SAFEXPLAIN
Safe and Explainable
Critical Embedded Systems based on AI

D2.1 Safety Lifecycle Considerations

Version 1.1

Documentation Information

Contract Number	101069595
Project Website	www.safexplain.eu
Contratual Deadline	31.03.2024
Dissemination Level	PU
Nature	R
Authors	Javier Fernández (IKR), Giuseppe Nicosia (EXI), Francesca Guerrini (EXI)
Contributors	Irune Agirre (IKR), Lorea Belategi (IKR), Carlo Donzella (EXI),
Reviewed by	Thanh Bui (RISE)
Keywords	AI, Functional Safety, FSM, AI-FSM, Explainability, V&V, Catalog Scenarios

This project has received funding from the European Union's Horizon Europe programme under grant agreement number 101069595.

Change Log

Version	Description Change
V0.1	First draft
V0.2	Reviewed version
V1.0	Final version
V1.1	Annexes appended and typos fixed

Table of Contents

Executive Summary

In the fourth to twelfth months of the project, the SAFEXPLAIN team, within the specified work package, concentrated on establishing safety techniques and restrictions for two key aspects of the Deep Learning (DL) development phase: (i) DL-software specification, design, and implementation (Task T2.1), and (ii) DL-software Verification and Validation (V&V) (Task T2.2). Finally, the results of this work have been evaluated by both project-internal (EXIDA partner) and external (TÜV Rheinland) entities, obtaining a set of necessary safety considerations to be addressed for future certifiability and, subsequently, a positive feedback assessment. This deliverable compiles the results, assessments, and reviews used to consolidate safety guidelines and arguments for DL-software adoption in the safety-critical domain (Task T2.5).

All the work collected in this deliverable has continuously monitor new standards and initiatives, proposing relevant extensions and adaptations when necessary.

1 Introduction

The development of safety-critical systems follows a well-known V-model, moving from safety goals to safety requirements, system architecture design, software and hardware architecture design, and implementation to obtain a system that is intended to be safe by construction. Then, the testing phase takes place from unit testing up to full system testing against its safety requirements. The Functional Safety Management (FSM) defines the required systematic approach (e.g., steps, actions, technical considerations) for developing safety-critical systems and other lifecycle phases, from concept definition up to decommissioning and disposal (for a more detailed explanation we refer the reader to the IEC 61508 standard [1]).

In recent years, the capabilities of Artificial Intelligence (AI) and particularly DL to perform advanced functions such as visual perception have led to their adoption in safety-related systems like autonomous vehicles. Whenever these functionalities implement safety requirements, they are also subject to provide evidence of their adherence to Functional Safety (FuSa) standards such as IEC 61508 [2]. Thus, the DL subsystem that implements safety requirements must be compliant with applicable safety development and management processes [3], [4], [5]. However, the general DL-based systems development process crashes frontally with traditional safety development processes [2], [5], [6]. For example:

1) DL softwar (SW) is designed monolithically following empirical training processes with example training data, rather than implementing specific safety requirements.
2) DL SW, as opposed to any other kind of SW in safety- critical systems, cannot be considered as correct by design due to the data driven nature and stochasticity in is engineering process.
3) DL SW design is no longer independent of data, and its parameters are set empirically based on training datasets.
4) DL SW imposes high-performance demands on the underlying hardware (HW) and its inherent complexity (both HW and SW) entails challenges to comply with safety standards. Moreover, there is a lack of guidance in the development process for safety-critical systems incorporating DL SW.

Therefore, effort has been dedicated to incorporating the recommendations from safety lifecycles identified in T1.3 into the development of T2.1. This entails specifying steps, safety techniques, and constraints for the left side of the V-cycle in DL software development. This task explores solutions aligned with existing standards and proposes new requirements for addressing challenges associated with DL-software, such as data specification and explainability.

Additionally, during these months, T2.1 has collaborated with WP3 (Deep Learning) to establish safety guidelines for DL algorithm development (T3.1).

Aiming to complete the entire development lifecycle of safety-related systems involving the use of AI, T2.2 complements T2.1 by addressing the right side of the V-model, focusing on the verification, validation, and testing of DL-software[1]. This task adapts or develops methodologies and testing techniques for DL-software Verification & Validation (V&V). It also considers quantifying the failure rate of DL-software to assess the overall system residual risk, similar to practices in FuSa standards for random hardware failures.

[1] It shall be noted that this deliverable employs the term AI to encompass the entire FSM annex. However, this AI-FSM annex primarily focused on DL constituents, as detailed in Section 3. Consequently, within this deliverable, the term AI denotes those phases or steps common to AI systems in general, while DL specifically refers to those related to DL.

All the work collected in this deliverable has continuously monitored new standards and initiatives, proposing relevant extensions and adaptations when necessary.

The rest of this document is structured as follows:

- Section 2 introduces a set of concepts to ease the understanding of this deliverable.
- Section 3 focuses on describing the contributions of our work related to defining a set of steps, safety techniques and restrictions to be followed in the left side of the V-cycle for the specification, design and implementation of DL-software. This section is directly related task T2.1. Additionally, this section maps current initiatives or standards focus on FuSa and the use of AI with the presented proposal. Furthermore, it outlines the activities carried out towards certifying the use of AI in safety-critical systems with TÜV Rheinland, which partially address T2.5.
- Finally, Section 4 collects the V&V strategy for the right side of the V-model. This section is directly related task T2.2 and has it focuses on the definition of a V&V strategy and associated methods for the V&V of DL components.

2 Background

As previously introduced, this section outlines the foundational aspects of this deliverable.

2.1 Functional Safety Management

FSM defines a development strategy that consists of a set of procedures, guidelines, and templates that define how a project with FuSa considerations should be executed (planning, involved team, activities, documents, configuration management, modification procedures, etc.). The main goal of the FSM is to ease the definition, organization, and control of the information generated during safety-critical project development while fulfilling the requirements of relevant FuSa standards. For instance, IKERLAN's FSM [1] has proven compliance with IEC 61508 [2] SIL 3, and hence, any new FuSa project that aims to meet with IEC 61508 up to SIL 3 can directly follow the procedures described on it and reuse the prepared templates. This FSM, referred to as "traditional FSM", is based on the V-model development process and structured in the following phases depicted in Figure 1:

- Ph0 Overall Life Cycle
- Ph1 System Concept Specification
- Ph2 System Architecture Specification
- Ph3 Module Detailed Design
- Ph4 Implementation
- Ph5 Module Testing
- Ph6 Integration Testing
- Ph7 Validation Testing

It can be observed that the system development process is broken down into two different development processes that also adhere to the V-model: i) the hardware development process, and ii) the software development process.

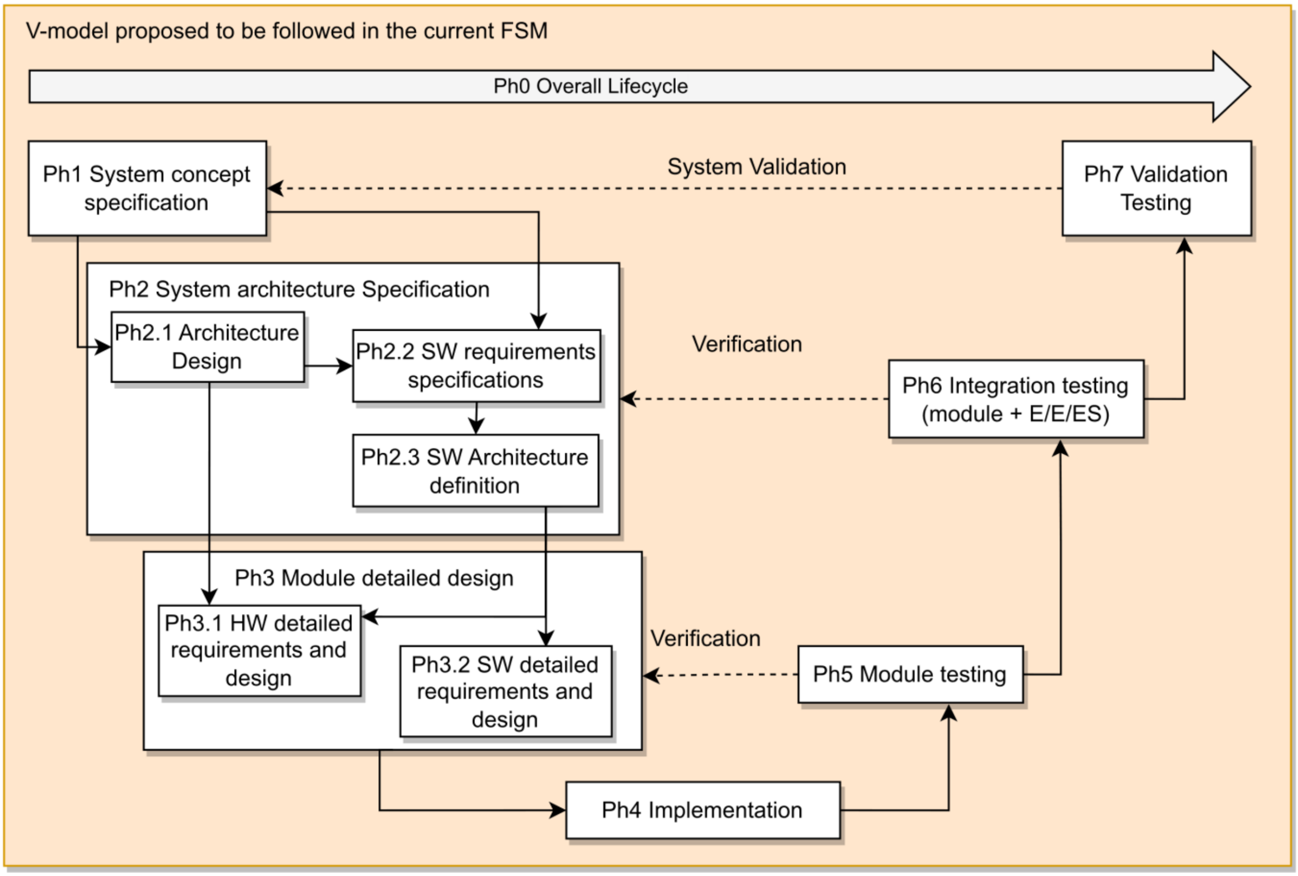


Figure 1. V-Model followed by traditional FSM of [1].

However, DL-based systems have some particularities concerning traditional FuSa systems that require new steps and considerations with respect to traditional safety systems. The main new challenges arise from the fact that DL systems result from data-driven learning processes, and some parts are not explicitly programmed as in traditional safety systems. This brings some new needs to the FSM, such as defining procedures for data management, dealing with sources of uncertainties, model bias, etc. [7]. These needs are covered by the Artificial Intelligence - Functional Safety Management (AI-FSM) introduced in next sections.

2.2 AI Notation

When referring to DL-based FuSa systems, this deliverable considers the definitions of the European Aviation Safety Agency (EASA) concept paper for Machine Learning (ML) application [7], which makes the decomposition shown in Figure 2.

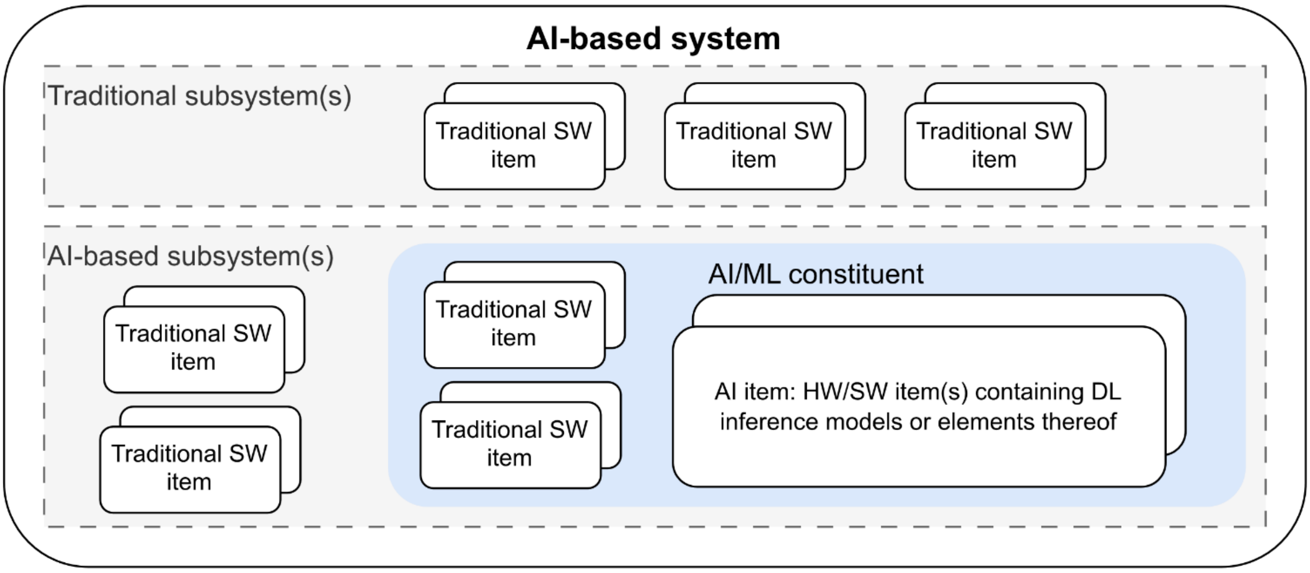


Figure 2: Artificial Intelligence (AI)-based system decomposition based on EASA concept paper [2]

Based on this decomposition, the EASA concept paper makes the following definitions [2]:

- AI-based system: systems encompassing traditional subsystem(s) and incorporating at least one AI-based subsystem.
- AI-based subsystem: subsystem that involves one or more AI/ML constituents.
- AI/ML constituent: It is a combination of software and hardware items that include at least one specialized hardware or software item containing at least one ML model.
- AI/ML item: specialized hardware or software item that builds the ML model(s).
- Traditional subsystem: subsystem that does not include any ML model.
- Traditional SW/HW item: hardware or software items that do not include ML model(s).

Our work focuses on the DL constituents, a subfield of ML. As a result, we use the terms “DL constituent” and “DL item” instead of “AI/ML constituent” and “AI/ML items”, respectively.

One of the main peculiarities of the DL lifecycle is the emergence of two distinct stages, deviating from the traditional V-model lifecycle. As illustrated in Figure 1, the DL lifecycle distinguishes between the learning and the inference stages.

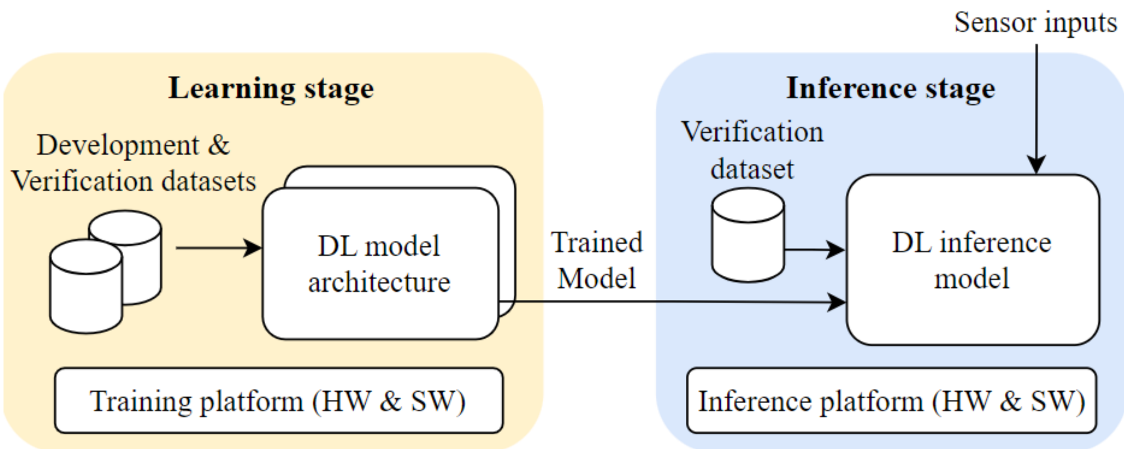


Figure 3: DL lifecycle stages

The main concepts of Figure 3 can be defined as follows:

- **DL model architecture:** A DL algorithm refers to the computational process that employs Neural Networks (NNs) to learn patterns or features from data. It encompasses the mathematical and computational operations involved in training a NN, adjusting its parameters (weights and biases), and optimizing its performance. DL algorithms include mechanisms like backpropagation, gradient descent, and various optimization techniques to minimize prediction errors during training. The algorithm defines the structure of the NN, the activation functions used, and how the network's parameters are updated based on the data.
- **DL inference model:** The trained model that has learned patterns and relationships from the training data undergoes a conversion to transform it into a format suitable for deployment and an optimization process to enhance its performance, reduce its size, or adapt it for resource-constrained environments. The resulting model is referred to as DL inference model. Although it can be considered that there is a single DL model with two operation modes, training and inference, it is worthwhile differentiate between then to better identify the phase of the development process.
- **Dataset**: In DL, a dataset refers to a collection of input data samples that are used to train, evaluate, and verify the DL model(s). These samples consist of input data and corresponding annotated target or output values (referred to as labels or annotations), allowing the model to learn patterns and relationships from the dataset in case of being employed during training or allowing to verify the expected output during and after the model(s) being trained. Datasets are a foundational component in the training and verification of DL models.
- **Training and inference platform:** The former relates to the underlying platform on which the DL model is developed, refined, and optimized using the datasets. The latter refers to the platform on which the DL model is finally deployed to perform its task(s).

In addition, the reader can observe two main stages in Figure 3:

1. **Learning stage**: This stage refers to the process of training a model and includes two main phases:
   - **Data Management.** Data Management is one of the most labor-intensive and crucial processes in DL development. This phase splits into four steps or activities[2]: i) data requirements specification, ii) data collection, iii) data preparation, and iv) data verification. Emphasize the significance of Data Management within every individual subphase. For instance, according to the data collection:
     - On one hand, the training data set establishes the behavior of the DL component, and its adequacy determines the desired behavior within the scope of operation, defined by the Operational Design Domain (ODD) and the operational scenarios.
     - On the other hand, verifying dataset entail checking whether the requirements defined are met. The proper identification of the cases more prone to jeopardize safety is essential.
   - **Learning Management.** Learning management is performed simultaneously with Data Management. It can be decomposed into four main steps: i) model requirements

[2] Hereinafter, this deliverable refers to those activities or subphases as steps.

specifications, ii) model design, ii) model training, iii) model evaluation and iv) model verification. This phase is performed in the training platform.

2. **Inference stage:** This stage refers to the adequacy of the trained model to be implemented in the deployment platform where it will perform the inference:
    - **Inference Management**: Once the model has been trained, evaluated and verified, it must be deployed over the final platforms where it will perform the inference. This platform may not be the same as the one used for the training and requires conversion and optimization of the trained model. Therefore, this phase requires additional model verification.

2.3 ISO 21448 Verification and Validation approach

The two previous subsections have explained how SAFEXPLAIN intends to cope with the extension of the traditional FuSa lifecycle to the novel AI concepts that cannot be reconciled into the existing current processes. As indicated, this is done by using the IEC 61508 as the reference standard for consolidated FuSa. However, there is an important area that is in between the traditional FuSa models and the emerging AI/ML/DL models: the so-called Safety of the Intended Functionality (SOTIF- ISO 21448 [8]).

While traditional FuSa and SOTIF share the same ultimate objective of achieving the “absence of unreasonable risk”, the former addresses “hazards caused by malfunctioning behaviour of E/E safety-related systems”, while the latter addresses “hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons”. SOTIF is not alternative to traditional FuSa, but complementary, and of paramount importance for AI-based functionalities, that typically fall into the second category.

Verification and Validation (V&V) is a very broad term that includes all activities that can be done to ensure that specifications and implementations are actually satisfying their requirements. Depending on the domains (System, Software, Hardware, Mechanics) we have an impressive array of partially common activities and methods such as Reviews, Inspections, Simulations, Prototyping, Analyses, Evaluations, Measurements, Testing, etc. As Testing is defined as a form of verification on the “executable model”, in the traditional V-model it is confined to the right-hand side, as the “tip of the V" represents the implementation.

For SAFEXPLAIN, an adaptation/extension of SOTIF to the ML/DL model is introduced. As SOTIF at the moment is fully defined for automotive only, the presented approach is integrated with ISO 26262 rather than with ISO/IEC 61508, but as ISO 26262 is entirely compliant with the IEC 61508 this is not introducing any inconsistency.

Considering that ML technologies are used for implementing the safety-related functionalities, the V&V strategy has been defined according to ISO 21448:2022 [8] to evaluate the safety of the functionalities allocated to ML algorithms by performing the appropriate testing activities (see ISO 21448:2022, D.2.3).

To identify the test cases and scenario sets that verify the functionality of ML-based components, an appropriate analysis of use cases and Operational Design Domain (ODD) shall be performed.

To obtain ISO 21448:2022 [8] compliance the goals listed in Figure 4 shall be met. It is worth mentioning that goal 2.1.5 is beyond the scope of the SAFEXPLAIN project, as it pertains to the evaluation of real-world scenarios.

