Guideline

Hazard Analysis and Risk Assessment

Guideline Version	2022.2	Revision Date 2022-08-12
Authors	Global Functional Safety Technical Forum	Creation Date 2009-10-21

Content

List of Tables

List of Figures

Note:
This document is the Guideline for the Functional Safety Document "FFSD 02 Hazard Analysis and Risk Assessment".

To create the document, the corresponding template shall be used. The Template in combination with the requirements of the Guideline represents the basis for an ISO 26262 aligned document.

For all persons involved in the creation or review of a document it is recommended to read and understand all Ford Functional Safety Guidelines in order to get a sufficient overview about the overall Safety Process.

As supporting documents, templates for meeting minutes and as well as open concerns exist. These supporting documents shall be used in accordance to the Functional Safety guidelines, as required.

The Functional Safety Document Set is available for Ford usage in the "Functional Safety Toolbox":

https://azureford.sharepoint.com/sites/GlobalFunctionalSafety/Functional%20Safety%20FAQ%20Wiki%20Page/Functional%20Safety%20Team.aspx.

Format Options
Hints: Light grey italic formatted text.
Examples: Blue text.

1. Hazard Analysis and Risk Assessment

1.1 Purpose

The purpose of the Hazard Analysis and Risk Assessment is to identify and classify the potential hazardous event of the item and to formulate safety goals related to the prevention or mitigation of these hazardous events in order to achieve an acceptable residual risk. For this, the item is evaluated with regard to its safety implications.
Safety goals and their assigned Automotive Safety Integrity Level (ASIL) are determined by a systematic evaluation of hazardous situations. The rationale of the ASIL determination considers severity, probability of exposure and controllability.

The tasks of the Hazard Analysis and Risk Assessment are:

- identification of potential hazardous events of the item based on functions, Malfunctioning Behaviours, system level effect, driving / operating situations, and vehicle level effects
- classification of potential hazardous events based on potential severity, probability of exposure in the operational situations, and controllability (ASIL determination)
- formulation of safety goals related to the prevention or mitigation of these hazards in order to achieve an acceptable residual risk

1.2 Responsibilities and Actions

This subsection describes the responsibilities and actions for preparation of the Functional Safety Document.

Preconditions for preparation of the document:
The person(s) responsible for the creation or release of the documents (document owner, key participants, and reviewers) shall:

- Read and understand this guideline and its related template.
  Note: The template and the guidelines together provide the basis for an ISO 26262 aligned document.
- Participate in an ISO 26262 Functional Safety training (internal Ford training or external training) to get an understanding of the complete safety process and the interrelation of the documents with the safety lifecycle.
- Inform the person responsible for the document "FFSD 01 Safety Plan" about his/her training status
  Note: this topic is normally considered within the Functional Safety Kick-Off Meeting. Persons joining the project at a later date shall register for the training and inform the person responsible for the Safety Plan autonomously.
- Provide their personal information (Contact Data, Experience/background) to the person responsible for the document "FFSD 01 Safety Plan"
  Note: this topic is normally considered within the Functional Safety Kick-Off Meeting. Persons joining the project at a later date shall inform the person responsible for the Safety Plan autonomously.

Creation of the document:
The person(s) responsible for the document shall:

- Identify person(s) needed to support the creation of the document and the person(s) responsible for document approval.
- Review the roles & responsibilities and timing plans described in the document "FFSD 01 Safety Plan" and provide updates in case of any changes
- Initiate and coordinate all meetings relevant for the realization of the document:
  - Prepare Meeting Agendas / Meeting Minutes.
    Note: It is recommended to use the supporting document “SUP-01 Meeting Minutes / Agenda" as template.
  - Review open concerns related to Functional Safety and provide updates to the Open Concern / Action Item List (status changes, new concerns…)
    Note: Depending on project needs, the open concerns can be included in a generic the open concern / action item list for the project or in a separate one related to the Functional Safety topics.

  - Perform project management activities to realize the document adequately
- Create and maintain the document according to the applicable guideline and use the corresponding template.
- Insert the document version releases (including version number, date, author and remarks describing the changes) in the Version Tracking table. A version shall be released at least each time the document is provided to another person (e.g. for review). Also, the final version shall be documented in the table (after successful review).
- For each document release, provide status information to the person responsible for the "FFSD 01.8 Safety Status Report"
- Document review date and personnel information.

Review of the document:

The person(s) responsible for the document shall:

- Identify persons needed for the review of the document.
- Review the roles & responsibilities described in the document "FFSD 01 Safety Plan" and provide updates in case of any changes
  Note: The level of independence and qualification of the person reviewing the document shall be aligned with ISO 26262.
- Initiate and coordinate all activities relevant for the Review of the document.
- Document Review Exceptions / Deviations / Findings in the template.
- Provide updates to the Open Concern / Action Item List (status changes, new concerns…)
- Provide updates to the open concern / action item list (status changes, new concerns…)
- See Section 2.4.9.

The person(s) responsible for the Review of the document shall:

- Review the document according to the template and the corresponding guideline.
- Provide review comments, including Exceptions / Deviations / Findings.

Relationship between document, Safety Case, Ford Functional Safety Assessment and Functional Safety Feature Status Report:

The person(s) responsible for the documents 01.1 – 01.7 and 02 – 08 shall:

- Provide the status of the document to the person responsible for the GPDS Functional Safety Feature Status
- Provide the complete document (including review results) to the person responsible for the "FFSD 10 Ford Functional Safety Assessment" and support the assessment activities.

Note that the document owner is the author and approver of this document. The approval process is to load the document into the central repository (VSEM) and releasing for use after completing reviews.

1.3 ISO 26262 References

This Functional Safety Documents covers following ISO 26262 work products:

ISO 26262 Work Product name	ISO 26262 reference
Hazard analysis and risk assessment report	Part 3, 6.5.1
Verification report of the hazard analysis and risk assessment	Part 3, 6.5.2

Table 1: ISO references

1.4 Input

	Input	Part(s)
FFSD / Other Input (Required)	FFSD 01.1 Item Definition / FFSD 01.10 Feature Document	
Other Input (Optional)	Previous Experience and Documentation of similar projects	
	Function Specification	
	FMEA (If new Hazardous Event is discovered)	
	Open Concerns / Action Items (from multiple sources)	

Table 2: Input

1.5 Output

	Output	Part(s)
FFSD	FFSD 02 Hazard Analysis and Risk Assessment	
	Summary of document for FFSD 09 Safety Risk Case	Summary of document
	Update Information for FFSD 01 Safety Plan	Training Status
Other Output	Updates for Open concerns / Action items	Status changes, new concerns
	Updates for FMEA (for QM Hazardous Events)	

Table 3: Output

1.6 Templates / Related Documents

FFSD	Guideline	FFSG02_HazardAnalysisAndRiskAssessment_Guideline.pdf (this document)
	Template	FFSD02_HazardAnalysisAndRiskAssessment_Template.xlsx
	Example	*see Examples - All Documents (sharepoint.com)*
Others		

Table 4: Templates / Related documents

2. Method and Requirements

2.1 Overview & Theoretical Background

2.1.1 ISO 26262 Scope

ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles, excluding mopeds. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities.

Systems and their components released for production, or systems and their components already under development prior to the publication date of ISO 26262:2018, are exempted from the scope of ISO 26262:2028. For further development or alterations based on systems and their components released for production prior to the publication of ISO 26262:2018, are addressed by tailoring the safety lifecycle depending on the alteration. ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of E/E safety-related systems.
ISO 26262 does not address the nominal performance of E/E systems.

ISO 26262 contains **normative** and **informative** sections. An item or process is aligned with the ISO 26262 if it complies with the normative sections of ISO 26262. Informative data is supplemental information such as additional guidance, supplemental recommendations, tutorials, commentary as well as background, history, development, and relationship with other elements. Informative data is not a requirement and is not mandatory for alignment but provides recommendations.

2.1.2 Challenges in Creating a HARA

We identified the following challenges in creating a HARA:

- Find right level of detail (to enable efficient review)
- Representatives from each stakeholder group is helpful
- Don’t forget relevant faults/malfunctions (to ensure completeness)
- Don’t forget relevant situations (to ensure completeness)
- Document assumptions (to strengthen the scope of the Hazard Analysis)
- Describe effect of malfunction in a comprehensible way (to allow Risk Assessment)
- Ensure consistency of cross-organizational malfunction descriptions
- Define Safety Goals such that the derivation/development of the system is supported
- Consistency in ratings between different HARAs within your organization and throughout Ford

2.1.3 General Approach

Figure 1 shows the general approach for generating a HARA.

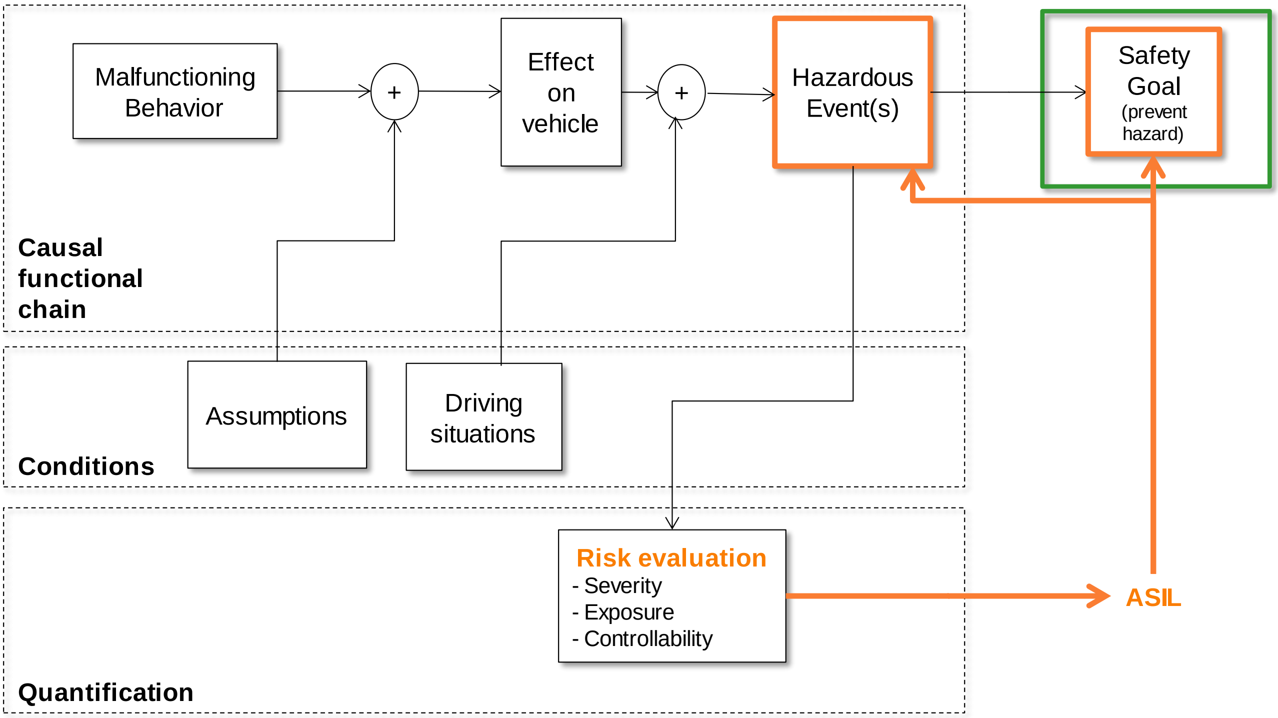


Figure 1: General HARA Approach

According to ISO 26262 Part 3, Section 6.4.1.2, "The item without internal safety mechanisms shall be evaluated during the hazard analysis and risk assessment, i.e. safety mechanisms intended to be implemented or that have already been implemented in predecessor items shall not be considered in the hazard analysis and risk assessment."

EXCEPTION: In the case that potential safety mechanism (e.g. limitation of the actuator performance) does not prevent the hazardous event (reduces only the residual risk) and/or this potential safety mechanism is separated from other controls (encapsulation of safety mechanism), a residual risk assessment (for detailed information see 2.4.5) considering the safety mechanism can be done. Therefore, the residual risk assessment shall consider the safety mechanism, if it is implemented according the highest ASIL level assessed for this hazardous event.[1]

When developing a HARA some basic analysis consideration can be employed, as listed in the table below. They describe behavioral, controllability, vehicle and other system functionality that can be assumed to be present in the vehicle, operator, passenger or pedestrian. These basic considerations shall not be explicitly called out in the HARA itself nor captured in the feature documentation. Changes to these basic considerations can be proposed through the Global Functional Safety Technical Forum.

Name	Category	Description
Feature Functional Scope Accuracy	Behavioral	The functional boundary of the feature correctly and completely describes the functionality in scope of the feature.

[1] Potential safety measures only reduce the residual risk of the hazardous event. That means the effect of the malfunction behavior is mitigated (e.g. to achieve a better controllability, to reduce the situation probability), but the safety measure is not able to prevent the hazardous event.

		This allows feature document to provide description of the feature scope. I.e., the feature document is the complete item description.
Vehicle Design Intent Functionality	Vehicle	The vehicle will behave within design intent in the absence of malfunctions. SOTIF will be considered as part of a different analysis. This allows for focus on results of malfunctions in analysis. Includes aspects of vehicle being maintained sufficiently to function within design bounds for the vehicle lifetime.
Feature/system Independence	Other Systems	Features, by definition, do not interact with other features. Therefore, the feature being analyzed for a HARA does not need to consider these types of interactions. Interactions with systems are considered. This allows for limiting the cascading results of malfunctions.
Operator & Participant Rationality	Controllability	In the presence of a potential hazardous event identified by the HARA analysis, vehicle/system operators, and participants in scenarios will, on average, behave rationally and will use information and means available in the scenario to attempt to avoid harm. This is the basis for controllability arguments involving operator and participants in the scenario with the average response being a reasonable attempt to mitigate or avoid harm based on available means and information.
Reasonably Expected Operation	Behavioral	In the presence of all driving situations identified by the HARA analysis, the feature will perform as intended in the absence of a malfunctioning behavior. This allows reasonable bounds on scenarios and potential hazardous events. Misuse should be specified separately as appropriate.

Table 5: Basic Analysis Consideration Table

2.1.4 Risk Analysis

For the analytical approach, a risk (R = risk) can be described as a function F, having three parameters:

- The frequency (f = frequency) of occurrence of a hazardous event,
- the controllability (C), i.e. ability to avoid the specific harm or damage through timely reactions of the persons involved and
- the potential severity (S) of the resulting harm or damage:

$$\mathbf{R = F (f, C, S)}$$

Note: Definition of hazard according to ISO 26262 and IEC 61508: potential source of harm

The frequency of occurrence f is, in turn, influenced by two factors:

One factor to consider is how frequently and for how long individuals find themselves in a situation where the hazardous event can occur. In ISO 26262 this is simplified to be a measure of the probability or frequency of the operational situation taking place in which the hazardous event can occur (E = exposure).

Another factor is the occurrence rate of faults in the. This is not considered during hazard analysis and risk assessment. Instead, the ASILs that result from the classification of E, S, C during hazard analysis and risk assessment determine the minimum set of requirements on the item in order to control or reduce the probability of random hardware failures and to avoid systematic faults.

The Hazard Analysis and Risk Assessment sub phase comprises three fundamental steps:

1. Situation Analysis and Hazard Identification

   The goal of the situation analysis and hazard identification is to identify the potential unintended behaviours of the item that could lead to a hazardous event.

   The situation analysis and hazard identification activity require a clear definition of the item, its functionality and its boundaries. It is based on the item's functional behaviour; therefore, the detailed (technical) design of the item does not necessarily need to be known.

