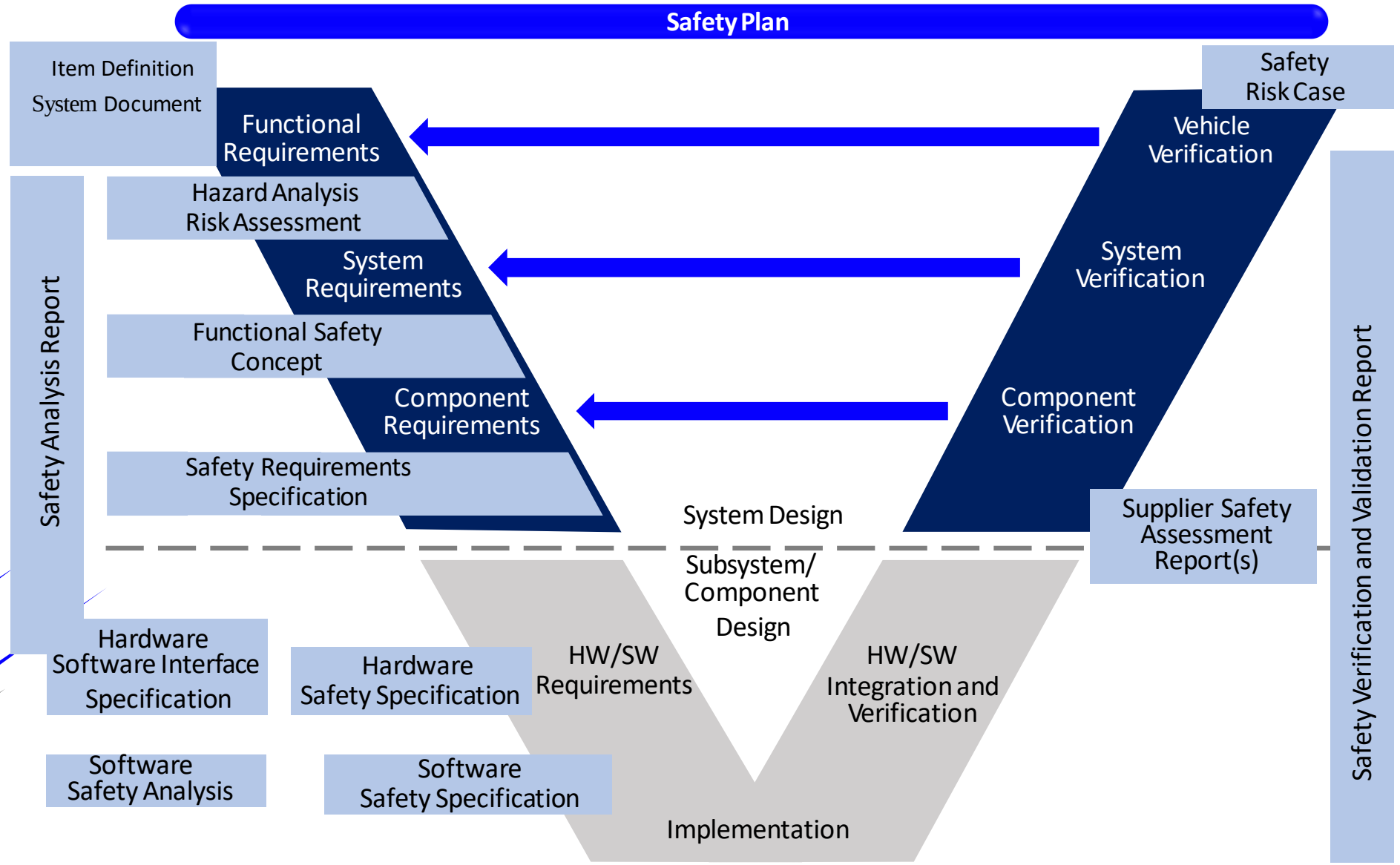
TOMCO®
SERVICE GROUP

BASICS OF HAZARD ANALYSIS RISK ASSESSMENT

Functional Safety Development Overview



Introduction: Objectives of Hazard Analysis Risk Assessment

The objective of the Hazard Analysis Risk Assessment (HARA) is:

To **identify and categorize the hazards** (at the vehicle level) that malfunctions of the item/feature can trigger

AND

To **formulate the Safety Goals** related to the prevention or mitigation of the hazardous events, in order to avoid unreasonable risk

Introduction: Safety and Risk - Contributions to a Hazard

TOMCO SERVICE GROUP

Operating modes

Environmental conditions

Correct usage, incorrect usage

Operational situations / vehicle usage scenarios

Accident Trigger

Malfunction

Situation analysis and hazard identification

Potential consequences of hazardous events

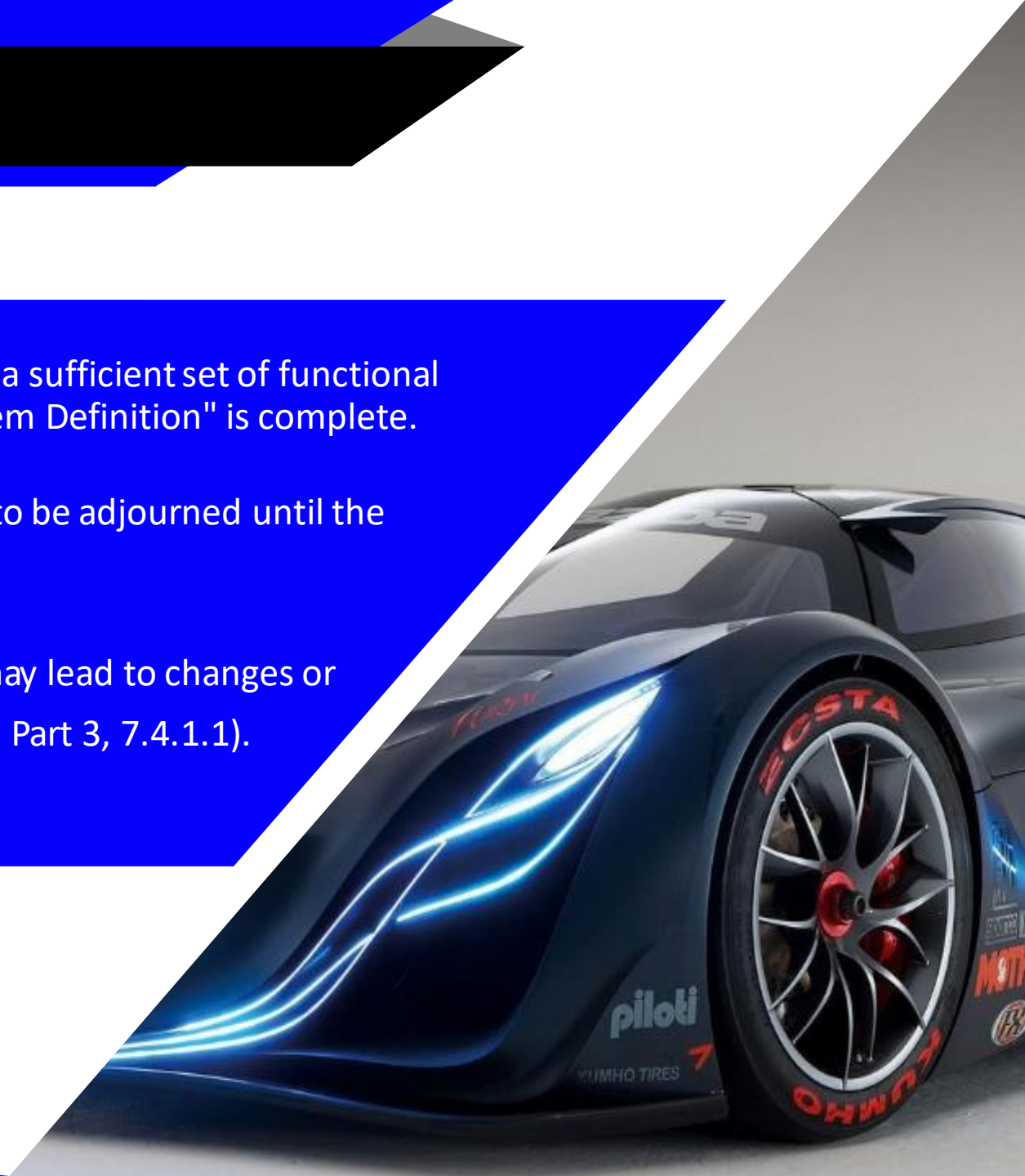
Unintended steering
No braking
More acceleration
Unintended airbag deployment

