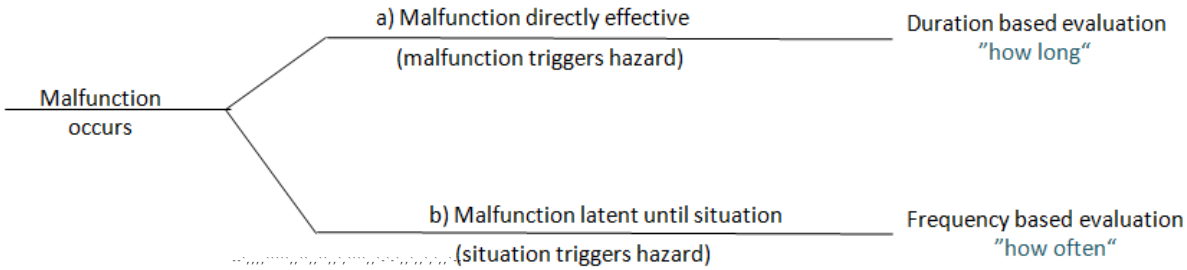
	E 1	E 2	E 3	E 4
ISO 26262 description (duration)	Not specified (very low probability)	<1% of average operating time	1 to 10% of average operating time	>10% of average operating time
Based on assumed operation time [h/yr]	<0.4 h/yr	4h/yr <x <=4 h/yr	4 h/yr <x <=40 h/yr	>40 h/yr
ISO 26262 description (frequency)	Less often than once a year	A few times a year	Once a month or more often	During almost every drive
Based on assumed number of drive cycles [1/yr]	<1/yr	1/yr <x <10/yr	10/yr < x <100/yr	>100/yr

For the given example, Exposure has to be rated duration based, as the malfunction can immediately cause the hazard[2]. Thus, it is calculated as follows:

- Calculation of mean time in situation: 4 seconds per drive cycle (from (1), (2) and (3))
- Assuming 1000 drive cycles per year, this gives 4000 seconds per year approximately about 1 hour per year
- This would be “E2” as it is less than 1% of the regular operation time of 400 h/yr.

However, this is only an experience based estimation, which is not (yet) fully backed up by statistical facts. Especially for parameters with a strong impact on the result, customer or field research data should be obtained.

[2] To decide whether duration based, or frequency-based Exposure evaluation is to be used, in most of the cases the following simple rule applies:



D.5.2 Evaluation of Scenarios with Strong Interdependency between Exposure, Severity and Controllability

F5-2: Unintended disengagement of rollaway prevention

For some malfunctioning behavior like example F5-2, a strong interdependency between Exposure, Severity and Controllability has to be analyzed for a set of scenarios to appropriately evaluate the risk. The subsequent paragraph shall give some additional guidance how this can be done.

Scenario for F5-2 (example for explanation)

Vehicle is stopped at a slope (engine off) with enough free space to roll (to pick up hazardous speed). Driver has left the car. Pedestrian is in hazard area (downhill) when the failure occurs.

Evaluation / Discussion

1st step: Discussion of relevant aspects of the scenario, to improve understanding

General description of scenario and definition of relevant parameters

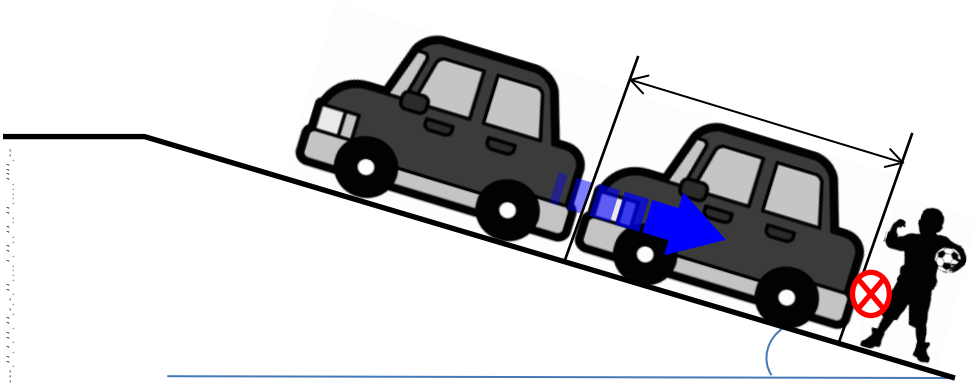


Figure D1 - Scenario F5-2 illustration

Conditions:

Before malfunction, the subject vehicle is stationary with engaged rollaway prevention.

Avoidance is impossible, because driver left.