2. Hazard Classification

   The hazard classification scheme comprises the determination of the severity (S), the probability of exposure (E) and the controllability (C) associated with the considered hazard of the item.

   To align ASIL ratings, S, E, and C classes shall be reviewed and revised.

   For a given hazard, this classification results in one or more combinations of S, E and C classes.
   Each such combination includes an estimation of the severity of a potential harm in a particular driving/operating situation and the exposure to the situation. The controllability rates how easy or difficult it is for the driver or other road traffic participant to avoid or mitigate the harm in the particular situation.

   Once severity, exposure and controllability are determined they are mapped to the Automotive Safety Integrity Level (ASIL) according

   Note: the mapping to the ASIL is done automatically in the template "FFSD02_HazardAnalysisAndRiskAssessment" after assigning S, E and C to the corresponding hazard.

3. Definition of Safety Goals

   Safety Goals are the top-level safety requirements of the item. The functional safety requirements necessary to avoid an unreasonable risk for each hazard are derived from the Safety Goals.

   Safety Goals shall fulfil following requirements:
   - A Safety Goal shall be expressed in terms of functional objectives (not in terms of technological solutions)
   - One Safety Goal shall be defined for each hazardous event rated as ASIL A, B, C or D in the hazard analysis.
   - For hazardous events rated as QM, the definition of a Safety Goal is optional
   - If a Safety Goals is assigned to different hazardous events, the highest ASIL of the hazardous events must be assigned

2.1.5 Situation Analysis and Hazard Identification

For an adequate realization of the situation analysis and hazard identification, following aspects shall be considered:

- Operational situations / vehicle usage scenarios (e.g. parking, rolling, driving at speed)

- Vehicle Operating modes (e.g. engine stopped, engine running) and Use Cases
- For Trucks and Buses (T&B), vehicle variances shall be considered (e.g. type of base vehicle, vehicle configuration, vehicle operation) as well as each relevant type of base vehicle. The variances in operational situations that have impact on technical parameters shall also be considered [2]
- Environmental conditions (e.g. road surface friction, side wind)
- Assumptions (e.g. conditions in which the item is assumed to behave in a safe manner, assumptions regarding driver behaviour)
- Interaction with other systems
- Correct Usage and foreseeable incorrect usage [3]

  Note: All operational situations and operating modes in which an item's malfunctioning behaviour is able to trigger hazards shall be described; both when the item is correctly used and when it is incorrectly used in a reasonably foreseeable way.

  Note: Hazards resulting only from the item behaviour, in the absence of any item failure, are outside the scope of this document.

In addition, it must be considered that different people could be endangered due to hazards:

- Driver
- non-motorist

The situations, modes and conditions shall be listed and detailed in order to ensure a comprehensible understanding. The item without any safety mechanism shall be evaluated during Situation Analysis and Hazard Identification (i.e. safety mechanisms intended to be implemented or already implemented in predecessor systems shall not be considered). [4]

Identified hazards outside the scope of ISO 26262 shall be highlighted and reported to the responsible persons (e.g. FMEA team, STPA team) [5] and the responsible team shall classify hazards according to procedures of the applicable safety discipline.
Example: toxicological hazards

The outcome of an FMEA or STPA analysis may identify new hazardous events that were not comprehended previously in the HARA. These hazardous events shall be added to the HARA at the time of identification and hazard identification shall be performed. A rereview of the HARA shall occur if any new hazardous events are added to the HARA.

[2] See ISO 26262, Part 3, 6.4.5.2/3, 6.4.5.6
[3] See ISO 26262, Part 3, 6.4.2.1/2
[4] See ISO 26262, Part 3, 6.4.1.2
[5] See ISO 26262, Part 3, 6.4.3.1

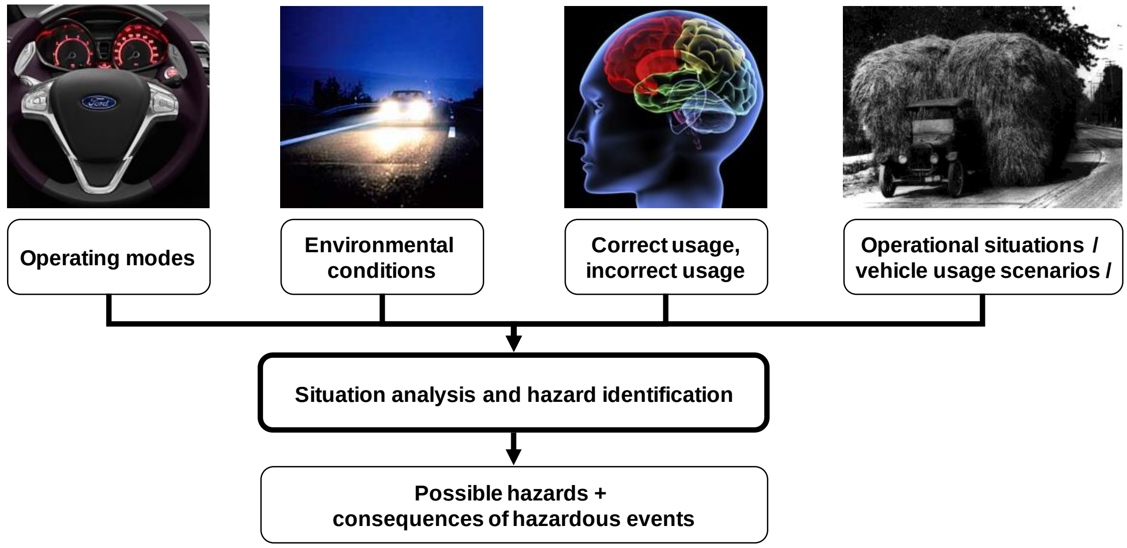

Operating modes
Environmental conditions
Correct usage, incorrect usage
Operational situations / vehicle usage scenarios /
Situation analysis and hazard identification
Possible hazards + consequences of hazardous events

Figure 2: Situation Analysis and Hazard Identification – fundamental Approach

In order to find relevant hazardous events, a combination of potential malfunctioning behaviour of an item, and situations must be investigated. Listing all permutations of scenarios, operating modes, environmental conditions and usage for a malfunctioning behaviour should be avoided. Although this approach may imply completeness, it often leads to excessive hazardous events, longer HARA development time, and increase in HARA maintenance, often without an increased benefit of identifying additional hazards. Adversely, analysing a subset of scenarios that do not cover the defined operational scenarios, could lead to missed hazards. Instead consider identifying scenarios, operating modes, environmental conditions and usage for a malfunctioning behaviour that could lead to a diversity of hazards, and unreasonable residual risk. This can be achieved by the following:

- Develop the hazardous events based on known operational scenarios, modes, conditions usage, and constraints captured in the Item Definition or Feature Document.
- Additionally, review the Situation Dictionary to see if the list prompts any potential additional scenarios. *Note: The situation dictionary is a compilation of known situations based on experience and former projects. If a developing item, requires a situation not captured in the situation dictionary, follow the process for requesting a new situation.*
- Brainstorm if there are any situations that could potentially lead to increase in risk of the hazardous event or identify a different hazard. For example, would severity, exposure or controllability be affected by a different situation. If there is potential the hazardous event's risk may increase, consider including the situation (see Table 6). Also consider other phases of the item's lifecycle in addition to operation, such as production, service and decommissioning. For example, the item has to be in a specific state in manufacturing that differs from the states during normal vehicle operation.
- Evaluate if there is potential to combine situations together to make several specific scenarios into a generic scenario with the same risk and hazards (see Table 5). This approach prevents the fragmentation of situations, which can lead to an inadmissible exposure reduction.

Note: All malfunctioning behaviours shall be covered by the hazardous events in the HARA. The combining of scenarios for hazardous events shall only occur for the same malfunctioning behaviour.

The following situation could be grouped into one situation, to provide a broader scenario driving a higher exposure rating.

Non-Motorist walking in front of vehicle in a parking lot. Driver applying brake.	Non-motorist crosses in front of vehicle, where vehicle is at a stop. Driver is applying brakes.
Non-Motorist crossing an intersection. First vehicle at intersection. Driver applying brake.	

Non-Motorist walking in front of vehicle in driveway. Driver applying brake.	

Table 6: Combining situations

It some cases, in contrast to Table 5, it may be valuable for hazardous events to be left as separate Hazardous Event line items in the HARA due to potential severity, exposure and controllability ratings being different.
In other cases, a scenario may be unique however it leads to the same hazard with potentially lower risk ratings.

For the example of a malfunctioning behaviour of unintended steering lets evaluate the following:

#	Situation	Rationality
1	Non-Motorist is walking along high-speed road. Vehicle is being driven at high-speed.	The exposure rating drops due to non-motorist walking along the high speed road, in comparison to just driving a high speeds. A potential collision with or without a non-motorist at high speed will be a high severity rating (based on SEC rating guidance). Assuming pedestrian is following law, facing towards traffic, the pedestrian has some controllability to move out of the way, and the driver to apply the brakes.
2	Vehicle is being driven at high speed, with obstacles alongside road.	Since it is common to have obstacles (e.g. parked vehicle, trees, guard rails, signs etc.) alongside the road and the vehicle is being driven at high speed, a high exposure rating could be applied, A potential collision at high speed for the driver will be assess to a high severity rating. The controllability rating would be higher than the previous scenario since the obstacles cannot move out of the way.

Table 7: Comparing Situations

Although the HARA could include both situation 1 and 2, situation 2 identifies the same hazard as situation 1 “Unintended Steering (self-steer)”, and a higher potential risk, for a similar driving scenario (driving at high speed and potentially colliding). It would be recommended to use situation 2, instead of including situations 1 and 2 in the HARA. However, this decision depends on the item and the considered malfunctioning behaviour.

Note: The potential ratings of Severity, Exposure, and Controllability, as described for the purpose of the example will be captured as high, medium and low. The Rationality column is used to summarize and compare S, E, and C rationales based on the scenario and malfunctioning behaviour. In the HARA rationales for hazardous event Severity, Exposure, and Controllability would be captured in the Severity Rationale, Exposure Rationale, and Controllability rationale columns respectively.

Misuse is the use of the system in a manner contrary to training, warnings or instructions provided by the manufacturer, as well as laws and applicable best practices. It is ***Foreseeable Misuse*** if at the time of design, the manufacturer was aware of the potential for or expectation of a given misuse. Many foreseeable misuses are common customer behaviours, or expectations of customers that are not explicitly in line with the design intent of a system. If the misuse is far beyond the operational bounds, capabilities or legal operation of the system in given conditions, it may be considered ***Negligent Operation***, particularly if harm may occur in the absence of a system malfunction. A HARA should exclude negligent operation scenarios, as it is not the malfunction that leads to the potential harm, but the operation of the system itself.

To account for foreseeable misuse when performing a HARA, it is recommended that Hazardous Events in which this can occur be documented on separate line items. One line-item will be for documenting the ASIL level of the Hazardous Event without the foreseeable misuse present. Subsequent line items will document the Hazardous Event with it present. More than one-line item may be necessary if there are multiple foreseeable misuses identified. By separating the Hazardous Event into multiple line, it allows the severity, exposure and controllability of each case separately.

Examples of foreseeable misuse may include:

- Not checking the mirrors before changing lanes or exiting vehicles
- Passengers in the bed of the pickup
- Not coming to a complete stop at stop signs
- Adjusting infotainment settings in traffic
- Excessive seat-recline while driving

2.1.6 Hazard Classification

All hazards identified during the previous stage shall be classified, except those which are outside the scope of ISO 26262.

Note: ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems including interaction of these systems. It does not address hazards as electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy, and similar hazards unless directly caused by malfunctioning behaviour of E/E safety related systems.

Note: Pets should be handled outside the scope of FuSa. It will follow normal QM development.

Some guidance for classification is given in https://azureford.sharepoint.com/sites/GlobalFunctionalSafety/GuidanceISO26262HARA/ReferenceForISO26262HARAofSEC%20FINAL.pdf, Guidance ISO26262 HARA Assessment of SEC and in https://azureford.sharepoint.com/sites/GlobalFunctionalSafety/Pages/Shared-HARA.aspx, Shared HARA (SHARA).

If classification of a given hazard with respect to severity, probability of exposure or controllability is unclear or doubtful, it must be classified conservatively.

Example: If classification of Exposure is difficult to distinguish between E2 and E3 (no clear justification for E2 possible), the higher value (E3) shall be chosen unless further evidence is available.

Note: For Trucks and Buses (T&B), when classifying the parameters for severity, exposure and controllability, an appropriate combination of the variance types for an item shall be considered. The appropriate combination can be determined based on engineering judgement.

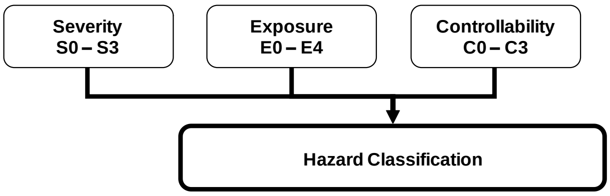


Figure 3: Hazard Classification – Fundamental Approach

2.1.6.1 Determination of potential severity (S)

Severity determination in accordance to ISO 26262 is solely related to harm to people, not to material damage, environmental pollution etc.

The severity shall be assigned to one of the severity classes S0, S1, S2 or S3 in accordance with Table 8.

Note: The risk assessment of hazardous events focuses on the harm to each endangered person – including the driver or the passengers of the vehicle causing the hazardous event, and other endangered persons such as cyclists, pedestrians or occupants of other vehicles.

Class	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Table 8: Classes of Severity[6]

There are operational situations that result in harm (e.g. an accident). A subsequent malfunctioning behaviour of the item in such an operational situation can increase, or fail to decrease, the resulting harm. In this case the classification of the severity may be limited to the difference between the severity caused by the initial operational situation (e.g. the accident) and the malfunctioning behaviour of the item.

Example 1: If an accident occurs, which is not caused by the malfunctioning behaviour of an item, the resulting harm from the accident is not considered for the classification of the severity.

Example 2: The item under consideration includes an airbag functionality to reduce harm caused by the crash. For an accident in which the airbag fails to deploy, the harm caused by the crash can be determined. If a correctly operating airbag would have reduced the harm of the same accident to a lower severity class, then only the difference is considered for the severity classification.

At Ford this kind of severity rating is called incremental severity, where the severity is the incremental amount of harm of the malfunctioning behaviour to the harm of the system behaviour (correctly operating) within the initial operating scenario. In order to use incremental severity:

1. Harm must exist within the scenario for a system behaviour, and
2. A difference of harm exists between the harm from the malfunctioning behaviour within a scenario and the harm from the system behaviour within the same scenario.

From Example 2, harm existed due to the collision occurring with the airbag functioning properly. The difference between the harm for the malfunctioning behaviour (e.g. airbag not deploying) and the system behaviour (e.g. air bag correctly deploying) in the same situation (e.g. collision) is used to rate the severity.

The usage of incremental severity in a HARA is to be evaluated on a case-by-case basis at the Global Functional Safety Technical Forum_meeting, to avoid artificially reducing ASIL ratings. Contact your local Application Functional Safety Engineer (AFSE) for awareness and to be placed on the agenda.

The severity class S0 may be assigned if the hazard analysis and risk assessment determines that the consequences of an unintended behaviour of the item are clearly limited to material damage. If a hazardous event is assigned to severity **class S0, no ASIL assignment is required**. [7]

ISO 26262 provides several informative examples which support the severity rating, see template, Tab "Severity".