Assumptions

Timing

When should a HARA be performed?

- The Hazard Analysis Risk Assessment shall start as soon as a sufficient set of functional requirements and the document “System Document or Item Definition" is complete.
- If functional requirements are unclear the analysis needs to be adjourned until the functional requirements have been clarified.
- The outcome of the hazard analysis and risk assessment may lead to changes or extensions of the functional requirements (See ISO 26262, Part 3, 7.4.1.1).



System Document

TOMCO SERVICE GROUP

OBJECTIVES

- **Define technical content** to which ISO 26262 is applied.
- **Describe** Item / Feature, its borders, dependencies, and interaction with environment and other commodities.

ACTIVITIES

- **Feature Description:**
  - state briefly the background and the purpose of the feature
  - feature variants and corresponding regions and markets
  - legal requirements (especially laws and regulations)
- **Feature Context:** document context diagram and influences
- **Feature Modeling:** contains Use Cases, Driving Scenarios, Operating Modes and State Charts to describe the functional behavior of the feature
- **Feature Requirements:** list functional requirements and non-functional requirements of the feature, related features / elements, or the environment
- **Architecture:**
  - show the logical and/or functional boundary diagram (implementation independent) architecture
  - elements of the commodity (NOTE The elements could be also based on other technology)
  - textual description to which the feature requirements are allocated to
- **Verification & Confirmation Review:** the Feature Document requires verification and confirmation reviews

WORK PRODUCTS

- Feature Document (Toolbox: Tomco_Sys_Document_Template)

Impact Analysis

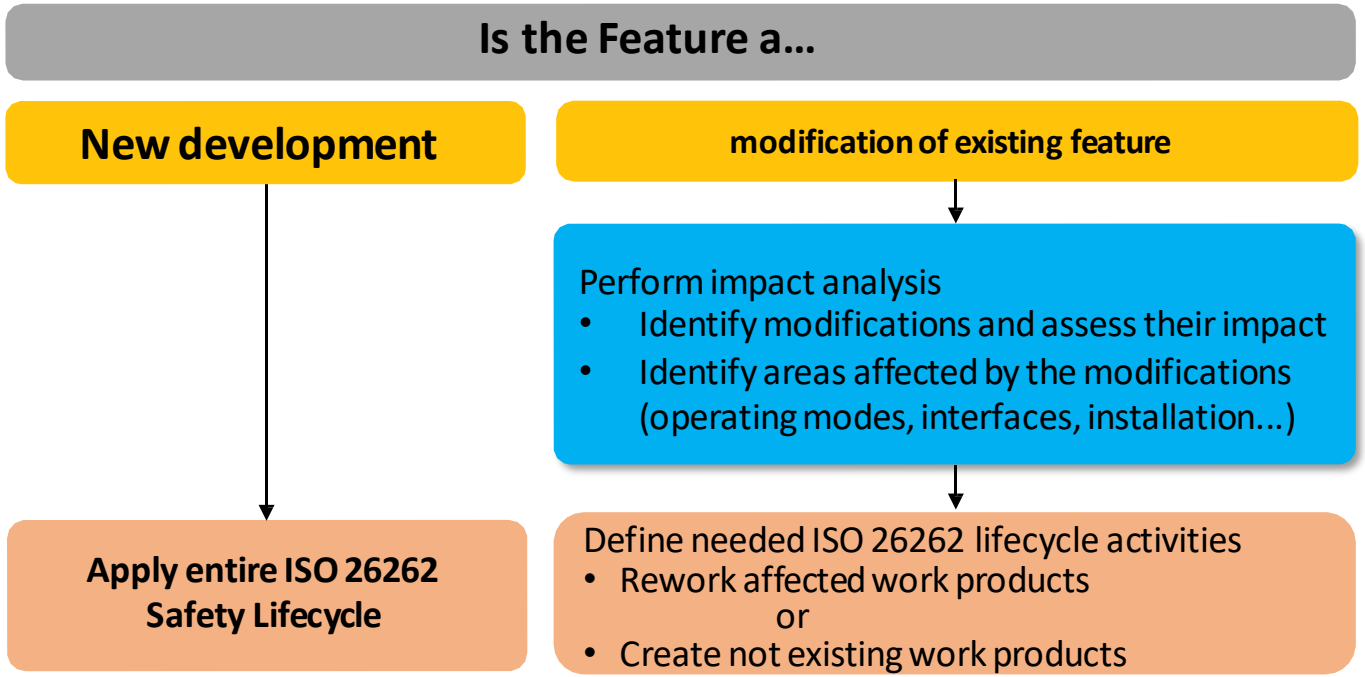
POLICY

All new features or existing features with major modifications need to undergo the functional safety process

OBJECTIVE

Make distinction between new commodity or modification to existing commodity **Define the safety lifecycle activities** in case of a modification