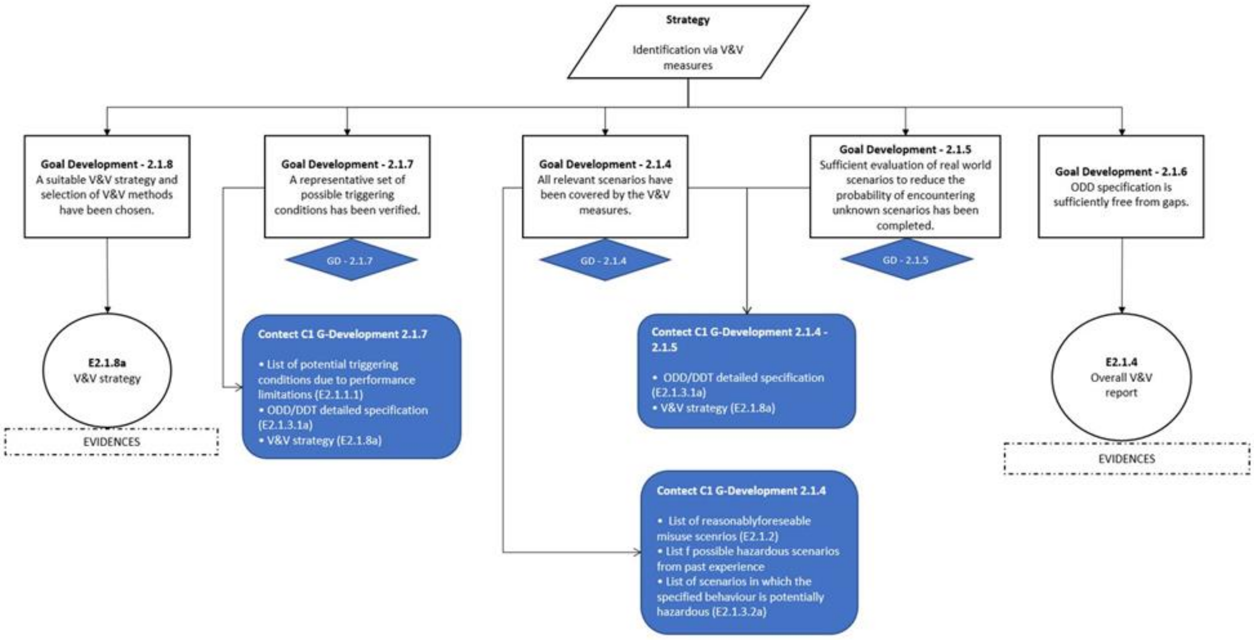


Figure 4. SOTIF compliance goals

Another relevant activity for testing is the identification of component boundaries that affect the evaluation of the accuracy and exhaustiveness of testing and the capability and suitability of the test oracle such as simulation, test data and the ground truth.

Testing activities shall be performed among the architectural levels depicted in Figure 5:

- Vehicle-level testing tests, to evaluate the hazardous behaviour at the vehicle level.
- Component-level testing tests, to evaluate the hazardous behaviour at the sense-plan-act level. For example:
  - Testing on the ML-based algorithm can be effective for finding unknown insufficiencies typical for the ML component (e.g. visualisations).
  - Testing at the component level, which, depending on the functionality, and the aspect to be tested, can be a better way to evaluate the behaviour of the algorithm which contains other related components (e.g. post processing filters in the example case of object detection).

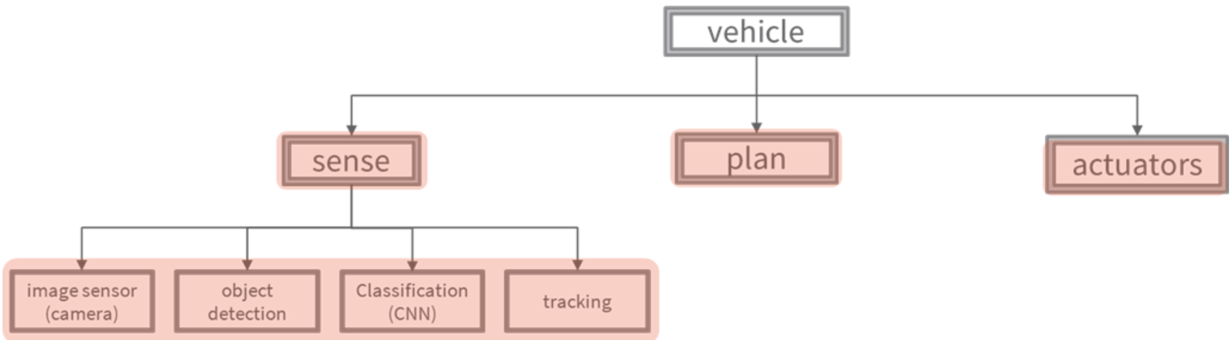


Figure 5. Architectural level in a vehicle

3 Safety Lifecycle for DL-Software Specification, Design and Implementation

This section defines the additional steps, actions and considerations that shall be addressed in the FSM when incorporating DL components into a safety-critical system. For that, it has been defined the AI-FSM annex that complement the traditional FSM with a set of documents guiding the development of those systems. The documents composing the AI-FSM are the followings:

- Main procedure. It provides a set of steps required to generate the basic structure for a specific safety-related project. It serves as an internal guideline for fulfilling the procedure template.
- Procedure template: This document compiles how functional safety has been assessed within the organization.
- Guidelines: These documents offer additional guidance for specific processes.
- Templates: Standard documents used to document the information consistently. They typically include examples and tables to be completed, serving as a starting point for collecting specific information. However, the proper fulfillment of these documents is subject to technical expert judgment for the specific application.
- Internal Reviews (IRs): reviews based on the activities of the left side of the safety lifecycle. The main objective is to check that the activities defined in each phase have been properly carried out, serving as a quality assurance.

The current version of this AI-FSM is restricted to DL constituents with the following features:

- DL algorithms based on supervised learning for visual perception classification tasks.
- Applications based on offline learning processes in which the model remains fixed at approval time, while excluding online learning processes.

3.1 AI Safety Lifecycle

In D1.1 [9] was conducted an analysis of the current functional safety standards addressing the use of AI in safety-related systems was conducted. Based on this state-of-the-art analysis and a review of new standards and emerging initiatives, this work has evaluated the main steps of the V-model that should be at least briefly modified, to accommodate the peculiarities of AI. After that, we have proposed a new development lifecycle according to the recommendations of these initiatives and standards, complementing them when necessary, and mapping the new phases related to AI with the traditional phases followed in a V-model lifecycle of safety-related systems.

As it can be observed in Figure 6, the current version of the development phase of the AI-FSM is grounded in the emerging initiatives and early stages standards existent at the time of writing, including EASA Concept Paper [7], AMLAS [10], ISO/IEC DTR 5469 [5] or the Automotive SPICE 4.0 [11]. In the future, the AI-FSM may be updated to extend the types of AI constituents addressed and to correspondingly conform to forthcoming iterations of emerging standards, such as ISO/CD PAS 8800 [6], IEC TS 6254 [12] or ISO/IEC 5338 [13], which are under development during the creation of the AI-FSM.

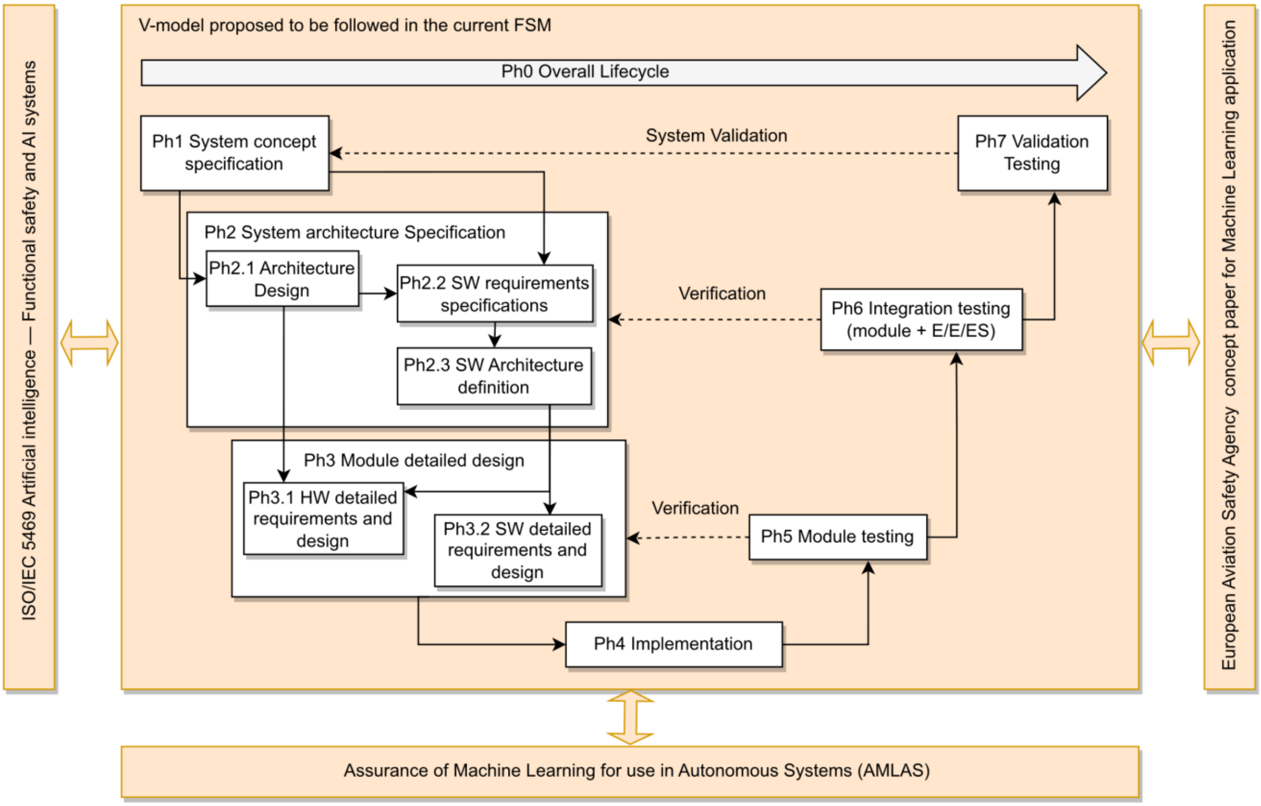


Figure 6. V-model proposed by traditional functional safety standards and AI initiatives for complementing it

The V-based lifecycle, as traditionally followed by FSM, has been expanded considering these concepts, as depicted in Figure 7. For improved visual distinction, the conventional lifecycle is denoted by white boxes, whereas DL components are illustrated using colored boxes. It is worth noting in Figure 7 that a sequence of numbered blue rhombuses symbolizes datasets originating from the Data Management phase. Additionally, there is a red rhombus that serves as a condition to check the results of the model evaluation. These elements will be elaborated further in the forthcoming documents that comprise this AI-FSM.

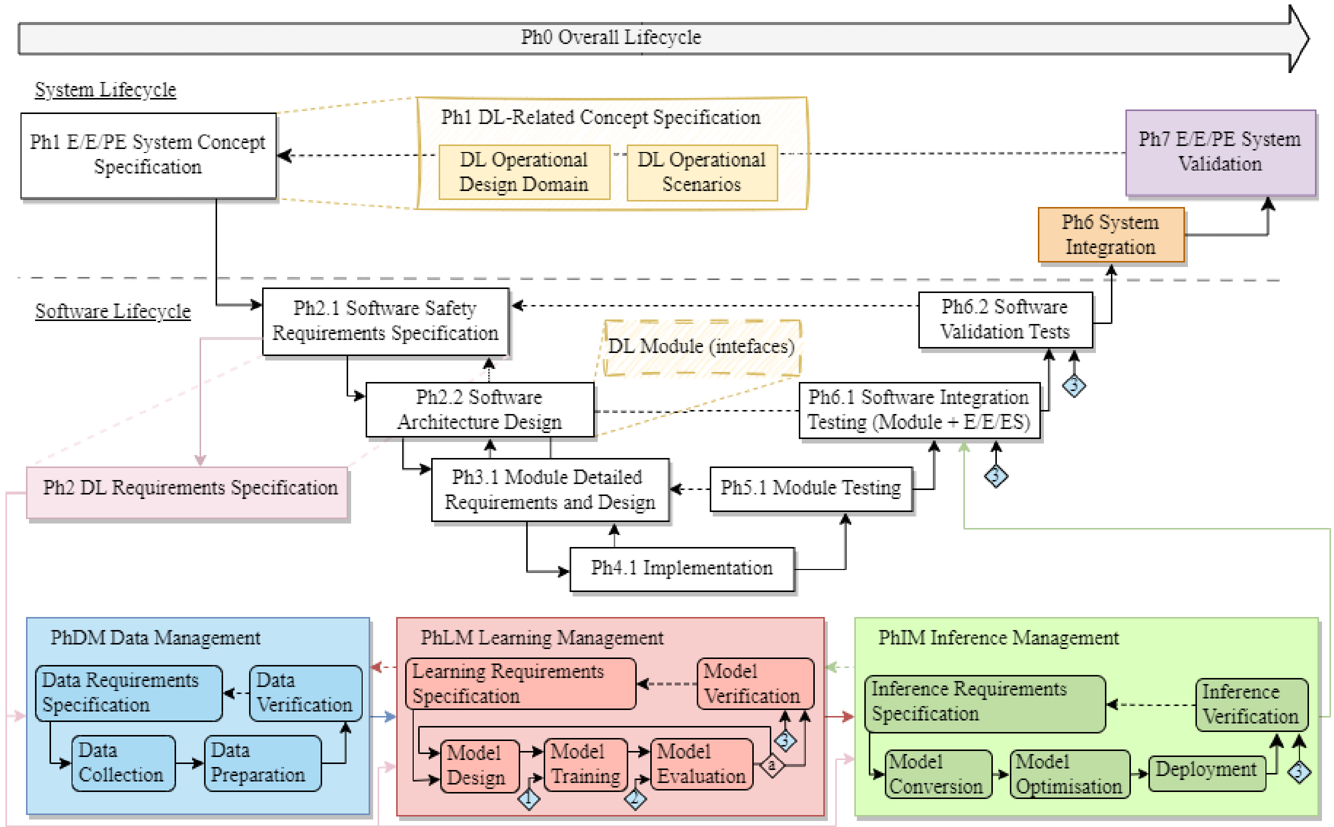


Figure 7. Mapping AI lifecycle with traditional functional safety lifecycle

3.2 AI-FSM Overview

Following the previously defined V-lifecycle the developed AI-FSM provides a new set of guidelines, templates, and internal review documents to complement the traditional FSM as it can be seen in Figure 8.

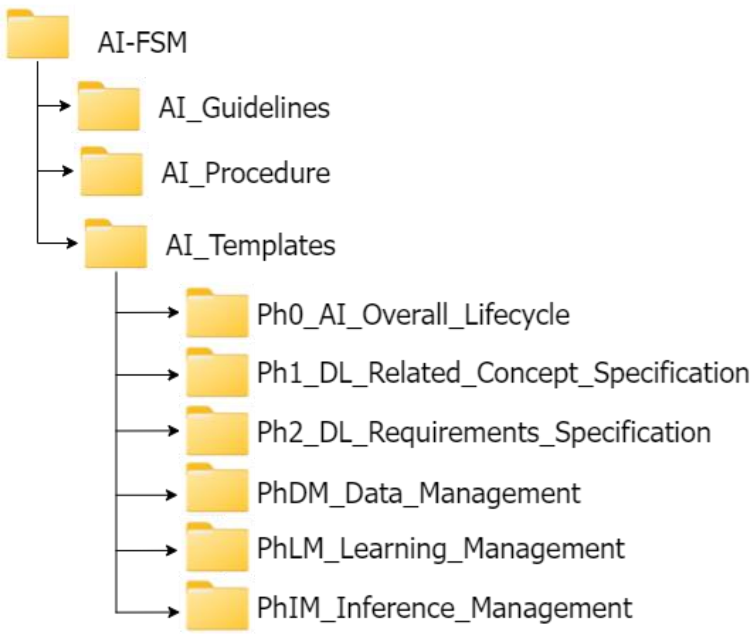


Figure 8. Folder structure

Note: Since AI-FSM utilizes templates from both the traditional FSM *and its own templates, this annex distinguishes the AI-FSM documents by color-coding them in orange and the traditional FSM documents in green. Additionally, the folders' names will be enclosed in quotation marks and the files' names created from the templates are written in* *__italics and underlined__.*

The structure of the documents that will be created throughout the AI-FSM and the nomenclature to denote them is defined in the *Ph0G0001_Doc_Structure.docx*. To facilitate the understanding of this deliverable, we have included the nomenclature for generating the file names, which follows a specific codification characteristic:

<REF>_<PhID><TypElement><Identifier>_<Short_name>

The meaning of each is as follows:

- REF. Project reference number.
- PhID. Identifier of the phase:
    - Ph0: relates to the Overall Lifecycle phase.
    - Ph1: relates to the DL-Related Concept Specification phase.
    - Ph2: relates to the DL-Requirements Specification phase.
    - PhDM: relates to the Data Management phase.
    - PhLM: relates to the Learning Management phase.
    - PhIM: relates to the Inference Management phase.
- TypElement:
    - D: Deliverable
    - T: Template
    - G: Guideline
    - P: Procedure
- Identifier: Unique identifier starting from 0000.

From this point on, this document only refers to the information or documents that differ from the traditional FSM. The rest should be generated and fulfilled following the traditional FSM.

The following tables describe the inputs and outputs for each step of the AI lifecycle as follows:

1. Table 1 collects the steps, inputs, outputs and templates associated with the Overall Lifecycle phase (Ph0).
2. Table 2 collects the steps, inputs, outputs and templates associated with the DL-Related Concept Specification phase (Ph1). Traditional FSM requires the definition of the software operating conditions to ensure that the safety-related system is used within the intended scope including factors such as temperature ranges, input conditions or process variables. However, within the AI domain, the array of input variables and operational scenarios can be exceptionally vast. Hence, in this phase, we incorporate the definition of the ODD and the operational scenarios to highlight what might require further engineering efforts.
3. Table 3 gathers the steps, inputs, outputs and templates associated with the DL Requirements Specification phase (Ph2). This includes the definition of the DL requirements.
4. Table 4 collects the steps, inputs, outputs and templates associated with the Data Management phase (PhDM).
5. Table 5 collects the steps, inputs, outputs and templates associated with the Learning Management phase (PhLM).
6. Table 6 collects the steps, inputs, outputs and templates associated with the Inference Management phase (PhIM).