→ C3 condition (There is no estimation about the avoidance action of pedestrian)

Parameters:

Grade (it influences the vehicles acceleration)

Distance between vehicle and pedestrian

2nd step: Simulation based calculation of relevant parameters

The speed at crash is calculated by using the acceleration by grade and vehicle-pedestrian distance (corresponding to duration) as parameters.

In combination with E and S judgments (limiting values) this can be used to derive the ASIL for all relevant situations.

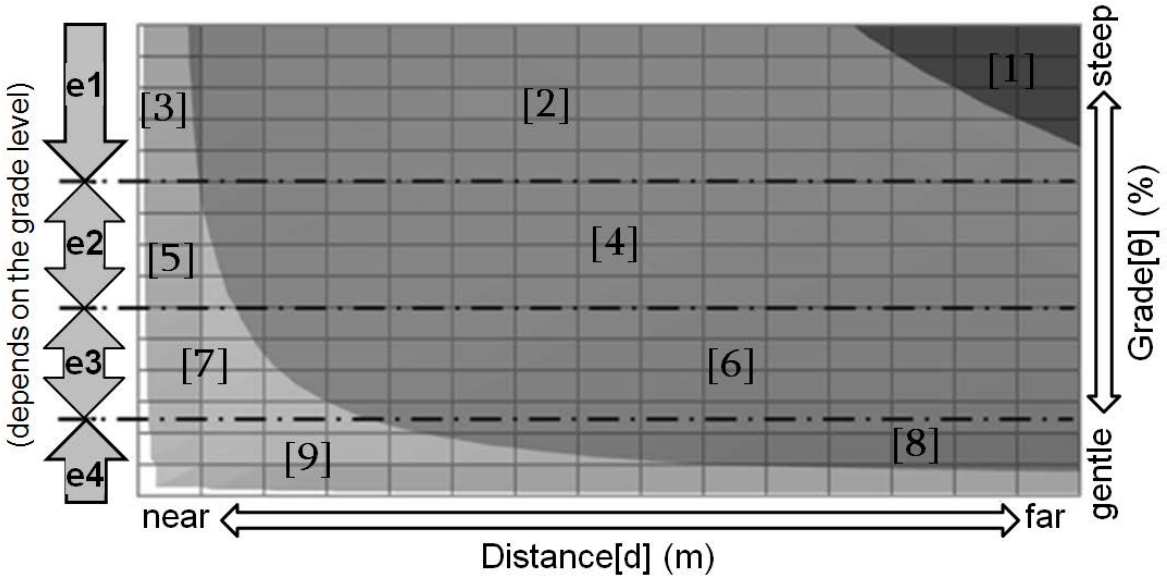


Figure D2 - Scenario F5-2 severity map

3rd step: Representative scenario and ASIL level

Controllability class is C3 for the overall scenario, because the driver has left the vehicle and pedestrian reaction is not assumed for near distance events. (Pedestrian's avoidance action is not examined, because there is no data about when pedestrian notices the moving vehicle)

Severity class based on the simulation as follows:

- Vertical: Grade of slope corresponds to magnitude acceleration (g)
- Lateral: Distance between vehicle and pedestrian corresponds to duration of acceleration

→ Result is collision speed as main S-criteria for rear crash against pedestrian

- (dark-gray area) → S3 Zone
- (gray area → S2 Zone
- (light-gray area → S1 Zone

Exposure class is a combined judgment from exposure conditions of e[θ] as probability to be at a certain grade and of e[d] as duration based probability that a pedestrian exists in the hazardous area. For example, in area [6] the overall Exposure is rated as E2 as a combination of e3[θ] and of e3[d].

Finally, for the HARA evaluation table, the example with the highest ASIL can be selected as “representative scenario”.

In addition, other scenarios have to be analyzed to find out which case leads to the highest ASIL. Some aspects that should be included in the HARA are:

- Situations with Driver still in the car (affects E and C)
- Driver distracted or leaves car in a hurry (affects E and C)
- Collision with vehicle coming from the side (affects S, E and C)

As far as appropriate, similar analytic approach as shown above can be used, to elaborate consistent representative scenarios.

D.5.3 Evaluation of Scenarios Related to Unintended Acceleration (without destabilization)

F3-1a: provide more drive torque than requested

The malfunctioning behavior to provide more drive torque than requested can lead to an unintended acceleration of the vehicle. For appropriate evaluation of the risk according to this hazard, several aspects have to be taken into account.