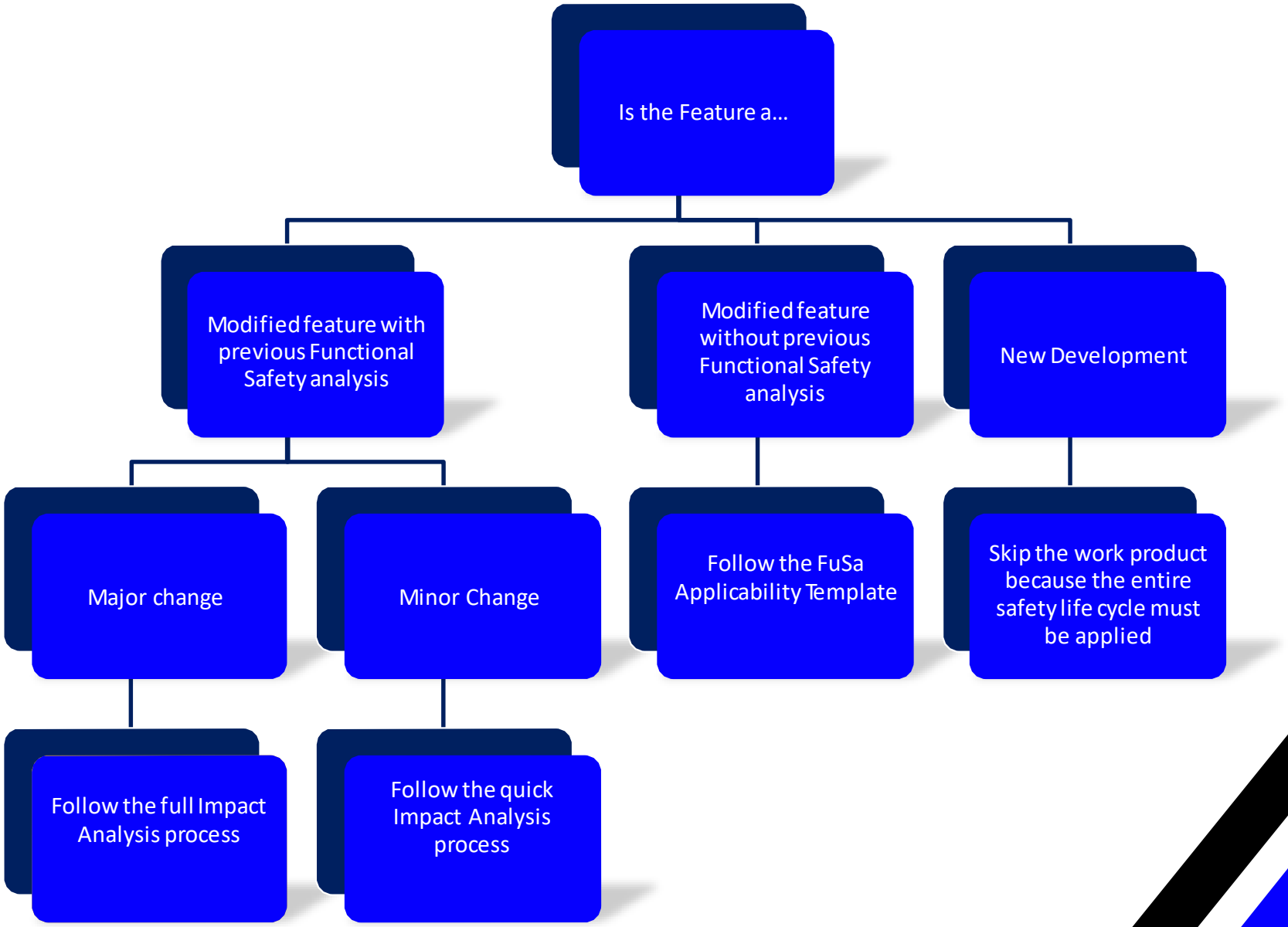
ACTIVITIES



WORK PRODUCTS

- Impact analysis – Word version (Toolbox: Tomco_ImpactAnalysis_Template)
- Impact analysis – Excel version (Toolbox: Tomco_ImpactAnalysis_Template)
- FuSa Applicability (Toolbox: Tomco_FunctionalSafetyApplicabilityTemplate)

Impact Analysis



TOMCO®
SERVICE GROUP

INPUT(S) FOR HAZARD ANALYSIS RISK ASSESSMENT

Hazard Analysis Risk Assessment (HARA)

TOMCO SERVICE GROUP

OBJECTIVES

- **Identify and categorize the hazards** caused by malfunctions of the item
- **Define Safety Goals** related to prevention or mitigation of the hazardous events

ACTIVITIES

- **Initiate the Hazard Analysis Risk Assessment**
  - Establish team with sufficient competencies
  - Use Feature Document as a base
  - Evaluate feature without any safety mechanism
- **Situation analysis and hazard identification**
  - Situation analysis
    - Describe operational situations and operating modes
  - Hazard identification
    - Describe hazards at vehicle level (“driver’s perspective”)
    - Identify consequences of hazardous events (potential impact on functions
- **Classification of hazardous events**
  - Rate Severity, Exposure, and Controllability and provide rationale
- **Determine ASIL** (measure of risk reduction needed to reduce the potential risk to an acceptable level of residual risk)
- **Define Safety Goals**
- **Perform confirmation review** by a person independent of developing department **and a verification review**

WORK PRODUCTS

- Hazard analysis and risk assessment (**Toolbox**: Tomco_HazardAnalysisAndRiskAssessment_ Template)

Definitions

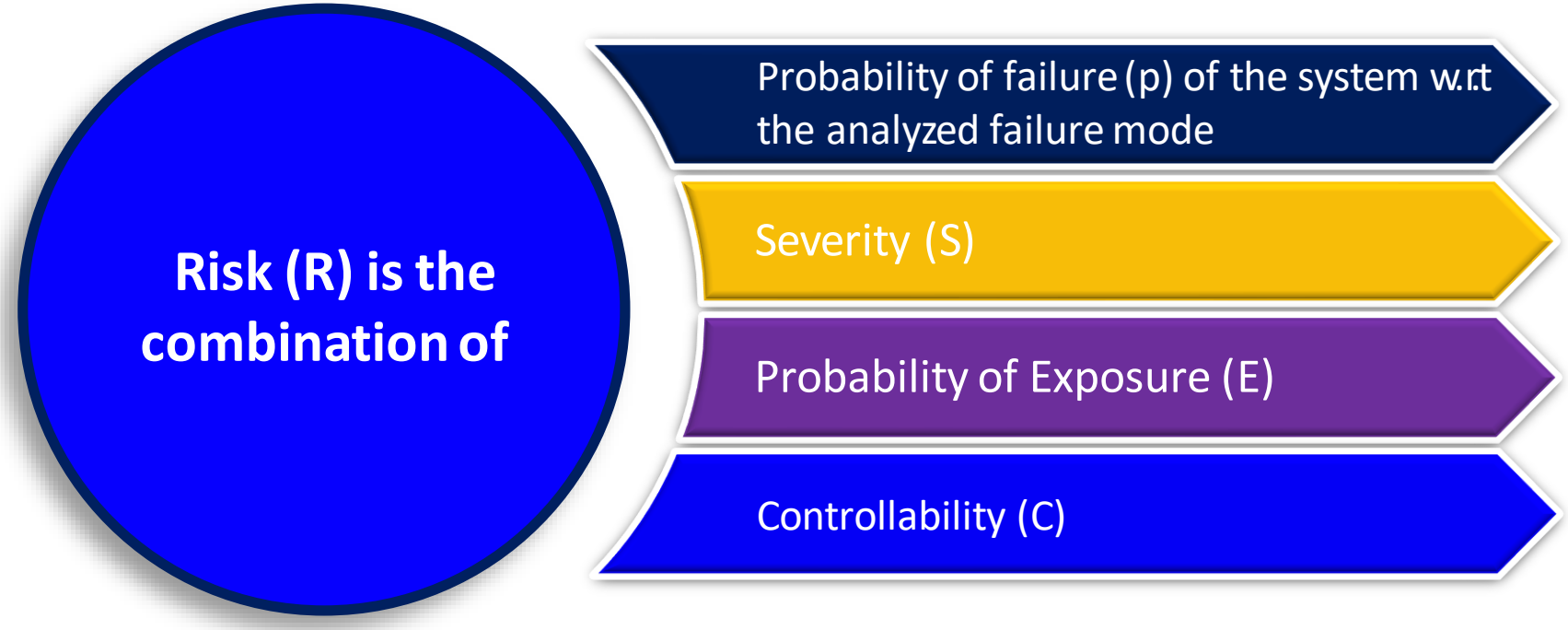
1. **Hazard** is defined as the potential source of harm (physical injury) caused by malfunctioning behavior

2. **Hazardous Event** is defined as the combination of a hazard and an operational situation

3. **Risk** is defined as combination of the probability of the occurrence of harm and the severity of that harm

ISO26262 Risk Definition

Risk is a combination of the following factors:



Hazard Analysis and Risk Assessment: evaluate **Potential Risk** of system in case of malfunction

➔ **"Thought Experiment"** assuming **that the failure mode is present (p = 1)**

Risk R = function (S, E, C)

➡ **Potential Risk = function (S, E, C)**

Participants / Team

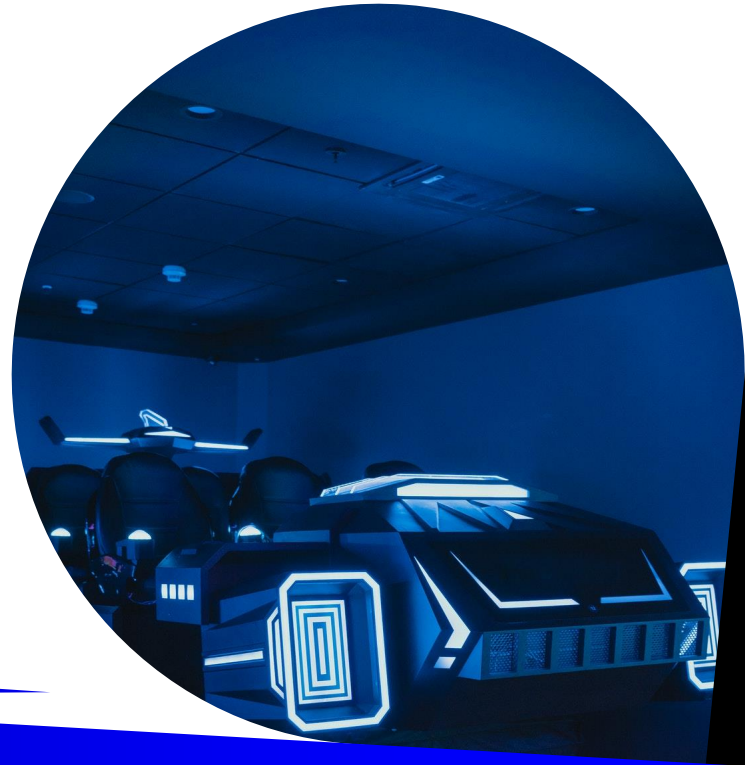
Establish and carry out Hazard Analysis Risk Assessment with a group of **experts** having good domain knowledge and experience in the behavior of commodity, elements, vehicle, and driver.

Mandatory:

- Functional safety experts from each affected domain
- Feature owner
- Function owner
- Distributed function owners (Chassis, EESE, Powertrain, etc.)

If required:

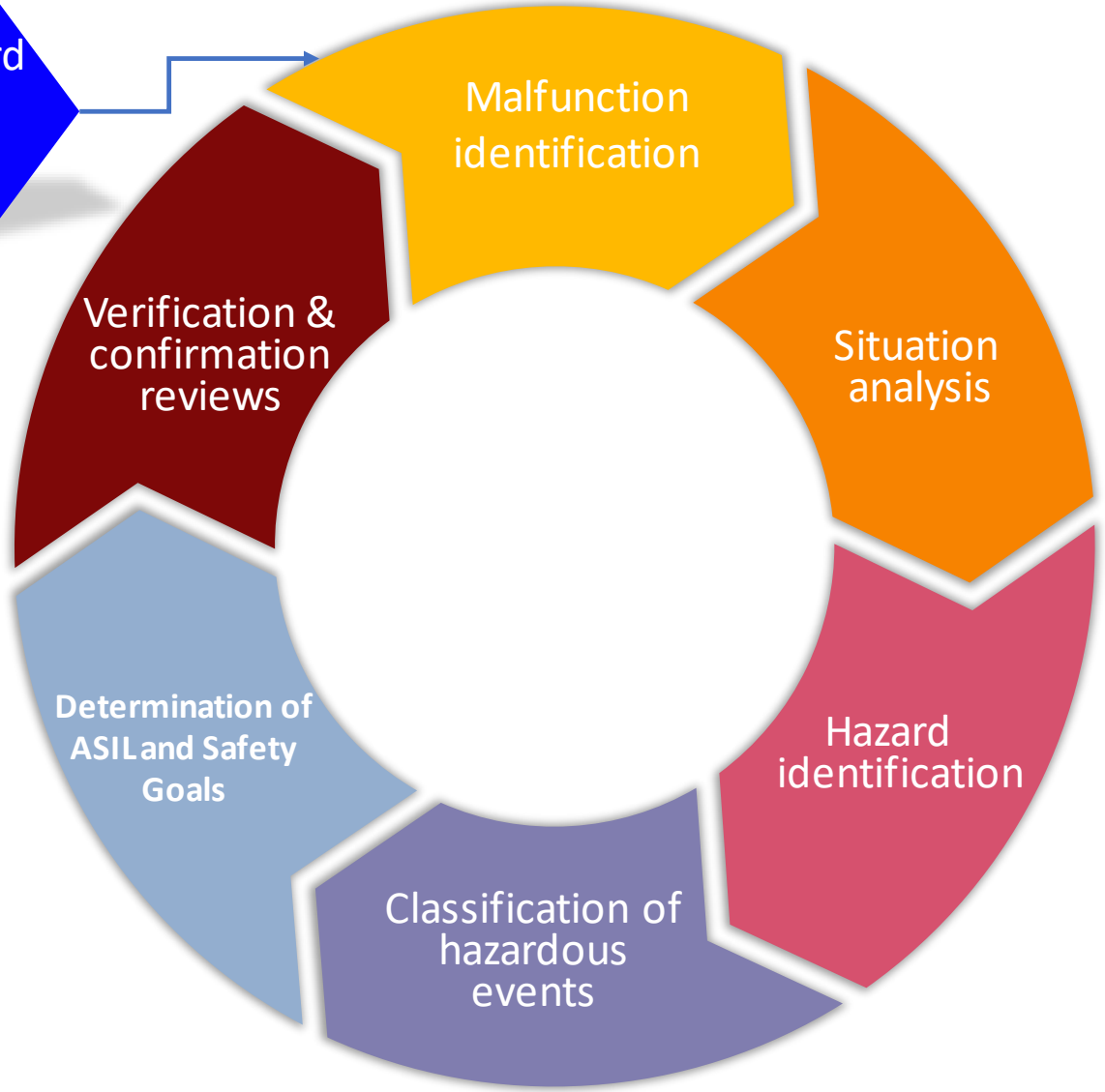
- Vehicle dynamic experts, e.g., for Exposure or Controllability rating
- HMI experts, e.g., for Controllability rating
- Accident research experts, e.g., for Severity or Exposure rating
- Other experts



Hazard and Risk Assessment Lifecycle

TOMCO® SERVICE GROUP

Initiation of the hazard analysis and risk assessment



Initiation of The Hazard Analysis Risk Assessment

- **The Hazard Analysis Risk Assessment shall be based on the Feature Document information.**
- **The Feature without internal safety mechanisms shall be evaluated during the Hazard Analysis Risk Assessment** (i.e., safety mechanisms intended to be implemented or that have already been implemented in predecessor Features shall not be considered in the Hazard Analysis Risk Assessment)

Malfunction and Hazard Identification

Malfunctioning Behavior is defined as a failure or unintended behavior on an Item/Feature with respect to its design intent.

Determine the major functions of the Item/Feature.

Use a HAZOP approach of 8 guidewords (No, Unintended, More, Less, Early, Late, Inverted, Intermittent) to define malfunctioning behaviors.