Table 1. Inputs and outputs of the overall lifecycle phase (Ph0)

Phase	Step	Inputs	Outputs	Corresponding templates
Ph0 AI Overall Life Cycle	Generate the AI-FSM document	REF_FSM_procedure	REF_Ph0D0001_AI-FSM_Procedure	*Ph0T0001_AI_FSM_template*
	V&V the AI-FSM document	REF_Ph0D0001_AI-FSM_Procedure	REF_Ph0D0002_AI-FSM_Procedure_IR	*Ph0T0001_AI_FSM_template_IR*
	Generate the AI_Document_List	REF_Document_list	REF_Ph0D0003_AI_Document_List	*Ph0T0002_AI_Document_List_template*
	V&V the AI_Document_List	REF_Ph0D0003_AI_Document_List	REF_Ph0D0004_AI_Document_List_IR	*Ph0T0002_AI_Document_List_template_IR*
	Generate AI version tracking	REF_version_tracking	REF_Ph0D0005_AI_Version_Tracking	*Ph0T0003_AI_Version_Tracking_template*
	V&V the AI version tracking	REF_Ph0D0005_AI_Version_Tracking	REF_Ph0D0006_AI_Version_Tracking_IR	*Ph0T0003_AI_Version_Tracking_template_IR*
	Generate AI organizational chart	REF_organizational_chart	REF_Ph0D0007_AI_Organizational_Chart	*Ph0T0004_AI_Organizational_Chart_template*
	V&V AI organizational chart	REF_Ph0D0007_AI_Organizational_Chart	REF_Ph0D0008_AI_Organizational_Chart_IR	*Ph0T0012_Organizational_chart_template_IR*
	Generate the AI log of tests	-	REF_Ph0D0009_AI_Log_of_Tests	*Ph0T0006_Log_of_Test_template*
	V&V the AI log of test	REF_Ph0D0009_AI_Log_of_Test	REF_Ph0D0010_AI_Log_of_Tests_IR	*Ph0T0006_Log_of_Test_template_IR*
	Generate the AI selection of tools	-	REF_Ph0D0011_AI_Tools_Selection	*Ph0T0010_Tools_selection_template*
	V&V the AI selection of tools	REF_Ph0D0011_AI_Tools_Selection	REF_Ph0D0012_AI_Tools_Selection_IR	*Ph0T0010_Tools_selection_template_IR*
	Generate the AI traceability matrix	-	REF_Ph0D0013_AI_Traceability_Matrix	*Ph0T0011_Traceability_matrix_template*
	V&V the AI traceability matrix	REF_Ph0D0013_AI_Traceability_Matrix	REF_Ph0D0014_AI_Traceability_Matrix_IR	*Ph0T0011_Traceability_matrix_template_IR*

Table 2. Inputs and outputs of the DL-Related Concept Specification phase (Ph1)

Phase	Step	Inputs	Outputs	Corresponding templates
Ph1 DL-rRelated Concept Specification	ODD definition	REF_System_Requirements_Specifications	REF_Ph1D0001_DL_Operational_Design_Domain	Ph1T0001_DL_Operational_Design_Domain_template
	V&V the ODD	REF_Ph1D0001_DL_Operational_Design_Domain	REF_Ph1D0002_DL_Operational_Design_Domain_IR	Ph1T0001_DL_Operational_Design_Domain_template_IR
	Operational scenarios definition	REF_System Requirements Specifications REF_Ph1D0001_DL_Operational_Design_Domain	REF_Ph1D0003_DL_Operational_Scenarios	Ph1T0002_DL_Operational_Scenarios_template
	V&V the operational scenarios	REF_Ph1D0003_DL_Operational_Scenarios	REF_Ph1D0004_DL_Operational_Scenarios_IR	Ph1T0002_DL_Operational_Scenarios_template_IR

Table 3. Inputs and outputs of the definition of the DL requirements specification phase (Ph2)

Phase	Step	Inputs	Outputs	Corresponding templates
Ph2 DL Requirements Specification	DL requirements specifications	REF_Software Requirements Specifications	REF_Ph2D0001_DL_Requirements_Specifications REF_Ph2D0003_DL_Requirements_Verification_Tests	Ph2T0001_DL_Requirements_Specifications_template Ph0T0009_Test_definition_and_results_template
		REF_Ph2D0001_DL_Requirements_Specifications REF_Ph2D0003_DL_Requirements_Verification_Tests	REF_Ph2D0002_DL_Requirements_Specifications_IR REF_Ph2D0004_DL_Requirements_Verification_Tests_IR	Ph2T0001_DL_Requirements_Specifications_template_IR Ph0T0009_Test_definition_and_results_template_IR

Table 4. Inputs and outputs of each step of the Data Management phase (related to Ph3, Ph4 and Ph5 of the traditional life cycle)

Phase	Step	Inputs	Outputs	Corresponding templates
PhDM Data Management	Data requirements specifications	REF_Ph2D0001_DL_Requirements_Specifications REF_Ph1D0001_DL Operational Design Domain REF_Ph1D0003_DL_Operational_Scenarios	REF_PhDMD0001_Data_Requirements_Specifications REF_PhDMD0007_Data_Requirements_Verification_Tests	PhDMT0001_Data_Requirements_Specifications_template Ph0T0009_Test_definition_and_results_template
		REF_PhDMD0001_Data_Requirements_Specifications REF_PhDMD0007_Data_Requirements_Verifica tion_Tests	REF_PhDMD0002_Data_Requirements_Specifications_I R REF_PhDMD0008_Data_Requirements_Verification_Tes ts_IR	PhDMT0001_Data_Requirements_Specifications_template_IR Ph0T0009_Test_definition_and_results_template_IR
	Data Collection	REF_PhDMD0001_Data_Requirements_Specifications	REF_PhDMD0003_Data_Collection_Log Collected data structured in datasets(3)	PhDMT0002_Data_Collection_Log_template
		REF_PhDMD0003_Data_Collection_Log	REF_PhDMD0004_Data_Collection_Log_IR	PhDMT0002_Data_Collection_Log_template_IR
	Data Preparation	REF_PhDMD0001_Data_Requirements_Specifications REF_PhDMD0003_Data_Collection_Log Raw data files structured in datasets(3)	REF_PhDMD0005_Data_Preparation_Log Prepared data structured in datasets(3)	PhDMT0003_Data_Preparation_Log_template
		REF_PhDMD0005_Data_Preparation_Log	REF_PhDMD0006_Data_Preparation_Log_IR	PhDMT0003_Data_Preparation_Log_template_IR
	Data Verification	REF_PhDMD0001_Data_Requirements_Specifications REF_PhDMD0007_Data_Requirements_Verification_T ests Datasets(3)	REF_PhDMD0007_Data_Requirements_Verification_Tests Verified datasets(3)	Document previously generated

[3] Datasets include: i) Development (training and validation) datasets and ii) verification dataset.

Table 5. Inputs and outputs of each step of the Learning Management phase (related to Ph3, Ph4 and Ph5 of the traditional life cycle)

Phase	Step	Inputs	Outputs	Corresponding templates
PhLM Learning Management	Learning Requirements Specifications	*REF_Ph2D0001_DL_Requirements_Specifications*	*REF_PhLMD0001_Learning_Requirements_Specifications* *REF_PhLMD0005_Learning_Requirements_Evaluation_Tests* *REF_PhLMD0007_Learning_Requirements_Verification_Tests*	*PhLMT0001_Learning_Requirements_Specifications_template* *Ph0T0009_Test_definition_and_results_template* *Ph0T0009_Test_definition_and_results_template*
		REF_PhLMD0001_Learning_Requirements_Specifications *REF_PhLMD0005_Learning_Requirements_Evaluation_Tests* *REF_PhLMD0007_Learning_Requirements_Verification_Tests*	*REF_PhLMD0002_Learning_Requirements_Specifications_IR* *REF_PhLMD0006_Learning_Requirements_Evaluation_Tests_IR* *REF_PhLMD0008_Learning_Requirements_Verification_Tests_IR*	*PhLMT0001_Learning_Requirements_Specifications_template_IR* *Ph0T0009_Test_definition_and_results_template_IR* *Ph0T0009_Test_definition_and_results_template*
	Model Design	*REF_PhLMD0001_Learning_Requirements_Specifications*	*REF_PhLMD0003_Model_Election_Log*	*PhLMT0002_Model_Election_Log_template*
		REF_PhLMD0003_Model_Election_Log	*REF_PhLMD0004_Model_Election_Log_IR*	*PhLMT0002_Model_Election_Log_template_IR*
	Model Training	*REF_PhLMD0003_Model_Election_Log* Training dataset	Trained Model(s)	*There is not a template, it should be considered as an implementation.*
	Model Evaluation	*REF_PhLMD0005_Learning_Requirements_Evaluation_Tests* Trained Model(s) Validation dataset [4]	*REF_PhLMD0005_Learning_Requirements_Evaluation_Tests* Evaluated Model(s)	*Document previously generated*
	Learning Model Verification	*REF_PhLMD0007_Learning_Requirements_Verification_Tests* Evaluated Model(s) Verification dataset	*REF_PhLMD0007_Learning_Requirements_Verification_Test* Verified Learning Model(s)	*Document previously generated*

[4] Although this document maintains the name "validation" according to AI nomenclature, it would not correspond to validation in the context of safety

Table 6. Inputs and outputs of each step of the Inference Management phase (related to Ph3, Ph4 and Ph5 of the traditional life cycle)

Phase	Step	Inputs	Outputs	Corresponding templates
PhIM Inference Management	Inference Requirements Specifications	REF_Ph2D0001_DL_Requirements_Specifications REF_PhLMD0001_Learning_Requirements_Specifications	REF_PhIMD0001_Inference_Requirements_Specifications REF_PhIMD0007_Inference_Requirements_Verification_Tests	*PhIMT0001_Inference_Requirements_Specifications* *Ph0T0009_Test_definition_and_results_template*
		REF_PhIMD0001_Inference_Requirements_Specifications REF_PhIMD0007_Inference_Requirements_Verification_Tests	REF_PhIMD0002_Inference_Requirements_Specifications_IR REF_PhIMD0008_Inference_Requirements_Verification_Tests_IR	*REF_PhIMD0002_Inference_Requirements_Specifications_IR* *Ph0T0009_Test_definition_and_results_template_IR*
	Model Conversion	REF_PhIMD0001_Inference_Requirements_Specifications Verified Learning Model	REF_PhIMD0003_Model_Conversion_Log Converted Model	*PhIMT0002_Model_Conversion_Log*
		REF_PhIMD0003_Model_Conversion_Log	REF_PhIMD0004_Model_Conversion_Log_IR	*PhIMT0002_Model_Conversion_Log_IR*
	Model Optimization	REF_PhIMD0001_Inference_Requirements_Specifications Converted Model	REF_PhIMD0005_Model_Optimization_Log Optimized Model	*PhIMT0003_Model_Optimization_Log*
		REF_PhIMD0005_Model_Optimization_Log	REF_PhIMD0006_Model_Optimization_Log_IR	*PhIMT0003_Model_Optimization_Log_IR*
	Inference Model Verification	REF_PhIMD0007_Inference_Requirements_Verification_Tests Optimized Model or Converted Model Verification dataset	REF_PhIMD0007_Inference_Requirements_Verification_Tests Verified Inference Model	*Document previously generated*

3.3 AI-FSM Detailed Procedure

This section guides the safety designer in the generation of the folders and documents to be generated and fulfilled during the development process.

Every time a new file is generated, first, it is required to replace the name of the project words in the header and in the front cover of the file with the name of the specific project, and secondly, the content (in **blue**) of the table in the Front cover (responsible of preparing, reviewing and approving the template). The corresponding revision number must be set for the specific project and the Review/Modification History table shall also be modified. Finally, the contract number, project website, contractual deadline, dissemination level (PU=Public, SEN=Sensitive) and the nature (R=Report or OTHER) must be updated.

New documents generated in the AI-FSM should be consolidated within a single folder. To achieve this, within the repository of the dedicated functional safety project, generate a new folder specific to the AI-FSM with the name “AI-FSM”. In the same way than in the traditional FSM, the AI-FSM folder should be divided into subfolders according to AI lifecycle phases. Therefore, within AI-FSM folder, the subsequent subfolders should be created:

1. “Ph0 AI Overall Lifecycle” folder. It will contain the documents resulting from the activities described in Section 3.3.1.
2. “Ph1 DL-Related Concept Specification” folder. It will contain the ODD and operational scenarios documents described in Section 3.3.2. These documents can be stored in the specific folder of the traditional FSM. However, to easily identify the documents related to the AI-FSM we recommend including them in this folder.
3. “Ph2 DL Requirements Specification” folder. It will contain the documents resulting from the activities described in Section 3.3.3, such as the DL requirements specification.
4. “PhDM Data Management” folder. It will contain all the information related to the data. We refer the reader to the *PhDMG0001_Data_Management_guideline.docx* document that provides all the information related to the Data Management phase. Additionally, the following folders shall be generated within the “PhDM Data Management” folder.
    a. “Datasets” folder. To store the data related to each dataset generated in the Data Management process. Inside this folder:
        i. “Development dataset” folder and within it:
            1. “Training dataset” folder: To store the data related to training dataset.
            2. “Validation dataset” folder: To store the data related to validation dataset.
        ii. “Verification dataset” folder: To store the data related to verification dataset.
    b. Inside each of the folders generated within the “Datasets” folder, the following datasets should be additionally generated:
        i. “Collected Data” folder: To store the raw data and predefined datasets collected during the data collection step.
        ii. “Prepared Data” folder: To store the data after being prepared in the data preparation step.

5. "PhLM Learning Management" folder. It will contain all the information related to the learning process. We refer the reader to the *PhLMG0002_Learning_Management_guideline.docx* document that provides all the information related to the Learning Management phase.
6. "PhIM Inference Management" folder. It will contain all the information related to the inference process. We refer the reader to the *PhIMG0003_Inference_Management_guideline.docx* document that provides all the information related to the Inference Management phase.

Subsection 3.3.1 explains the modifications to be performed in the overall lifecycle (Ph0). The new documents to be generated regarding phase 1 (Ph1) in Subsection 3.3.2. The documents related to the DL Requirements Specification phase in Subsection 3.3.3 and the documents associated with Data, Learning and Inference Management phases in Subsections 3.3.4, 3.3.5, and 3.3.6 respectively. It should be noted that the steps performed in the last three phases of the AI-FSM (PhDM Data Management, PhLM Learning Management, and PhIM Inference Management) correspond to three phases in the traditional lifecycle (Ph3 Module detailed design, Ph4 Implementation, and Ph5 Module testing), as will be explained later.

3.3.1 AI Overall Lifecycle – Phase 0 (Ph0)

In this phase, documents related to the overall lifecycle must be specified. These documents guide through the whole lifecycle complemented with the traditional FSM documentation:

Phase Definition

1. Create the *REF_Ph0D0001_AI-FSM_Procedure.docx* from *Ph0T0001_AI_FSM_template.docx*. This document is generated in order to specify the procedure and project specific information. The current document (*Ph0P0001_AI_Procedure.docx)* eases the generation and organization of the required information.
2. The *Document_List.docx* file lists all the files generated throughout the project. In the traditional FSM, the document is generated from the *Ph0T0002_Document_List_template.docx* template. To differentiate between projects including AI and those that do not, create a new document list to gather the documents related to AI-FSM using the *Ph0T0002_AI_Document_List_template.docx* template. This *REF_Ph0D0003_AI_Document_List.docx* file should either be merged within the *Ph0T0002_Document_List_template.docx* template from the traditional FSM or explicitly explained in the *Document_List.docx* that those documents related to AI are gathered in the *REF_Ph0D0003_AI_Document_List.docx* document.

3. The *Version_Tracking.docx* file collects the relationship between the different elements of a safety project. In the traditional FSM, this document is generated from *Ph0T0001_Version_Tracking_template.docx* template, and its fulfillment is guided by *Ph0G0003_FSM_Version_Tracking_guide.docx* from the traditional FSM. To differentiate between projects including AI and those that do not, create a new version tracking document to gather the relationship related to AI-FSM using the *Ph00T0003_AI_Version_Tracking_template.docx* template. *REF_Ph0D0005_AI_Version_Tracking.docx* document should either be merged within the *Version_Tracking.docx* from the traditional FSM or explicitly explained in the *Version tracking.docx* that those relationship between the different elements of the AI project are gathered in the *REF_Ph0D0005_AI_Version_Tracking.docx* document.

4. The *Organizational_Chart.docx* file outlines the relationship between the company organisation and the methodology, identifies the main roles involved in a safety or cybersecurity project, and the relationships between these roles. In the traditional FSM, this document is generated from *Ph0T0012_Organizational_Chart_template* template, and its fulfillment is guided by *Ph0G0004_Organizational_Chart_guide.docx* from the traditional FSM. To differentiate between projects including AI and those that do not, create a new organizational chart document to gather the relationship related to AI-FSM using the *Ph00T0004_AI_Organizational_Chart_template* template. *REF_AI_organizational_chart.docx* document should either be merged within the *Organizational_Chart.docx* from the traditional FSM or explicitly explained in the *Organizational_Chart.docx* that those relationship between the different participants of the AI project are gathered in the *REF_AI_Organizational_Chart.docx* document.
5. The *Log_of_Tests.docx* file collects all the tests performed during the project and is generated from the from *Ph0T0006_Log_of_Test_template* template. To differentiate between projects including AI and those that do not, create a new log of tests document to monitor all tests related to AI-FSM using the same template than in the traditional FSM. The content of this *AI_Log_of_Tests.docx* should either be included in the *Log_of_Tests.docx* or explicitly explained in the *Log_of_Tests.docx* that those tests related to AI-FSM are stored in the *AI_Log_of_Tests.docx* document.
6. In the traditional FSM, the *Tools_Selection.docx* file is generated including all the tools or frameworks employed through the lifecycle of the project, using the *Ph0T0010_Tools_Selection_template.docx* template. To prevent inconsistencies or omission of information, create a *REF_Ph0D0011_AI_Tools_Selection.docx* file from the traditional template to include AI tools and frameworks. Again, this file should either be merged within the *Selection_of_Tools.docx* file from the traditional FSM or explicitly explained in the traditional *Selection_of_Tools.docx* that those related to AI are gathered in the *REF_Ph0D0011_AI_Tools_Selection.docx*.
7. In the traditional FSM, the interdependences of the requirements at different levels of the development process, as well as the relationship between requirements and verification or validation mechanisms, are documented in the *Traceability_Matrix.docx* document, using the *Ph0T0011_Traceability_Matrix_template.docx* template. The use of DL involves the apparition of the following interdependencies (as well as the testing mechanisms associated):
    a. Software requirements specifications and DL requirements specifications.
    b. DL requirements specifications and data requirements specifications.
    c. DL requirements specifications and learning requirements specifications.
    d. DL requirements specifications and inference requirements specifications.

   As before, create a *REF_Ph0D0013_AI_Traceability_Matrix.docx* file from the traditional template. This file should either be integrated into the *Traceability_Matrix.docx* file or clearly explained in the traditional *Traceability_Matrix.docx* that interdependencies related to AI are documented in the *REF_Ph0D0013_AI_Traceability_Matrix.docx.*

V&V activities:

- Generate the *REF_Ph0D0001_AI-FSM_Procedure_IR.xlsx*, *REF_Ph0D0004_AI_Document_List_IR.xlsx*, *REF_Ph0D0010_AI_Log_of_Tests_IR.xlsx*, *REF_Ph0D0012_AI_Tools_Selection_IR.xlsx* and

REF_Ph0D0014_AI_Traceability_Matrix_IR.xlsx from *Ph0T0001_AI_FSM_IR.xlsx*, *Ph0T0002_Document_List_IR.xlsx*, *Ph0T0006_Log_of_Tests_template_IR.xlsx*, *Ph0T0010_Tools_Selection_IR.xlsx* and *Ph0T0011_Traceability_Matrix_IR.xlsx*, respectively.

3.3.2 DL-related Concept Specification – Phase 1 (Ph1)

This section presents the information related to the DL-related Concept Specification phase. It includes the ODD and the operational scenarios, which must be defined in order to specify the operational conditions, environmental conditions, etc., that limit the system's defined safety functionality.

Phase Definition

The documents to be generated in the system folder are the following ones:

- Generate the *REF_Ph1D0001_DL_Operational_Design_Domain.docx* file from the *Ph1T0001_DL_Operational_Design_Domain_template.docx* template and save it with the name of the specific project. The objective of this document is to define the environment conditions in which the system will operate, the ODD, thus defining the scope in which requirements will be described.
- Generate the *REF_Ph1D0003_DL_Operational_Scenarios.docx* file from the *Ph1T0002_DL_Operational_Scenarios_template.docx* template and save it with the name of the specific project. The purpose of this document is to specify operations, scenarios, and environmental conditions for the system, in which the system has to function according to the specification. This specification must be under the ODD. These operational scenarios include standard situations, but also challenging environments and cornerstone situations.

Reminder: -Update the state of REF_Ph0D0003_AI_Document_List.docx.

V&V activities:

- Generate the *REF_Ph1D0002_DL_Operational_Design_Domain_IR.xlsx* and the *REF_Ph1D0004_DL_Operational_Scenarios_IR.xlsx* from *Ph1T0002_DL_Operational_Design_Domain_IR.xlsx* and *Ph1T0004_DL_Operational_Scenarios_IR.xlsx*, respectively.

Reminder: -Update the state of REF_Ph0D0003_AI_Document_List.docx.

3.3.3 DL Requirements Specification – Phase 2 (Ph2)

This section presents the information related to the DL Requirements Specification phase. It encompasses the generation of safety, operational, functional and non-functional requirements specification as well as interface requirements.

Phase Definition

- Generate the *REF_Ph2D0001_DL_Requirements_Specifications.docx* file from the *Ph2T0001_DL_Requirements_Specifications_template.docx* template and save it in the repository of the specific project with the name of the file for the specific project.
- Generate the *REF_Ph2D0003_DL_Requirements_Verification_Tests.docx* file from the *Ph0T0009_Test_definition_and_results_template.docx* template and save it in the repository of the specific project with the name of the file for the specific project.

Reminder: -Update the state of REF_Ph0D0003_AI_Document_List.docx.
- Update the REF_Ph0D0013_AI_Traceability_Matrix.docx.

V&V activities

- Generate the *REF_Ph2D0002_DL_Requirements_Specifications_IR.xlsx* and the *REF_Ph2D0004_DL_Requirements_Verification_Tests.xlsx* internal review documents from *Ph2T0001_DL_Requirements_Specifications_IR.xlsx* and *Ph0T0009_Test_definition_and_results_IR.xlsx,* respectively.

Reminder: -Update the state of REF_Ph0D0003_AI_Document_List.docx.

3.3.4 Data Management – Phase DM (PhDM)

As previously mentioned, this document refers the reader to the *Ph3G0001_Data_Management_guideline.docx* for further guidance on this phase. The objective of this document is to guide the Data Management process required by DL constituents in the lifecycle of safety-related systems. It can be decomposed into 4 steps as can be seen in Figure 9. It is important to note that in the first iteration of the process, the data collection and data preparation steps do not need to be considered if previously generated and verified datasets are being employed for the specific application.

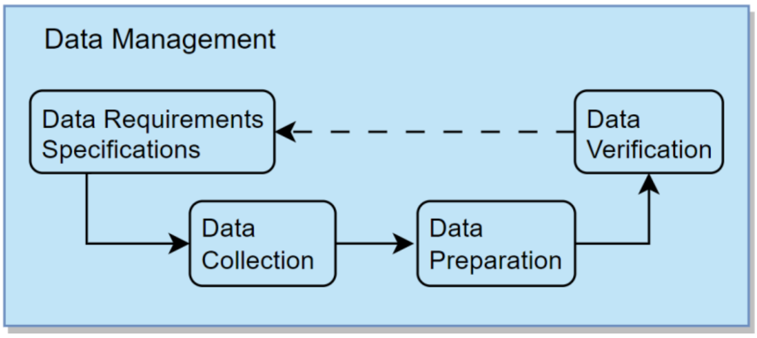


Figure 9. Data Management phase

The final objective of this phase is the generation of the following datasets:

- Development dataset[5]. This dataset is split into two sub datasets:
  - Training dataset: Dataset employed to train the model.
  - Validation[6] dataset: Dataset used to evaluate if the model achieves a predefined performance and, in some cases, stops the training phase.
- Verification[6] dataset: This dataset expands upon the previous validation dataset to assess whether the model maintains its performance requirements with data not utilized during development. It must encompass sufficient information and data to ensure the appropriate behavior of the DL constituent within the expected ODD and operational scenarios.