The most significant scenarios for evaluation tend to be situations where the vehicle follows another car and a rear-front-crash is possible and situations where vehicle speed is rather low and pedestrians are in the hazardous area in front of the car. The following paragraph gives some additional guidance on how to evaluate these scenarios for the own specific system and vehicle:

Driving behind another car

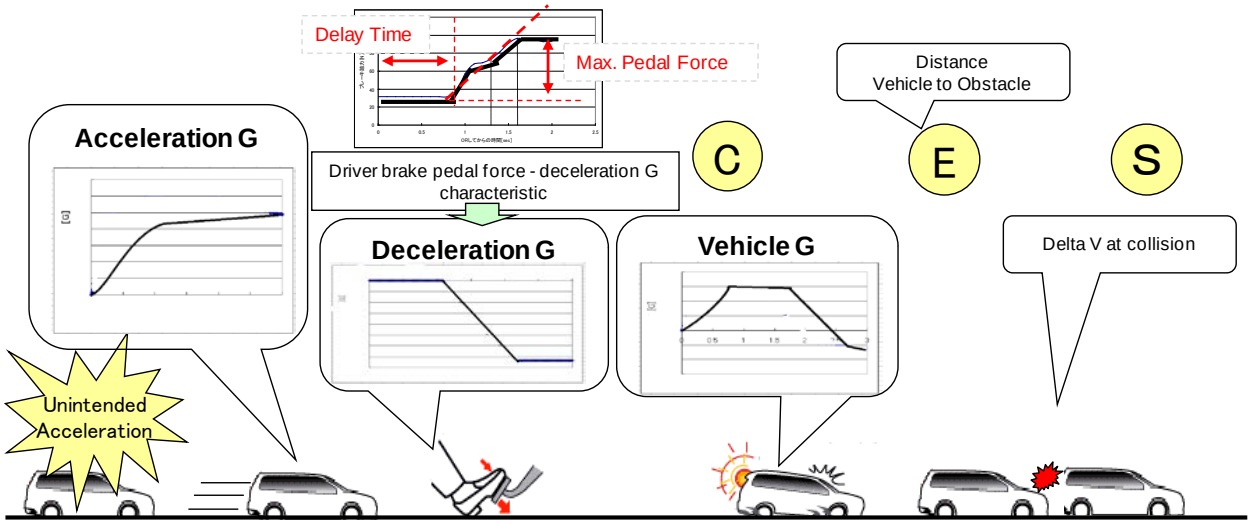


Figure D3 - Scenario F3-1a illustration

To properly evaluate the risk several parameters shown in the Figure D1 have to be analyzed:

- the vehicles acceleration dynamics
- the effective deceleration resulting from driver's reaction to press the brake pedal with a certain force
- the Exposure rates for different distances between the two vehicles
- the Exposure rates for different types of vehicles if these lead to different severity (e.g., if the other vehicle is a heavy truck, delta v at collision is higher, but probability to follow a truck is lower than to follow a regular passenger car)

Driving at low speed with pedestrian in hazardous area

This scenario applies whenever the vehicle is driving at low speed (e.g., 1st gear) and pedestrians are somewhere in driving direction of the car. Common examples are crossroads or parking lots.

To appropriately evaluate the risk, one approach is to focus on the most critical situation where fatal injury is probable (e.g., due to run-over) and the chance to avoid this specific harm by controlling the vehicle is small. This is the case when some boundary conditions are true:

- Driving maneuver where driver can easily fail to control the situation
- Pedestrian is present in the hazard area in front of the car
- No other obstacle between vehicle and pedestrian prevents collision
- Pedestrian is in a position where run-over is probable.

NOTE: The last condition depends on the specific vehicle design, as run-over is considered to be more likely to happen for some cars than for others in the same situation. Examples for relevant vehicle specific aspects are: ground clearance, frontal profile, passive pedestrian protection measures.

Guidance on Exposure evaluation:

A significant proportion of drive cycles include areas where pedestrians are present (e.g., crossroads, parking lots). However, it is evaluated that only a certain proportion of the driving time is spent at this locations and pedestrians are not always in the hazardous area in front of the car.

As focus is on the run-over scenario, the probability is reduced further to a certain extent. However, there is no conclusive data available at the moment to decide the Exposure class as a general result for any vehicle.

It is up to the reader to evaluate this issue for his own specific system and vehicle under analysis and to take care with any new data that might become available after release of this document to help decide what the Exposure class should be.

APPENDIX E - EXAMPLES AND GUIDANCE FOR SUSPENSION FUNCTIONS HARA

E.1 INTRODUCTION

This informative Appendix provides an example of the HARA for the suspension control functions. Section E3 provides a HAZOP analysis to identify the malfunction behaviors of the few suspension control functions. Some of the suspension control malfunctions, the resulting vehicle level hazards and the associated ASIL range are provided as examples in Section E4. It must be noted that this Appendix does not represent a complete HARA for all of the suspension control function but a subset of functional safety hazards for few suspension control functions for guidance.