The effect of the malfunctioning behavior at the Vehicle level is the Hazard.

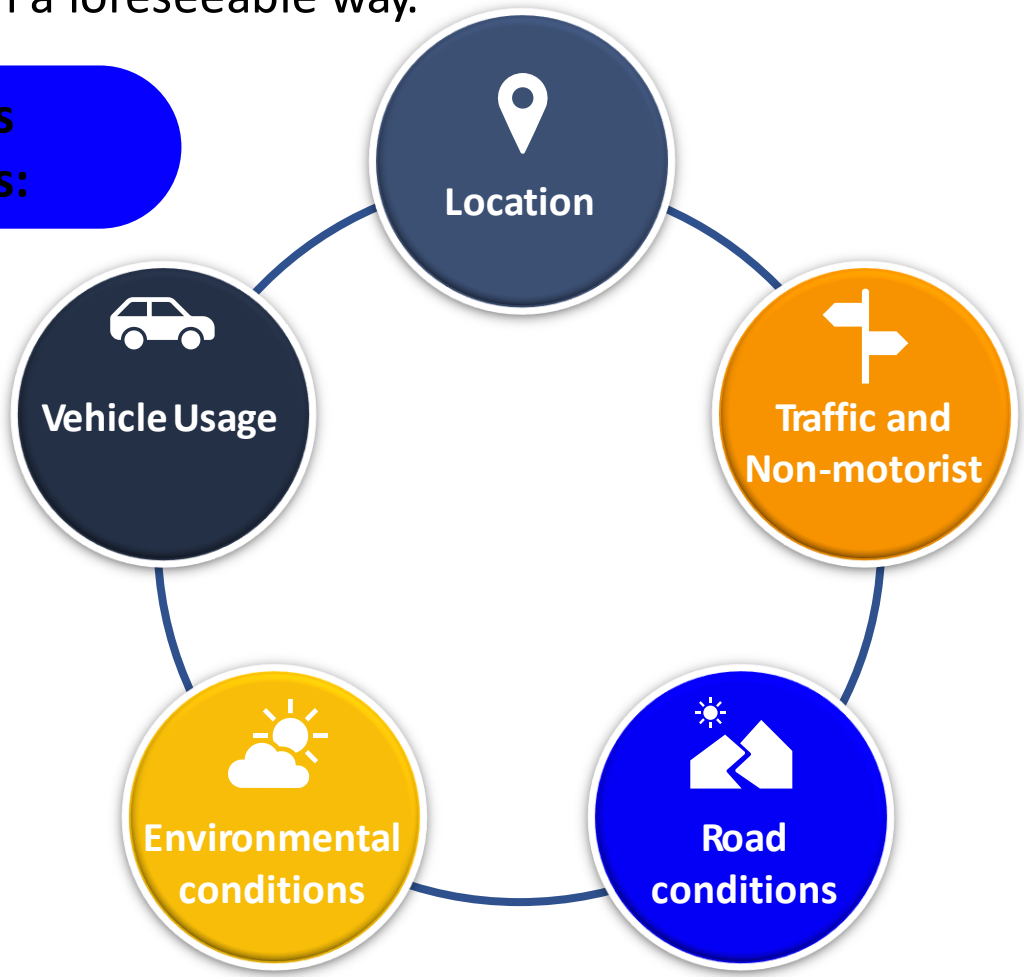
Hazards shall be defined by addressing all identified operational situations, operating modes, use cases and environmental conditions relevant for the system and its functionalities.

The hazards shall be determined systematicallyby using adequate techniques – Tomco has developed a hazard dictionary for hazard identification and a process for adding hazards to the hazard dictionary (see your AFSE for help in adding hazards to the hazard dictionary).

Situation Analysis

Situation Analysis – The **operational situations and operating modes** in which a commodity's malfunctioning behavior will result in a hazardous event shall be described, both for cases when the vehicle is correctly used and when it is incorrectly used in a foreseeable way.

There are 5 situation categories available to construct scenarios:



Assumptions

- **Used in HARA to provide additional information about the effect that a specific malfunctioning behavior will have at the vehicle level:**
  - explain how certain SEC ratings and SEC rationales were determined
  - provide more information about the specifics of an item's operating conditions when the malfunction occurs
- **Only assumptions which are necessary to describe and rate the hazardous events are documented in the HARA.** Generic assumptions about the item behavior are documented within the Item Definition or Feature Document.
- **Are grouped into the following categories**:

- Assumptions used for, or resulting from the HARA which are relevant for ASIL/QM determination shall be identified and shall be validated in later analysis

ASIL Concept

A AUTOMOTIVE

S SAFETY

I INTEGRITY

L LEVEL

ASIL Ratings

Safety Goals

Functional Safety Requirements

ASIL-related risk parameters

Parameter	Definition	Example
Severity	Extent of harm to one or more individuals	Potential vehicle collision at high speed
Exposure	State of being in an operational situation that can be hazardous if coincident with the failure mode under analysis	Driving on a high-speed road
Controllability	Ability to avoid a specified harm or damage through timely reactions of the persons involved, possibly with support from external measures	A driver can press on the brake pedal to slow the vehicle

Parameter Ratings

Severity (S)	S0	No injuries
	S1	Light and moderate injuries
	S2	Severe injuries, possibly life-threatening, survival probable
	S3	Life-threatening injuries (survival uncertain) or fatal injuries
Exposure (E)	E0	Incredible
	E1	Very low probability
	E2	Low probability
	E3	Medium probability
	E4	High probability
Controllability (C)	C0	Controllable in general
	C1	Simply controllable
	C2	Normally controllable
	C3	Difficult to control or uncontrollable

Severity (S)

The Severity of potential harm shall be estimated based on a defined rationale for each hazardous event. The Severity shall be assigned to one of the Severity classes S0, S1, S2, or S3 in accordance with the following table (please refer to the HARA guideline / Guidance for ISO 26262 HARA Assessments Of S/E/C for more info)

Class	S0	S1	S2	S3
Description	**No injuries**	light and moderate injuries	Severe injuries, possibly life-threatening, survival probable	Life-threatening injuries (survival uncertain) or fatal injuries
Informative Examples *Note: This examples base on ISO 26262, but are modified by the Functional Safety Team.* **These values are not absolute values. They should not be blindly followed. They must be adjusted by the team performing the Hazard Analysis according to the application, experience and market. The chosen value shall be justified.**				
Informative examples	Bumps with roadside infrastructure	Side impact with a narrow	Side impact with a narrow	Side impact with a narrow
	Pushing over roadside post, fence, etc.	Side collision with a passenger car (e.g. intrudes upon passenger compartment) with low speed	Side collision with a passenger car (e.g. intrudes upon passenger compartment) with medium speed	Side collision with a passenger car (e.g. intrudes upon passenger compartment) with high speed
	Light collision	Rear/front collision with another passenger car with low speed	Rear/front collision with another passenger car with medium speed	Rear/front collision with another passenger car with high speed
	Light grazing damage	Collision with minimal vehicle overlap (10-20%)		
	Damage entering/exiting parking space			
	Leaving the road without collision or rollover		Pedestrian/bicycle accident while turning (city intersection and streets)	Pedestrian/bicycle accident (e.g., 2-lane road)
		Front collision (e.g., rear- ending another vehicle, semi- truck, etc.) without passenger compartment deformation		Front collision (e.g., rear-ending another vehicle, semi-truck, etc.) with passenger compartment deformation

Severity (S) - Incremental Severity

ISO 26262-6:2018, Clause 6.4.3.3

- There are operational situations that result in harm (e.g. an accident). A subsequent malfunctioning behavior 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 behavior of the item.