[5] In order to ensure robustness, both the training and validation datasets should encompass corner cases while also guaranteeing their representativeness of the ODD.

[6] The definitions of "validation" and "verification" can vary across different technology areas or domains. In the realm of AI, "validation" typically denotes a step in the process aimed at ensuring the convergence of the developing model to terminate the AI training process. This differs significantly from the V&Vconcepts commonly used in the functional safety community.

Furthermore, it should gather data to handle corner case situations that pose safety risks and confirm the fulfillment of performance requirements.

Additionally, the following data artifacts must be generated and stored:

1. Development (training and validation) and verification datasets, previously defined. These datasets are composed of:
   i. Collected data (raw data files). Refers to all data gathered during the collection step, including data generated from datasets, sensors, and synthetically generated data[7].
   ii. Prepared data. Encompasses all data that has undergone a cleaning, processing, or annotation process.
2. Verified datasets. Correspond with Development (training and validation) and Verification datasets that meet the data requirements specifications after performing the data verification step.

The subsequent documents should be stored in the "PhDM Data Management" folder, located within the "AI-FSM" folder:

Phase Definition

- Generate the *REF_PhDMD0001_Data_Requirements_Specification.docx* file from the *PhDMT0001_Data_Requirements_Specification_template.docx* template and store it in the repository of the specific project with the name of the file for the specific project. This step would relate to Phase 3 in the traditional FSM. This document collects the data requirements specifications refined from the DL requirements specifications previously defined in phase 2.
- Generate the *REF_PhDMD0009_Data_Requirements_Verification_Tests.docx* file from the *Ph0T0009_Test_definition_and_results_template.docx* template and save it in the repository of the specific project with the name of the file for the specific project. Defining the test of this template corresponds with Phase 3 of traditional FSM while the implementation and the collection of results correspond to Phase 5. Data requirement tests encompass a set of metrics to assess whether the Data requirement specifications have been fulfilled, the test definitions, and their corresponding outcomes.
- Generate the *REF_PhDMD0003_Data_Collection_Log.docx* document from *PhDMT0002_Data_Collection_Log_template.docx* and store it in the "PhDM Data Management" folder. This document collects information related to the description of the data collected in the project as well as information of the data generated. Completing this step is analogous to Phase 4 in the traditional FSM.
- Generate the *REF_PhDMD0005_Data_Preparation_Log.docx* file from the *PhDMT0003_Data_Preparation_Log.docx* template and store it in the "PhDM Data Management" folder. This template has been generated in order to collect all actions and decisions taken when preparing data. This file includes a guide that eases the generation and organization of the required information. Fulfilling this step would relate to the Phase 4 in the traditional FSM. Document collecting the information relative to cleaning, processing and annotating the data.

[7] The use of synthetic data together with real world data can produce the AI model to get biased during training. The use of synthetic data is subject to demonstrate that this bias is not included.

Reminder: -Update the state of REF_Ph0D0003_AI_Document_List.docx.
- Update the REF_Ph0D0013_AI_traceability_matrix.docx.

V&V activities

- Generate the *REF_PhDMD0002_Data_Requirements_Specifications_IR.xlsx*, *REF_PhDMD0010_Data_Requirements_Verification_Tests_IR.xlsx*, *REF_PhDMD0004_Data_Collection_Log_IR.xlsx* and *REF_PhDMD0006_Data_Preparation_Log_IR.xlsx* from *PhDMT0001_Data_Requirements_Specifications_IR.xlsx*, *Ph0T0009_Test_definition_and_results_IR.xlsx*, *PhDMT0002_Data_Collection_Log_IR.xlsx and PhDMT0003_Data_Preparation_Log_IR.xlsx*, respectively.

Reminder: -Update the state of REF_Ph0D0003_AI_Document_List.docx.

3.3.5 Learning Management – Phase LM (PhLM)

As previously mentioned, from this process we refer the reader to the *Ph3G0002_Learning_Management_guideline.docx* for further guidance. This document provides guidance for the Learning Management process. Learning Management is carried out in parallel with Data Management. It can be broken down into five steps, as illustrated in Figure 10. In that figure, the three numbered blue rhombuses represent inputs from the Data Management phase, which correspond to the training dataset (rhombus labelled with the number 1.1), the validation dataset (rhombus labelled with the number 1.2) and the verification datasets (rhombus with the number 2). Additionally, there is an extra red rhombus, which serves as a condition to check the results of the model evaluation. In the model evaluation fails to meet the criteria, a new iteration of the model design, model training and model evaluation steps must be performed until the model is successfully validated.

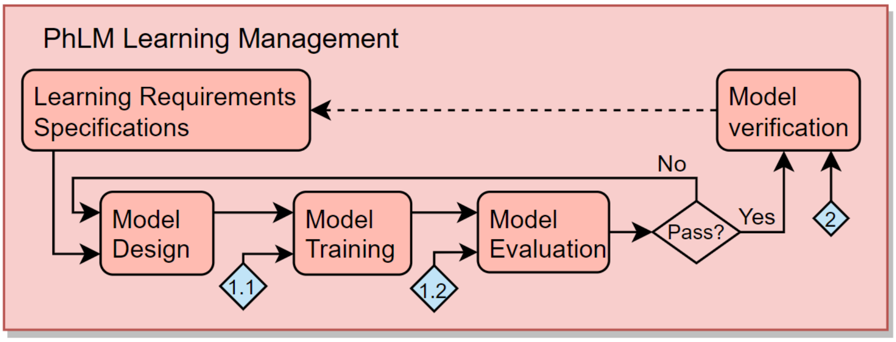


Figure 10. Learning Management phase

Additionally, the following artifacts must be generated and stored:

1. Trained model(s). Models that have undergone training on labeled datasets (training dataset) to learn patterns and relationships for making predictions on new data.
2. Evaluated model(s). Models that have been evaluated using separate datasets (validation dataset) to assess if they achieve a predefined performance and, in some cases, stops the training phase.
3. Verified Learning Model(s). Models that have been evaluated using separate datasets (verification dataset) to assess their generalization capabilities and identify potential issues.

The subsequent documents should be stored in the "Learning Management" subfolder that is part of the "AI-FSM" folder:

Phase Definition

- Generate the *REF_PhLMD0001_Learning_Requirements_Specification.docx* file from the *PhLMT0001_Learning_*Requirements_Specification_template.*docx* and store it in the repository of the specific project with the name of the file for the specific project. This step refines the DL requirements specifications previously defined in Phase 2, focusing on the needs of the Learning process.
- Generate the *REF_PhLMD0005_Learning_Requirements_Evaluation_Tests.docx* file from the *Ph0T0009_Test_definition_and_results_template.docx* and save it in the repository of the specific project with the name of the file for the specific project.
- Generate the *REF_PhLMD0007_Learning_Requirements_Verification_Tests.docx* file from the *Ph0T0009_Test_definition_and_results_template.docx* and save it in the repository of the specific project with the name of the file for the specific project.
- Generate the *REF_PhLMD003_Model_Election_Log.docx* file from *PhLMT0002_Model_Election_log_template.docx* and save it in the repository of the specific project with the name of the file for the specific project. Collecting the DL models designed and the criteria for the election of the most suitable DL model.

Reminder: -Update the state of REF_Ph0D0003_AI_Document_List.docx.
- Update the REF_Ph0D0013_AI_Traceability_Matrix.docx.

V&V activities

- Generate the *REF_PhLMD0002_Learning_Requirements_Specifications_IR.xlsx*, *REF_PhLMD0006_Learning_Requirements_Evaluation_Tests_IR.xlsx*, *REF_PhLMD0008_Learning_Requirements_Verification_Tests_IR.xlsx* and *REF_PhLMD0004_Model_election_log_IR.xlsx* from *PhLMT0001_Learning_Requirements_*Specifications_*IR.xlsx, Ph0T0009_Test_definition_and_results_IR.xlsx, Ph0T0009_Test_definition_and_results_IR.xlsx and PhLMT0002_Model_Election_log_IR.xlsx*, respectively.

Reminder: -Update the state of REF_Ph0D0003_AI_Document_List.docx

3.3.6 Inference Management – Phase IM (PhIM)

As it was previously mentioned, we refer the reader to the *PhIMG0003_Inference_Management_guideline.docx* for further guidance on this process. Its purpose is to provide guidance for the Inference Management phase. This phase can be broken down into five primary steps, as illustrated in Figure 11. In that figure, the blue rhombuses represent input from the Data Management phase, corresponding to the verification dataset (Rhombus labelled with the number 2).

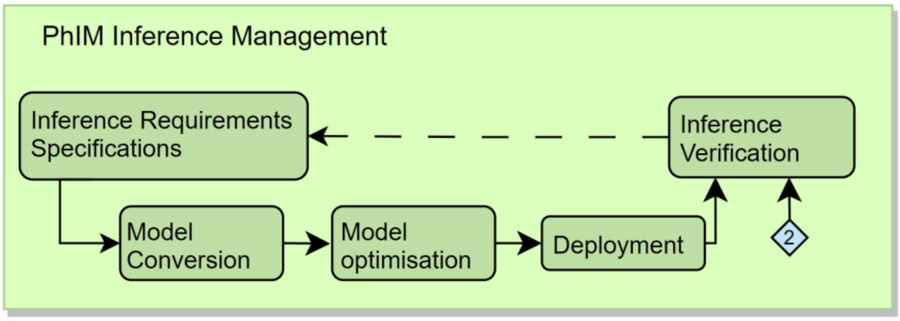


Figure 11. Learning Management phase

Additionally, the following artifacts must be generated and stored:

1. Converted Model. The initial model undergoes a conversion process to transform it into a format suitable for deployment or compatibility with a specific target inference platform.
2. Optimized Model. Following the conversion, the model may undergo optimization to enhance its performance, reduce its size, or adapt it for resource-constrained environments. Optimization aims to maintain or improve the model's accuracy while making it more efficient for deployment.
3. Verified Inference Model. The final outcome is the verified inference model, which has undergone a comprehensive verification process. This involves checking the optimized model (or the converted model in cases where the optimization step is not performed) against specified criteria to ensure that the model adheres to the inference requirements specifications.

The subsequent documents should be stored in the "Inference Management" subfolder, located in the "AI-FSM" folder.

Phase Definition

- Generate the *REF_PhIMD0001_Inference_Requirements_Specifications.docx* file from the *PhLMT0001_Inference_*Requirements_Specifications_template.*docx* and save it in the repository of the specific project with the name of the file for the specific project. This document collects the data requirements specifications refined from the DL requirements specification previously defined in phase 2.
- Generate the *REF_PhIMD0007_Inference_Requirements_Verification_Tests.docx* file from the *Ph0T0009_Test_definition_and_results_template.docx* and save it in the repository of the specific project with the name of the file for the specific project. Inference requirements tests encompass a set of metrics to assess whether the inference requirements specification have been fulfilled, the test definitions, and their corresponding outcomes.
- Generate the *REF_PhIMD003_Model_Conversion_Log.docx* file from *PhIMT0002_Model_Conversion_Log_Template.docx* and save it in the repository of the specific project with the name of the file for the specific project. Document collecting the information relative to the process of converting the model from training to inference.
- Generate the *REF_PhIMD005_Model_Optimization_Log.docx* file from *PhIMT0003_Model_Optimization_Log_template.docx* and save it in the repository of the specific project with the name of the file for the specific project. Document collecting the information relative to the process of optimizing the model.

Reminder: -Update the state of REF_Ph0D0003_AI_Document_List.docx.
- Update the REF_Ph0D0013_AI_Traceability_Matrix.docx.

V&V activities

- Generate the *REF_PhIMD0002_Inference_Requirements_Specifications_IR.xlsx*, *REF_PhLMD0004_Model_Conversion_Log_IR.xlsx*, *REF_PhLMD0006_Model_Optimization_Log_IR.xlsx* and *REF_PhLMD0008_Learning_Requirements_Verification_Tests_IR.xlsx* and from *PhIMT0001_Learning_Requirements_*Specifications*_IR.xlsx, PhIMT0002_Model_Conversion_Log_IR.xlsx, PhIMT0003_Model_Optimization_Log_IR.xlsx and Ph0T0009_Test_definition_and_results_IR.xlsx*, respectively.

Reminder: -Update the state of REF_Ph0D0003_AI_Document_List.docx

3.4 Mapping the AI-FSM with current standards

This section focuses on mapping AI-FSM with ISO/IEC TR 5469 standard and ASPICE4.0.

3.4.1 Mapping ISO/IEC 5469 with AI-FSM

As previously outlined in "D1.1 Requirements, Success Criteria and Platforms", ISO/IEC TR 5469, titled "Artificial Intelligence – Functional Safety and AI Systems", seeks to address the integration of AI-based solutions into safety-critical systems. Its objectives include identifying relevant properties, safety risk factors, available methodologies, and potential limitations to ensure the appropriate implementation of AI methods in safety functions. Importantly, this standard is not tied to any specific application domain. At the time of writing D1.1, it was still in the development phase, and the information was extracted from early drafts. The current deliverable has been written based on the just-published first version of the standard.

In accordance with this standard, the AI-FSM has embraced an approach rooted in the conventional functional safety lifecycle, which is based in the V-model. This methodology involves identifying and modifying the V-model to accommodate the unique characteristics of the AI lifecycle. Specifically, the standard draws upon ISO/IEC 5338 "Information technology — Artificial intelligence — AI system life cycle processes" [13] to delineate the processes inherent in the AI lifecycle. Furthermore, the standard includes an informative annex mapping the technical processes of ISO/IEC 5338 and the phases of the IEC 61508 standards, without delving into the specifics.

ISO/IEC TR 5469 proposes to use the three-stages realization principle depicted in Figure 12 to generate acceptance criteria. These stages (data acquisition, knowledge induction and processing and generation of outputs) directly corresponds with Data Management, Learning Management and Inference Management of the AI-FSM. As ISO/IEC TR 5469 outlines, that principle is traditionally used in three steps: First one is related to the definition of the desirable properties for each phase. Second, identification of topics related to the previously defined properties and those methods and techniques that can be employed to their achievement. Finally, that methods are employed to generate an acceptance argument that satisfies the desirable properties. That is directly aligned with the proposed lifecycle in AI-FSM in which of each of the phases start with the definition and refinement of specifications and tests to verify the fulfilment of those specifications, a set of actions to be performed regarding the specific phase and finally the verification of that set of tests to ensure compliance with the requirements.

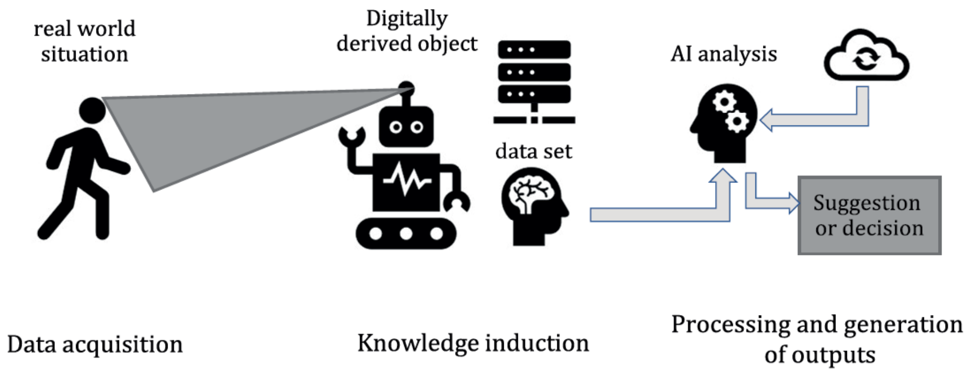


Figure 12. Three-stages realization principle [5]

This deliverable outlines in Table 7, the main points that have been covered following recommendations of the ISO/IEC TR 5469 along with some considerations that can be addressed to complement AI-FSM:

Table 7. Recommendations adopted in the AI-FSM

Lifecycle phase	Recommendations of ISO/IEC TR 5469 adopted in the AI-FSM
DL Requirements Specification	The AI-FSM guides and provides examples regarding the definition and refinement of requirements at different stages of the AI lifecycle. However, it specifies that these requirements are project-dependent, emphasizing that the presented requirements specification does not replace expert judgment on technical content. Similarly, ISO/IEC TR 5469 defines a set of specific requirements or properties indicating that their formulation can be based on existing standards, while anticipating the development of new ones covering the AI peculiarities. In terms of techniques and measures for application in safety-related systems involving AI, ISO/IEC TR 5469 conducts an informative analysis of the applicability in those presented in Annexes A and B of IEC 61508-3:2010. While the AI-FSM does not analyze them, it leaves the selection of the most appropriate techniques and measures to the expertise of the safety designer in the specific safety-related system domain.
PhDM Data Management	ISO/IEC TR 5469 collects through the document a set of recommendations associated with the datasets that shall be collected in the data acquisition phase. Among the training data requirements, we can list completeness and representativeness of the input domain, sufficiency diversity in the data or proper distribution of the application context, among others. Furthermore, test data requirements must be representative of the operational scenarios, cover variations of situations involving risks or be diverse and sufficient enough to properly verify that training has been properly carried out, among other requirements. Additionally, this standard states requirements related to clearly specify sets of data attributes or ensure the independence between test and training data and therefore, independence between the teams collecting

	the data and the teams performing the tests or ensure that data are free of malicious modifications or alterations (ensuring the credibility of data source and data collection processes), which can be englobe as data requirements and requirements related to the process respectively. For that, AI-FSM decomposes the requirements related to data management phase into: dataset requirements specification, data requirements specifications and data processes requirements specification (involving data collection and data preparation). The previously defined requirements are included and collected in those groups, aligning the AI-FSM with the ISO/IEC TR 5469.
PhLM Learning Management	ISO/IEC TR 5469 focuses of identifying properties of AI systems and their associated risks leaving aside the specification of the application phase. AI-FSM has collected the recommendations proposed by the standard according to their phase aiming to ease the development process and avoiding systematic errors. Among them can be cited the detection and mitigation of training errors during the training phase, avoiding over-fitting of the model or ensuring the robustness of the model. One of the aspects considered out of the scope of the current version of the AI-FSM relates to the continuously monitoring the AI system to provide incident feedback one the model has been validated. This aspect, worthy of consideration, is expected to be covered in future versions.
PhIM Inference Management	Mapping between AI-FSM and ISO/IEC during the inference management phase is quite straightforward. It underscores the importance of ensuring portability between training and inference platforms to prevent translational errors caused by memory incompatibilities in data management. Moreover, it indicates the feasibility of applying most of the techniques outlined in IEC 61508-3 for safe model deployment, including fault detection during inference and diverse monitoring with redundant systems. However, there is a notable difference currently not addressed in the AI-FSM concerning actuation and the requirement to provide evidence of the model's safety performance once it has been approved and is in operation. This aspect is anticipated to be addressed in future extensions of the AI-FSM.

3.4.1.1 Some early conclusions

After assessing the compliance of SAFEXPLAIN AI-FSM with ISO/IEC TR 5469, it appears that there are no discrepancies between SAFEXPLAIN AI-FSM and the ISO/IEC TR 5469 standard. One of the discussion topics during the review meeting of the safety technical assessment task conducted with TÜV Rheinland addressed this point (this assessment will be introduced in Section 3.5), leading TÜV Rheinland to conclude that SAFEXPLAIN AI-FSM is aligned with ISO/IEC TR 5469.

Additionally, the ISO/IEC TR 5469 standard delves into the identification of specific AI properties and risk factors, identifying issues related to V&V_techniques, proposing solutions, as well as mitigation and control measures. These aspects of the development lifecycle that can be employed when applying the AI-FSM to complement it.

3.4.2 Mapping ASPICE 4.0 with AI-FSM

The Automotive Systems Process Improvement and Capability dEtermination (ASPICE [11]) ML Model was originally developed according to the "Plug-in" concept as the Hardware model by a dedicated Working Group withing the supervision of Verband der Automobilindustrie (VDA), quality standards developed by Germany's national automaker, and International Assessor Certification Scheme (Intacs™) association. It started later than other 'plugin' models for other domains but as ML is affecting many critical aspects of modern automotive development it was given a special priority for integration in the full ASPICE Process Reference Model (PRM)/ Process Assessment Model (PAM) 4.0.

In the following picture an early public presentation of the key ML activities is reproduced. It shows the original idea of "positioning" the 4 new Machine Learning Engineering (MLE) processes as a distinct "mini-V" taking place of the "tip of the V" in the traditional Software Engineering (SWE) V-model. This mini-V includes a separate process belonging to a different process group, specifically created for ML Data Set Management.