General Disclaimer

This informative Appendix contains example ASILs for select hazard case. Unless otherwise noted, these ASILs were the result of consensus of vehicle manufacturers and suppliers prior to the publication and use of SAE J2980, and is a reference for these existing systems only. While the ASILs provided represent the consensus of the taskforce members, it must be noted that the ASILs could be lower or higher depending upon the vehicle, function authority and tuning.

E.2 ITEM DEFINITION: FUNCTIONAL CONCEPT SUMMARY

Suspension control functions generally are intended to enhance the vehicle handling characteristics during cornering maneuvers and improve the vehicle ride comfort by damping the effects of road noise, and vibrations. For the scope of this analysis, four suspension control functions are considered namely: Damper Control, Level Control, Stiffness Control, and Roll Control. These controls can vary from passive, semi-active to active controls. In semi-active and active controlled functions, electronic sensors and controls may be used to achieve the actuation of suspension dampers, air-springs, shock absorbers, roll bars, and other suspension devices.

E.3 HAZOP ANALYSIS

Table E1 shows the HAZOP analysis to identify the malfunction behaviors of few suspension control function. Many of the suspension control malfunctions are mapped to more than one vehicle hazard. The vehicle hazards are provided in Table E2 under Section E4.

Table E1 - HAZOP analysis of suspension control functions

System Function versus. HAZOP Guidewords	Loss of Activation	Incorrect Activation			Unintended Activation (When none was requested)	Output Stuck at a Value (Failure of function to update as intended)
		Incorrect Activation (More than requested)	Incorrect Activation (Less than requested)	Incorrect Activation (Activation in Opposite Direction)		
Damping Control (Control the damping coefficient)	Loss of Damping Control	Excessive Damping Control	Reduced Damping Control	Reverse Damping Control (Damping in the opposite direction than requested)	Unintended Damping (Autonomous Damping)	Stuck Damping
Level Control: (Control the level at each wheel)	Loss of Level Control	Excessive Level Control	Reduced Level Control	Reverse Level Control	Unintended Level Control	Stuck Level Control
Stiffness Control (Control the stiffness of the suspension)	Loss of Stiffness Control	Excessive Stiffness Control	Reduced Stiffness Control	Reverse Stiffness Control	Unintended Stiffness Control	Stuck Stiffness Control
Roll Control (Improves roll stability to the vehicle)	Loss of Roll Control	Excessive Roll Control	Reduced Roll Control	Reverse Roll Control	Unintended Roll Control	Locked Roll Control

E.4 HARA

Table E2 shows some examples of the HARA for few Suspension control functions

Table E2 - Example HARA analysis of suspension functions

Hazard ID	Function	Malfunctioning Behavior(s)	Vehicle Level Hazard	Assumptions	Hazard Detailed Description	Potential accident scenario(s)- considering worst case mishap potential	ASIL Assessment	Comments or Considerations (if applicable)
Suspension Hazard #1	**Damping Control**	Unintended or Incorrect Damping Control	Unintended Vehicle Motion (Lateral, Longitudinal, Vertical)	Semi Active Suspension System: Controlling the damping coefficient of the damper. The vehicle may not be stable under all states of damping control.	Malfunction of the damping control leading to potential loss of longitudinal and or lateral tractive forces at the tire under some driving conditions. This could lead to unintended reduction of vehicle stability or increased stopping distance during braking.	Driving scenario is under tight cornering conditions or lane change conditions (midrange lateral acceleration between 0.3 to 0.5 g) and road disturbance is exciting the vertical resonant frequency of the un-sprung mass.	**Can Range from QM to ASIL A depending upon vehicle**	ASIL classification of individual suspension functions depends on the vehicle, the function authority and design. If the authority of damping control function is such that the vehicle is stable under all possible malfunctioned states of the damping control, the hazard does not apply.
Suspension Hazard #2	**Level Control**	Incorrect or unintended level control at one or more wheels	Unintended Vehicle Motion (Lateral, Longitudinal, Vertical)	Active Level control function independently at each wheel	Unintended or incorrect level control at one or more wheel impacts the center of gravity (CG) of the vehicle or incorrect distribution of the forces at the wheels.	Worst case driving scenario is under tight cornering conditions or double lane change conditions (midrange lateral acceleration between 0.3 to 0.5 g) where the malfunction could induce yaw or roll moments in the vehicle.	**Can Range from QM to ASIL C depending upon vehicle**	ASIL classification of individual suspension functions depends on the vehicle, the function authority and design. If the authority of Level control function is such that the vehicle is stable under all possible malfunctioned states of the level control, the hazard does not apply.