Example : 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.

Severity (S) - Incremental Severity

This kind of severity rating is called incremental severity

- This severity is the incremental amount of harm of the malfunctioning behavior to the harm of the system behavior (correctly operating) within the initial operating scenario. In order to use incremental severity:
  - Harm must exist within the scenario for a system behavior, and
  - A difference of harm exists between the harm from the malfunctioning behavior within a scenario and the harm from the system behavior within the same scenario.

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

Severity (S) - Incremental Severity

How do we handle this at Tomco?

- When used, incremental severity shall be denoted as such. For the Example here, an S3 would be reduced to S1 by correct operation, the following would be used to indicate the incremental severity:

"S3 high speed collision, reduced to S1 by correct function of <feature>, S3-S1 = S2 (incremental severity)."

- The usage of incremental severity in a HARA is to be evaluated on a *case-by-case* basis at the Functional Safety Technical Governance Board meeting. This is to avoid artificially reducing ASIL ratings. So, the teams are required to contact their local Application Functional Safety Engineer (AFSE) for awareness and to be discussed.

Exposure (E)

The Probability of Exposure of each operational situation shall be estimated based on a defined rationale for each hazardous event. The probability of Exposure shall be assigned to one of the probability classes, E0, E1, E2, E3 and E4, in accordance with the following Table (please refer to the HARA guideline / Guidance for ISO 26262 HARA Assessments Of S/E/C for more info)

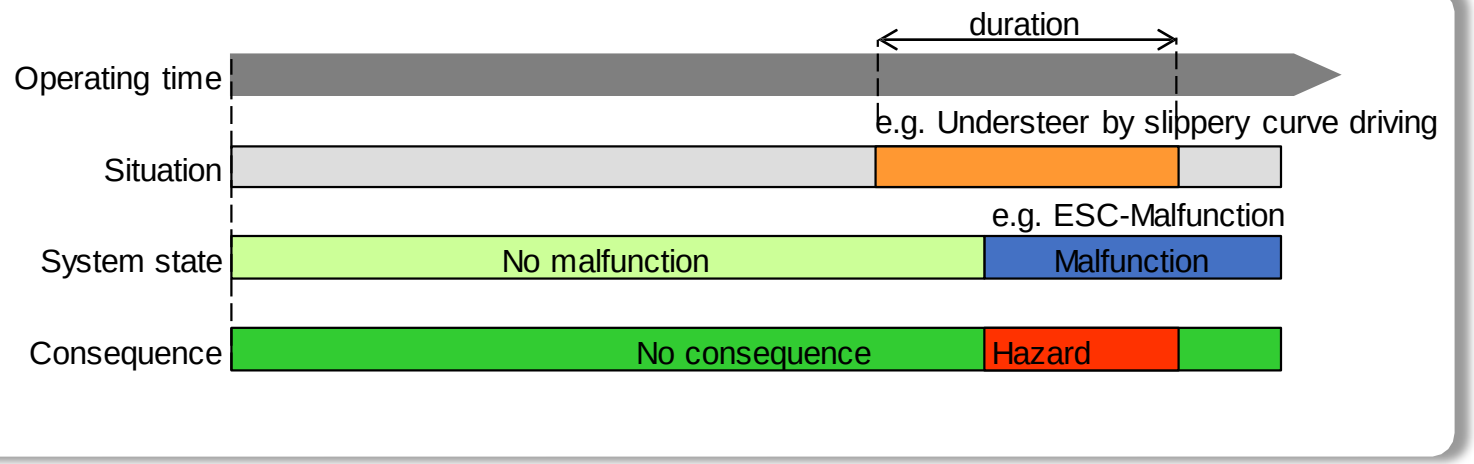
Guideline for Estimate	**Duration (% of average operating time)**				
	E0	E1	E2	E3	E4
	-	<0.1%	<1%	1%-10%	>10%
The probability of exposure can be typically estimated by the proportion of total operating time (ignition on). In special cases the total operating time can be the vehicle life-time (including ignition off)."					

Guideline for Estimate	**Frequency of operational situation**				
	E0	E1	E2	E3	E4
	Situations which are considered to be unusual or incredible. E.g. natural disasters like earthquake, hurricane, forest fire	Occur less often than once a year for the great majority of drivers	Occur a few times a year for the great majority of drivers	Occur once a `month or more often for an average driver	Occur during almost every drive on average

Exposure (E) – Duration vs. Frequency

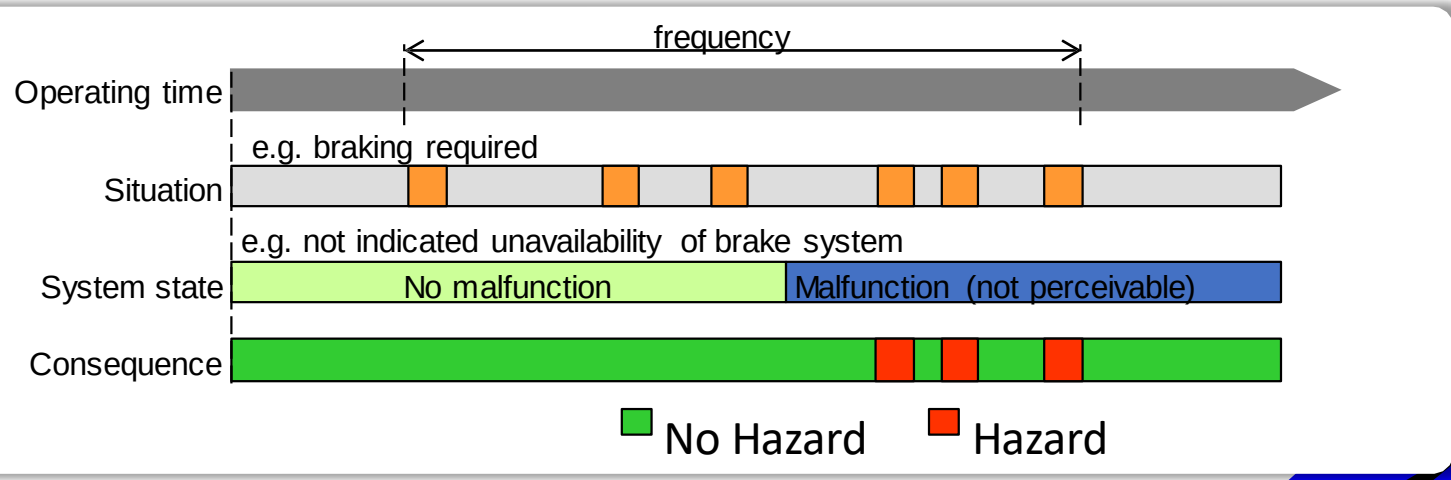
DURATION

Malfunction is perceivable for the driver if it occurs prior to critical situation (drivers will not enter critical situation e.g. adopt their driving behavior)



FREQUENCY

Malfunction is not perceivable for the driver prior to the potential critical situation.