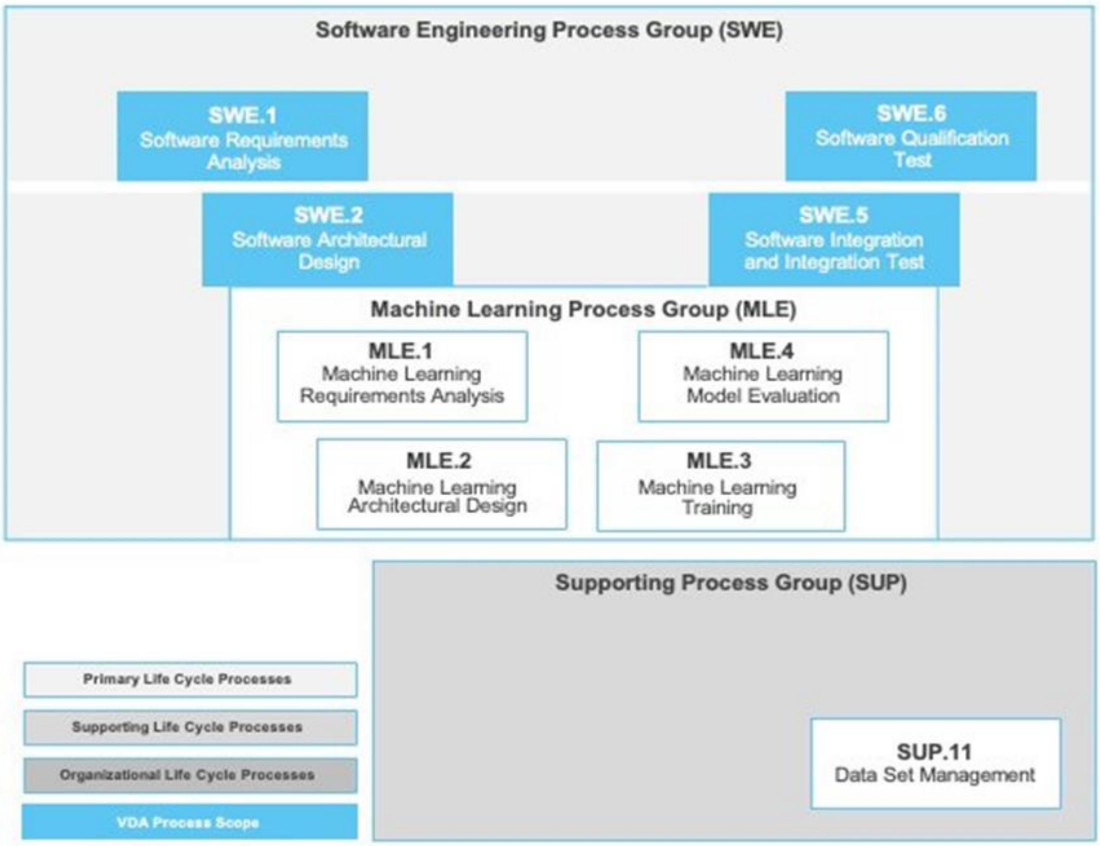


Figure b. SWE process group including the MLE and SUP process group.

3.4.2.1 Current status of ASPICE MLE as integrated in ASPICE PAM 4.0

The scheme just presented has been further elaborated and finally included into ASPICE 4.0, Annex C.3 "Integration of Machine Learning Engineering Processes", where, expectedly, special relevance is given to the concept of ML architecture:

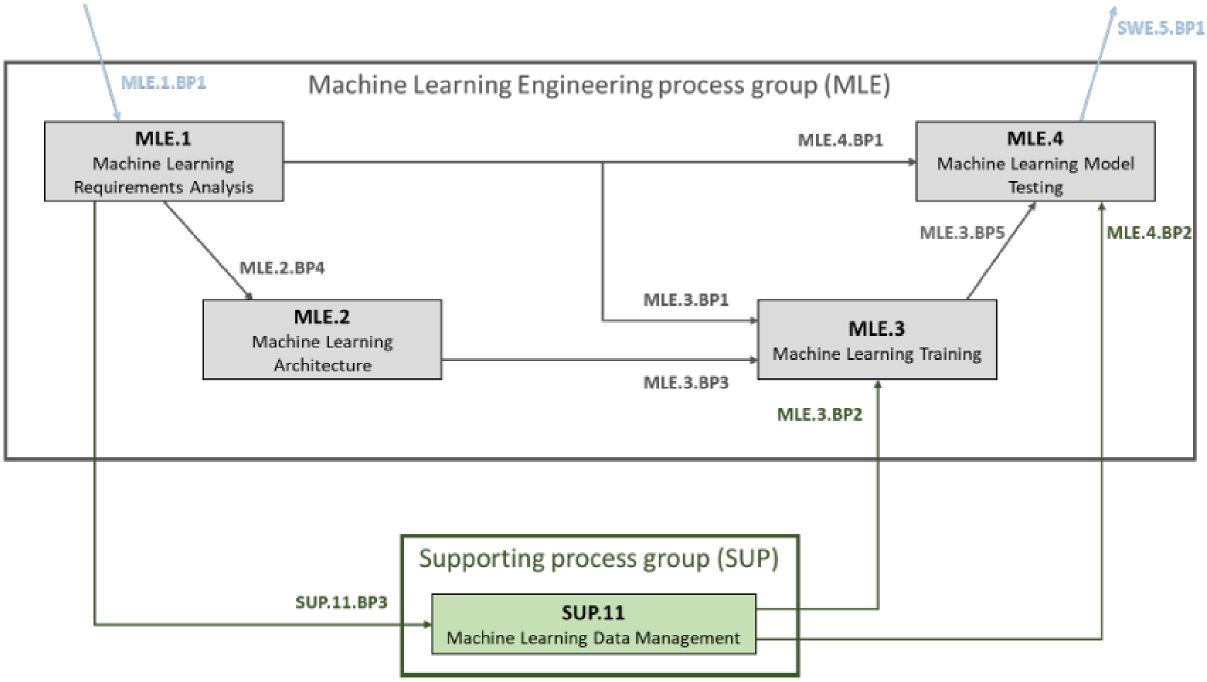


Figure 13. Interdependencies within MLE and SUP.11 (Figure C.4 in [11])

In the Annex C.3 even a specific example of ML architecture is offered, in order to support the following statement: *"ML architecture typically consists of an ML model and other ML architectural elements, which are other (classical) software components […] and provided to train, test, and deploy the ML model."*

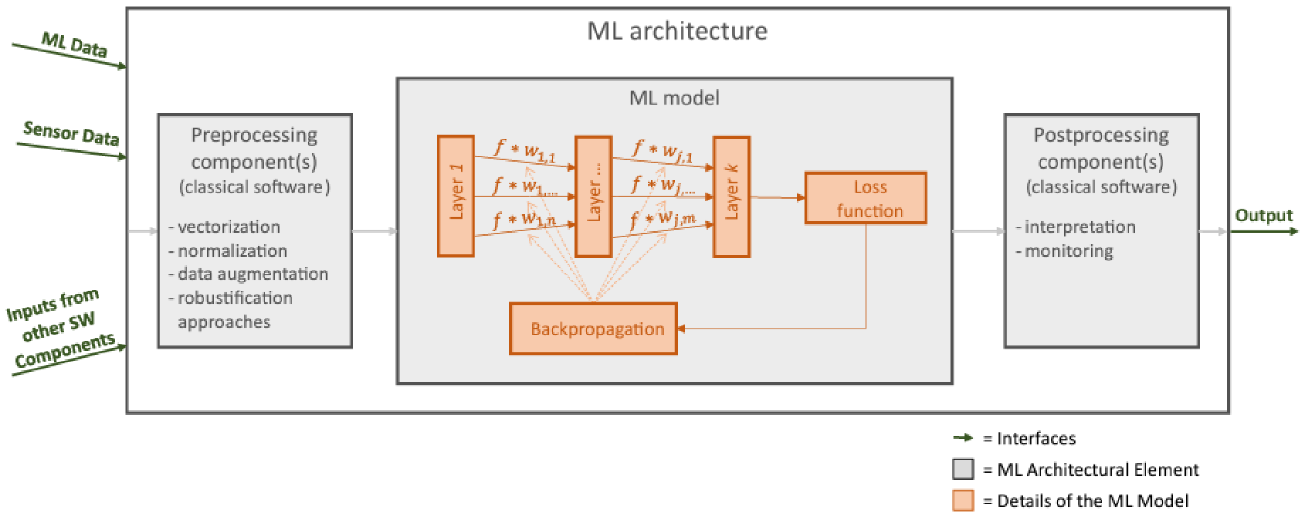


Figure 14. Example of an ML Architecture (Figure C.5 in [11])

Following the general ASPICE model, each of the processes are defined with a set of output work-products (WPs), now called Information Items (IIs). Not all of them are equally characterizing the processes, what follows is a reasoned list of the 'most characterizing' WPs (or IIs) for each of the five MLE processes[8]:

[8] This list includes the ID number and the name of the most characteristic IIs. We refer the reader to Annex B of ASPICE 4.0 for an in-depth explanation, including a list of potential characteristics associated with them.

MLE.1 Machine Learning Requirements Analysis

- *None specific II, but specific* ML requirements *are expected as a subset of SW requirements.*

MLE.2 Machine Learning Architecture

- 04-51 ML architecture (includes 01-54 Hyperparameters)
- 01-54 Hyperparameter

MLE.3 Machine Learning Training

- 08-65 ML training and validation approach (a.k.a. strategy)
- 03-51 ML data set
- 01-53 Trained ML model

MLE.4 Machine Learning Model Testing

- 08-64 ML test approach (a.k.a. strategy)
- 03-51 ML data set
- 11-50 Deployed ML model
- 13-50 ML test result

SUP.11Machine Learning Data Management

- 19-50 ML data quality approach (a.k.a. strategy)
- 16-52 ML data management system (part of Configuration Management)
- 03-53 ML data (all ML-related data, includes 03-51 ML data set)

3.4.2.2 Initial comparison ASPICE / SAFEXPLAIN ML models (I)

An initial, tentative comparison between the processes of the MLE models of ASPICE on one side and AI-FSM has been made and here a summary of the earliest findings is presented.

- **MLE.1 *vs* DL Requirements specifications.** Mapping makes clear that all DL requirements are a subset/derived from SW requirements and that Ph2 DL Architecture specifications are there to satisfy those requirements.
- **MLE.2 *vs* Ph2 DL Architecture specifications.** Mapping makes clear that all Ph2 DL Architecture specifications are actually design (part of the overall SW architecture), and that needed complementary traditional architectural design descriptions (elements, interfaces…) are expected to be defined.
- **MLE.3 *vs* PhLM Learning Management.** The "learning requirements specifications" appears to be mappable with the "training and verification/validation approach" and "ML data set"; the Trained Model is a common basic outcome.
- **MLE.4 *vs* PhIM Inference Management.** The "inference requirements specifications" appears to be mappable with the "ML test approach" and "ML data set"; the Deployed Model (i.e., Tested, Re-verified) is a common basic outcome.
  It is unclear the reason for the major difference in the naming (i.e. "Model Testing" vs "Inference"); please note that in early ASPICE MLE draft MLE.4 is called "ML Model Evaluation".
- **SUP.11 *vs* PhDM Data Management.** Mapping is quite straightforward between *Practices and IIs* on one side and *Activities and outcomes* on the other.

3.4.2.3 Some early conclusions

It appears there are no significant gaps in the SAFEXPLAIN AI-FSM model in terms of compliance to the ASPICE MLE model; SAFEXPLAIN consortium on one side and VDA-Quality Management System (QMS) and Intacs™ on the other side have already expressed strong interest in collaborating towards further alignment.

A big advantage in adopting both approaches is that SAFEXPLAIN AI-FSM model (like EASA's guidelines and other draft standards dedicated to "Safe AI") are already incorporating FuSa aspects while the ASPICE MLE Model is "pure Quality Management (QM)", thereby allowing a process "discipline decomposition", that has proved quite effective with ASPICE and ISO 26262 in the last decade.

By distinguishing "from the start" Process Quality aspects from FuSa aspects of ML/DL applications, a paradigm can be established to be further extended to Cybersecurity, too, addressing the most critical pillars of *Trustworthy AI*, according to both of the most important pieces of AI regulation already in place, the EU AI Act and the US President Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

3.5 Safety technical Assessment and Expert certification review

The safety technical assessment and expert certification review is associated with T2.5, scheduled to take place from month 13 to month 36. This task encompasses two main activities: one involving the AI-FSM and the other pertaining to the railway safety concept. As of the writing of this deliverable (M16), the activity related to the AI-FSM has been completed, with the assessment of the railway safety concept planned for future deliverables.

The methodology followed to perform this assessment is depicted in Figure 15, along with the dates on which each action has been performed:

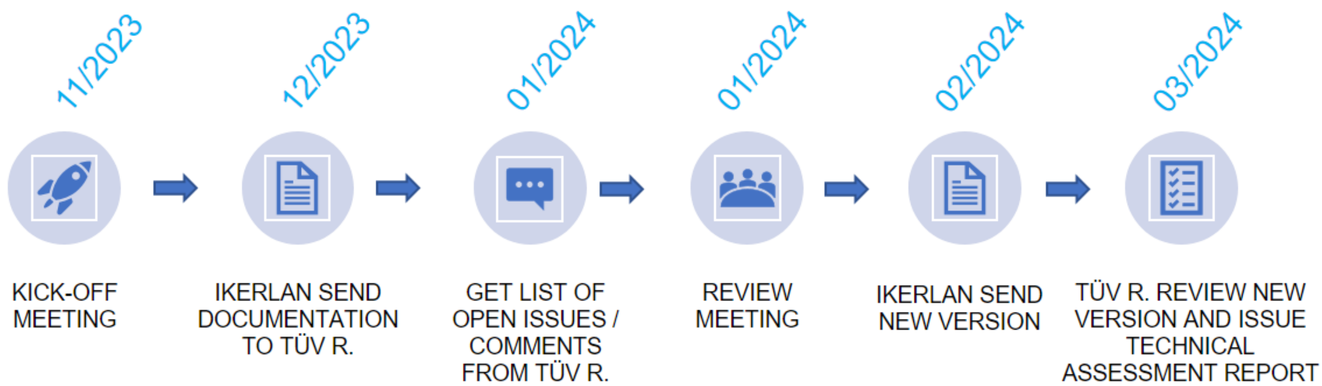


Figure 15. AI-FSM review steps and plan

According to this methodology, the current deliverable provides the presentation of the review meeting that include the main reviews from TÜV Rheinland entity (Annex A). The TÜV Rheinland assessment emphasizes the validity of AI-FSM approach. Important topics addressed during review meetings include general document structure, dataset usage, model selection, the use of the term "validation", data representativeness, and possible conflicts between robustness and the inclusion of corner cases in the different datasets. The review meeting focused on information exchange and experience sharing related to these topics. TÜV Rheinland considers that the AI-FSM content is deemed adequate for a research project, meeting the requirements of standards such as IEC 61508 and ISO/IEC TR 5469. The document covers essential aspects outlined in ISO/IEC TR 5469, including analysing AI technology and selecting an appropriate life cycle model. They conclude that the AI-FSM describes rigorously and substantially the important points to form a basis for future work.

4 DL Safety Lifecycle for DL-software V&V

In the previous chapter has been introduced the AI-FSM, a Functional Safety lifecycle extension to cover ML/DL processes and allow their assessment according to the current ISO/IEC 61508 (Functional Safety (FuSa) of E/E/PE Safety-related Systems). AI-FSM has already successfully passed a first review by both TUV and EXIDA.

In this chapter is explained the developed AI-V&V strategy and associated methods for the V&V of ML/DL components. Such approach extends the traditional FuSa approach from addressing only "hazards caused by malfunctioning" (as in ISO/IEC 61508 and ISO 26262), to also include "hazards resulting from functional insufficiencies" (as in ISO 21448, a.k.a. SOTIF).

The main goal of the V&V strategy is to:

- evaluate the potentially hazardous scenarios,
- provide the necessary evidence (e.g., test reports, …) to demonstrate the ability of the sense-plan-act elements (sensors, processing/decision algorithm) to provide their proper functionality,
- provide the necessary evidence (e.g., test reports, …) to demonstrate the robustness of the system or functionality against the triggering condition,
- provide the necessary evidence (e.g., test reports, …) to demonstrate the absence of unreasonable risk due to hazardous behaviour of the intended functionality or the achievement of an acceptable risk level.

To achieve the main objective of the V&V strategy, the following test methods, according to ISO 21448 and ISO 26262, were considered:

- ISO 21448 (testing activities are focused on the scenarios):
- Analysis of environmental conditions and operational use cases (Method H, Table 6)
- Analysis of triggering conditions (Method N, Table 6)
- ISO 26262 (testing activities are focused on proving the safety requirements implementation and performance of safety mechanism):
- Requirements-based test (Method 1a - ISO 26262-4 table 13)
- Fault injection test (Method 1b - ISO 26262-4 table 13; Method 1d - ISO 26262-4 table 14)
- Long-term test (Method 1c - ISO 26262-4 table 13; Method 1b - ISO 26262-4 table 14; Method 1d - ISO 26262-4 table 16)
- Performance test (Method 1a - ISO 26262-4 table 14)

The following section provides an explanation of the main parts of the proposed V&V strategy. This section is decomposed according to the steps to be carried out during the proposed V&V strategy:

1. Section 4.1 outlines the definition of a scenario catalogue, based on selected use cases and applicable ODDs.
2. The definition of the scenario catalogue allows the derivation of the test cases to verify the set of intended functionalities in the subsection 4.2.
3. Finally, subsection 4.3 provides an application example in the automotive domain.

4.1 Catalogue of Scenarios

The purpose of the scenario catalogue is to define the set of known hazardous and not-hazardous scenario in which the intended functionality is intended to operate.

For each scenario shall be identified the scenario conditions/constraints, such as, but no limited to the following's ones:

- The Ego vehicle[9] conditions/constraints (e.g., vehicle speed, lateral acceleration, longitudinal acceleration/deceleration, lateral/longitudinal/angle offset with respect to (w.r.t.) the target, …)
- The target vehicle conditions/constraints (e.g., vehicle speed, lateral acceleration, longitudinal acceleration/deceleration, lateral/longitudinal/angle offset w.r.t. the ego vehicle, …)
- Environmental conditions (e.g., day or night lux threshold, weather condition)
- Road surface (e.g., µ condition)
- Pre-conditions (e.g., vehicles speed, vehicles path, steering inputs, throttle pedal inputs, ….)
- The probability of exposure (duration) of the scenario derived by the combination of probability of exposure values related to the considered scenario. The probability values are derived from VDA-702:2015 [14].

Two different scenario catalogues are available, an extended version including several scenarios (see "D2.1_Annex_B_Scenario_Catalogue_V1R3.pdf", Section 7.2: Annex B) and a reduced version (see "D2.1_Annex_C_V&V_Strategy_application_V1R1.pdf", Section 7.3: Annex C) aligned with the automotive use case developed by NAVINFO in D5.1

4.2 Test Cases

The Test cases shall be defined over all the architectural levels of application, as depicted in Figure 16:

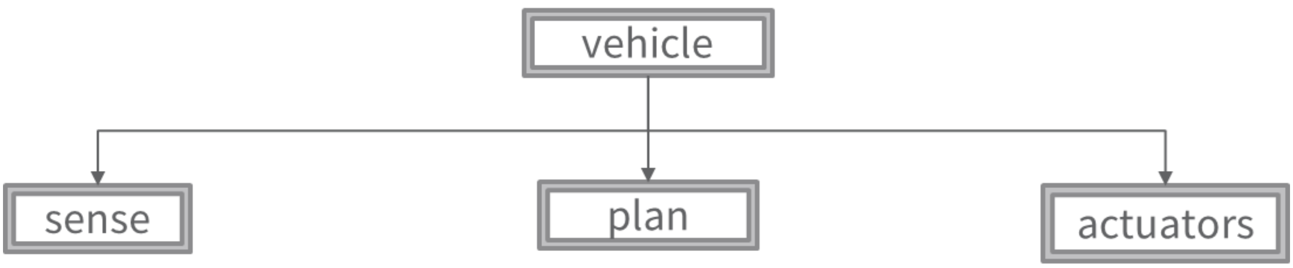


Figure 16. Architectural levels of application

By Test case we mean a set of condition (on a certain component/element, road conditions, weather conditions, driver inputs, etc) needed to perform controlled testing activities. The main scope of a test case is to determine, after their execution, if the features within a system are performing as expected and to confirm that the system satisfies all related standards, and requirements allocated to it.

[9] Ego vehicle - vehicle fitted with functionality that is being analysed [8]

The Application considered in this case is related to the Automotive domain, but the proposed V&V strategy can be applied to other domains too (e.g., railway, aerospace, …) by applying the proper adaptation on considered use case and scenarios.

Starting from the test cases defined at vehicle level, the test cases for the sub-elements are derived to allow the evaluation of the sense-plan-act components behaviour.

4.3 Examples in the automotive domain

In the following subsection is reported an example of one of the scenarios included in the V&V strategy application (see "D2.1_Annex_C_V&V_Strategy_application_V1R1.pdf", Section 7.3: Annex C) adapted to the automotive use case developed by NAVINFO in D5.1.

In the example the following information are provided:

- A description of the Scenario with its conditions/constraints.
- A description of Test Cases at vehicle level and the related expected behaviour at vehicle, sense, plan and actuator levels.