Suspension Hazard #3	**Stiffness Control**	Incorrect or unintended stiffness control at one or more wheels	Unintended Vehicle Motion (Lateral, Longitudinal, Vertical)	Active stiffness control function independently at each wheel	Malfunction of the stiffness control leading to potential loss of longitudinal and or lateral tractive forces at the tire under some driving conditions. This could lead to unintended reduction of vehicle stability or increased stopping distance during braking.	Worst case is uneven diagonal distribution under driving scenario of tight cornering conditions or double lane change conditions (midrange lateral acceleration between 0.3 to 0.5 g) where the malfunction could induce yaw or roll moments in the vehicle.	**Can Range from QM to ASIL B depending upon vehicle**	ASIL classification of individual suspension functions depends on the vehicle, the function authority and design. If the authority of Stiffness control function is such that the vehicle is stable under all possible malfunctioned states of the stiffness control, the hazard does not apply.
Suspension Hazard #4	**Roll Control**	Unintended or Incorrect Active Roll Control	Unintended Vehicle Motion (Lateral, Longitudinal)	Active roll control independently controls the roll moment at each axle	Malfunction of the roll control leading to potential loss of longitudinal and or lateral tractive forces at the tire under some driving conditions. This could lead to unintended reduction of vehicle stability or increased stopping distance during braking	Unintended roll moment under high lateral acceleration driving conditions could cause vehicle instability	**Can Range from QM to ASIL B depending upon vehicle**	ASIL classification of individual suspension functions depends on the vehicle, the function authority and design. If the authority of Active Roll control function is such that the vehicle is stable under all possible malfunctioned states of the roll control, the hazard does not apply.

E.5 OTHER CONSIDERATIONS

Suspension control can vary from passive, semi-active to active control. When performing suspension control function HARA, the analyst should consider the type and authority of the control function to influence vehicle handling and the overall vehicle design to assess the ASIL for the safety goal. The resultant ASIL is vehicle dependent.

APPENDIX F - EXAMPLES AND GUIDANCE FOR BRAKE AND PARK BRAKE FUNCTIONS HARA

F.1 INTRODUCTION

This Appendix offers examples, guidance and arguments for the use of the HARA to determine the ASIL, and meet the requirements of ISO 26262:2011 [1]. Only the most relevant malfunctioning behavior and vehicle level hazards regarding Brake and Park Brake functions were considered. This Appendix does not represent a complete HARA for the Brake and Park Brake functions. These examples do not necessarily define the minimum or maximum ASIL for any specific vehicle system. They are intended as guidance to assess the particular vehicle hazard. The results of each hazard discussion are presented in one of three ways:

i. ASIL and ASIL ranges

ii. No ASIL agreed, but the upper ASIL bound was determined

iii. No ASIL agreed, but guidance to support parameters for ASIL determination

Even where consensed ASIL values are published, different ASIL determination processes and different S, E, C values may have been used. In a HARA for a particular application, additional situations have to be evaluated to find out which one gives the highest ASIL, for a particular safety goal.

The examples have been composed by functional safety experts from several worldwide producing vehicle manufacturers and suppliers (USA, Europe, Asia). Most of the workgroup members already had completed their own in-house HARA for Brake and Park Brake functions for different vehicles and/or different specific Brake and Park Brake systems prior to the compilation of this Appendix.

General Disclaimer

This informative Appendix contains example ASILs for select hazard case. Unless otherwise noted, these ASILs were the result of consensus of vehicle manufacturers and suppliers prior to the publication and use of SAE J2980, and is a reference for these existing systems only. While the ASILs provided represent the consensus of the taskforce members, it must be noted that the ASILs could be lower or higher depending upon the vehicle, function authority and tuning.

F.2 ITEM DEFINITION: FUNCTIONAL CONCEPT SUMMARY

Two primary functions are included in this Appendix: the Brake function and the Park Brake function. A brief functional description for each function is provided in this section. More comprehensive definitions can be found in SAE standards such as J2627 and J2564. The HAZOP for each of the primary functions is contained in Section F3.

F.2.1 Brake Function

The purposes of the brake primary function covered in this Appendix are:

- To provide deceleration to the vehicle based on driver input from the brake pedal or based on input from other systems in the vehicle such as driver assistance systems

- To provide stability in situations near the physical limits of vehicle dynamics by actuation of wheel brake (i.e., by the functions Stability Control, Antilock Braking System (ABS), and Electronic Brake Distribution).

F.2.1.1 Stability Control

The stability control function is a safety assist or safety enhancing feature. The primary functionality is to assist the driver in maintaining control of the vehicle. Stability control utilizes sensors in the vehicle to determine whether the intent of the driver’s inputs is consistent with the vehicle’s direction. If stability control detects an inconsistency, it can control braking or throttle function to help correct the inconsistency.