2.1.6.2 Determination of the probability of exposure (E)

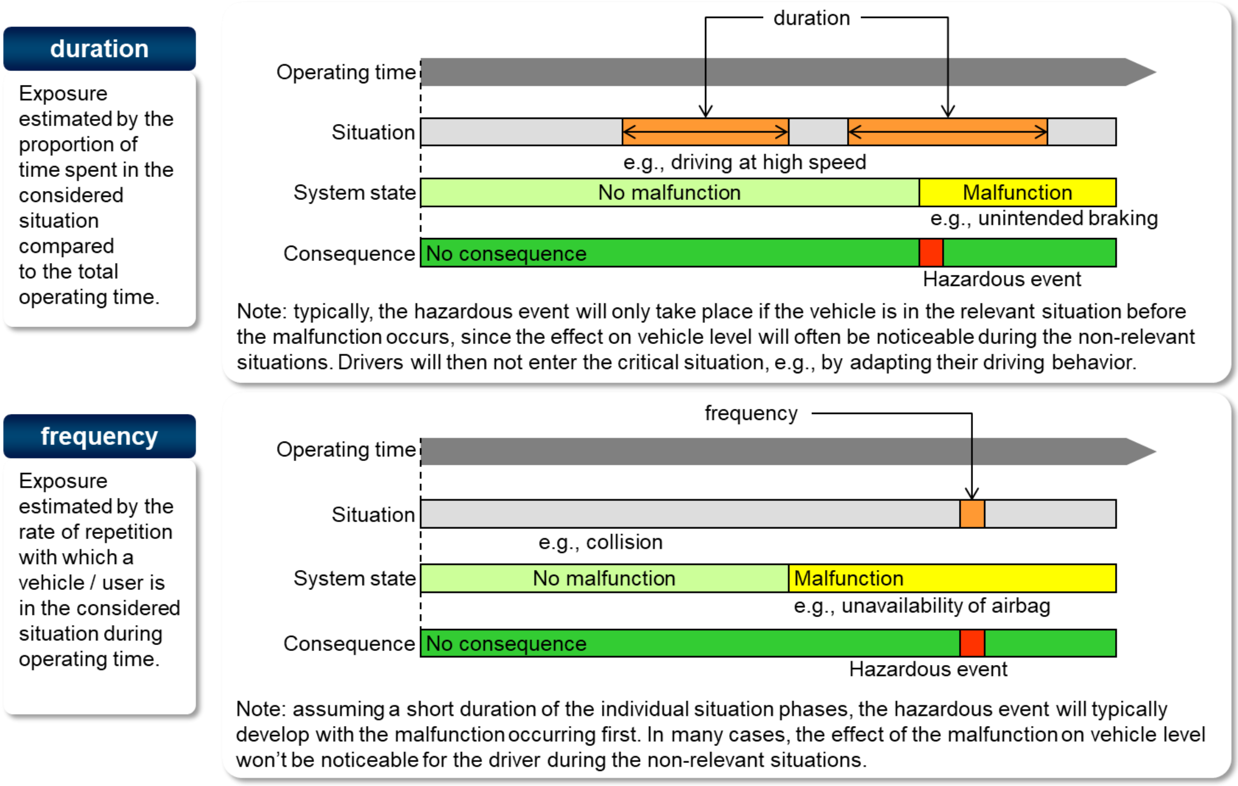
The probability of exposure of each operational situation combined with the trigger of the hazard shall be estimated and shall be assigned to one of the probability classes E0, E1, E2, E3 and E4 in accordance with Table 9.

Class	**Exposure**				
	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Table 9: Classes of probability of exposure

According to ISO 26262, the exposure can be rated according to the type “duration” and the type “frequency”. The appropriate rating type has to be selected (see Figure 4):

[6] See ISO 26262, Part 3, 6.4.3.2, 6.4.3.3
[7] See ISO 26262, Part 3, 6.4.3.4



duration

Exposure estimated by the proportion of time spent in the considered situation compared to the total operating time.

Note: typically, the hazardous event will only take place if the vehicle is in the relevant situation before the malfunction occurs, since the effect on vehicle level will often be noticeable during the non-relevant situations. Drivers will then not enter the critical situation, e.g., by adapting their driving behavior.

frequency

Exposure estimated by the rate of repetition with which a vehicle / user is in the considered situation during operating time.

Note: assuming a short duration of the individual situation phases, the hazardous event will typically develop with the malfunction occurring first. In many cases, the effect of the malfunction on vehicle level won't be noticeable for the driver during the non-relevant situations.

Figure 4: Duration rating versus frequency rating

In general, most situations can be rated using duration exposure. Here are some examples for situations that have a completely different (higher) rating for exposure:

- No light activation in tunnel
- Park sensor failure when driving in reverse
- Launching in unintended direction
- Wrong steering direction in park maneuver
- No airbag deployment in a crash situation
- Self-steer in case of hands-off driving

For such situations, a frequency exposure should be considered.

Note: If not using duration, annotate in the rationale.
Note: The probability of the malfunction shall not be considered. In doubt, contact your AFSE.
Note: Perception of the driver for a malfunction can be rated in the controllability.

Class E0 may be used for those situations that are suggested during hazard analysis and risk assessment, but which are considered incredible, and therefore not explored further. A rationale shall be recorded for the exclusion of these situations. If a hazardous event is assigned to **exposure class E0, no ASIL assignment is required**. [8]

There are operational scenarios where several unlikely situations are combined that result in a lower probability of exposure than E1. For Hazardous Events rated S3, C3, E1 with an operational scenario that could be considered of this type, QM may be argued.

Example: For the malfunction of a high voltage system erroneously supplying power. The combined operational situations are: a crash which deploys the airbag; with the vehicle lying partly in the water; and the high voltage system partially exposed without causing an internal short circuit.

[8] See ISO 26262, Part 3, 6.4.3.5/7

Example: A malfunction with the ABS system (NO), where the ABS does not engage when it is needed, would fall under the frequency type exposure rating. Since the ABS malfunction (NO) will not be perceivable to the driver unless the driving conditions require the ABS system to activate (ex: rain, snow, slippery driving conditions). Therefore, an ABS malfunction (NO) would require the frequency strategy to determine the exposure rating for that type of malfunction.

Note: Safety mechanisms such as driver warning lights should not be considered when determining if the malfunction is perceivable or not by the driver.

Note: For Trucks and Buses (T&B), the number of vehicles of a given type of base vehicle shall not be considered when estimating the probability of exposure. Additionally, the number of vehicles equipped with a specific configuration shall not be considered when estimating the probability of exposure. [9]

The usage arguing QM due to this type of operating scenario combination is to be evaluated on a case-by-case basis at the Global Functional Safety Technical Forum meeting, to avoid artificially reducing ASIL ratings. Contact your local Application Functional Safety Engineer (AFSE) for awareness and to be placed on the agenda.

ISO 26262 provides several informative examples which support the exposure rating, see template, Tab "Exposure".

2.1.6.3 Determination of controllability (C)

The controllability, by the driver or other traffic participants, of each hazardous event shall be estimated. The controllability shall be assigned to one of the controllability classes C0, C1, C2 and C3 in accordance with the Table 10.

Class	**C0**	**C1**	**C2**	**C3**
Description	**Controllable in general**	**Simply Controllable**	**Normally Controllable**	**Difficult to Control or Uncontrollable**

Table 10: Classes of controllability rating[10]

Class C0 may be used for hazards addressing the unavailability of the item if they do not affect the safe operation of the vehicle (e.g. driver assistance system) or if an accident can be avoided by routine driver actions. If a hazardous event is assigned to the controllability **class C0, no ASIL assignment is required.** [11]

The controllability rating can also be affected by the Estimated Hazard Manifestation Time. The effect the HMT has on the rating should be assessed on a case by case basis, objectively considering the below factors and how they pertain to the unique circumstances of the hazardous event being considered. Depending on the operational scenario and the type of malfunctioning behaviour, a longer Estimated HMT may give the driver enough time to gain control of the hazardous event, which would result in a lower controllability rating.

When determining the controllability consider the following factors:

- How perceptible is the malfunctioning behaviour?
- How easy is it for the driver to prevent the hazard (what actions are required)?
- How much time does the driver have to react (See Hazard Manifestation Time below)?

Example: If windshield fogging builds up over a long enough time to allow the driver to put the vehicle in a safe state (say 30 sec – 1 min), the Controllability rating may be lowered.

[9] See ISO 26262, Part 3, 6.4.5.4/5
[10] See ISO 26262, Part 3, 6.4.3.8
[11] See ISO 26262, Part 3, 6.4.3.9

Example: If loss of propulsion occurs in the garage when attempting to drive away from the house, C0 can be chosen as any driver can put the car back in park.

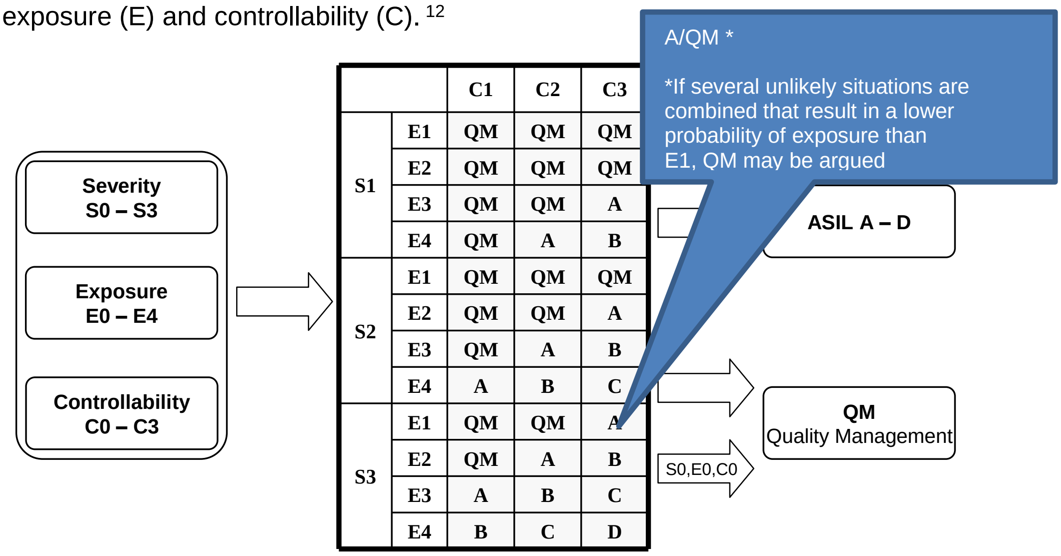
Note: Dedicated regulations that specify a functional performance with regard to the applicable hazardous event can be used as part of a rationale when selecting a suitable controllability class, if applicable, and supported by evidence, e.g. real usage experience.

Example: A dedicated regulation that covers the requirements for the certification of a vehicle system with a precise definition of forces or acceleration values in the case of a failure.

ISO 26262 provides several informative examples which support the controllability rating, see template, Tab "Controllability".

2.1.6.4 Determination of ASIL

The ASIL-Level shall be determined for each hazardous event based on the classification of severity (S), probability of exposure (E) and controllability (C). [12]


Severity
S0 – S3
Exposure
E0 – E4
Controllability
C0 – C3
A/QM *
*If several unlikely situations are combined that result in a lower probability of exposure than E1, QM may be argued
ASIL A – D
S0,E0,C0
QM
Quality Management

		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

Figure 5: ASIL Determination – Fundamental Approach

Note: Four ASILs are defined: ASIL A, B, C and D, where ASIL A is the lowest safety integrity level and ASIL D the highest one. In addition to these four ASILs, the class QM (Quality Management) denotes no requirement according to ISO 26262. QM hazardous event can have consequences with regards to safety, but quality processes are sufficient to manage the identified risk.

It shall be ensured that the chosen level of detail of the list of operational situations:

1) does not lead to an inappropriate lowering of the ASIL. [13]
2) does not lead to an inappropriate increasing of the ASIL.

Inappropriate lowering of the ASIL may occur when similar situations with similar Controllability and Severity are divided into situations with reduced Exposure. Inappropriate increasing of the ASIL may occur when situations with dissimilar Controllability or Severity are considered together with an increased Exposure.

The outcome of the ASIL determination shall include: the operational situations and operating modes with severity, probability of exposure, controllability and the resulting ASIL.

[12] See ISO 26262, Part 3, 6.4.3.10/11
[13] See ISO 26262, Part 3, 6.4.2.7

2.1.7 Identifying the Hazard Manifestation Time (HMT)

For each ASIL rated (A-D), Hazardous event it is necessary to develop an estimate of the time it takes for the Hazard to occur. This is important because it enables us to develop the Fault Tolerant Time Interval constraint in future work products. As an overview, the Fault Tolerant Time Interval is the minimum period of time beginning with a fault and ending with the Hazard. When examined more closely this interval can be broken up into two different sub intervals. The first interval is the Malfunctioning Behaviour Manifestation Time (or MBMT). It measures the time it takes for a fault to propagate through the system and start causing the malfunctioning behaviour. Stated differently:

> ***Malfunctioning Behaviour Manifestation Time (MBMT)****: The minimum time span from the occurrence of the fault to the manifestation of the Malfunctioning Behaviour at the vehicle level.*

The second interval, the Hazard Manifestation Time (HMT) measures how long it takes for the malfunctioning behaviour to lead to the Hazard. Or in other words:

> ***Hazard Manifestation Time (HMT)****: The minimum time span from the onset of the Malfunctioning Behaviour to the violation of the Safety Goal.*

These two intervals summed together produce the FTTI (see Figure 6 below).

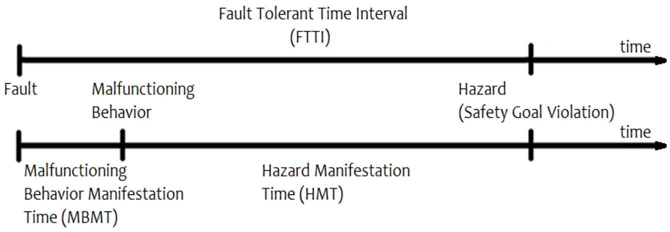


Figure 6: Fault Tolerant Time Interval, Malfunctioning Behaviour Manifestation Time and Hazard Manifestation Time

For the purposes of the HARA, the interval of interest is the HMT, since it is mostly dependent on the operational scenarios and type of malfunctioning behaviour. Therefore, it is required to provide an estimated HMT for each ASIL rated (A-D) hazard listed in the HARA. There are many reasons why an Estimated HMT is useful this early in the Functional Safety process:

- It assists in the identification of the worst-case scenarios for timing constraints.
- It helps with the initial work that will need to be done in the Functional Safety Concept.
- It provides an initial estimation of the timing constraint of a hazard, which allows others to determine the feasibility of the safety mechanism.
- It allows Ford to provide suppliers estimated timing information that is not normally available during the early phases of development.

For example, we could have a HARA with a Malfunctioning Behaviour of “Unintended Steering” and a Scenario: “driving at speed on a highway”. The task before us would be to estimate how long it would take for the Hazard to occur. In the HARA the Hazard selected from the Hazard Dictionary would be “Unintended Steering” however we could define the Harm as occurring once the vehicle exits its current lane. With this in mind, it is possible to develop a rough estimate of the HMT, even without the physical details of the vehicle. By developing HMT estimates for each Hazardous Event, we can then determine the HMT targets for each Safety Mechanism established in the Functional Safety Concept later in the process.
It is recommended to give a conservative estimate early on if it is not possible to get an exact number.

2.1.8 Definition of Safety Goals

One Safety Goal shall be defined for each hazardous event rated as ASIL A, B, C or D in the hazard analysis and risk assessment. [14]

Note: For hazardous event classified in the hazard analysis with QM, a safety goal can be defined.