Controllability (C)

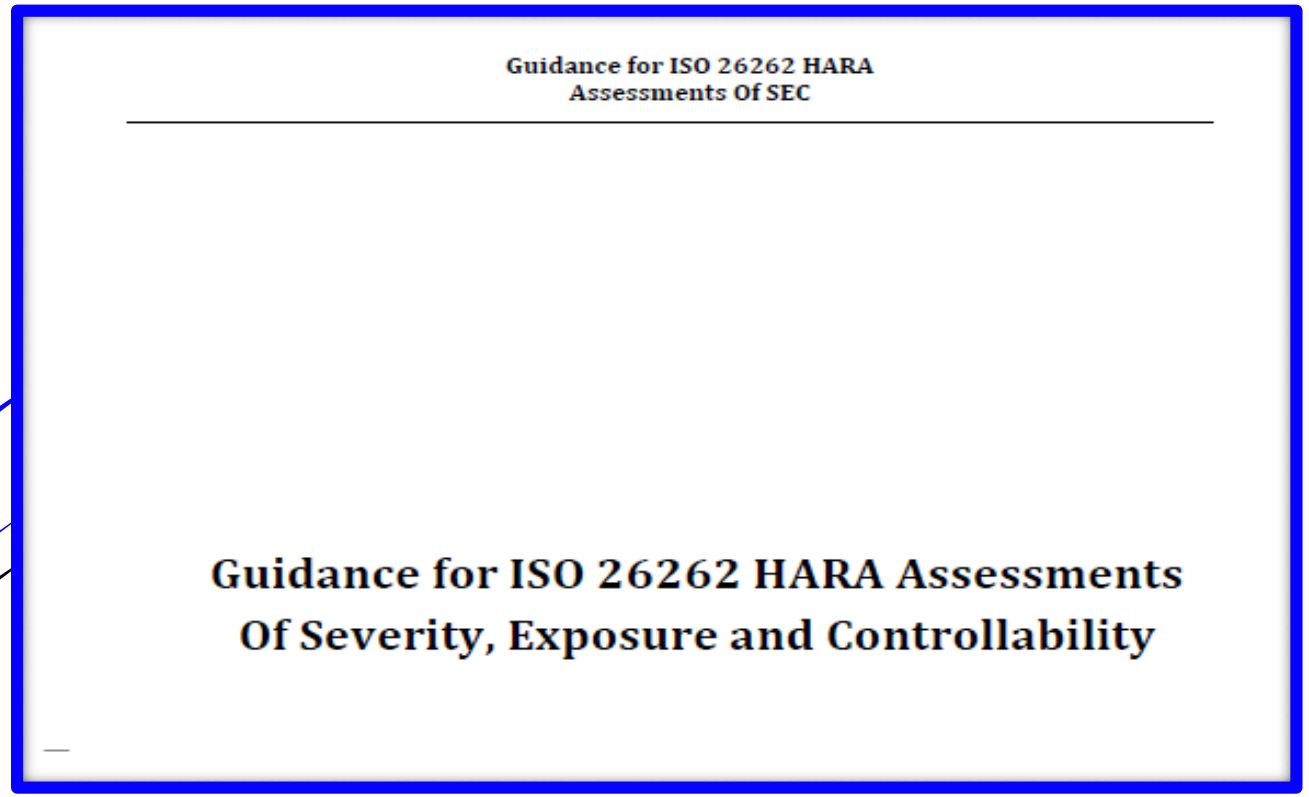
The Controllability of each hazardous event, by the driver or other persons potentially at risk, shall be estimated based on a defined rationale for each hazardous event. The Controllability shall be assigned to one of the Controllability classes C0, C1, C2, and C3 in accordance with the following Table (please refer to the HARA guideline / Guidance for ISO 26262 HARA Assessments Of S/E/C for more info).

Table 2 – Classes of Controllability				
	Classes			
	C0	**C1**	**C2**	**C3**
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable
Driving Factors and Scenarios	Controllable in general	99% or more of all drivers or other traffic participants are usually able to avoid harm	90% or more of all drivers or other traffic participants are usually able to avoid harm	Less than 90% of all drivers or other traffic participants are usually able, or barely able, to avoid harm

Guidance for Severity, Exposure and Controllability

1. Tomco has created a set of guidelines to aid in developing Severity, Exposure and Controllability ratings.

2. This guide may be found on the Tomco Functional Safety Database as well as on Functional Safety Shared Drive:



Shared Hazard Analysis and Risk Analysis (SHARA)

- The **Shared Hazard Analysis Risk Assessment** was created as a guide to help engineers generate a new HARA.
- The SHARA contains approved Hazards, Effects on the vehicle level, ASIL ratings, Safety Goals from each of the following domains; Powertrain, Chassis – Braking, Chassis – Steering, Body, EESE.
- SHARA information is stored in the "SHARA" SysML model stored on the Teamwork Cloud in the "Templates and Examples" directory.
- **The SHARA facilitates the following**:
  - Improved consistency of ASIL ratings and Safety Goals
  - Enables reuse of frequently-used hazardous events
  - Improved alignment of abstraction levels for hazardous events and safety goals between domains
  - Shortening the learning curve of engineers creating a HARA for the first time
  - Provides a list for hazards and safety goals relevant to each domain

This document may be found on the Tomco Functional Safety **DATABASE** as well as on Functional Safety Shared Drive.