F.2.1.2 Antilock Braking System (ABS)

ABS is a safety assist or safety enhancing feature whose primary function it is to prevent wheel lock in order to help avoid uncontrolled skidding or to help reduce stopping distance. ABS monitors the speed of each wheel and controls the brakes in a specific cadence if it detects a wheel spinning slower or faster than the others.

F.2.1.3 Electronic Brake Distribution (EBD)

EBD's primary function is to optimize the efficiency and stability of the base brake system. It prevents overbraking of the rear wheels by adjusting rear brake pressure closer to the ideal brake force distribution, thus optimizing rear axle braking irrespective of vehicle loading.

F.2.2 Park Brake Function

The park brake primary function is to hold the vehicle stationary. The park brake sub-functions covered in this Appendix are park brake activation or park brake engagement and park brake disengagement, both based on driver request.

F.3 HAZOP ANALYSIS

F.3.1 Brake Primary Function

Table F1 shows the HAZOP analysis to identify the malfunction behaviors of the Brake function. Table F2 shows the mapping of the Brake malfunctions to vehicle hazards.

Table F1 - HAZOP analysis for brake function

		Incorrect Function Activation				
Function	Loss of Function	More than Requested	Less than Requested	Opposite Direction than Requested	Unintended Function Activation	Output Stuck at a Value (Failure of function to update as intended)
Deceleration	Loss of Braking	Excessive Braking	Insufficient Braking	N/A	Unintended Braking	Locked Braking

Table F2 - Mapping of brake malfunction behaviors to vehicle hazards

Malfunction Behaviors	Vehicle Hazards
Unintended Braking	Unintended Vehicle Longitudinal Deceleration
Locked Braking	
Excessive Braking	
Insufficient Braking	Unintended Reduction in Vehicle Deceleration
Loss of Braking	
Unintended Braking	Unintended Vehicle Lateral Motion
Locked Braking	
Excessive Braking	
Unintended Loss of Stability, ABS, or EBD Control Functions	Unintended Loss of Vehicle Brake Control Function

F.3.2 Park Brake Primary Function

Table F3 shows the HAZOP analysis to identify the malfunction behaviors of the Park Brake function. Table F4 shows the mapping of the Park Brake malfunctions to vehicle hazards.

Table F3 - HAZOP analysis for park brake function

Function	Loss of Function	Incorrect Function Activation			Unintended Function Activation	Output Stuck at a Value (Failure of function to update as intended)
		More than Requested	Less than Requested	Opposite Direction than Requested		
Engage Park Brake	Loss of Ability to Engage Park Brake	N/A	Insufficient Park Brake Apply	N/A	Unintended Engage of Park Brake	Loss of Ability to Disengage Park Brake
Disengage Park Brake	Loss of Ability to Disengage Park Brake	N/A	Insufficient Release of Park Brake	N/A	Unintended Disengage of Park Brake	N/A

Table F4 - Mapping of park brake malfunction behaviors to vehicle hazards

Malfunction Behaviors	Vehicle Hazards
Unintended Engage of Park Brake	Unintended Vehicle Lateral Motion
	Unintended Vehicle Longitudinal Deceleration
Unintended Disengage of Park Brake	Unintended Longitudinal Vehicle Motion
Park Brake Fails to Engage	
Insufficient Park Brake Apply	
Park Brake Fails to Disengage	Unintended Loss of Vehicle Longitudinal Motion
Insufficient Release of Park Brake	