- The ASIL determined for the hazardous event shall be assigned to the corresponding safety goal
- If similar safety goals are determined, they can be combined into one safety goal
- If similar safety goals are combined into a single one, the highest ASIL shall be assigned to the combined safety goal

Additionally, the Fault Tolerant Time Interval can be specified, including physical limits and constraints (the fault tolerant time interval is the time-span in which a fault or faults can be present in a system before a hazardous event occurs).

The Fault Tolerant Time Interval is the period of time between the occurrence of a functional fault and this fault actually becoming dangerous (if undetected). If this time is affected / influenced for this Safety Goal, this influence shall be described.[15]

If during the identification of the "fault tolerant time interval" a significant dependency on the operating condition is identified, each operating condition shall be considered.

Note: If fault tolerant times cannot be specified quantitatively during creation of the Hazard and Risk Assessment, parameters can be used and specified in the Functional Safety Concept or the Fault Tolerant Time Interval can be directly specified in the Functional Safety Concept.

[14] See ISO 26262, Part 3, 6.4.4.1

[15] See ISO 26262, Part 3, 8.4.2.3 b) and e)

2.2 Applied Template

The ISO 26262 standard does not prescribe in detail the approach of the Hazard Analysis and Risk Assessment but does make requirements on partial and final results. That gives the user a certain degree of freedom in the realization of this document as long as the postulated steps that have been mentioned before are fulfilled.
At Ford, the template for document "FFSD 02 Hazard Analysis and Risk Assessment" comprises the complete Hazard Analysis and Risk Assessment and covers all necessary aspects for a successful and complete realization. The template, an Excel-document, consists of eleven tabs and is divided into four major sections as shown in the Figure 7. The engineer responsible for this document shall fill out all these sections.

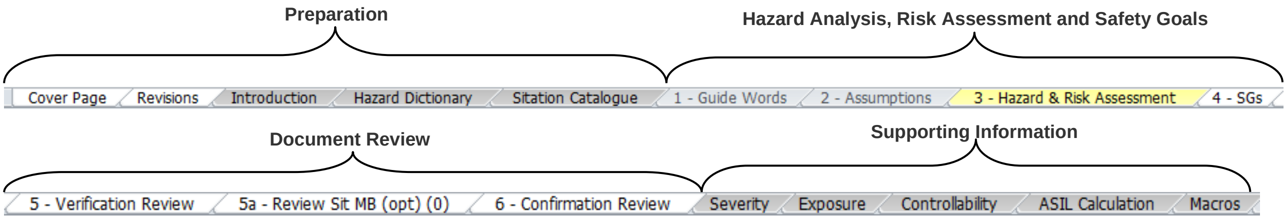


Figure 7: Template Overview

Section "Preparation"

- Cover page

  It summarizes the fundamental functional safety project information such as commodities, vehicle program and document version / owner.

- Revisions

  This Tab documents revisions of this document as well as all persons involved in the realization of hazard analysis and risk assessment.
  Note: The organizational input is described in section 2.3.2.
  Note: The version control / revisions are explained in section 1.2.

- Introduction

  This Tab contains document-specific information and references to the project documentation.

- Situation Dictionary

  This Tab supports the Situation Analysis and Hazard Identification by addressing all relevant situations.
  Note: The situations are abstracted to general categories. If a situation does not fit into a general category, contact the Domain AFSE.

Section "Hazard Analysis, Risk Assessment and Safety Goals"

- 1 - Guide Words

  This Tab contains guide words used to develop the Hazard & Risk Assessment. In this Tab the relevant malfunctioning behaviours are identified.

- 2 – Assumptions

  The intent of this Tab is to summarize and document all relevant assumptions that have been made within the Hazard Analysis and Risk Assessment. With the progress of the project the content shall be reviewed continuously and updated if necessary. A consistent documentation of the assumptions is necessary because the Tab "2 – Assumptions" is the first place to look at if item is re-used in another context.

For each assumption, the purpose shall be described. Parameters with description, preliminary limits, and units can be added if appropriate.

Assumptions documented in the Item Definition shall be documented in Tab "2 – Assumptions" and considered during the Hazard Analysis if they have impact on the Risk Assessment.
Example: e.g. vehicle not used in off-road, all vehicles equipped with ABS
Note: Assumptions on "Driver Actions" to ensure controllability (e.g., driver can override erroneous acceleration of Adaptive Cruise Control by braking) shall be included in Tab Hazard & Risk Assessment.

- 3 - Hazard & Risk Assessment

  This Tab documents the results of the Situation Analysis and Hazard Identification, the Hazard Classification, the Safety Goals and the review comments and result for each hazardous event.

.

- 4 - SGs

  This Tab documents summarizes all defined Safety Goals

Section "Document Review"

- 5 - Verification Review

  This Tab documents the execution of verification reviews and the relating results regarding appropriate completeness, identified deviations and resulting decisions or actions.

- 5a - Review MB Situations (optional)

  This optional tab supports the review for consistency and completeness of the relation between malfunctioning behaviour and situations. It can be generated by a macro.

- 6 - Confirmation Review

  This Tab documents the execution of confirmation reviews and the relating results regarding alignment to ISO 26262, identified deviations and resulting decisions or actions.

Section "Supporting Information"

- Severity

  This Tab provides an overview of the severity classification derived from the Abbreviated Injury Scale (AIS). Additionally, it contains exemplary scenarios with example severity ratings.

- Exposure

  This Tab provides an overview of the probability of exposure classification and contains exemplary scenarios with example ratings.

- Controllability

  This Tab provides an overview of the controllability classification and contains exemplary scenarios with example ratings.

- ASIL Calculation

  This Tab contains a table for the automatic ASIL calculation as a function of the selected classification of S, E, and C.

- Macros

  This Tab contains information about macros included in the Excel-template.

2.3 Preparation of Hazard Analysis and Risk Assessment

2.3.1 Timing

The HARA shall start as soon as a sufficient set of functional requirements and the document "FFSD 01.1 Item Definition" is available.[16] A feature shall have a Feature ID and be placed in the Global Feature Dictionary II prior to performing a HARA.
If a feature does not have a Feature ID (placed in the Global Feature Dictionary II), it shall be checked if the criteria defined in GFD-II Overview and Refined Feature Definition_v1.5.pptx (sharepoint.com) are fulfilled, e.g.:

- Control the transformation of customer inputs (influences on the Feature by customers, the environment, or other entities) to customer outputs (influences on the customer and on other entities such as the environment, not on other Features)
- realized by one or more components and systems
- can have variants that are engineered together (e.g., ACC + iACC)
- full input to output (end-to-end) scope

A cross-system HARA covering several features may be created (with customer outputs and dedicated properties/calibration and maybe no customer inputs) for re-using it in several features. The Hazardous Events of such a HARA shall be part of a Feature HARA
If functional requirements are incomplete or unclear the analysis needs to be adjourned until the functional requirements have been completed. The outcome of the HARA may lead to changes or extensions of the functional requirements.
All available information shall be inserted at <PS>/<TSC>. The time between <PS>/<TSC> and UNV0/UPV0 shall be used to review the existing information and adopt them according to program specific aspects. The document has to be completed at UNV0/UPV0. [17]
Note: Failing to deliver this work product will change the program status to red (Status/progress is not on track and an Approved 5D or Approved Conformance Plan is required to recover).

2.3.2 Participants / Team

The team shall include persons with a good knowledge and domain experience of the behaviour of the possible items and elements, and of the way that a vehicle and its driver can behave.

Therefore, the Hazard Analysis and Risk Assessment shall be carried out within a group of experts:

Mandatory:

- Functional Safety Experts
- System Owner
- Function Owner

If required:

- Vehicle Dynamic Experts, e.g. for Exposure or Controllability rating
- HMI Experts, e.g. for Controllability rating
- Accident Research Experts, e.g. for Severity or Exposure rating
- Medical Experts, e.g. for Severity rating
- Other Experts

The core team (with mandatory participants) and other meeting participants (with participants from “if required”-list above) shall be inserted into Tab “Revisions” with

- Name
- E-Mail
- Function / Department
- Company

[16] See ISO 26262, Part 3, 6.4.1.1
[17] The authoritative source for all milestone information is on Templates, Guidelines and Examples - FuSa Guidelines (ford.com).

- Phone

The revisions of the Hazard Analysis shall be documented in Tab “Revisions” as described section 1.2.

2.3.3 Definitions, Abbreviations/Acronyms and Document References

This information shall be documented in Tab “Introduction”.

Note: Terms already used in upstream documents can be copied into the lists of definitions, abbreviations and acronyms. MS Office automation may be used for the creation of these lists.

2.4 Realization of Hazard Analysis and Risk Assessment Document

2.4.1 Procedure: Guide Words

To support a systematic approach to identify malfunctioning behaviour, a set of system behaviours shall be prepared before performing the Hazard Analysis & Risk Assessment (the system behaviour of the system shall be taken from FFSD 01.1 Item Definition / FFSD01.10 Feature Document).

On tab “1 – Guide Words” a list of recommended guide words is given. There are eight guidewords:

- **No** - the expected system behavior is not performed at all or there is no result
- **Unintended** - the system behavior is performed, or a result is delivered when not appropriate
- **Early** - the system behavior is performed, or the result is delivered too early
- **Late** - the system behavior is performed, or the result is delivered too late
- **More** - the output/result of the system behavior is higher than intended
- **Less** - the output/result of the system behavior is lower than intended
- **Inverted** - the output/result of the system behavior is the opposite of the expected output
- **Intermittent** - while a system behavior is expected, its output toggles between the expected value and no output

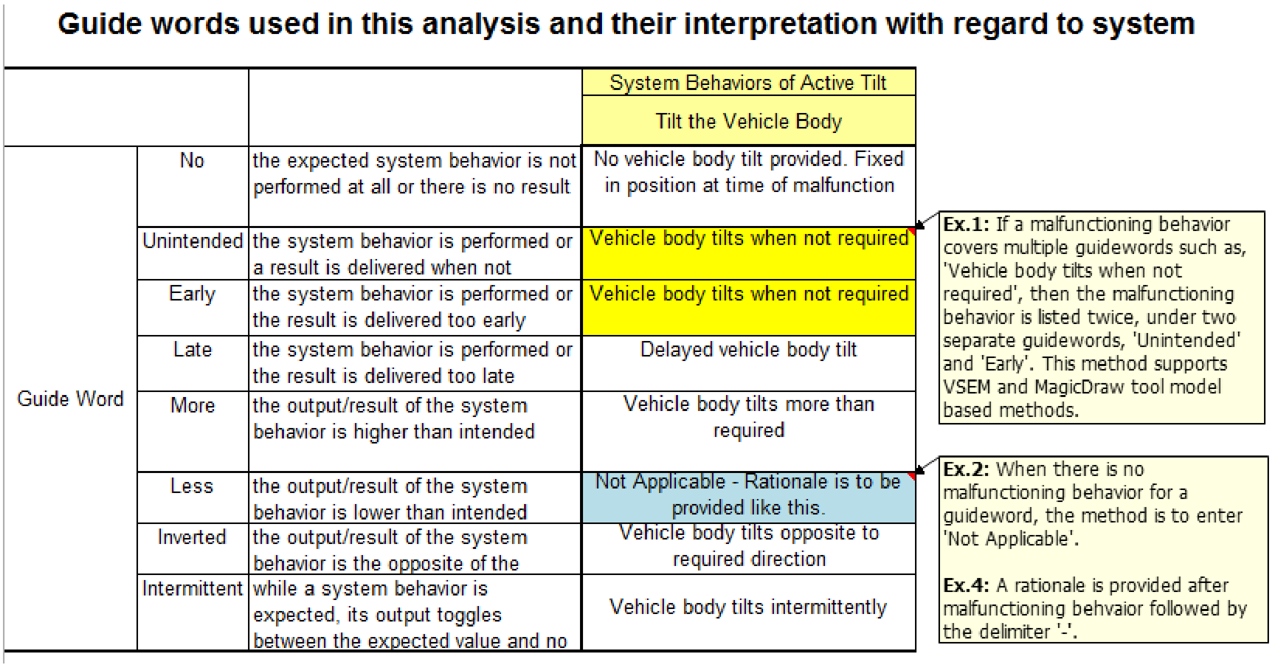
System Behaviours collected from the Item Definition or Feature Document are inputs. For each system behaviour, walk through each guideword to determine possible malfunctioning behaviours.

For each guide word, insert an explanation to describe the malfunctioning behaviour in context of the specific system behaviour.
Example: For Electrical Steering Column Lock Function, “Unintended” means that ESCL locks in situations where it is not allowed.

Insert the selected system behaviour given in the FFSD01.1 Item Definition / FFSD01.10 Feature Document. Add name and description for each system behaviour.

For each system behaviour, the guide words need to be evaluated. All guide words for a system behaviour that do not yield a malfunctioning behaviour shall be captured as "Not Applicable" (see **Ex. 2**) with a rationale in the Guide Words tab if not obvious. The delimiter (before the rationale in the same cell) has to be a “-“ (see **Ex. 4**).

It shall be also described if several guide words are combined in one Malfunctioning Behaviour. In this case, the identical guide word description shall also be inserted for these guide words. One malfunctioning behaviour may cover several guidewords. In this case, use the same malfunctioning behaviour in both the guideword/system behaviour cells. (see **Ex. 1**, and **Ex. 3**). Avoid using the terms like 'referred to' or 'covered by' for the malfunctioning behaviour.
Example: For Electrical Steering Column Lock Function, “Early”, “More” and “Intermittent” are not considered separately, because in context if the ESCL function they are sub-aspects of “Unintended”.



Guide words used in this analysis and their interpretation with regard to system

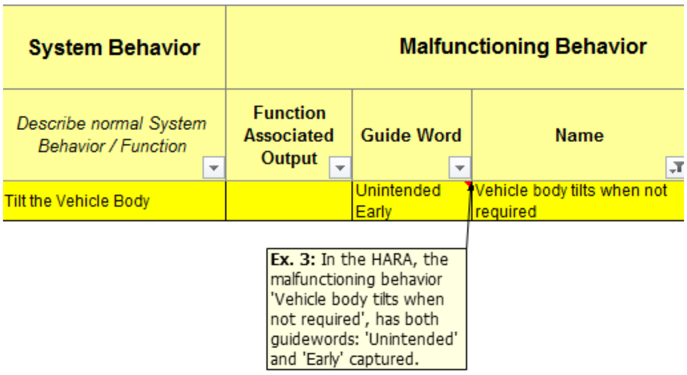
			System Behaviors of Active Tilt Tilt the Vehicle Body
Guide Word	No	the expected system behavior is not performed at all or there is no result	No vehicle body tilt provided. Fixed in position at time of malfunction
	Unintended	the system behavior is performed or a result is delivered when not	Vehicle body tilts when not required
	Early	the system behavior is performed or the result is delivered too early	Vehicle body tilts when not required
	Late	the system behavior is performed or the result is delivered too late	Delayed vehicle body tilt
	More	the output/result of the system behavior is higher than intended	Vehicle body tilts more than required
	Less	the output/result of the system behavior is lower than intended	Not Applicable - Rationale is to be provided like this.
	Inverted	the output/result of the system behavior is the opposite of the	Vehicle body tilts opposite to required direction
	Intermittent	while a system behavior is expected, its output toggles between the expected value and no	Vehicle body tilts intermittently

Ex.1: If a malfunctioning behavior covers multiple guidewords such as, 'Vehicle body tilts when not required', then the malfunctioning behavior is listed twice, under two separate guidewords, 'Unintended' and 'Early'. This method supports VSEM and MagicDraw tool model based methods.

Ex.2: When there is no malfunctioning behavior for a guideword, the method is to enter 'Not Applicable'.