4.3.1 Example of Scenario Catalogue

The scenario provided in this deliverable represent a vehicle driving following a target vehicle on highway, as depicted in Figure 17. When the distance with the target vehicle decreases so that the driver is in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle.

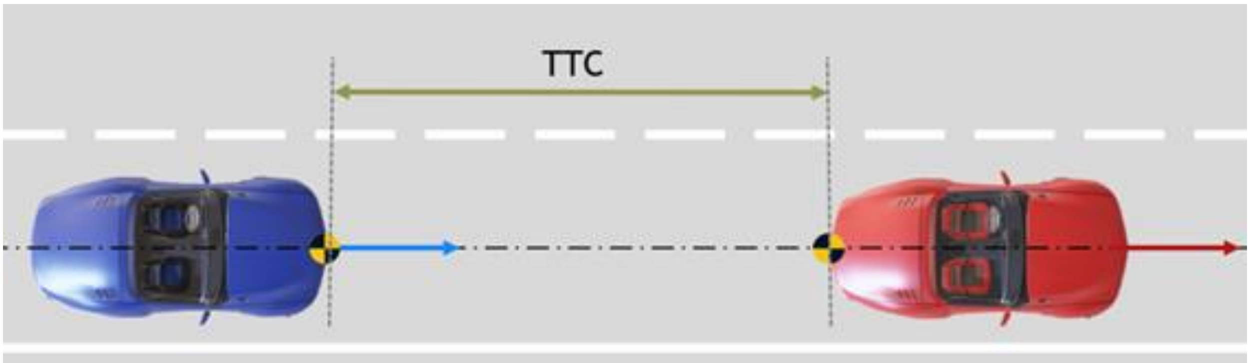


Figure 17. Visual representation of the scenario example

The scenario conditions/constraints are the followings:

1. The Ego vehicle (depicted in blue Figure 17) drives with a longitudinal acceleration lower than 2 m/s^2 towards a moving target vehicle (depicted in red Figure 17) and is at a distance corresponding to a Time To Collision (TTC) of at least 4 s.
2. The Ego vehicle speed range is [50 km/h, 130 km/h]
3. The target vehicle drives at 80 km/h

- The following environmental conditions shall be present:
  - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
  - Dry and night with maximum 10 lux
- Road surface is asphalt or concrete.
- The following pre-conditions shall be respected:
  - Both vehicles shall keep steady speed and path.

- Steering angle shall be lower than the override threshold.
- Yaw rate shall be lower than the override threshold.

4. The probability of exposure (duration) of these scenario conditions is E2, considering the following combinations:
   - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time): E.g., 10% of 8000h = 800 h
   - Driving with normal longitudinal acceleration (<2m/s2) – E4 (>10 % of average operating time): E.g., 10% of 8000h = 800 h

4.3.2 Driving in Highway– E4 (>10 % of average operating time): E.g., 10% of 8000h = 800 h **Example of Vehicle level test case**

The following intended functionality capabilities shall be demonstrated:

4.3.2.1 *Step 1*. Track the red target vehicle and evaluate it as no-collision relevant.

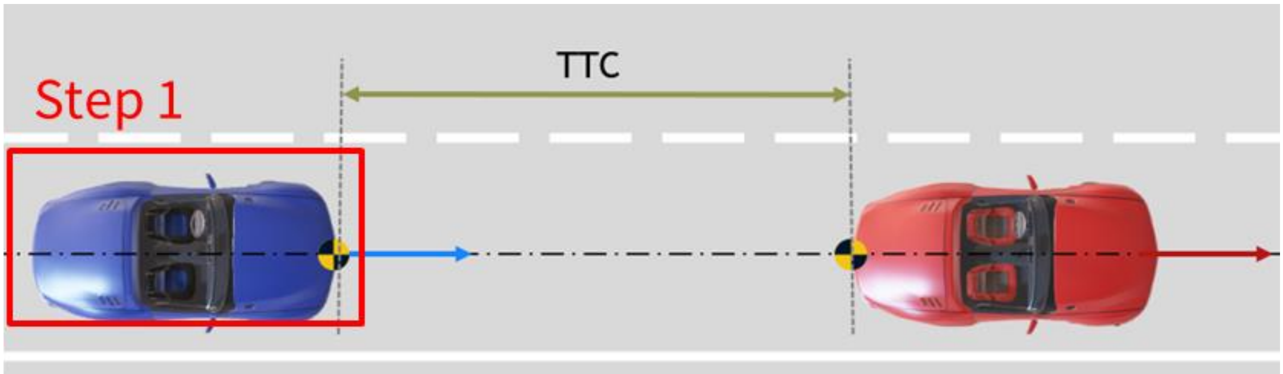


Figure 18. Vehicle level test case Step 1

Pass/Fail Criteria:

1. Vehicle level:
   - Warning = It is not expected the provision of any warning to the driver.
   - Braking = It is not expected the provision of braking intervention.
2. Sense level:
   - It is expected that the object is being detected and classified as a Car.
3. Logic level:
   - It is expected that the Object, considering the safety distance between the ego-vehicle and the target vehicle, is being evaluated as "no-collision" relevant.
4. Actuator level:
   - Warning = It is not expected the provision of any warning to the driver.
   - Braking = It is not expected the provision of braking intervention.

4.3.2.2 ***Step 2*****. When the distance, between the ego vehicle and the red target vehicle, is equal to or less than the Time To Warning (TTW), the intended functionality shall evaluate the red target vehicle as collision relevant and provide at least 0,8 s before the start of the emergency braking the visual and audible warning to the driver (UN Regulation N° 152 clause 5.2.1.1, 5.5.1).**

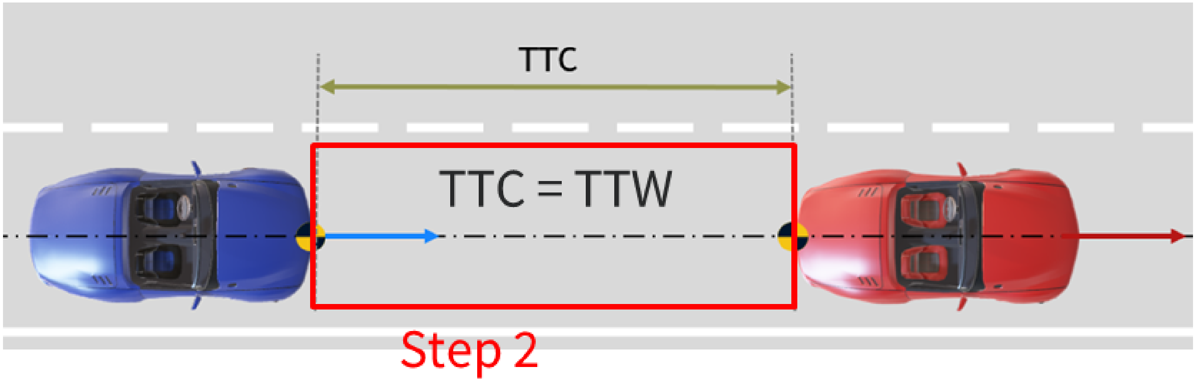


Figure 19. Vehicle level test case Step 2

Pass/Fail Criteria:

1. Vehicle level:
   - Warning = It is expected the provision, at least 0.8 s before the start of the emergency braking according to UN Regulation N° 152 [15][10], of audible and visual warning to the driver.
   - Braking = It is not expected the provision of braking intervention.
2. Sense level:
   - It is expected that the object is being detected and classified as a Car.
3. Logic level:
   - It is expected that the Object, considering that the safety distance between the ego-vehicle and the target vehicle is equal to TTW, is being evaluated as “collision” relevant.
4. Actuator level:
   - Warning = It is expected the provision, at least 0.8 s before the start of the emergency braking according to UN Regulation N° 152, of audible and visual warning to the driver.
   - Braking = For this step it is not expected the provision of braking intervention.

[10] UN Regulation N° 152 is the Regulation applicable for the approval of vehicles of Category M1 and N1 concerning an on-board system to:

- Avoid or mitigate the severity of a rear-end in lane collision with a passenger car.Avoid or mitigate the severity of an impact with a pedestrian

4.3.2.3 **<u>Step 3</u>. When the distance, between the ego vehicle and the red target vehicle, is equal to the Time To Collision AEB (TTC AEB), the intended functionality shall, if no driver reaction occurs, shall decelerate the vehicle providing at least 5.0 m/s2 (UN Regulation N° 152 clause 5.2.1.2).**

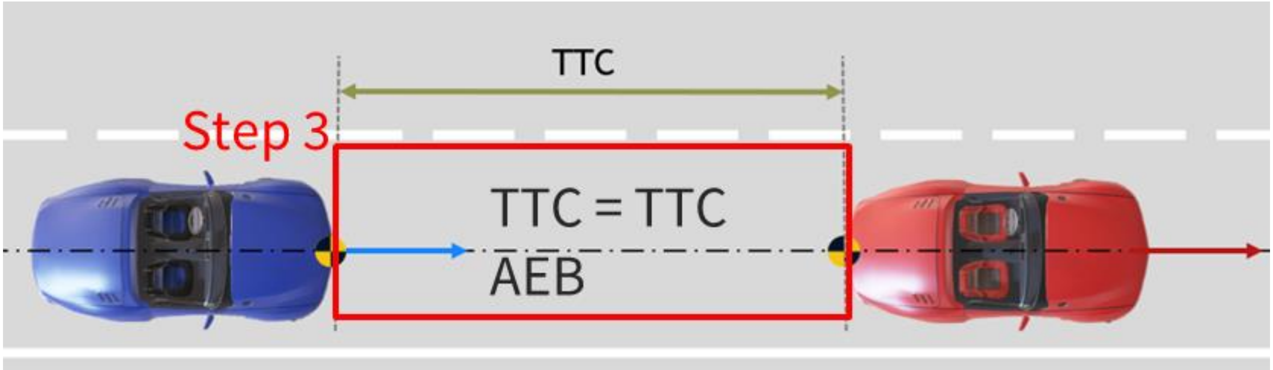


Figure 20. Vehicle level test case Step 3

Pass/Fail Criteria:

1. Vehicle level:
   - Warning = It is expected the provision, at least 0.8 s before the start of the emergency braking according to UN Regulation N° 152, of audible and visual warning to the driver.
   - Braking = It is expected a deceleration of at least 5 m/s2, according to UN Regulation N° 152.
2. Sense level:
   - It is expected that the object is being detected and classified as a Car.
3. Logic level:
   - It is expected that the Object, considering that the safety distance between the ego-vehicle and the target vehicle is equal to TTC AEB, is being evaluated as “collision” relevant.
4. Actuator level:
   - It is expected the provision, at least 0.8 s before the start of the emergency braking according to UN Regulation N° 152, of audible and visual warning to the driver.
   - It is expected a deceleration of at least 5 m/s2, according to UN Regulation N° 152.

5 Acronyms and Abbreviations

Below is a list of acronyms and abbreviations employed in this document:

- AEB – Autonomous Emergency Braking
- AI – Artificial Intelligence
- AI-FSM – Artificial Intelligence - Functional Safety Management
- ASPICE – Automotive SPICE
- DL – Deep Learning
- EASA – European Aviation Safety Agency
- FSM – Functional Safety Management
- FuSa – Functional Safety
- II – Information Items
- ISO – International organization for standardization
- ML – Machine Learning
- MLE – Machine Learning Engineering
- NN – Neural Network
- ODD – Operational Design Domain
- PAM – Process Assessment Model
- PRM – Process Reference Model
- QM – Quality Management
- QMS – Quality Management System
- SOTIF – Safety Of the Intended Functionalities
- SPICE – Systems Process Improvement and Capability dEtermination
- SWE – Software Engineering
- TTC – Time To Collision
- TTW – Time To Warning
- VDA – Verband der Automobilindustrie
- V&V – Verification and Validation
- WP – Work Product

6 Bibliography

[1] T. Gantevoort, «Functional Safety Management certificate related to IEC 61508 Parts 1-7:2010 - Phase 10 (E/E/PE safety related Systems Realisation), Certified Company: IKERLAN Technological Research Centre, Certificate No. 968/FSM 138.01/16,» TÜV Rheinland Industrie Service GmbH Automation and Functional Safety, 2016.

[2] IEC, «IEC 61508(-1/7): Functional safety of electrical / electronic / programmable electronic safety-related systems,» 2010.

[3] J. Perez-Cerrolaza, J. Abella, M. Borg, C. Donzella, J. Cerquides, F. J. Cazorla, C. Englund, M. Tauber, G. Nikolakopoulos y J. L. Flores, «Artificial Intelligence for Safety-Critical Systems in Industrial and Transportation Domains: A Survey,» *ACM Comput. Surv.,* 2023.

[4] A. Brando, I. Serra, E. Mezzetti, F. J. Cazorla, J. Perez-Cerrolaza y J. Abella, «On Neural Networks Redundancy and Diversity for Their Use in Safety-Critical Systems,» *Computer,* vol. 56, pp. 41-50, 2023.

[5] ISO/IEC JTC 1/SC 42 Artificial intelligence, «ISO/IEC DTR 5469 Artificial intelligence — Functional safety and AI systems,» 2023.

[6] ISO/TC 22/SC 32 Electrical and electronic components and general system aspects, «ISO/CD PAS 8800 Road Vehicles — Safety and artificial intelligence,» 2023.

[7] European Union Aviation Safety Agency (EASA), «EASA Concept Paper: guidance for Level 1 & 2 machine learning applications,,» 2023.

[8] ISO, «21448 Road vehicles - Safety of the intended functionality,» 2022.

[9] SAFEXPLAIN, D2.2: SAFEXPLAIN DL safety architectural patterns and platforms, Deliverable of the HEU SAFEXPLAIN project, Grant Agreement No. 101069595, 2024.

[10] R. Hawkins, C. Paterson, C. Picardi, Y. Jia, R. Calinescu y I. Habli, «Guidance on the Assurance of Machine Learning in Autonomous Systems (AMLAS),» Assuring Autonomy International Programme (AAIP), University of York, 2021.

[11] VDA QMC Working Group 13, «Automotive SPICE Process Assessment / Reference Model,» 06 06 2023. [En línea]. Available: https://vda-qmc.de/wp-content/uploads/2023/06/Automotive-SPICE-PAM-40-Gelbbandrelease.pd. [Último acceso: 09 2023].

[12] IEC, «IEC TS 6254 - Information technology — Artificial intelligence — Objectives and approaches for explainability of ML models and AI systems, Under Development».

[13] ISO/IEC, «ISO/IEC WD 5338 Information technology — Artificial intelligence — AI system life cycle processes,» Dec 2023. [En línea]. Available: https://www.iso.org/standard/81118.html.

[14] VDA 702, «Situationskatalog E-Parameter nach ISO 26262-3,» 2015.

[15] UN Regulation No 152, «Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking System (AEBS) for M1 and N1 vehicles,» 2020.

7 Annexes

This section collects the annexes attached together with the deliverable D2.1.

7.1 Annex A: Review meeting presentation

This document refers the reader to the attached document "D2.1_Annex_A_Review_meeting.pdf". In that presentation is included the main set of reviews from TÜV Rheinland entity.

7.2 Annex B: Scenario Catalogue

This document refers the reader to "D2.1_Annex_B_Scenario_Catalogue_V1R3" attached document, which contains the entire automotive Scenario catalogue.

7.3 Annex C: V&V Strategy Adapted to Automotive Use Case

This document refers the reader to "D2.1_Annex_C_V&V_Strategy_application_V1R1" attached document, which contains the scenario catalogue adapted to the Automotive use case and related test cases.

SAFEXPLAIN

Safe and Explainable
Critical Embedded Systems based on AI

Safe and explainable critical embedded systems based on AI

1st review meeting

Javier Fernández

ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

Funded by the European Union

This project has received funding from the European Union's Horizon Europe programme under grant agreement number 101069595.

Attendees

ikerlan
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

- Irune Agirre
- Javi Fernández
- Lorea Belategi
- Ana Adell
- Irune Yarza

TÜVRheinland®
Precisely Right.

- Hendrik Schäbe
- Ralf Röhrig

BSC Barcelona Supercomputing Center
Centro Nacional de Supercomputación

- Jaume Abella
- Francisco Cazorla

Agenda

- TÜV Rheinland collaboration
- Contextualization
- Proposed Lifecycle
- AI-FSM Generalities
- AI-FSM in-depth

TÜV Rheinland collaboration

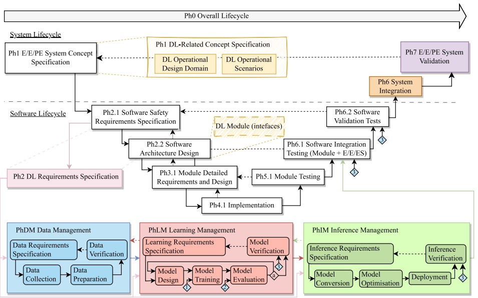
IKERLAN requests TÜV Rheinland to carry out the following tasks:

WP 0	Virtual kick off meeting to introduce the project and the planned activities to TÜV
WP 1	AI-safety functional safety management (AI-FSM): IKERLAN is currently working on the adaptation of Ikerlan's SIL 3 FSM to consider new procedures required by AI systems (data management, training, inference). IKERLAN requests TÜV Rheinland to review the documentation (FSM guidelines and templates) and provide feedback and a review report.
WP 2	Railway safety concept: TÜV review and assessment of a safety concept, where AI is used for visual perception tasks of a railway safety function for collision avoidance.

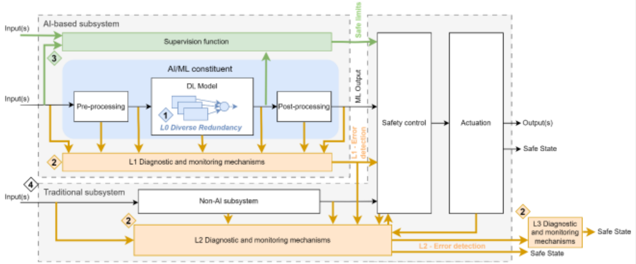
[Quotation]

- WP0: This meeting
- WP1- Activity 1: AI-FSM
- WP2- Activity 2: Railway safety concept

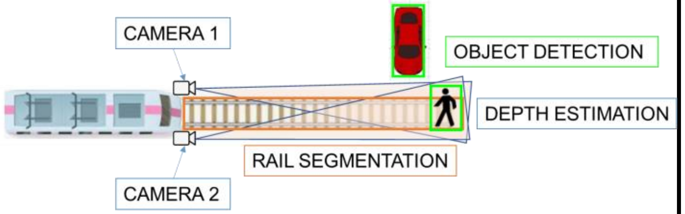
Reference software development process



Reference safety architecture



Railway case study



Methodology – per actitivy

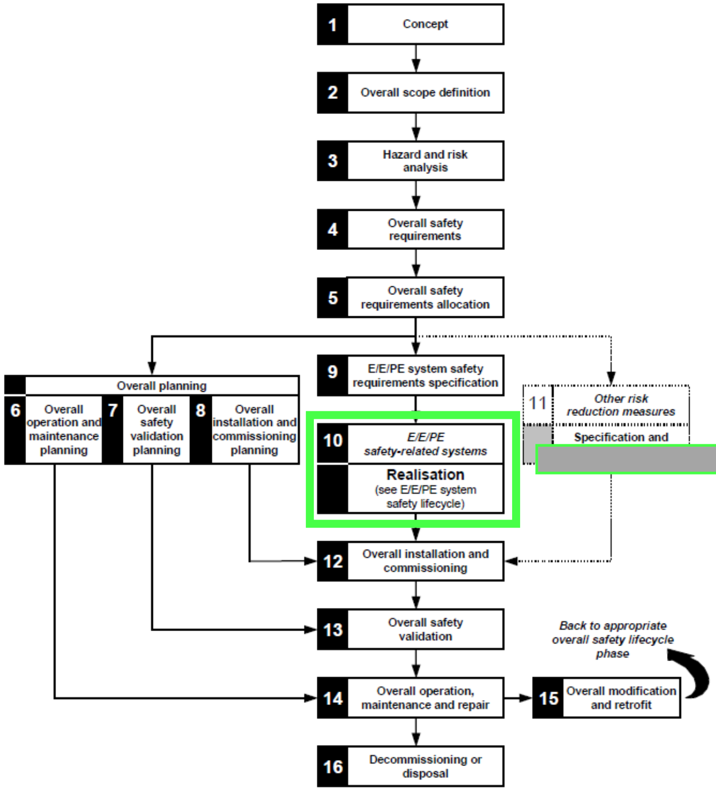
1. KICK-OFF MEETING ✓
2. IKERLAN SEND DOCUMENTATION TO TÜV R ✓
3. REVIEW MEETING ✓ — *This meeting*
4. GET LIST OF OPEN ISSUES / COMMENTS FROM TÜV R
5. IKERLAN SEND NEW VERSION
6. TÜV R REVIEW NEW VERSIÓN AND ISSUE TECHNICAL ASSESSMENT REPORT