ASIL Ratings

D

C

B

A

QM

Highest ASIL

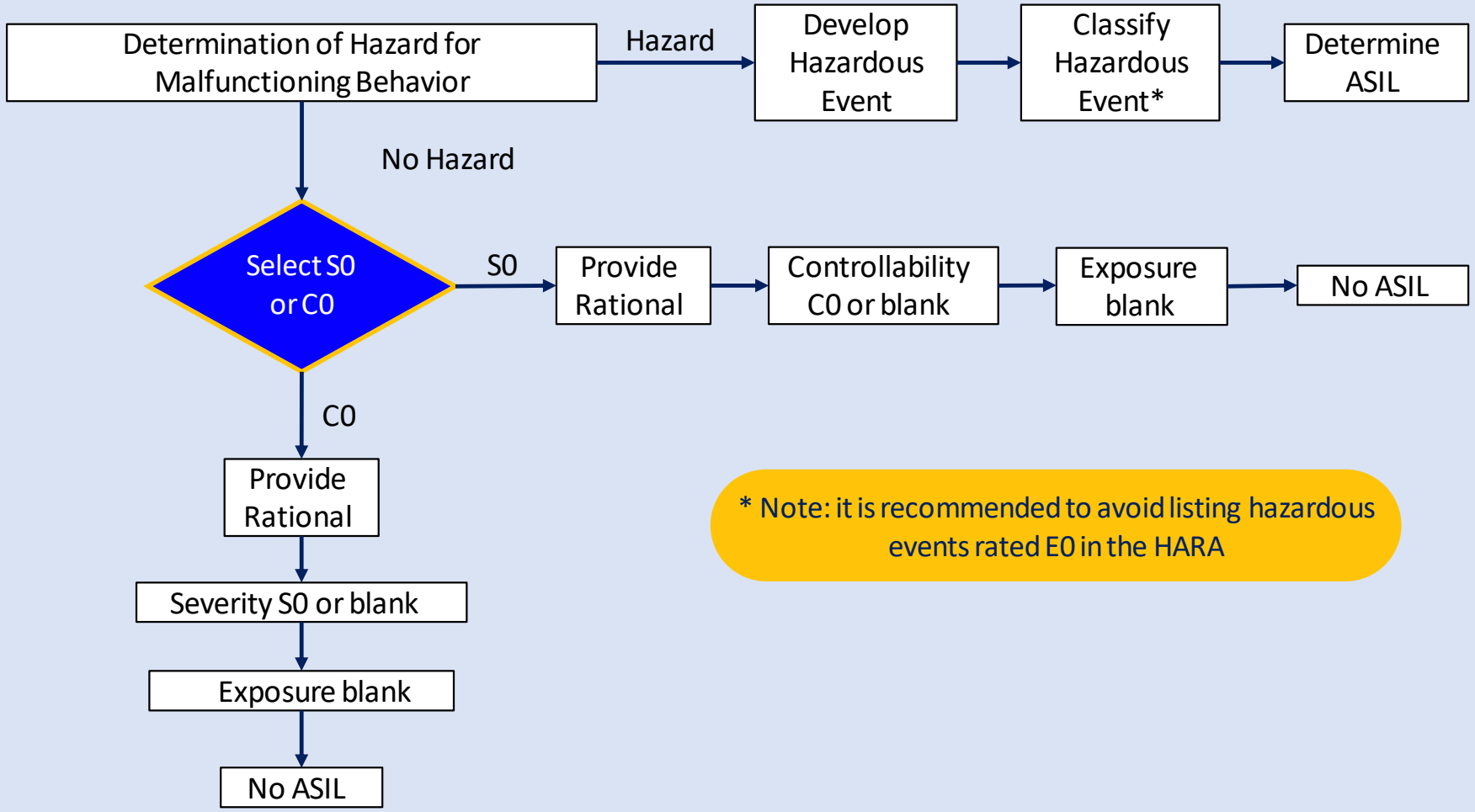
Lowest ASIL

(Quality Management) Development supported by established Quality Management is sufficient. No further actions are required by ISO 26262.

		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

Adapted from ISO 26262-3:2018, table 4, page 10.

Procedure for Handling S0, C0



ASIL and Risk Reduction Efforts

Safety Integrity Level	Quantitative Analysis of Hardware Failures	Notified as Highly Recommended in Part 4, 5, 6 Tables
QM	None	0
ASIL A	None	~ 50
ASIL B	Recommended	~ 80
ASIL C	Highly recommended	~ 130
ASIL D	Highly recommended	~ 150

Hazard Manifestation Time (HMT)

Hazard Manifestation Time (HMT): The minimum time span from the onset of the malfunctioning behavior to the violation of the safety goal. The HMT is specific to a scenario and malfunctioning behavior only. At the concept level this is independent of the system design

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.

Safety Goal

A Safety Goal shall be determined for each hazardous event with an ASIL A-D as determined in the hazard analysis. If similar Safety Goals are determined, these may be combined into one Safety Goal

The ASIL determined for the hazardous event shall be assigned to the corresponding Safety Goal. If similar Safety Goals are combined into a single one the highest ASIL shall be assigned to the combined Safety Goal

Rules for Defining Safety Goal

- 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)
- For each hazardous event rated as ASIL A, B, C or D a safety goal shall be assigned
- One safety goal can be assigned to several hazardous events
- It is at the discretion of the engineer to define safety goals for hazardous events rated as “QM”. QM rated events shall be covered in the FMA process
- The safety goal needs to be clear enough to tell the design team: “What to do!”
- The safety goal shall not predefine the technical solution

Verification vs Confirmation Review

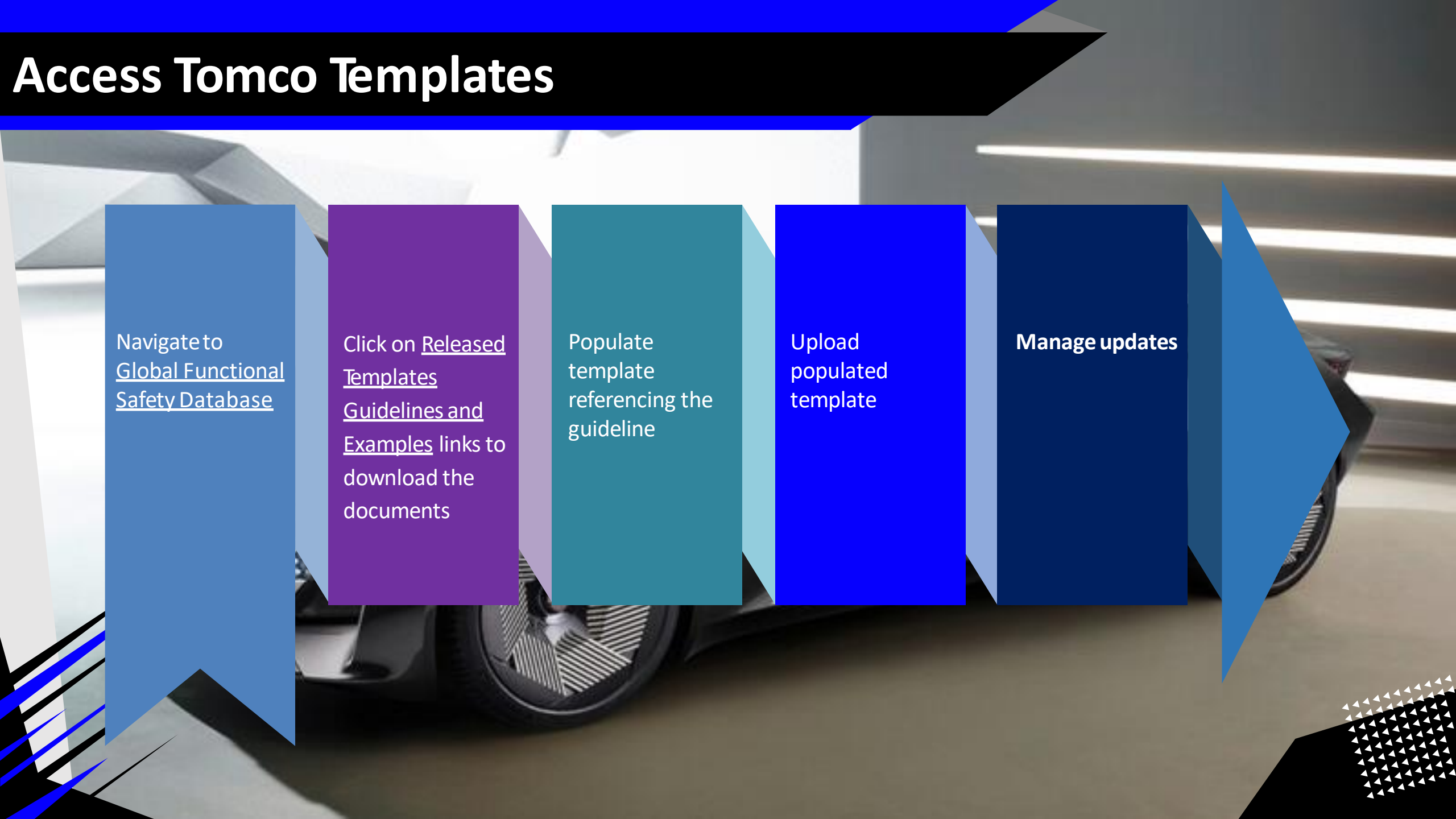
V VERIFICATION REVIEW

- Evaluates the thoroughness of a Functional Safety Document (FSD)
- Performed after the FSD is tentatively completed, prior to the confirmation review
- Performed by the working team responsible for creating the FSD with support from technical experts for the feature and the Application Functional Safety Engineer (AFSE) in the team's respective organization

C CONFIRMATION REVIEW

- Reviews the compliance of the FSD with the appropriate ISO 26262 requirements
- Performed after the verification review
- The person(s) performing the review must be trained, have project experience, and have sufficient independence

Access Tomco Templates



TOMCO®
SERVICE GROUP

THANK YOU!