Ex.4: A rationale is provided after malfunctioning behvaior followed by the delimiter '-'.

Table 11: Guide Words Tab



System Behavior	Malfunctioning Behavior		
Describe normal System Behavior / Function	Function Associated Output	Guide Word	Name
Tilt the Vehicle Body		Unintended Early	Vehicle body tilts when not required

Ex. 3: In the HARA, the malfunctioning behavior 'Vehicle body tilts when not required', has both guidewords: 'Unintended' and 'Early' captured.

Table 12: Guide Words in Tab 3

Tab “1 - Guide words” shall be inserted at <PS>/<TSC>. The document must be completed at UNV0/UPV0. [18]

2.4.2 Procedure: Assumptions

- Describe a consideration that has an Impact on Severity, Exposure, or Controllability ratings vs similar systems
- Provide clarity about related functionality, systems, or expected vehicle behaviour
- Provide a rationale for expected user behaviours

[18] The authoritative source for all milestone information is on Templates, Guidelines and Examples - FuSa Guidelines (ford.com).

- Provide clarity about expected standard design practices
- Document assumptions of functional boundaries or allocation of function relevant to the HARA

All assumptions used within the HARA must be verified for each vehicle program. The verification can be done by deriving a functional safety requirement(s) for the assumption (see in the Functional Safety Concept [FFSD03]) and verify the requirement within the functional safety V&V process (see Functional Safety Guideline chapter 2.1.5 Assumptions) or verifying the assumption in the HARA directly. It should be closed by adding a reference in the column “Reference to corresponding documentation” in Tab Assumptions

Note: If a core HARA or a HARA from an earlier program is re-used, the verification of the assumptions can be documented within the “Initiation of Lifecycle” of the item.

If all hazardous events are only QM and no Functional Safety Concept [FFSD03] is created and no other Functional Safety Document are created (also no Safety Plan), references to the corresponding documentation (e.g., owner's manual, other Hazard Analyses and Risk Assessment [FFSD02], production plan, engineering specification) shall be documented in column 'Reference to corresponding documentation' in 'Tab 2 - Assumptions'.

The procedure for documenting assumptions is as follows:

- **Ref:** A unique identifier for the feature specific assumption. This will be used in the Situation Analysis and Hazard Identification section of the HARA
- **Name:** A short description that gives a high-level overview of the assumption.
- **Category:** A general category that the assumption falls under. It can be one of the following four:
    - Behavioural – Assumptions related to human reactions, either operator, passenger or pedestrian.
    - Controllability – Assumptions related to controllability of the vehicle
    - Other Systems – Assumptions about the operation of other systems/features within a vehicle
    - Vehicle – Assumptions about vehicle design
- **Description:** A detailed description that describes the assumption.
- **Purpose:** The purpose of the assumption.
- **Reference:** Any documentation that supports the assumption

Examples of how to fill out the assumptions table in the HARA are below:

Ref	Name	Category	Description	Purpose	**Reference to corresponding documentation** (e.g., owner's manual, other Hazard Analyses & Risk Assessment [FFSD02], production plan, engineering specification) (optional if no FFSD03 is created)
A1.x	Track Safety Gear	Other Systems	Head protection in accordance with Snell SA2020 will be worn by the driver while operating on the track surface. Track will have runoff zones and impact reduction barriers specifically designed to reduce collision/impact severity.	to provide rationale for reducing high speed collision severity in some track scenarios from general purpose road/vehicle use typical severity	Feature document, summary of typical track rules
A2.x	Blind Spot Check Before Lane Change	Controllability	Driver on average expected to check in blind spots using mirrors and visual inspection prior to changing lane on multilane road.	Provide context for rating of general controllability when changing lanes	
A3.x					
A4.x					

Table 13: Assumptions example

2.4.3 Procedure: Situation Analysis and Hazard Identification

Step 1: Enter Functions

Starting with the left-hand side of the Hazard Analysis and Risk Assessment (Tab “3 – Hazard & Risk Assessment”) the main-functions of the system (from Functional Specifications and from document “FFSD 01.1 Item Definition”) shall be filled into the table.

Each system behaviour (function) shall be inserted into the first column of the table as shown in Table 14.

The system behaviour (functions) summarizes the related functionality of the system under consideration.

It is important to ensure that this step is done on the right level of detail. It shall be avoided to have a too detailed level with too many functions / sub-functions in the Hazard & Risk Assessment table to make the table accessible.

System Behavior	Malfunctioning Behavior				Effect on System Level	Scenario Description: Location	Scenario Description: Traffic & People	Scenario Description: Road Conditions	Scenario Description: Environmental Conditions	Scenario Description: Vehicle Usage	Scenario Description: Additional Details/ Example/ Remarks	Effect on Vehicle Level	Hazard	Assumptions	Hazardous Event (Risk ID)
Describe normal System Behavior / Function	Function Associated Output	Guide Word	Name	Constraints	*Describe Effect on System Level*	*Ref: see Tab "Situation Dictionary"*	*Ref: see Tab "Situation Dictionary"*	*Ref: see Tab "Situation Dictionary"*	*Ref: see Tab "Situation Dictionary"*	*Ref: see Tab "Situation Dictionary"*	*Describe the situation including details or examples of situations and additional remarks*	*Describe effect on Vehicle Level*	*Pick corresponding hazard from Hazard Dictionary*	*Ref: see Tab 2 (optional)*	*Assign a short name and risk id*
System Behavior 01: Tilt the vehicle body															
System Behavior 01: Tilt the vehicle body															
System Behavior 01: Tilt the vehicle body															

Table 14: Step 1 of the Analysis and Hazard Identification

Step 2: Identify Functional Malfunctioning Behaviours

The “Malfunctioning Behaviour” columns support the further structuring of the analysis. For each System Behaviour, the different Malfunctioning Behaviours shall be determined.[19]

Again it is important to perform this task on appropriate level. The Malfunctioning Behaviour consideration within the Hazard Analysis and Risk Assessment shall support the generation of a complete set of malfunctioning behaviours on functional level as input for the further Hazard Analysis. The task of the Malfunctioning Behaviour consideration is not a verification of an existing design – this will be done with appropriate safety analyses (FMEA, FTA…) in later steps of the Functional Safety process.

It could be helpful to start the Malfunctioning Behaviour consideration from the outputs point of view.

[19] See ISO 26262, Part 3, 7.4.2.2.3 (hazardous event)

The Hazard Analysis and Risk Assessment is a thought experiment based upon the assumption that a failure occurs in the system. This is different from a FMEA approach. The outcome is the ASIL (Automotive Safety Integrity Level), reflecting the criticality of the hazardous event and determining the minimum set of requirements to avoid random hardware failures and systematic faults.

In addition the Malfunctioning Behaviour columns enhance the search and filter functionality within the table.

System Behavior	Malfunctioning Behavior				Effect on System Level	Scenario Description: Location	Scenario Description: Traffic & People	Scenario Description: Road Conditions	Scenario Description: Environmental Conditions	Scenario Description: Vehicle Usage	Scenario Description: Additional Details/ Example/ Remarks	Effect on Vehicle Level	Hazard	Assumptions	Hazardous Event (Risk ID)
Describe normal System Behavior / Function	Function Associated Output	Guide Word	Name	Constraints *(optional)*	*Describe Effect on System Level*	*Ref: see Tab "Situation Dictionary"*	*Ref: see Tab "Situation Dictionary"*	*Ref: see Tab "Situation Dictionary"*	*Ref: see Tab "Situation Dictionary"*	*Ref: see Tab "Situation Dictionary"*	*Describe the situation including details or examples of situations and additional remarks*	*Describe effect on Vehicle Level*	*Pick corresponding hazard from Hazard Dictionary*	*Ref: see Tab 2* *(optional)*	*Assign a short name and risk id*
System Behavior 01: Tilt the vehicle body	Tilt actuator	no	No vehicle body tilt provided. Fixed in position at time of malfunction												

Table 15: Malfunctioning Behaviours

Each Malfunctioning Behaviour is characterized by the following information:

- Function Associated Output
  In this row, output of the addressed system or subsystem shall be written down.
  Example: brake pressure, powertrain torque, steering angle, steering column lock actuator
  Remark: It could be helpful to start the Malfunctioning Behaviour consideration from the actuators point of view

- Malfunctioning Behaviour Guide Word
  In this column, all guide words from tab “Guide words” shall be inserted. Multiple entries can be inserted if they have the same description.
  Remark: The Malfunctioning Behaviour analysis shall consider those cases in which the System/Feature has side effects to other systems or the driver. E.g. “ACC (Adaptive Cruise Control) inhibits driver braking”. These side effects cannot directly been assigned to a System Behaviour of the system (allow driver braking is no System Behaviour of ACC).

- Malfunctioning Behaviour Name
  A sufficient description of the Malfunctioning Behaviour shall be inserted into column “Name”. This description can be taken from the Tab “1 – Guide Words”.
  Note: In previous versions, “Malfunctioning Behaviour Constraints” could be added. The content of this attribute has to be moved to other attributes. This list provides guidance which attributes may be used and includes some examples.
  Assumptions:
  The fulfilment of other Safety Goals may be assumed for another entry in the same HARA.
  In some cases, there are constraints regarding the vehicle state in which the failure can occur $^{(\text{Examples for 1})}$ *or safety measure defined as Safety goal in this HARA is in place* $^{(\text{Examples for 2})}$.
  Note: Driver may have different expectations on the behavior of a feature depending on if a feature is activated or is not activated.
  Example for 1: Parking mode is active. Feature is only active below 12 kph because of legal limit (another line with more than 12 kph is necessary).
  Example for 1: ACC is On /ACC is Off.

Example for 2: Braking is limited to deceleration of at most 40 kph (another line with a Safety Goal covering more than 40 kph is necessary).
Example for 2: Acceleration is limited to 0.15 g (another line with a Safety Goal covering more than 0.15 g is necessary).
Example for 2: Steering angle control is available only below 12 kph (another line with a Safety Goal covering more than 12 kph is necessary).
Example for 2: Steering torque is limited to 3 Nm (another line with a Safety Goal covering more than 3 Nm is necessary)
Note: This Assumption should not be tracked in the V&V.

Effect on Vehicle Level:
If the effect of a malfunction (e.g. battery drop) causes other failures (e.g. no wiper, no ABS) they should be documented in the attribute "Effect on Vehicle Level".
If for effect of a malfunction different output value ranges should be rated (e.g., Unintended acceleration < 0.15g, Unintended acceleration > 0.15g), the ranges should also be documented in the attribute "Effect on Vehicle Level".

***Situation** (especially in "Additional Details"):*
If a failure is to be considered in only a special situation this should be documented in the Situations attributes. In this case, the appropriate situation shall be selected and "Additional Details" shall be documented.
E.g. "low speed road" + "driving at speed"

Step 3: Describe Effect on System Level

- Effect on System Level
  The column "Effect on System Level" shall describe how the system behaves in presence of the malfunctioning behaviour.

System Behavior	Malfunctioning Behavior				Effect on System Level	Scenario Description: Location	Scenario Description: Traffic & People	Scenario Description: Road Conditions	Scenario Description: Environmental Conditions	Scenario Description: Vehicle Usage	Scenario Description: Additional Details/ Example/ Remarks	Effect on Vehicle Level	Hazard	Assumptions	Hazardous Event (Risk ID)
Describe normal System Behavior / Function	Function Associated Output	Guide Word	Name	Constraints *(optional)*	*Describe Effect on System Level*	*Ref: see Tab "Situation* Dictionary"	*Ref: see Tab "Situation* Dictionary"	*Ref: see Tab "Situation* Dictionary"	*Ref: see Tab "Situation* Dictionary"	*Ref: see Tab "Situation* Dictionary"	*Describe the situation including details or examples of situations and additional remarks*	*Describe effect on Vehicle Level*	*Pick corresponding hazard from Hazard Dictionary*	*Ref: see Tab 2* *(optional)*	*Assign a name (incl. hazard and sit.) and risk id in brackets*
System Behavior 01: Tilt the vehicle body	Tilt actuator	no	No vehicle body tilt provided. Fixed in position at time of malfunction		System does not update vehicle body tilt angle when required.										

Table 16: Effect on System Level

Step 4: Identify relevant Situations

For each Malfunctioning Behaviour, all operational situations, system/operating modes, use cases and environmental conditions (solemnly or in combination) that could lead to a potential Hazard shall be identified.

Before checking the situation list, a team discussion about possible hazardous situation shall take place. The list of relevant situations from the team discussion shall be completed by checking the known situations list in the template.

Initially, the relevant situations (Location, Traffic & People, Road Conditions, Environmental Conditions, and Vehicle Usage) shall be identified and considered in the Hazard Analysis and Risk Assessment. As the analysis progresses the situations maybe revised.

The Situation Analysis shall be on appropriate level from the perspective of the driver (or other persons at risk).

For each scenario description column (Location, Traffic & People, Road Conditions, Environmental Conditions, and Vehicle Usage), relevant situations shall be documented. Permutation of different situation aspects shall be avoided, and similar situations shall be combined.

The situation columns (Location, Traffic & People, Road Conditions, Environmental Conditions, and Vehicle Usage) are combined with a logical AND. Several entries in one cell are combined with a logical OR. Any deviation of this general rule shall be documented in column "Scenario Description: Additional Details/ Example/ Remarks" (e.g. Surrounding traffic with high speed *(T 2.16)* AND no driver and passenger(s) in vehicle *(T 3.2)*). The column "Scenario Description: Additional Details/Example/Remarks" can additionally contain further details, remarks or examples of situations. The column "Scenario Description: Additional Details/Example/Remarks" can also contain details from the situation description.

System Behavior	Malfunctioning Behavior				Effect on System Level	Scenario Des-cription: Location	Scenario Des-cription: Traffic & People	Scenario Des-cription: Road Conditions	Scenario Des-cription: Environ-mental Conditions	Scenario Des-cription: Vehicle Usage	Scenario Des-cription: Additional Details/ Example/ Remarks	Effect on Vehicle Level	Hazard	Assump-tions	Hazard-ous Event (Risk ID)
Describe normal System Behavior / Function	Function Asso-ciated Output	Guide Word	Name	Con-straints *(optional)*	*Describe Effect on System Level*	*Ref: see Tab "Situation Dictionary "*	*Ref: see Tab "Situation Dictionary "*	*Ref: see Tab "Situation Dictionary "*	*Ref: see Tab "Situation Dictionary "*	*Ref: see Tab "Situation Dictionary "*	*Describe the situation including details or examples of situations and additional remarks*	*Describe effect on Vehicle Level*	*Pick corres-ponding hazard from Hazard Dic-tionary*	*Ref: see Tab 2* *(optional)*	*Assign a name (incl. hazard and sit.) and risk id in brackets*
System Behavior 01: Tilt the vehicle body	Tilt actuator	no	No vehicle body tilt provided. Fixed in position at time of malfunction		System does not update vehicle body tilt angle when required.	High speed road	Not Relevant / Any traffic	Not Relevant / Any road conditions	Not relevant / Any environment condition	Driving at speed Steering while turning	Normal driving at higher vehicle speed. **Medium** lat. acc. < TBD				

Table 17: Listing of Driving / Operating Situations

The Tab "Situations" encloses prepared tables. The Hazard Analysis team shall use the tables to identify whether a listed situation is relevant in combination with the identified Malfunctioning Behaviour.

Note: The situation list is not complete for all systems/features in general. In Tab 3Therefore it needs to be extended in case of new situations (or combinations of situations) identified. Adequate techniques are: brainstorming, checklists, p-diagrams, etc.
If new situations have been identified, they shall be added to the list and the functional safety steering team shall be informed in order to update the template.