F.4 HARA

F.4.1 Brake Function HARA

Table F5 shows some examples of the HARA for Brake function

Table F5 - Example HARA analysis for brake function

Hazard ID	Function	Malfunctioning Behavior	Vehicle Level Hazard	Assumptions	Hazard Description	Worst-case Mishap Potential	ASIL Assessment							Comments / Considerations
							S	Rationale	E	Rationale	C	Rationale	ASIL	
Braking Hazard 1	Deceleration	Unintended Braking	Unintended Vehicle Longitudinal Deceleration	No wheel locking	The braking system provides braking when no braking is requested	Rear collision if vehicle behind is traveling too closely and unable to stop	Contributing parameters may include vehicle speed & time gap (characteristic derived from both vehicle speeds), the magnitude of deceleration G by malfunction, mass ratio of involved vehicles, safety equipment, and occupant restraints, reaction time and rate & magnitude of deceleration G of following vehicle (driver capability). Other parameters may also be considered.							- See Section F1, point (iii)
Braking Hazard 2	Deceleration	Insufficient Braking	Unintended Reduction in Vehicle Deceleration	None	The braking system provides less braking than requested	Potential collision due to insufficient braking	Dependent on Brake reduction magnitude						QM~D	- See Section F1, point (ii)
Braking Hazard 3	Deceleration	Unintended Braking	Unintended Vehicle Lateral Motion	Locking of wheels, affecting vehicle stability	The braking system provides braking when no braking is requested	Potential for vehicle to depart lane and collide with other vehicles, pedestrians, or objects	S3	Worst-case potential mishap could lead to S3 Severity	E4	Everyday driving on high mu road surfaces	C3	Difficult to control	D	- See Section F1, point (ii)
Braking Hazard 4	Drag Control	Unintended activation of Drag Control	Unintended Vehicle Acceleration				Hazard item is covered under the Propulsion Appendix. See Propulsion Appendix Section D4.2 (Hazard ID F3) for details.							
Braking Hazard 5	Traction Control	Unintended activation of Traction Control	Unintended loss of Vehicle Acceleration				Hazard item is covered under the Propulsion Appendix. See Propulsion Appendix Section D4.2 (Hazard ID F3) for details.							
Braking Hazard 6	Stability Control	Unintended Loss of Brake Yaw Control Feature	Unintended Loss of Vehicle Brake Yaw Stability Control	Driver require high Lateral G	The stability control function is unavailable		S3	Worst-case potential mishap could lead to S3	E1	Rare case	C3	Difficult to control	A	Without warning indicator
Braking Hazard 7	ABS	Unintended Loss of ABS	Unintended Loss of Vehicle ABS	Driver require Deceleration on low mu	The ABS is unavailable		S3	Worst-case potential mishap could lead to S3	E1	Rare case	C3	Difficult to control	A	Without warning indicator
Braking Hazard 8	Electronic Brake Distribution	Unintended Loss of EBD	Unintended Loss of Vehicle EBD	Driver require high deceleration	The EBD is unavailable		S3	Worst-case potential mishap could lead to S3	E1 ~E3	Depends on vehicle (brake design and vehicle concept)	C3	Difficult to control	QM~C	- See Section F1, point (ii)

F.4.2 Park Brake Function HARA

Table F6 shows some examples of the HARA for Park Brake function.

Table F6 - Example HARA analysis for park brake function

Hazard ID	Function	Malfunctioning Behavior	Vehicle Level Hazard	Assumptions	Hazard Description	Worst-case Mishap Potential	ASIL Assessment							Comments / Considerations
							S	Rationale	E	Rationale	C	Rationale	ASIL	
Park Brake Hazard 1	Park Brake	Unintended Engage of the Rear Park Brake	Unintended Lateral Vehicle Motion	None	Rear Park Brake activates when not intended.	Activation of park brake when vehicle is in motion could lead to lateral motion and collision with other vehicles, pedestrians, or objects.	S3	Worst-case potential mishap could lead to S3 Severity.	E4	>10% of average operating time since could happen on any road layout; ISO 26262/2011/Part 3, Table B.2 - Road Layout.	C3	Less than 90% of all drivers or other traffic participants may be able to avoid harm with an unintended lateral motion.	D	Worst-Case Scenario
Park Brake Hazard 2	Park Brake	Unintended Engage of the Rear Park Brake	Unintended Vehicle Longitudinal Deceleration	None	Rear Park Brake activates when not intended.	Activation of park brake when vehicle is in motion could lead to rear collision if following vehicle is too close and unable to stop.	Dependent on vehicle dynamics taking into consideration such as the Brake Design and Vehicle Concept.						QM~C	- See Brake Hazard ID 01 for additional considerations
Park Brake Hazard 3	Park Brake	Unintended Disengage of Rear Park Brake	Unintended Longitudinal Vehicle Motion	Manual Transmission; Vehicle transmission is not in park.	Rear Park Brake disengages when not desired.	Potential worst-case mishap scenario is if driver is not in the vehicle with engine running when park brake disengages.	Item is covered under the Propulsion Appendix. See Propulsion Appendix Section D5.2 and Section D4.2 (Hazard ID F5-2) for details.							
Park Brake Hazard 4	Park Brake	Rear Park Brake Fails to Engage	Unintended Longitudinal Vehicle Motion	None	Rear Park Brake fails to engage when needed.	Park brake fails to engage leading to unintended longitudinal motion and potential collision with other vehicles, pedestrians, or objects.	Item is covered under the Propulsion Appendix. See Propulsion Appendix Section D5.2 and Section D4.2 (Hazard ID F5-3) for details.							
Park Brake Hazard 5	Park Brake	Rear Park Brake Fails to Disengage	Unintended Loss of Longitudinal Vehicle Motion	None	Rear Park Brake fails to disengage when requested to.	Vehicle is parked and unable to move, so not a hazard.	Item is covered under the Propulsion Appendix. See Propulsion Appendix Section D4.2 (Hazard ID F5-4) for details.							