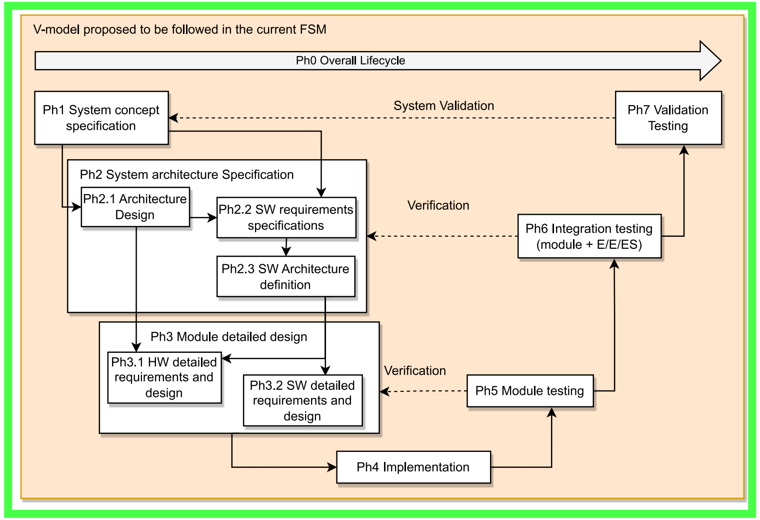
Per each activity (WP1 and WP2)

Equivalent to that obtained in previous EU projects (e.g., UP2DATE)

Contextualization

SIL 3 FSM (IKERLAN)

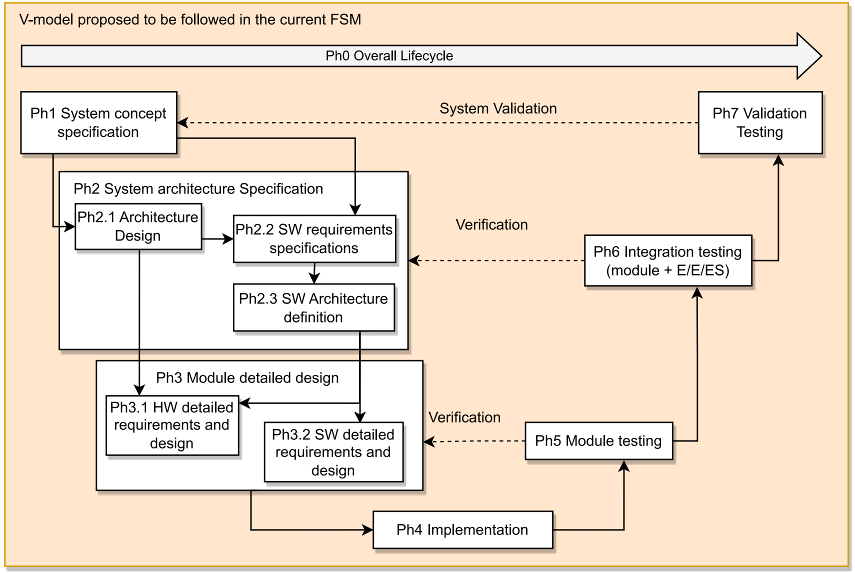




Contextualization

SIL 3 FSM (IKERLAN): Development process

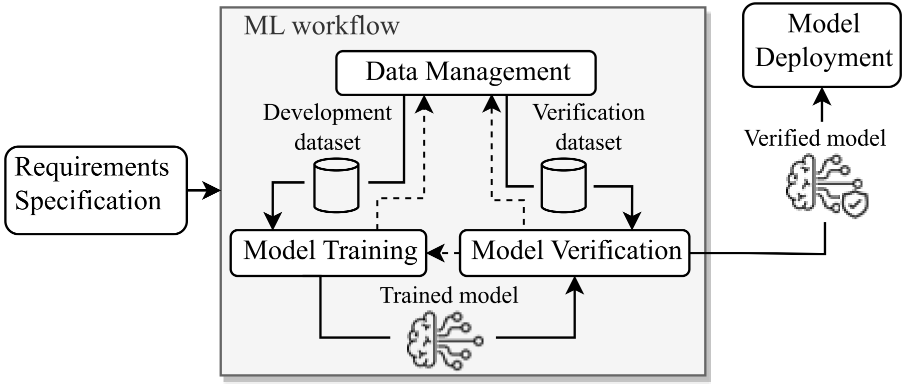
- Traditional lifecycle is based on the V-model development process and structured in the following lifecycle phases:
  - Ph0 Overall Life Cycle
  - Ph1 System Concept Specification
  - Ph2 System Architecture Specification
  - Ph3 Module Detailed Design
  - Ph4 Implementation
  - Ph5 Module Testing
  - Ph6 Integration Testing
  - Ph7 Validation Testing



Contextualization

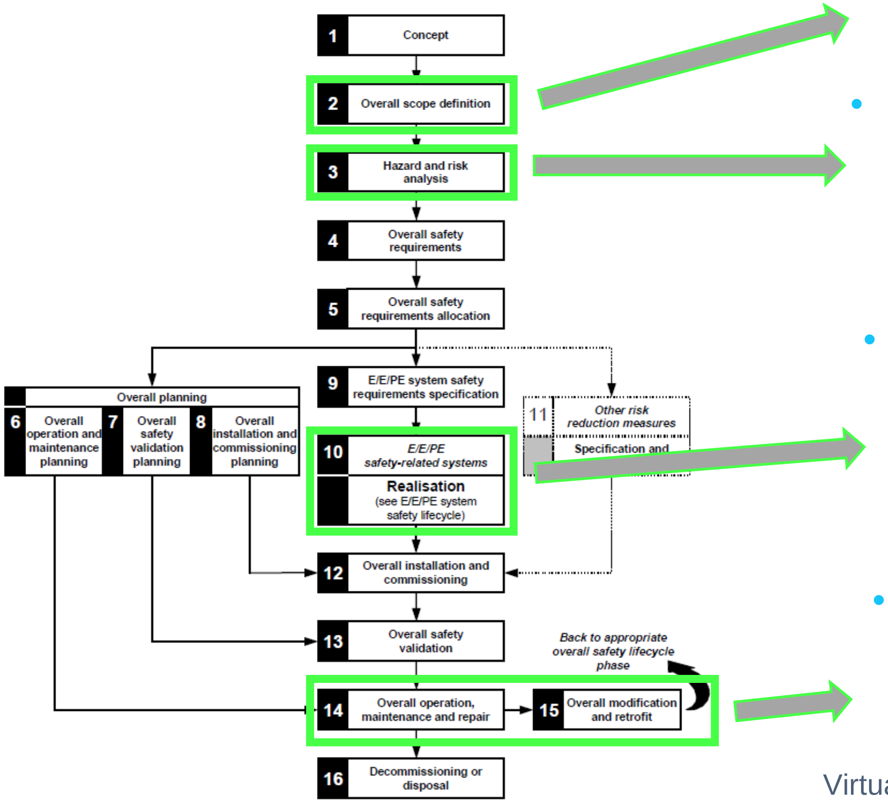
AI lifecycle phases

- Five main stages:
  - Requirements Specification
  - Data Management
    - Development dataset
      - Training + Validation* dataset
    - Verification dataset
  - Model training
    - Trained model
  - Model verification
    - Verified model
  - Model Deployment
    - Inference model



Contextualization

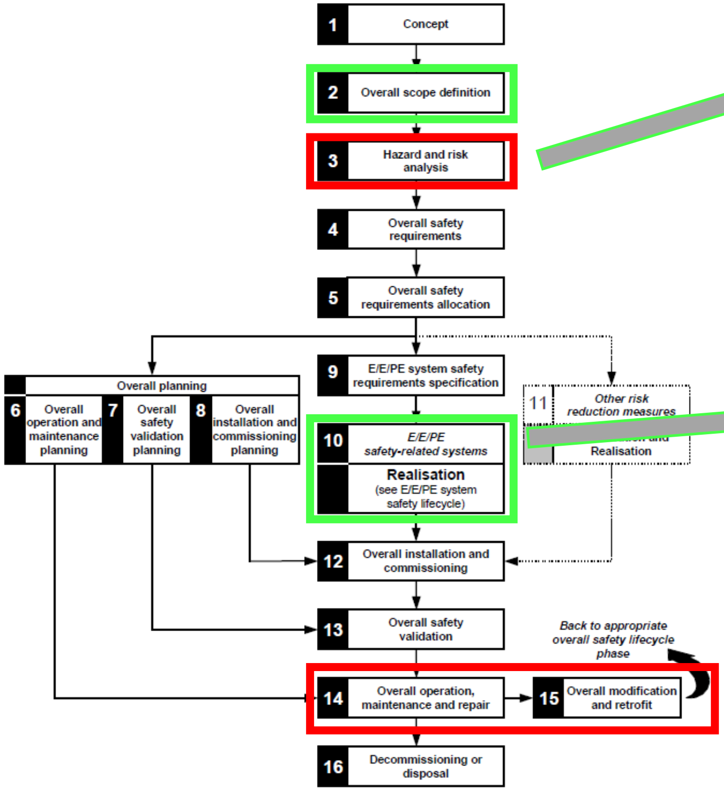
Phases affected by including DL



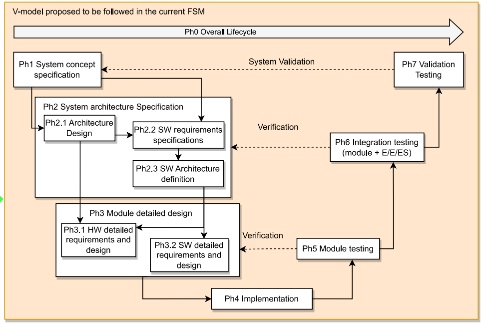
- Definition of the ODD and operational scenarios
- HARA shall identify potential hazards caused by the DL-based system. The ODD and operational scenarios are used as input for this stage.
- New phases not contemplated by the traditional V-model:
  - Data management
  - Learning management
  - Inference management
- In traditional software, after a product release an update involves a re-assessment process taking a lot of time. This can be challenging in DL models since their product lifecycle is more likely to be updated.

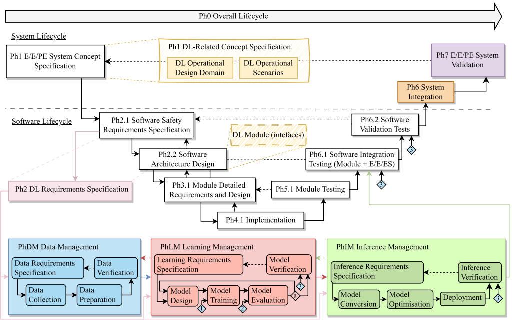
Contextualization

Current state of the AI-FSM



- Not contemplated in the current version. The following version will consider recommendations from standards such as SOTIF.

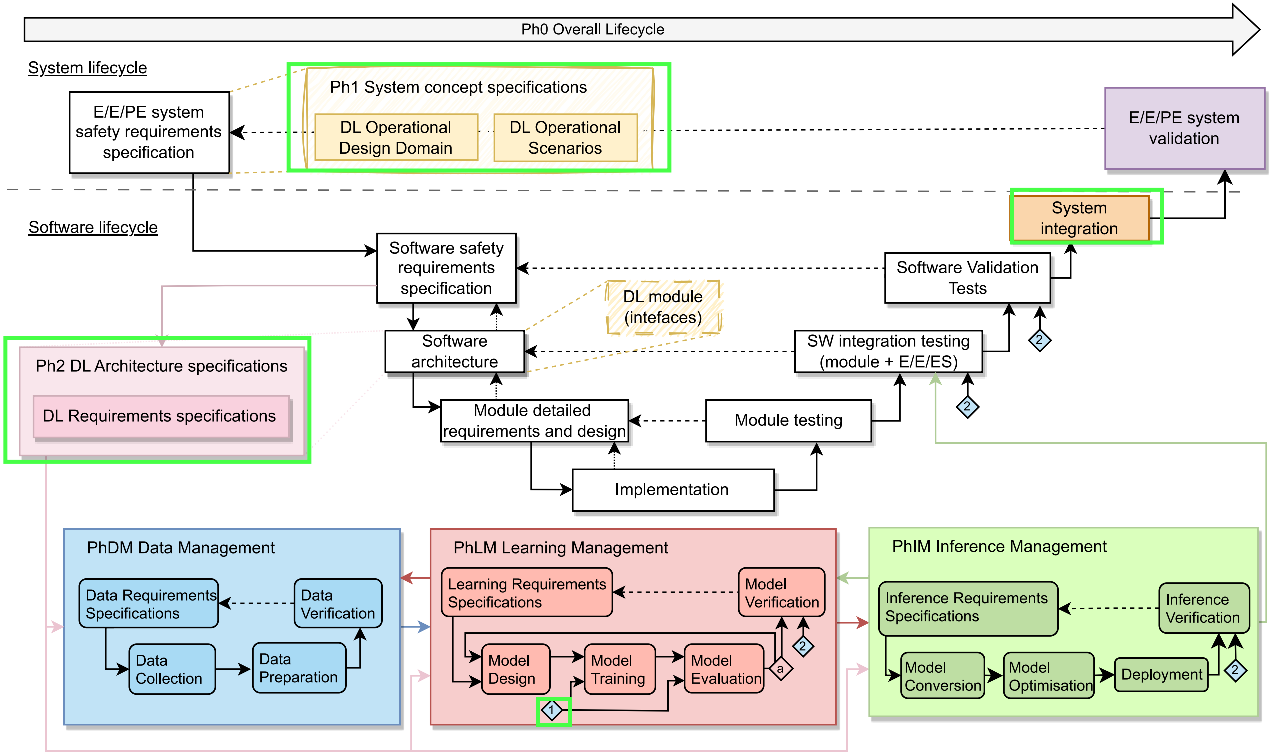




- The current version does not contemplate how to address this challenge.

Proposed lifecycle

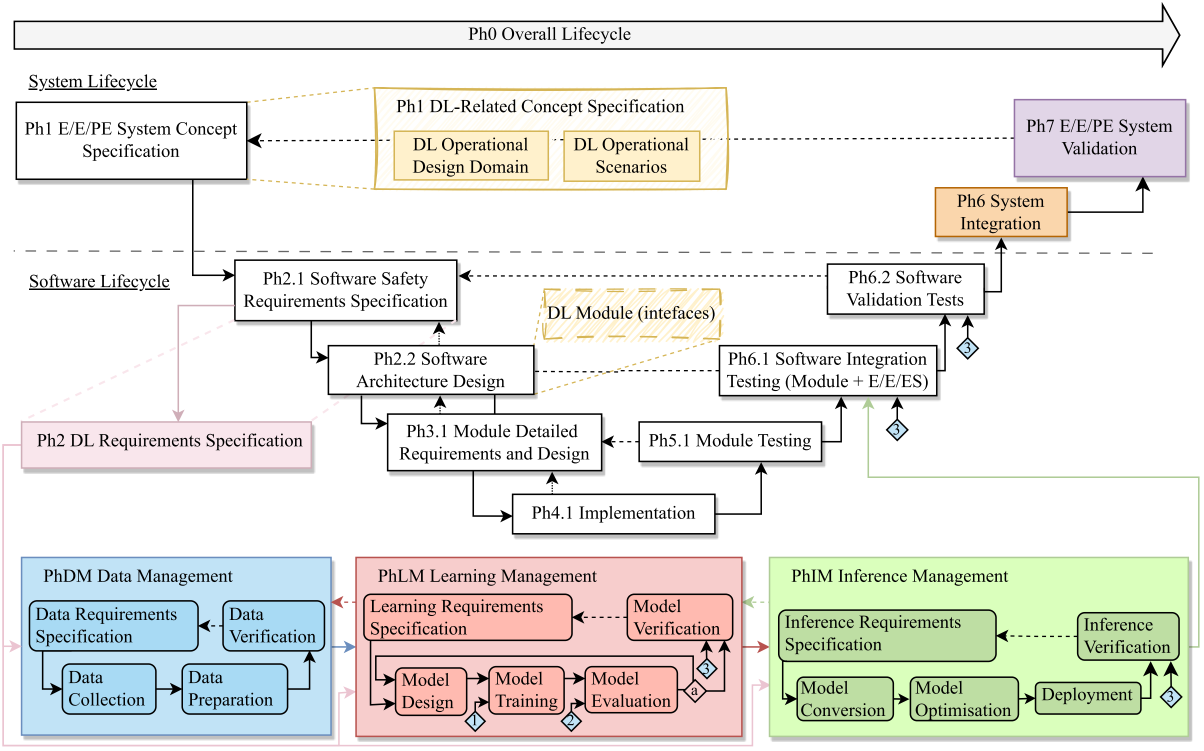
- IEC 61508 traditional functional safety lifecycle (Software V-model) + AI lifecycle



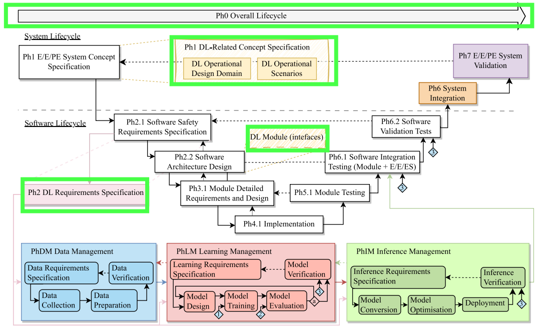
SAFEXPLAIN

Proposed lifecycle

- IEC 61508 traditional functional safety lifecycle (Software V-model) + AI lifecycle -> Modified

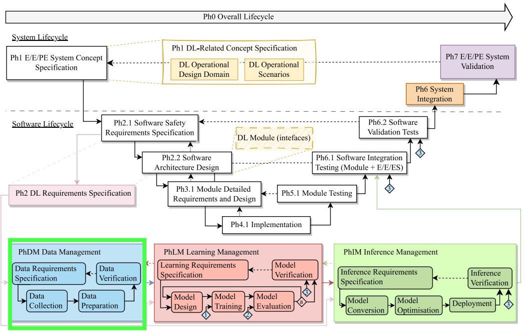


Proposed lifecycle: phases' objectives



- **<u>Ph0 Overall Lifecycle:</u>** It is a transversal phase that ***collects*** all the ***generic project information***
  - Documents generated
  - Organization chart
  - Tools selection
- **<u>Ph1 DL-Related Concept Specification:</u>** This phase encompasses the ***definition*** of the ***DL Operational Design Domain (ODD)*** and ***operational scenarios*** in which the DL will operate. In the case the safety-related system entails the use of DL, these definitions are required besides the traditional description of the use case and the definition of the operation reflected in the requirements.
- **<u>DL Modules (interfaces):</u>** This box highlights that Ph2.2 shall define all the interfaces of the DL modules.
- **<u>Ph2 DL Requirements Specification</u>**: This phase ***allocates*** the ***software requirements to DL*** constituents and ***refines them***:
  - Safety, operation, functional and non-functional requirements specification (among others)

Proposed lifecycle: phases’ objectives



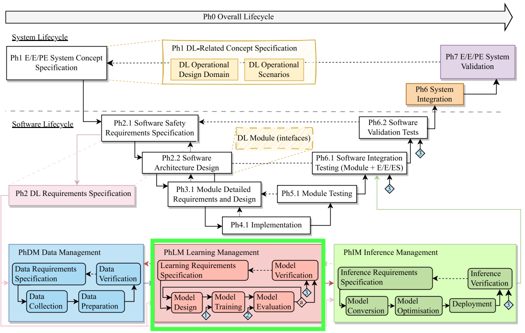
- **PhDM Data Management**. It is responsible for collecting and preparing the datasets. Four steps:
  - Data req. Specifications. It allocates the DL req. to the data req. and refine them. It shall collect:
    - Data and datasets req.
    - Req. Associated with the collection and preparation steps.
    - Data filename policy.
    - Degree of differentiation.
  - Data collection. It involves collecting all the data to generate the datasets:
    - Data gathering. It involves gathering data from different sources.
    - Data generation. It relates to generating new data to complete the data gathering.
  - Data preparation. In this step, the previous data is cleaned, processed, or annotated to meet the reqs.
  - Data Verification. This phase checks if the datasets meet the data req. specification.

All actions and decisions taken shall be documented

  - Inputs:
    - DL reqs specifications
    - ODD
    - Operational scenarios
  - Ouputs generated:
    - Development dataset (training + validation)
    - Verification dataset

SAFEXPLAIN

Proposed lifecycle: phases’ objectives

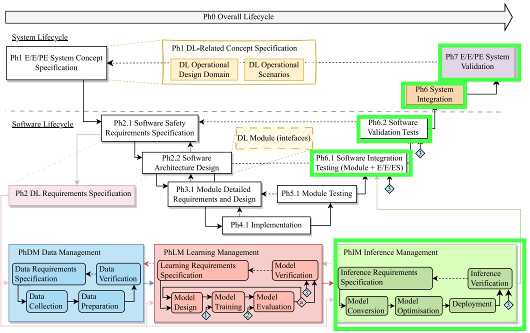


- **PhLM Learning Management**. It is responsible for generating a DL model that meets the DL req. specification. Five steps:
  - Learning req. Specifications. It allocates the DL req. to learning reqs. and refine them. It shall collect:
    - Qualitative and quantitative learning reqs.
    - Model selection criteria.
    - Reqs. associated with the model design and training.