<u>Following Steps shall be performed for each Malfunctioning Behaviour:</u>

The situation can be split into the following aspects:

- Location
- Traffic & People

- Road Conditions
- Environmental Conditions
- Vehicle Usage

For each aspect, a table exists in Tab “Situation Dictionary” and a column exists in Tab “3 - Hazard & Risk Assessment”.

The situation in which an item’s malfunctioning behaviour is able to trigger hazards shall be identified. For a systematic approach, the tables in Tab “Situation Dictionary” shall be used. If an operational situation is identified as relevant for the Malfunctioning Behaviour, the corresponding reference number shall be added in corresponding column in Tab “3 - Hazard & Risk Assessment” by selecting the appropriate term from a dropdown list.

Ref.	Location
L 1	Not relevant / Any location (L 1)
L 2	Parking (L 2)
L 3	Secondary road - city (L 3)
L 4	Secondary road - country (L 4)
L 5	Highway (freeway / autobahn) (L 5)
L 6	Off-road (L 6)
…	…

Table 18: Examples of Location

Step 5: Describe Effect on vehicle level and select Hazard

The column “Describe effect on Vehicle Level” shall contain the vehicle level effect which could occur in case of a potential item's malfunctioning behaviour.[20] In this column the vehicle level effect can be explained or illustrated.

Note: If malfunctioning behaviour induces the loss of several functions of the item, then the situation analysis and hazard identification consider the combined effects. For instance, a fault in the vehicle power supply may lead to the simultaneous loss of the functions "engine torque", "electrical power steering" and the "front lights". Loss of the functionality of a braking system (ESC) can lead to the simultaneous unavailability of driver assistance functions.

In the column “Hazard” from the Hazard Dictionary Tab from the same file, the corresponding hazard shall be selected. If the necessary hazard is not in the dictionary, contact your AFSE.

If the effect of a System Behaviour in the described situations does not lead to a hazard, the corresponding cell in the column "Hazard" shall contain "No Hazard".[21]

System Behavior	Malfunctioning Behavior				Effect on System Level	…	Scenario Description: Additional Details/ Example/ Remarks	Effect on vehicle level	Hazard	Assumptions	Hazard-ous Event (Risk ID)
Describe normal System Behavior / Function	Function Asso-ciated Output	Guide Word	Name	Con-straints *(optional)*	*Describe Effect on System Level*	…	*Describe the situation including details or examples of situations and additional remarks*	*Describe effect on Vehicle Level*	*Pick corres-ponding hazard from Hazard Dic-tionary*	*Reference: see Tab "2 - Assumptions"* *(optional)*	*Assign a name (including hazard and situation) and risk id in brackets*

[20] See ISO 26262, Part 3, 7.4.2.2
[21] See ISO 26262, Part 3, 7.4.2.2

System Behavior 01: Tilt the vehicle body	Tilt actuator	no	No vehicle body tilt provided. Fixed in position at time of malfunction		System does not update vehicle body tilt angle when required.	…	Normal driving at higher vehicle speed. **Medium** lat. acc. < TBD	*Vehicle body does not tilt. Vehicle center of gravity moves in opposite direction to the center of the curve.*	*Degraded Vehicle Stability*		

Table 19: Effect on vehicle level / Hazard

Note: The effect on vehicle level must be described regardless of leading to a hazard or not.

HAZARD DICTIONARY

The Hazard Dictionary is a tab in the HARA containing the most relevant hazards. The description of the same hazard can be different according to each case and shall be stated at Hazardous Events. The blue cells can be used until the hazard is globally aligned.

Step 6: Hazardous Event

The technical problem / concern which are a potential source of harm including the related operational condition shall be described by a row. In the column "Hazardous Event" an expressive name (including hazard and situation) and a Risk ID (in brackets) shall be documented.

Note: For features which perform only a warning of the driver (visual or acoustical), following has to be considered:
The controllability parameter describes if the driver can control a malfunctioning behaviour, not the probability of a driver failure caused by an incorrect warning. Therefore, a rating of the controllability of false positives and false negatives for such features may be not appropriate. In this case, the warning should be classified as “No Hazard” and a rationale should be provided in column “Details / Example / Remark”. This is only applicable for “standard” driver warning (e.g. warning lamp or chime), which ensure that the driver is not physically affected e.g. by glaring.

If necessary, following additional information can be documented:

- Assumptions (optional)
  Within this column, all assumptions considering the hazard or its derivation shall be entered and linked to the Tab “2 - Assumptions” where the supposition shall be written down in detail.
  ESCL-Example: Driving direction (forward / rearward) irrelevant.

System Behavior	Malfunctioning Behavior					…	Scenario Description: Additional Details/ Example/ Remarks	Effect on vehicle level	Hazard	Assumptions	Hazardous Event (Risk ID)
Describe normal System Behavior / Function	Function Asso-ciated Output	Guide Word	*Name*	Con-straints *(optional)*	*Describe Effect on System Level*	…	*Describe the situation including details or examples of situations and additional remarks*	*Describe effect on Vehicle Level*	*Pick corres-ponding hazard from Hazard Dic-tionary*	*Reference: see Tab "2 - Assumptions"* *(optional)*	*Assign a name (including hazard and situation) and risk id in brackets*
System Behavior 01: Tilt the vehicle body	Tilt actuator	no	No vehicle body tilt provided. Fixed in position at time of malfunction		System does not update vehicle body tilt angle when required.	…	Normal driving at higher vehicle speed. **Medium** lat. acc. < TBD	*Vehicle body does not tilt. Vehicle center of gravity moves in opposite direction to the center of the curve.*	*Degraded Vehicle Stability*		*No Tilt 2 - Normal driving in a curve*

Table 20: Hazardous Event

In Tab "2 – Assumptions, the assumptions are documented with details. Assumptions are used in the HARA to provide additional information about the effect a specific malfunctioning behavior will have on the vehicle level. This information is added is to help explain how certain SEC ratings and SEC rationales were determined at, or to provide more information about the specifics of an item’s operating conditions when the malfunction occurs. The (technical) assumptions are classified into following categories:

- Behavioral
- Vehicle
- Other Systems
- Controllability

Note: Only assumptions which are necessary to describe and rate the hazardous events shall be documented in the HARA. Generic assumptions about the item behavior and item context which do not affect the hazardous events shall be documented within the Item Definition or Feature Document.

Behavioural assumptions are only used to document the functionality of the item if a non-dedicated internal safety mechanism is already applied.

Note: Ford defines internal safety mechanisms to include technical solutions that include both E/E technologies and those implemented by other technologies (e.g. mechanical or hydraulic technology) which are in scope of the item's boundary diagram.
Note: A non-dedicated safety mechanism of an item includes things that are part of basic standard system design, e.g. use of the correct wire insulation.

Vehicle assumptions are only used to document if a specific vehicle design is considered in the HARA (e.g. Front Wheel Drive (FWD), Automatic Transmission, or Manual Transmission).

Other Systems assumptions are used to document assumptions on systems outside the item only for the following cases:

- if the availability of assumed functionality on other systems/sub-systems is a non-dedicated safety mechanism of the item and the assumed functionality is sufficiently independent (e.g. ESC improves the controllability). At least the following relationships shall be analysed within the V&V statement to close the assumption:
  - Usage of common actor(s) or ECU's
  - Usage of common input signals
  - Common cause and cascading failures of the power supply

  Note: Availability does not require that the assumed functionality cannot be deactivated by driver, but the function shall be on by default at each vehicle start-up event. In other words, it shall not be assumed functionality that can be deactivated permanently. If the driver can temporarily deactivate an assumed functionality, the HARA shall analyse the malfunctioning behaviour with and without the assumed functionality. It is expected that the exposure rating would be lower for cases where the functionality is temporarily disabled (e.g. ESC disabled by driver would have a low exposure). In addition, the driver shall be able to recognize when the assumed functionality fails, e.g. warning lamp switched on within cluster.

- if a non-dedicated external safety mechanism (outside the Item's boundary diagram) is already applied
  Note: Example of a non-dedicated external safety mechanism includes use of fire retardant material for the firewall in an engine bay.

- if an external (outside the Item's boundary diagram) safety mechanism of E/E technologies was implemented to align with ISO 26262 and the safety mechanism fulfils at least the required ASIL if the hazardous event is analysed without the safety mechanism.
  Note: This method can be applied to determine the residual risk, if a dedicated external safety measure already reduces the risk of malfunction behaviour, e.g. steering torque limitation improves the controllability to "C1" controllable level.

The category "Controllability" can be used to add additional information to the SEC rationales or to assume on an action of the driver or other persons to ensure the controllability. These assumptions can include already existing information of costumer clinics (e.g. controllability tests) or real world data (e.g. EuroFOT[22] data).

[22] European Large Scale Field Operational Test

2.4.4 Procedure: Hazard Classification

The objective of the hazard classification is to assess the level of risk reduction required for the hazards.[23]

The following steps need to be performed:

1. Estimation of potential severity
2. Estimation of the probability of exposure
3. Estimation of controllability

Scenario Description: Additional Details/ Example/ Remarks	Effect on vehicle level	…	Hazardous Event (Risk ID)	S	Severity	E	Exposure	C	Controllability	ASIL
Describe the situation including details or examples of situations and additional remarks	*Describe effect on Vehicle Level*	…	*Assign a name (including hazard and situation) and risk id in brackets*	Category	Rationale *(description of reasonable expected consequences, if not obvious)*	Category	Rationale *(including description of accident trigger, if not obvious)*	Category	Rationale *(including action to avoid harm)*	
Normal driving at higher vehicle speed. **Medium** lat. acc. < TBD	*Vehicle body does not tilt. Vehicle center of gravity moves in opposite direction to the center of the curve.*	…	*Vehicle not steerable at high speed*	*S 3*	*Potential collision with obstacles at high speed*	*E3*	*Driving at high speed (E4), lower probability of medium lateral acceleration (E3), medium probability.* *Frequency rated, because pre-existing failure leads to hazardous event in case of next turning with high lat. acc.*	*C2*	*Driving at high speed (E4), lower probability of medium lateral acceleration (E3), medium probablity.* *Frequency rated, because pre-exisiting failure leads to hazardous event in case of next turning with high lat. acc.*	B

Table 21: Hazard Classification

The following classification shall be specified for each hazard:

Severity[24]

Describe the potential outcome of accidents caused by the hazardous event (reasonable expected consequences). Consider reasonable sequences of events for the situation being evaluated. This is not necessarily worst case but the expected outcome. Do not put a comment about the extent of the expected injuries.

Examples:

- Potential front collision with another vehicle at high speed
- Potential side collision with another vehicle at medium speed with crossing traffic
- Potential low speed collision with a non-motorist

Note: see FFSD02, Tab Severity

Note: If different accident scenarios are identified (leading to different severity ratings), it shall be reconsidered to split the hazard (separate rows for each hazard).

Estimate the severity of potential harm for each hazardous event and assign appropriate severity rating S0, S1, S2 or S3 in column “S” in accordance with Tab "Severity". If “No hazard” is identified, select either S0 or C0 and provide a detailed rationale on why there is no hazard. If C0 is selected when “No hazard” is identified, Severity should be either S0 or "blank".

If a hazard is identified, severity shall be assessed by considering the possible harm to each endangered person – including the driver or the passengers of the vehicle causing the hazardous event, and other endangered persons such as cyclists, pedestrians or occupants of other vehicles. Select S1, S2 or S3 and provide a rationale for the estimated severity.

[23] See ISO 26262, Part 3, 7.4.3

[24] See ISO 26262, Part 3, 7.4.3.2

Exposure[25]

Estimate the probability of exposure of each operational situation by considering the content of the columns "Scenario Description".

The following structure can be used for the rationale: “<Driving Location> (E#); lower probability of <being in situation> (E#), <Description>”. Examples are:

- Secondary road (E4); lower probability of passing (E2), low probability
- Intersection (E4); lower probability of being required to get out of the way of other vehicle (E2), low probability
- Freeway at speed (E4), high probability

Note: see FFSD02, Tab Exposure

If a specific/dedicated initiator or enabler needs to be present, in combination with the malfunctioning behaviour of the system, to lead to a potential accident it shall be documented in column "Exposure".

Example: A failure of the brake system and a preceding vehicle could lead to a rear-end collision with the preceding vehicle. Here, the preceding vehicle is the accident trigger for this dedicated accident.

Estimate the probability of exposure of each operational situation. Consider the content from columns "Driving Situation", "Operating Mode / Environmental Condition", "Details / Example / Remark", and "Accident Trigger".

It is not worst-case exposure for a single market or vehicle but the exposure over total market for the vehicle line under consideration. Hence, the exposure rating shall be adjusted accordingly.

Example: For vehicles equipped with a tow-bar, the exposure for towing is significantly higher as for the total market.

Note: The number of vehicles equipped with the item shall not be considered when estimating the probability of exposure.

Note: The hazard analysis and risk assessment is performed assuming all vehicles are equipped with the item. This means that the argument "the probability of exposure can be reduced, because the item is not present in every vehicle (as only some vehicles are equipped with the item)" is not valid.

Estimate the probability of exposure of each operational situation and assign the appropriate exposure rating E0, E1, E2, E3 and E4 in accordance with Tab "Exposure". Select the rating for the Exposure in column "E".

1. If “No hazard” is identified, no Exposure rating is necessary, and it may be "blank".
2. If a hazard is identified, select E0, E1, E2, E3 or E4 and provide a rationale for the estimated exposure. It is recommended to avoid listing hazardous events rated E0 in the HARA.

For a common format of the rational consider the explanation in the template, Tab “Exposure”.

Controllability[26]

Provide a rationale for the estimated controllability. The following structure can be used for the rationale: “(All/Almost all/Most/Few) drivers (or other traffic participants) are usually able to avoid the hazard by <actions>, <Description>”. Examples are:

- Almost all drivers will avoid collision by steering back to the vehicle's lane and braking, or oncoming vehicles will be able to manoeuvre out of the way, simply controllable
- Most drivers will detect the vehicle movement and take action by braking and steering prior to collision, normally controllable
- Few drivers or other vehicles are usually able avoid a collision in situations requiring acceleration to achieve safety when no alternate action is possible, difficult to control or uncontrollable

Note: see FFSD02, Tab Controllability

Describe the possibilities of the driver or other endangered persons able to gain control of the hazardous event in order to avoid the specific harm.

It is not worst-case controllability by a driver or other traffic participants but the controllability over

[25] See ISO 26262, Part 3, 7.4.3.4
[26] See ISO 26262, Part 3, 7.4.3.7

total market for the vehicle line under consideration.

Note: It is assumed that the driver is in an appropriate condition to drive with respect to the general population (for example not exhausted), has the appropriate driver training (has a driver's license) and is complying with legal regulations.
Note: It is not the aim of a hazard analysis to investigate the misuse. However, for the malfunctioning behaviours of the system, investigated in the hazard analysis, the impact of reasonably foreseeable misuse has to be considered, e.g. "not keeping the required distance to the vehicle in front" as a common behaviour.
.

If in the rationale is any (implicit) assumptions about the controllability (e.g., the driver will oversteer an unintended behaviour), an explicit assumption (see Section 2.4.2) shall be defined and referenced. [27]

Estimate the controllability of each hazardous event and assign appropriate controllability class C0, C1, C2 and C3 in accordance with Tab "Controllability".

1. If "No hazard" is identified, select either C0 or S0 and provide a detailed rationale on why there is no hazard. If S0 is selected when "No hazard" is identified, controllability should be either C0 or "blank".
2. If a hazard is identified, select C1, C2 or C3 and provide a rationale for the estimated controllability.

For a common format of the rational consider the explanation in the template, Tab "Controllability".