F.5 EXPLANATIONS AND DETAILS TO THE EXAMPLES

In this part of the Appendix, some more detailed background information is given about how an evaluation may be been done for the examples in Table F4.

F.5.1 Evaluation of scenario related to unintended vehicle longitudinal deceleration (applicable to Brake Hazard 1 and Park Brake Hazard 2)

The malfunctioning behavior is described as providing more brake torque without driver intent which can lead to an unintended deceleration of the vehicle. For appropriate evaluation of the risk according to this hazard, several aspects may be taken into account. The most significant scenarios for evaluation tend to be situations where the vehicle with malfunction is followed by another car and a rear-front-crash is possible. The following paragraph gives some additional guidance on how to evaluate this scenario for the own specific system and vehicle:

(1) Driving behind another car

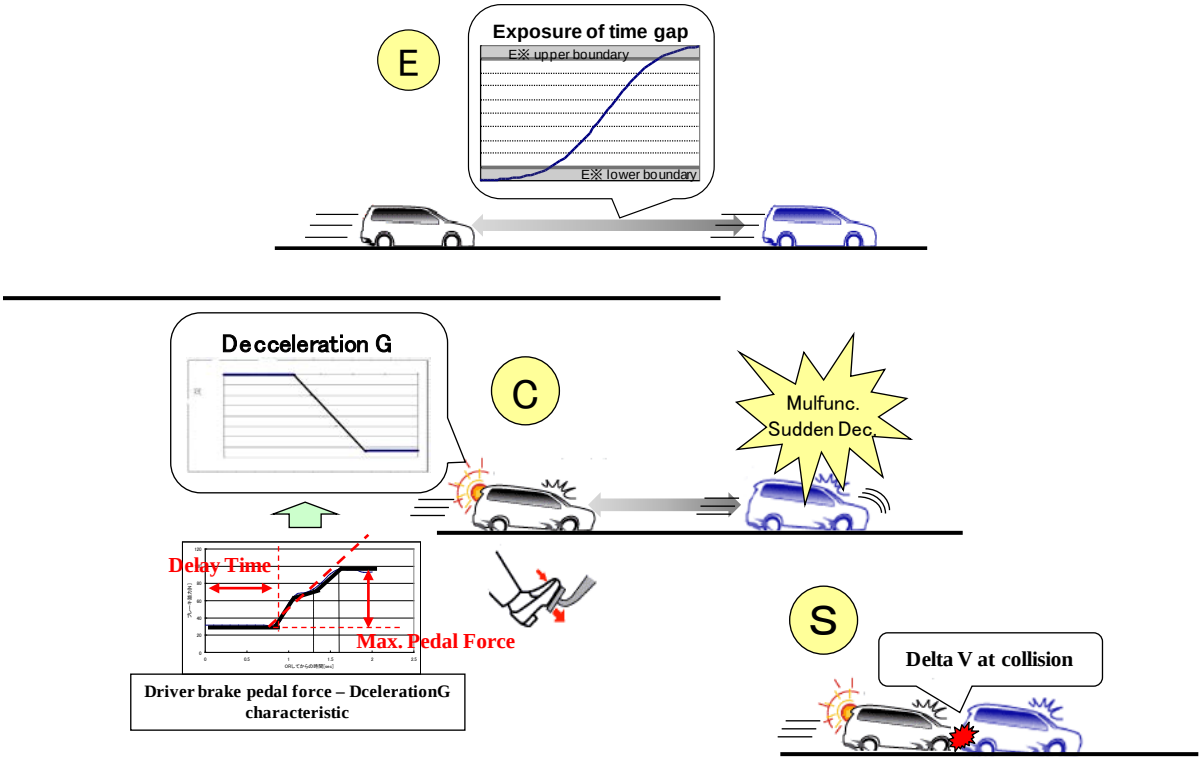


Figure F1

To properly evaluate the risk several parameters shown in Figure F1 may be included in the analysis:

- the vehicles deceleration dynamics + malfunction
- the effective deceleration resulting from driver's reaction (following vehicle) to press the brake pedal with a certain force and rate
- the Exposure rates for different distances between the two vehicles at different speeds
- the Exposure rates for different types of vehicles if this lead to different Severity (e.g., if the other vehicle is a heavy truck, delta v at collision is higher, but probability to be followed by a truck is lower than to follow a regular passenger car

Based on the deceleration dynamics of the vehicle system and malfunction potential, the possible combinations (e.g., following distances, collision speeds, reaction time, etc.) plays a significant role within the analysis and may lead to a range of ASILs. Additional study is needed to appropriately assess the malfunctioning behavior for the vehicle environment.