ASIL[28]

Based on the classification of S, E and C, the ASIL determination is done automatically by the tools (i.e., Excel formulas, VSEM, MagicDraw plugin).

Note: When inserting a new row in the Excel-Template, be aware to copy the formulas in column "ASIL" from the preceding row.

[27] See ISO 26262, Part 3, 7.4.2.7 and 7.4.2.3
[28] See ISO 26262, Part 3, 7.4.4.1

2.4.5 Procedure: Estimating the Hazard Manifestation Time

With each Hazardous Event now assigned an ASIL we can begin assessing the Hazard Manifestation Time (HMT). Before beginning it is important to first review the Hazardous Events (HEs) necessary to understand the timing constraints of the system. In previous steps HEs were created in an attempt to capture the worst-case S, E and C ratings. In this step we instead try to capture the HEs that reflect the worst-case scenario HMT time (with shorter times being worse). If the existing HEs already capture the worst-case HMT, then no further HEs are needed. For the purposes of determining which HEs are important to consider it's necessary to still determine the S, E and C ratings of each newly created HE. Having done this, we can exclude all blank or QM rated HEs from consideration, even if they represent the worst-case HMT, since the risk they pose is acceptable without additional intervention.

Once all the HEs are created and rated, the next step is to assess each situation to establish an HMT value. Normally this would be a difficult task to complete without knowing the details of the vehicle/platform for the technology. However, at this stage in the development process the only thing that is required is an estimate in the form of a range of time. To help with this the HMT estimate cells are drop down menus that provide a set of ranges to choose from.

Aside from the HMT Estimate there is a column for stating a Rationale. Use this column to capture the arguments and reasoning used to determine the HMT Estimate. Possible Rationales include references to papers, a description of the point where the Hazard occurs, or elaborations of the driving scenario, physics or expected driver behaviour.

When trying to determine an Estimated Hazard Manifestation Time, the following things should be considered:

- It is not meant to be an exact time. It is based on an engineering judgement of the functionality of the feature. This can include knowledge the timing of Hazard Manifestation Times for similar hazardous events in other features.
- Determining this time is not expected to require rigorous analysis. Testing is not required to determine the Estimated HMT.
- A literature review/assessment can be done if it is difficult to determine an appropriate Estimated HMT, but it is not required.
- When more than one Estimated HMT is possible, choose the more conservative value.
- If a worst-case timing scenario that is not already captured in a Hazardous Event is determined during the HARA development, add it to the HARA and determine its S, E and C. If the Hazardous Event is ASIL rated A-D, determine its Estimated HMT.

After the HMT estimates are completed for each ASIL rated HE, we can start developing the Safety Goals.

2.4.6 Procedure: Definition of Safety Goals

A safety goal is a high-level safety requirement based on the hazards identified in the HARA.[29]

The following rules apply to safety goals:

- The safety goals shall be clear and precise.
- The safety goals shall not contain technical details.
- The safety goals shall be such that they can be implemented by technical means (e.g. avoid referring to non-measurable data)
- Each safety goal shall have a unique identifier: **SG XX**
- Each safety goal shall have a name that describes the goal.
- One Safety Goal shall be defined for each hazardous event rated as ASIL A, B, C or D in the hazard analysis.

  For hazardous events rated as QM, a safety goal can be derived (optionally). If no safety goal is defined, the hazard needs to be either considered in the FMEA or a requirement has to be defined. It is the responsibility of the Functional Safety Engineer to notify the Feature Owner of all the QM rated hazardous events. This will allow the Feature Owner to update any documentation to account for new requirements.
- One safety goal can be assigned to several hazards.
- Having too many safety goals should be avoided by having the details in the Functional/Technical Safety Concept.

The Safety shall be defined in Tab “05 - SGs" with an ID, a name, a detailed text / description, a rationale, the ASIL, and a status.

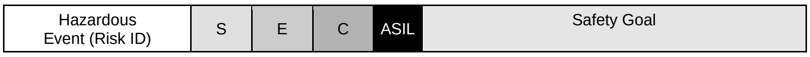
The highest ASIL of the addressed hazard will be the hazard of the Safety Goal and shall be inserted into the column “ASIL” in Tab “5 - SGs". This can be done manually of by using the template macro. The status is an attribute defined by an engineering team to track status (“In-Progress”, “Ready for Review”, “Approved”, or “Rejected”). Requirement development teams can use the ‘Requirement Status’ field to manage maturation of requirements. The ‘Requirement Status’ field does not necessarily indicate that a cascaded requirement is reconciled by an affected activity for implementation.

Status	Definition
In-Progress	Currently developing requirement, requirement is Work-In-Progress (WIP).
Ready for Review	Requirement is developed, and is ready for team review.
Approved	Requirement was review and agreed upon by the working team.
Rejected	Requirement was reviewed but not approved for implementation.

Table 22: Status Definition

Recommend process for the development team to track the safety requirement’s status: The development team may adjust the process for tracking safety requirement status, based on current teams’ processes, and needs.

In Tab “3 - Hazard & Risk Assessment”, column “ID SGxx”, the Safety Goal ID has to be inserted. The Safety Goal name is automatically filled out.



Hazardous Event (Risk ID)	S	E	C	ASIL	Safety Goal

[29] See ISO 26262, Part 3, 7.4.4.3, 7.4.4.4 and 7.4.4.5

Assign a short name and risk id	Category	Category	Category		ID SGxx	Name
HE001: Vehicle not steerable at high speed	S3	E4	C3	D	SG 01	*Locking of the steering column when vehicle is moving with high speed shall be prevented*

Table 23: Safety Goals

2.4.7 Procedure: Handling of Safety Goals

For all Hazardous events rated ASIL A/B/C/D, a Safety Goals shall be defined, and Functional Safety Requirements shall be derived in the Functional Safety Concept [FFSD03].

Hazardous events rated as QM will be covered by the FMA process. It is required in the FMA process to check all relevant HARAs for Hazards to be addressed. The Functional Safety engineer is responsible to notify the Functional Safety engineer of all QM rated hazardous events identified in the HARA. In the review comment can be noted that the Functional Safety engineer is informed.

If a QM safety goal described on a level that it cannot be directly implemented, the engineering specification shall document the implementation concept including the derived requirements.

Note: Reasons may exist to cover a Safety Goal rated as QM in the Functional Safety Concept [FFSD03]. This proceeding is allowed if a rationale exists.

2.4.8 Residual Risk Assessment

The residual Risk is the remaining risk after a safety mechanism has been applied. According ISO 26262 Part 1 is a safety mechanism a “technical solution implemented by E/E functions or elements (1.32), or by other technologies (1.84), to detect faults (1.42) or control failures (1.39) in order to achieve or maintain a safe state (1.102)”. Such a safety mechanism can be a limitation device that improves e.g. the controllability or a monitoring device that ensures the operation of the system only within specific situations (e.g. reduces the exposure). There might be also additional kinds of other safety mechanisms that mitigates the risk but does not ensure a Safety Goal without additional safety measures.

The goal of safety mechanisms is usually to reduce the risk to an acceptable level. However, it might be useful to define cascading safety architectures where the risk of potential malfunctions is stepwise mitigated to an acceptable level. In this case, the residual risk analysis can be done to identify the effectiveness of the first order safety measure and to identify the necessary safety integrity (ASIL) for the additional safety measure(s).

After analysing all system behaviours of the item without any safety measure (within system boundary) and the creation of corresponding Safety Goals, in the Functional Safety Concept, safety mechanisms will be developed to fulfil the Safety Goal(s). For safety measures that mitigate a hazard, but do not prevent the hazard completely, it is useful to analyse the effectiveness of the safety mechanism by analysing the residual risk of the malfunction behaviour considering the safety mechanism in place[30].
This can be done within the HARA, or by using similar techniques as in the HARA. It can also be done in the Functional Safety Concept.
In case the safety mechanism realized in a platform system / base system:

- Create in the feature HARA references to Hazardous Events a platform system / base system (associated to the used Safety Goal)

  Note: It is sufficient to reference the Hazardous Events associated to the used Safety Goal

- For MagicDraw, the referencing mechanism should be used (only read access for feature using these Hazardous Events, latest version will be shown and exported)

In the Excel-based approach:

- the concrete version of the Base-HARA shall be inserted

[30] This is only allowed, as the safety mechanism will be implemented with the highest required ASIL.

- For Descriptions, Effect On System Level, Situations/Operating modes, Effect On Vehicle Level, SEC rationales, a reference to the Base-HARA can be inserted
- The cells for SEC rating shall contain the rating for highest ASIL of all referenced Hazardous Events
- All Risk-IDs for used Safety Goal(s) being relevant for the feature shall be referenced
- In the referenced Safety Goal(s), it should be stated which team realizes these Safety Goal(s) (with FSC, SRS, Safety V&V, Safety Case …)

When a Safety Goal and the corresponding Hazardous Events are referenced, following documents of the platform system / base system shall be checked for modifications (also for each re-application, see FFSD01.2, checking for relevance for feature):

- FFSD02 HARA (of platform system / base system)
- FFSD03 FSC (of platform system / base system)
- FFSD08 Safety V&V Report (of platform system / base system)
- FFSD09 Safety Case (of platform system / base system)

A reference to these documents shall be added to the VSEM folder of the feature.

In case of feature with an ASIL in the other lines (leading to FSDs for this feature), the base documents shall include references to these documents.

For example, a malfunctioning behaviour that is rated S3/E4/C3 (ASIL D) without safety mechanism. The controllability will be improved by a safety mechanism (e.g. a limitation device) which reduces the controllability rating to C1. In this case, the residual risk (S3/E4/C1) would be ASIL B. Therefore, another safety mechanism needs to be developed to bring the residual risk to an acceptable level or the item (or at least a part of the item) needs to be implemented according to the residual ASIL. In this example, the implementation of the safety mechanism (limitation device) with ASIL D, allows the implementation of the item according ASIL B instead of ASIL D. This ASIL cascade as shown in Figure 8 might reduce the implementation effort. Is the safety mechanism more effective, such that the residual risk is on an acceptable level (S3/E4/C0), the item can be also implemented with QM measures.
Note: the effectiveness of the safety mechanism might be driven by performance.

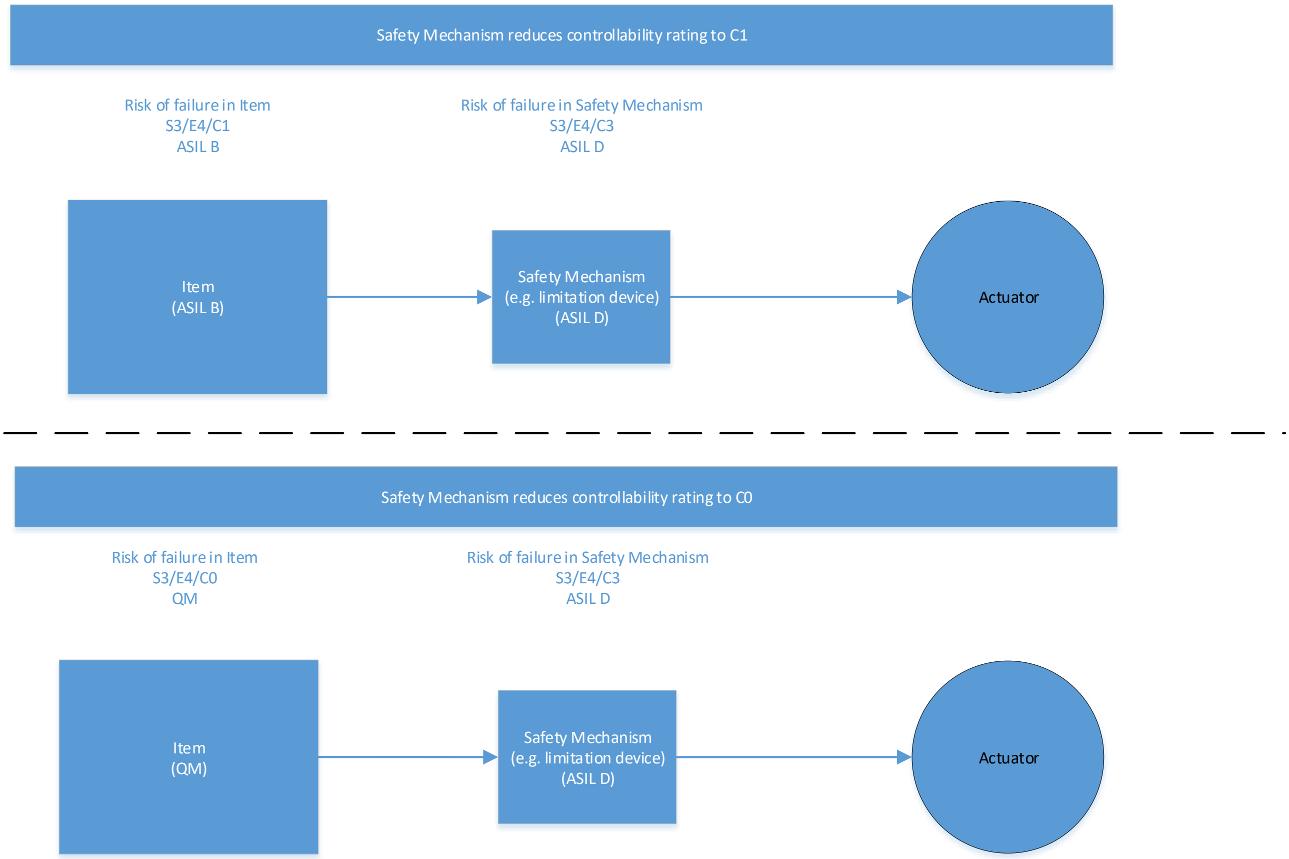


Figure 8: Residual Risk Assessment example

2.4.9 Execution and Results of Verification Review

2.4.9.1 Verification Review

To check the Hazard Analysis and Risk Assessment, a Verification Review shall be performed.

HARA Verification Reviews are performed in order to evaluate the completeness and correctness of the HARA[31]. The verification review shall be performed after the working team has finished the HARA and shall be performed prior to the confirmation review.

The verification review shall be performed by the working team responsible for creating the HARA with support from the AFSE (Application Functional Safety Engineer) in the team's respective organization. For example, if the project is in the Powertrain domain, the team would invite the Powertrain AFSE to the verification review according to the table provided below.

The AFSE will provide ISO 26262 functional safety guidance while evaluating the system behaviours, malfunctioning behaviours, hazardous events, and ASIL determinations contained within the HARA. The AFSE will also provide guidance when completing the checklist in tab "5 - Verification Review" of the HARA.

Prior to the verification review meeting, please provide the Item Definition / Feature Document and HARA to your AFSE. For example, if you are having a verification review for a HARA, provide your AFSE with the Item Definition and HARA about a week prior to the review.

The verification review shall be done

- persons different from the document owner, or
- by the whole team working on the document (if the team consists of at least 3 persons).

The person responsible for the verification review shall

- have had a ISO 26262 training,
- be a domain expert, such as someone from the working team or technical experts on the technology.

When the HARA is aligned with the supplier's HARA, it shall be checked if Safety Goals from different HARAs rely on correct functionality of the supplier's element/component/subsystem."

The review results shall be inserted into the document.

The following Figure 9 depicts the overall process of verification and confirmation review. As can be seen, it is important to maintain accurate version control of the HARA document to capture, which version of the HARA has been reviewed by which reviewer. This is especially the case if the document undergoes multiple edits and rounds of reviews. Note that if the confirmation review requires major changes to the HARA (e.g., new hazardous events, modified ASIL ratings), another verification review shall be performed.
Upon completion of verification and confirmation reviews the reviewed HARA shall be uploaded to VSEM as VDOC. It is recommended to initiate a VSEM workflow to capture final review decisions by all reviewers.

[31] ISO 26262, Part 3, 8.4.5

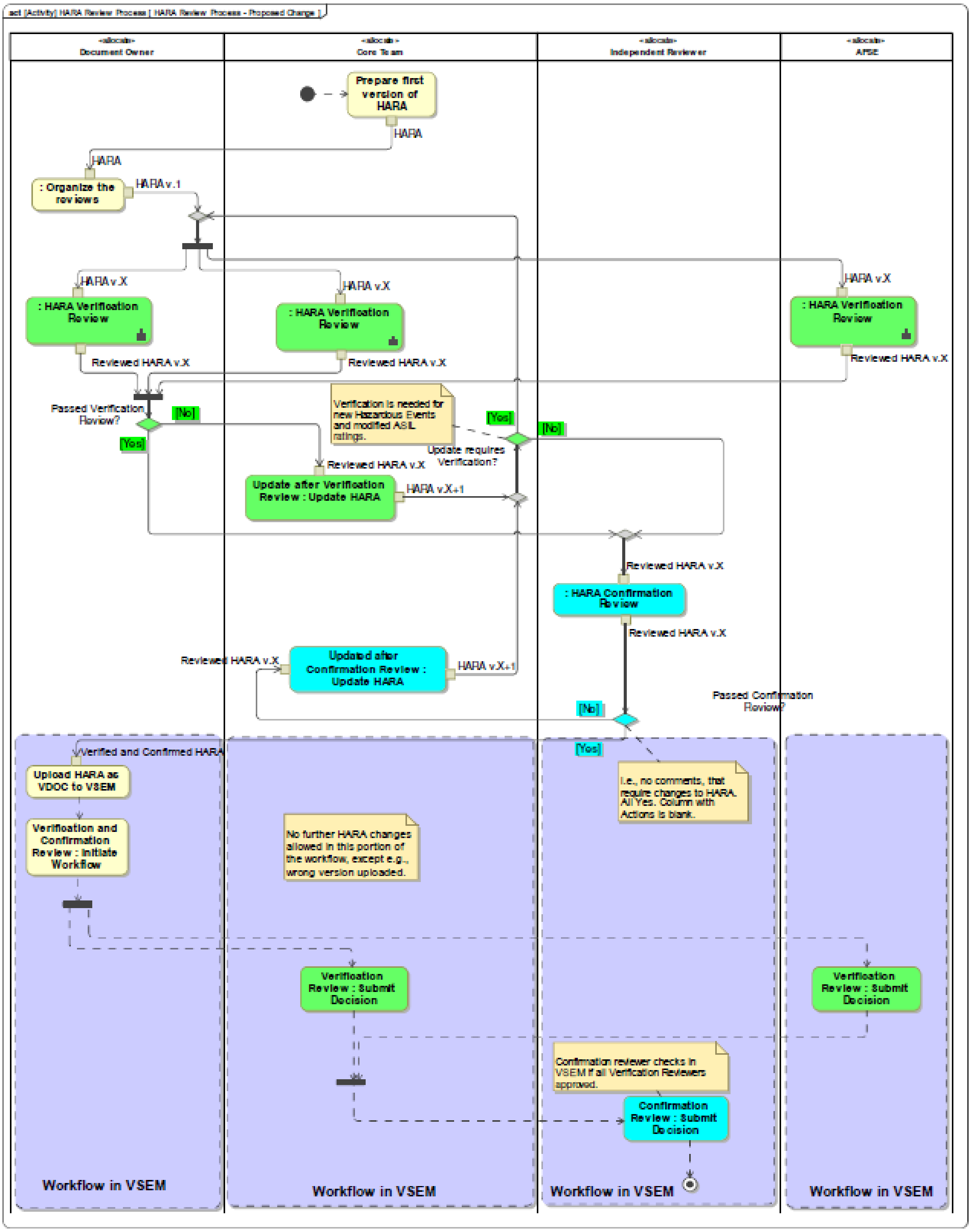

act [Activity] HARA Review Process [HARA Review Process - Proposed Change]
«allocate»
Document Owner
«allocate»
Core Team
«allocate»
Independent Reviewer
«allocate»
APSE
Prepare first version of HARA
HARA
HARA
: Organize the reviews
HARA v.1
HARA v.X
: HARA Verification Review
HARA v.X
: HARA Verification Review
HARA v.X
: HARA Verification Review
Reviewed HARA v.X
Reviewed HARA v.X
Reviewed HARA v.X
Verification is needed for new Hazardous Events and modified ASIL ratings.
Passed Verification Review?
[No]
[Yes]
[Yes]
[No]
Update requires Verification?
Reviewed HARA v.X
Update after Verification Review : Update HARA
HARA v.X+1
Reviewed HARA v.X
: HARA Confirmation Review
Reviewed HARA v.X
Reviewed HARA v.X
Updated after Confirmation Review : Update HARA
HARA v.X+1
Passed Confirmation Review?
[No]
[Yes]
Verified and Confirmed HARA
Upload HARA as VDOC to VSEM
Verification and Confirmation Review : Initiate Workflow
No further HARA changes allowed in this portion of the workflow, except e.g., wrong version uploaded.
I.e., no comments, that require changes to HARA. All Yes. Column with Actions is blank.
Verification Review : Submit Decision
Verification Review : Submit Decision
Confirmation reviewer checks in VSEM if all Verification Reviewers approved.
Confirmation Review : Submit Decision
Workflow in VSEM
Workflow in VSEM
Workflow in VSEM
Workflow in VSEM

Figure 9: HARA Review Process

2.4.9.2 Review in Tab "3 - Hazard & Risk Assessment"

For each row in Tab "3 - Hazard & Risk Assessment", the consistency of the safety goals with related hazard analyses and risk assessments shall be checked.

S	E	C	ASIL	Safety Goal			Verification Review Comment (optional)	Review Status (optional)	Actions	Reference to Open concerns/ Action items
Category	Category	Category		ID SGxx	Text	Name		Not Reviewed / In Progress / Completed		
S3	E4	C3	D	SG 01	*Locking of the steering column when vehicle is moving with high speed shall be prevented*	*Locking of the steering column when vehicle is moving with high speed shall be prevented*	*Is value for exposure OK?*		*E has to be validated by N.N.*	*43*

Table 24: Verification Review, Actions, and Reference to Open concerns / Action items

The review results should be inserted into the column "Verification Review Result Text" of Tab "3 - Hazard & Risk Assessment". If multiple reviewers provide comments for a given hazardous event, the reviewers' names and comments shall be inserted as multiple lines of the same cell. For short HARAs and in case of no remarks, only the Column "Review Status" can be used.

The status should be tracked in column "Review Status". It can be "Not Reviewed", "In Progress" or "Completed".

If the result is not OK, document necessary action items in column "Actions" and insert a reference into column "Reference to Open concerns/ Action items". As soon as an action is completed, both entries shall be removed and the corresponding cells shall be empty.

If additional reviews are needed, in the existing cell a new entry with a new date shall be added.

2.4.9.3 Review in Tab "5 - Verification Review"

In addition, the hazard analysis and risk assessment and including the safety goals shall be reviewed to provide evidence for appropriate selection with regard to operational situations and hazard, alignment with the item definition and consistency with related hazard analyses and risk assessments of other items.[32]

The document owner shall insert persons needed for the reviews of the document, the dates of review completion and the reviewed versions of the document into the table 1 in Tab "5- Verification Review ".

Multiple people may be listed in a single row if they complete the review at the same day and based on the same version.

The following aspects shall be checked during the review.

Completed according to Guidelines?		**Yes / No**
Hazard Analysis - Team	Did the team working on the HARA include AFSE participation throughout development of the HARA, from each relevant domain in the analysis, so that they can help ensure ratings are consistent across the domains?	
Hazard Analysis - Complete	Are all of the tabs (Cover Page, Revisions, Introduction, Guide Words, Assumptions, HARA, and SGs) filled out and complete?	
Hazard Analysis - Situations	Are all of the situations used in the HARA part of the Ford Situation Dictionary? For any situations created specifically for this project, was there something unique about this item that warranted creating a new situation? Did any new situation go through the proper situation approval process?	

[32] See ISO 26262, Part 3, 7.4.5.1

Hazard Analysis - Hazards	Are all of the hazards used in the HARA part of the Ford Hazard Dictionary? For any hazards created specifically for this project, was there something unique about this item that warranted creating a new hazard? Did any new hazard go through the proper hazard approval process?	
Hazard Analysis - Guide Words	All in-scope functionality in the Item Definition is considered and malfunctioning behaviour (failure mode) consideration is sound.	
	Guidewords are appropriately defined according to the system behavior of the item	
Hazard Analysis - Assumptions	Assumptions listed in Tab "Assumptions" are reasonable and consistent	
	If no FFSD03 FSC is created: For all assumptions, a reference is given.	
Hazard Analysis - Hazard & Risk Assessment	Lessons learned (documented in the Feature Document) or already known safety requirements (documented in the Item Definition) from previous development or related Items were considered to check the completeness of the Safety Goals and assumptions. *Note: This is not applicable, e.g., if there are no lessons learned from related Items. In these cases, insert "yes".*	
	All pertinent situations (operational situations, system/operating modes, use cases, and environmental conditions) or their combinations in which the malfunctioning behavior can lead to a hazardous event are considered. All situations are from the situation dictionary. If multiple situations are in a single cell they are treated as an AND of the situations in the cell. *Note: Tab 5a can be used to support this review activity. This tab can be used to check that for each malfunctioning behavior, all relevant situations (or their combinations) are considered, and/or for all situations (or their combinations), all relevant malfunctioning behaviors are considered.* *Note: A complete factorial of all operational situations is not required, but all of the important situations that could affect the ASIL for a hazard should be covered.*	
	Considered situations are reasonable and consistent with the item definition *Note: Tab 5a can be used to support this review activity.*	
	Hazard are identified, S, E and C classification is reasonable, based on global averages (not worst case) and consistent, ASILs are determined S, E and C classifications have been reviewed and are consistent with the ratings from the domain that has expertise in the hazard (Powertrain, EESE, Chassis, Body). For example: Unintended Acceleration hazard reviewed by Powertrain, and Unintended Self-Steer hazard reviewed by Chassis. (see column "verification review" in 3 - Hazard & Risk Assessment)	
	Severity is based on average harm and it is consistent with the Guidance for ISO 26262 HARA Assessments of SEC. Have severity ratings been reviewed by ASO when there was questions on the likely average harm?	
	All assumptions in the controllability rationale are listed in Tab 2 and referred	
	Each QM hazard has been reviewed with the Feature Owner so that it can be included in a FMEA or a requirement can be derived.	

	Safety Goals are determined • The safety goals shall be clear and precise. • The safety goals shall not contain technical details. • The safety goals shall be such that they can be implemented by technical means (e.g. avoid referring to non-measurable data)	
	The Hazardous Events are consistent among comparable items, including ASILs, to have consistent risk assessment across items in the organization *Note: The shared guidance for S, E, C parameters and SHARA should be used.*	
	The ASIL(s) are aligned with supplier. *Note: ASIL alignment is necessary only if the suppliers have made a HARA on their own* *Note: otherwise, alignment of the interfacing document is recommended; depending on the interfacing level, this may be affected Safety Goal, FSR or TSR"* *Note: The alignment can be done using the Safety Goals.* *Note: It is not necessary to align the wording and the SEC rating.* *Note: The alignment is not applicable if no supplier is selected. In these cases, insert "Yes (n/a)" and a comment in 'Review Exceptions / Deviations / Findings'.* *Note: The alignment should only be done with those suppliers with a direct interface to the feature development team* *Note: This can be checked using meeting minutes of the supplier alignment meeting.*	

Table 25: Technical Review 2, Actions, Reference to Open concerns/ Action items

During each review, the line items in the table 2 in Tab "5 – Verification Review" shall be evaluated and the status shall be documented. "Yes" shall be inserted if the corresponding part of the document is completed according to the Guidelines.
Note: If something not filled out and there is rationale why it is not filled out, the question would be answered with 'yes'. It is alternatively possible to give the justification in the section below the review table ("Review Exceptions / Deviations / Findings") instead of giving it the relevant section the document (preferred).

If "No" is inserted, exceptions, deviation or findings and resulting actions shall be described in the corresponding section.

After the last review, all review results in the table 2 in Tab "5 – Verification Review" shall be "Yes".

2.4.9.4 Review in Tab "5a - Review Sit MB (opt)"

The generation of Tab 5a is supported by a macro.
Note: The macro is not included in the files exported by VSEM/MagicDraw but the template from VSEM can be used to generate Tab 5a.

The tab can be used to check the consistency and completeness of situations and malfunctioning behaviours.

All situations and all used combinations of situations are in the column on the left hand side. In the headline, the malfunctioning behaviours are listed.
To support the review, a reference to the Safety Goal addressing the combination of malfunctioning behaviour and situation (combination) is inserted.

This tab supports the review if all relevant malfunctions are addressed for a certain situation.
In column "For this Situation or Situation combination, relevant Malfunctioning Behaviours are considered" the result of the team review shall be documented.

This tab also supports the review if all relevant situations (and their combinations) are addressed for a certain malfunctioning behaviour.
In row “For this Malfunctioning Behaviour, relevant Situations and/or their combinations are considered” the result of the team review shall be documented.

To ensure that review results are not deleted or overwritten, the macro creates a new tab with a number in braces on each execution.

2.4.10 Execution and Results of Confirmation Review

To ensure alignment to ISO 26262, a Confirmation Review shall be performed.[33]

For ASIL C and D Features, Confirmation reviews are combined with the Functional Safety Assessment Activity. Contact Functional Safety Assessment Team to perform the Confirmation Review and Ford Functional Safety Assessment.

For QM, ASIL A and ASIL B Features the normal review process with I3 Independence shall be followed.

The document owner shall insert persons needed for the confirmation review of the document, their level of independence, the dates of review completion and the reviewed versions of the document into the table 1 in Tab “6 - Confirmation Review". Multiple people may be listed in a single row if they complete the review at the same day and based on the same version.
Modified based on template change

The person responsible for the confirmation review shall

- be trained and have project experience with ISO 26262 and
- have level of independence of I3 (the confirmation measure shall be performed, by a person who reports to a separate Department Manager and was not involved in creation of the work product).

During each review, the line items in the table 2 shall be evaluated and the status shall be documented. “Yes” shall be inserted if the corresponding part of the document is completed according to ISO 26262.
Note: If something not filled out and there is rationale why it is not filled out, the question would be answered with ‘yes’. It is alternatively possible to give the justification in the section below the review table (“Review Exceptions / Deviations / Findings”) instead of giving it the relevant section the document (preferred).
If “No” is inserted, exceptions, deviation or findings shall be described and resulting actions shall be defined.

For “delta reviews”, refer to FFSG_Ford_Functional_Safety_Guideline Section 2.4.3.

Review results can be inserted into the column "Confirmation Review Results" of Tab "3 - Hazard & Risk Assessment".

[33] See ISO 26262, Part 2, 6.4.7

Appendix A

Preferred Vocabulary:

- Occupant
- Non-motorist
- Relative Speed
- Potential Collision
- Undesired
- Unintended
- Other Vehicle
- Vehicle
- Intended Path
- Divided Highway
- Secondary Road
- Parking
- Off Road
- Reduced/Degraded
- Driving Surface

Vocabulary to be avoided:

- Children
- Pedestrian
- E.g. 25 - 45 mph
- Crash
- Worst case
- Unwanted
- Passenger car
- Leave the Road
- Non-freeway road