All actions and decisions taken shall be documented

  - Model design. It focuses on the specification of a set of DL models that best suit the application.
  - Model training. In this step, the specified models are generated employing the training dataset.
  - Model evaluation. Once the model(s) are trained, they are evaluated employing the validation dataset.
  - Model verification. This phase not only evaluates the generalization capabilities and identifies potential issues using the verification dataset but also checks if the reqs. are met.
  - Inputs:
    - Development dataset (training + validation) from PhDM
    - Verification dataset from PhDM
    - DL req. specification
- Ouputs:
  - Trained model
  - Evaluated model
  - Verified learning model

Proposed lifecycle: phases’ objectives



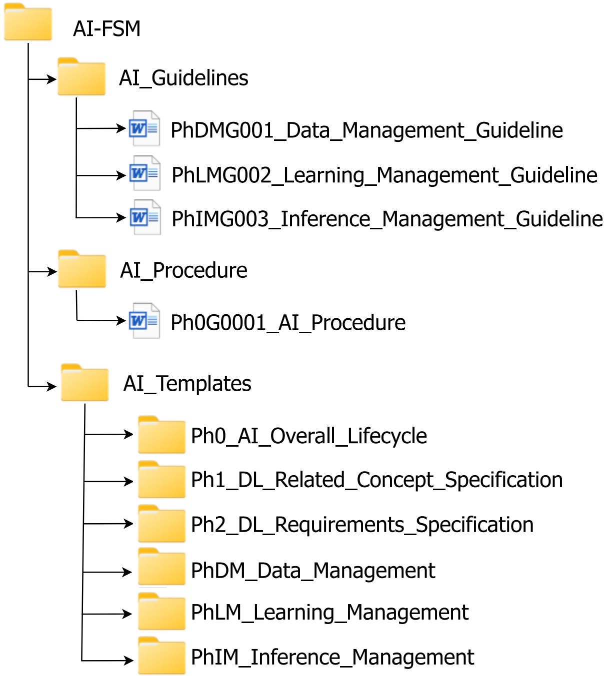
- **PhIM Inference Management**. Its purpose is to adapt the verified model for its deployment on the target HW while ensuring that it still meets the DL reqs. after converting and even optimising it. Five stages:
  - Inference req. specification. It allocates the DL and learning reqs. to inference reqs. and refine them. It shall collect:
    - Inference reqs.
    - Req. associated with the model conversion, optimization and deployment
  - Model conversion. The model is transformed into a format suitable for deployment that must ensure compatibility with the specific target inference platform.
  - Model optimisation. the model may undergo optimization to enhance its performance, reduce its size, or adapt it for resource-constrained environments.
  - Deployment. This steps entails the implementation of the model in the target platform.
  - Inference verification. This phase not only evaluates the generalization capabilities and identifies potential issues using the verification dataset but also checks if the reqs. are met.
  - Input:
    - Verified learning model from PhLM
    - Verification dataset from PhDM
    - Learning and DL req. specification
  - Ouput:
    - Verified inference model

AI-FSM Generalities

Types of documents:

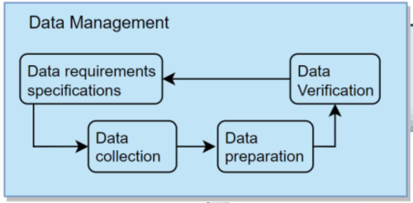
- Main procedure: It provides a set of steps required to generate the basic structure for a specific safety-related project. It serves as an internal guideline for fulfilling the procedure template.
- Procedure template: This document compiles how functional safety has been assessed within the organization.
- Guidelines: These documents offer additional guidance for specific processes.
- Templates: Standard documents used to document the information consistently. They often include examples and tables to be completed.
- Internal Reviews (IRs): reviews based on the activities of the left side of the safety lifecycle. Objective: Check that the activities defined in each phase have been properly carried out:
  - Quality Assurance

Folder Structure proposed:



AI-FSM Generalities

- PhDM Data Management



Guideline

PhDMG001 Data Management Guideline

Version 0.1

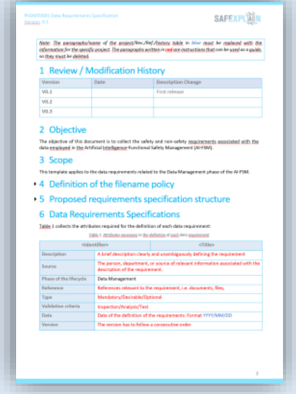
Documentation Information

Contract Number	101069595
Project Website	www.safexplain.eu
Contractual Deadline	DD.MM.YYY
Dissemination Level	PU or SEN -see DoA
Nature	R or OTHER -see DoA
Author	Irune Agirre, Javier Fernández
Modified by	Lorea Belategi
Reviewed by	Name (Partners' short name)
Approved by	Name (Partners' short name)
Keywords	AI, Functional safety, FSM, Explainability

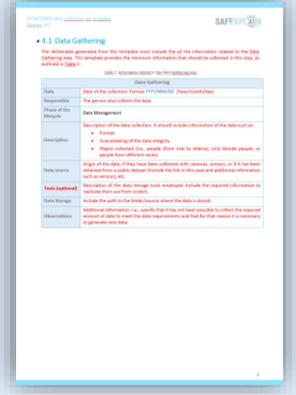
This project has received funding from the European Union's Horizon Europe programme under grant agreement number 101069595.

Templates

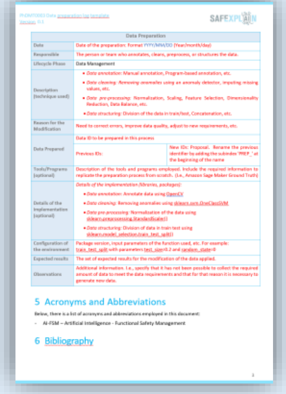
Data reqs.



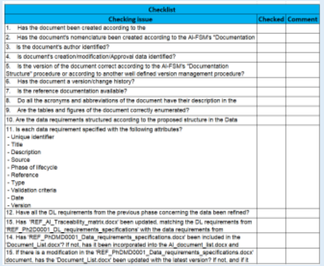
Data Collection

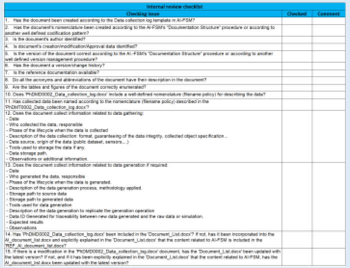


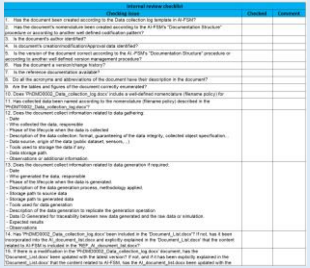
Data Preparation



IRs

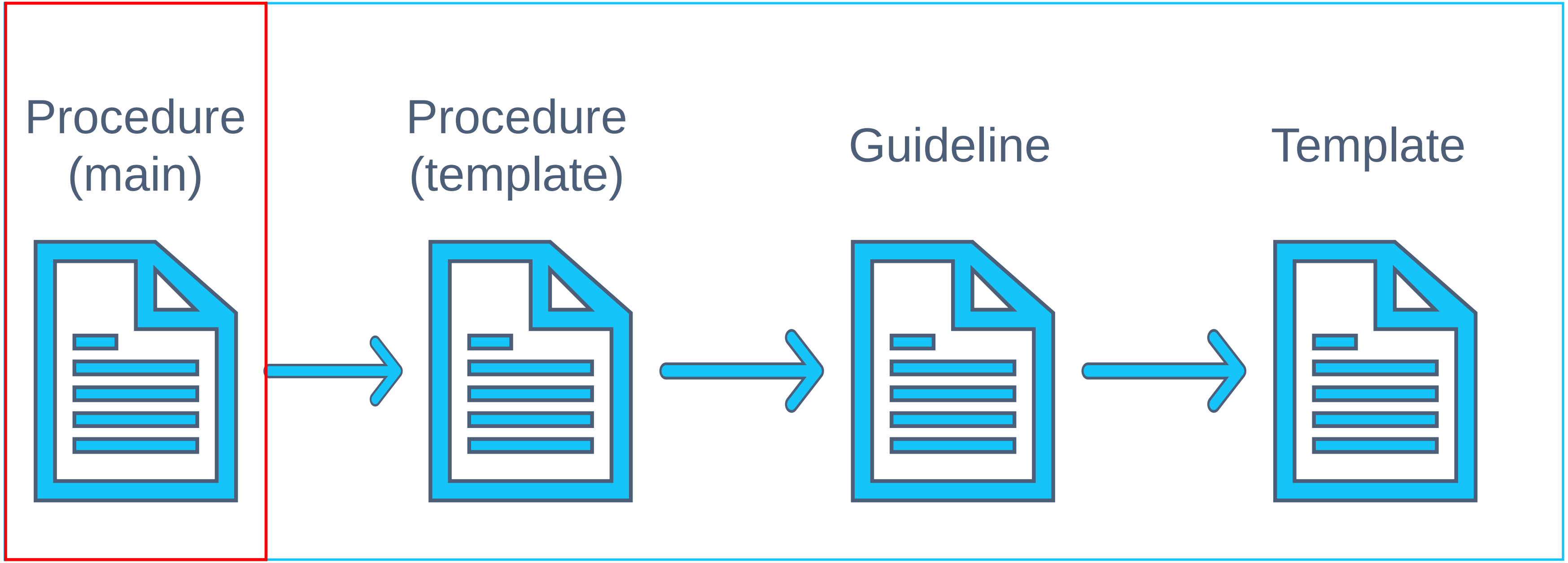




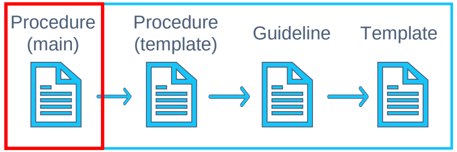


Any questions or topics to discuss?

AI-FSM in-depth: Procedure (main)

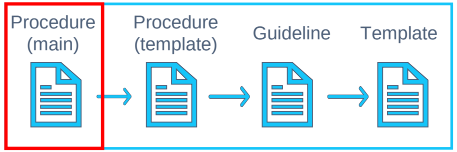


AI-FSM in-depth: Procedure (main)



- Defines the context:
  - AI definitions.
  - Limitations of the current AI-FSM version.
- Defines the traditional FSM lifecycle and the AI lifecycle.
- Expands the traditional FSM lifecycle, mapping it with the AI lifecycle.
- Proposes a folder structure for storing the documents and artifacts for each phase.
- Describes the inputs and outputs of each phase, identifying the corresponding template for their generation.
- Describes how these templates shall be generated and stored for each phase.

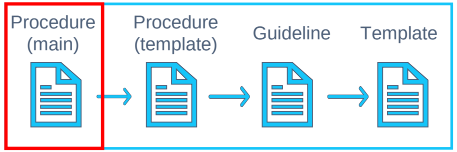
AI-FSM in-depth: Procedure (main)



C1

The procedure is the main document and refers to the other documents. It provides information on the necessary additional steps and measures to be taken, when AI is incorporated in a functional safety management. An overall life cycle is defined and considered. Aspects of data management, learning and inference management (concerning the AI) are included

AI-FSM in-depth: Procedure (main)



Ph0 Overall lifecycle

Table 1. Inputs and outputs of the overall lifecycle phase (Ph0)

Phase	Step	Inputs	Outputs	Corresponding templates
Ph0 AI Overall Life Cycle	Generate the AI-FSM document	*REF_FSM_procedure*	*REF_Ph0D0001_AI-FSM_Procedure*	*Ph0T0001_AI_FSM_template*
	V&V the AI-FSM document	*REF_Ph0D0001_AI-FSM_Procedure*	*REF_Ph0D0002_AI-FSM_Procedure_IR*	*Ph0T0001_AI_FSM_template_IR*
	Generate the AI_Document_List	*REF_Document_list*	*REF_Ph0D0003_AI_Document_List*	*Ph0T0002_AI_Document_List_template*
	V&V the AI_Document_List	*REF_Ph0D0003_AI_Document_List*	*REF_Ph0D0004_AI_Document_List_IR*	*Ph0T0002_AI_Document_List_template_IR*
	Generate AI version tracking	*REF_version_tracking*	*REF_Ph0D0005_AI_Version_Tracking*	*Ph0T0003_AI_Version_Tracking_template*
	V&V the AI version tracking	*REF_Ph0D0005_AI_Version_Tracking*	*REF_Ph0D0006_AI_Version_Tracking_IR*	*Ph0T0003_AI_Version_Tracking_template_IR*
	Generate AI organizational chart	*REF_organizational_chart*	*REF_Ph0D0007_AI_Organizational_Chart*	*Ph0T0004_AI_Organizational_Chart_template*
	V&V AI organizational chart	*REF_Ph0D0007_AI_Organizational_Chart*	*REF_Ph0D0008_AI_Organizational_Chart_IR*	*Ph0T0012_Organizational_chart_template_IR*
	Generate the AI log of tests	-	*REF_Ph0D0009_AI_Log_of_Tests*	*Ph0T0006_Log_of_Test_template*
	V&V the AI log of test	*REF_Ph0D0009_AI_Log_of_Test*	*REF_Ph0D0010_AI_Log_of_Tests_IR*	*Ph0T0006_Log_of_Test_template_IR*
	Generate the AI selection of tools	-	*REF_Ph0D0011_AI_Tools_Selection*	*Ph0T0010_Tools_selection_template*
	V&V the AI selection of tools	*REF_Ph0D0011_AI_Tools_Selection*	*REF_Ph0D0012_AI_Tools_Selection_IR*	*Ph0T0010_Tools_selection_template_IR*
	Generate the AI traceability matrix	-	*REF_Ph0D0013_AI_Traceability_Matrix*	*Ph0T0011_Traceability_matrix_template*
	V&V the AI traceability matrix	*REF_Ph0D0013_AI_Traceability_Matrix*	*REF_Ph0D0014_AI_Traceability_Matrix_IR*	*Ph0T0011_Traceability_matrix_template_IR*

AI-FSM in-depth: Procedure (main)

Procedure (main) → Procedure (template) → Guideline → Template

Ph1 System Concept Specification → Ph1 DL-Related Concept Specification

Table 2. Inputs and outputs of the System Concept Specification phase (Ph1)

Phase	Step	Inputs	Outputs	Corresponding templates
Ph1 System Concept Specification	ODD definition	REF_System_Requirements_Specifications	REF_Ph1D0001_DL_Operational_Design_Domain	Ph1T0001_DL_Operational_Design_Domain_template
	V&V the ODD	REF_Ph1D0001_DL_Operational_Design_Domain	REF_Ph1D0002_DL_Operational_Design_Domain_IR	Ph1T0001_DL_Operational_Design_Domain_template_IR
	Operational scenarios definition	REF_System Requirements Specifications REF_Ph1D0001_DL_Operational_Design_Domain	REF_Ph1D0003_DL_Operational_Scenarios	Ph1T0002_DL_Operational_Scenarios_template
	V&V the operational scenarios	REF_Ph1D0003_DL_Operational_Scenarios	REF_Ph1D0004_DL_Operational_Scenarios_IR	Ph1T0002_DL_Operational_Scenarios_template_IR

Requirements Specification

C2

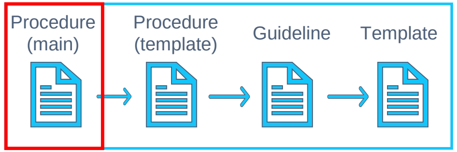
Table 3. Inputs and outputs of the definition of the DL requirements (Ph2)

It is important that the ODD is complete. Let's discuss this.

Ph2 System Architecture Specification	DL requirements specifications	REF_Software Requirements Specifications	REF_Ph2D0001_DL_Requirements_Specifications REF_Ph2D0003_DL_Requirements_Verification_Tests	Ph2T0001_DL_Requirements_Specifications_template Ph0T0009_Test_definition_and_results_template
		REF_Ph2D0001_DL_Requirements_Specifications REF_Ph2D0003_DL_Requirements_Verification_Tests	REF_Ph2D0002_DL_Requirements_Specifications_IR REF_Ph2D0004_DL_Requirements_Verification_Tests_IR	Ph2T0001_DL_Requirements_Specifications_template_IR Ph0T0009_Test_definition_and_results_template_IR
	DL component	REF_Software Requirements Specifications REF_Ph2D0005_DL_Component_Description	REF_Ph2D0005_DL_Component_Description REF_Ph2D0006_DL_Component_Description_IR	Ph2T0002_DL_Component_Description_template Ph2T0002_DL_Component_Description_template_IR

SAFEXPLAIN

AI-FSM in-depth: Procedure (main)



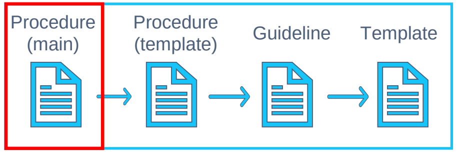
PhDM Data Management

Table 4. Inputs and outputs of each step of the Data Management phase (related to Ph3, Ph4 and Ph5 of the traditional lifecycle)

Phase	Step	Inputs	Outputs	Corresponding templates
PhDM Data Management	Data Requirements Specifications	REF_Ph2D0001_DL_Requirements_Specifications REF_Ph1D0001_DL_Operational_Design_Domain REF_Ph1D0003_DL_Operational_Scenarios	REF_PhDMD0001_Data_Requirements_Specifications REF_PhDMD0007_Data_Requirements_Verification_Tests	PhDMT0001_Data_Requirements_Specifications_template Ph0T0009_Test_definition_and_results_template
		REF_PhDMD0001_Data_Requirements_Specifications REF_PhDMD0007_Data_Requirements_Verification_Tests	REF_PhDMD0002_Data_Requirements_Specifications_IR REF_PhDMD0008_Data_Requirements_Verification_Tests_IR	PhDMT0001_Data_Requirements_Specifications_template_IR Ph0T0009_Test_definition_and_results_template_IR
	Data Collection	REF_PhDMD0001_Data_Requirements_Specifications	REF_PhDMD0003_Data_Collection_Log Collected data structured in datasets(1)	PhDMT0002_Data_Collection_Log_template
		REF_PhDMD0003_Data_Collection_Log	REF_PhDMD0004_Data_Collection_Log_IR	PhDMT0002_Data_Collection_Log_template_IR
	Data Preparation	REF_PhDMD0001_Data_Requirements_Specifications REF_PhDMD0003_Data_Collection_Log Raw data files structured in datasets(1)	REF_PhDMD0005_Data_Preparation_Log Prepared data structured in datasets(1)	PhDMT0003_Data_Preparation_Log_template
		REF_PhDMD0005_Data_Preparation_Log	REF_PhDMD0006_Data_Preparation_Log_IR	PhDMT0003_Data_Preparation_Log_template_IR
	Data Verification	REF_PhDMD0001_Data_Requirements_Specifications REF_PhDMD0007_Data_Requirements_Verification_Tests Datasets(1)	REF_PhDMD0007_Data_Requirements_Verification_Tests Verified datasets(1)	*Document previously generated*

(*) Datasets include: i) Development (training and validation), ii) verification datasets.

AI-FSM in-depth: Procedure (main)

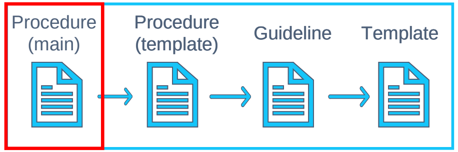


PhLM Learning Management

Table 5. Inputs and outputs of each step of the Learning Management phase (related to Ph3, Ph4 and Ph5 of the traditional lifecycle)

Phase	Step	Inputs	Outputs	Corresponding templates
PhLM Learning Management	Learning Requirements Specifications	REF_Ph2D0001_DL_Requirements_Specifications	REF_PhLMD0001_Learning_Requirements_Specifications REF_PhLMD0005_Learning_Requirements_Evaluation_Tests REF_PhLMD0007_Learning_Requirements_Verification_Tests	*PhLMT0001_Learning_Requirements_Specifications_template* *Ph0T0009_Test_definition_and_results_template* *Ph0T0009_Test_definition_and_results_template*
		REF_PhLMD0001_Learning_Requirements_Specifications REF_PhLMD0005_Learning_Requirements_Evaluation_Tests REF_PhLMD0007_Learning_Requirements_Verification_Tests	REF_PhLMD0002_Learning_Requirements_Specifications_IR REF_PhLMD0006_Learning_Requirements_Evaluation_Tests_IR REF_PhLMD0008_Learning_Requirements_Verification_Tests_IR	*PhLMT0001_Learning_Requirements_Specifications_template_IR* *Ph0T0009_Test_definition_and_results_template_IR* *Ph0T0009_Test_definition_and_results_template*
	Model Design	REF_PhLMD0001_Learning_Requirements_Specifications	REF_PhLMD0003_Model_Election_Log	*PhLMT0002_Model_Election_Log_template*
		REF_PhLMD0003_Model_Election_Log	REF_PhLMD0004_Model_Election_Log_IR	*PhLMT0002_Model_Election_Log_template_IR*
	Model Training	REF_PhLMD0003_Model_Election_Log Training dataset	Trained Model(s)	*There is not a template, it should be considered as an implementation.*
	Model Evaluation	REF_PhLMD0005_Learning_Requirements_Evaluation_Tests Trained Model(s) Validation dataset (2)	REF_PhLMD0005_Learning_Requirements_Evaluation_Tests Evaluated Model(s)	*Document previously generated*
	Learning Model Verification	REF_PhLMD0007_Learning_Requirements_Verification_Tests Evaluated Model(s) Verification dataset	REF_PhLMD0007_Learning_Requirements_Verification_Test Verified Learning Model(s)	*Document previously generated*

AI-FSM in-depth: Procedure (main)

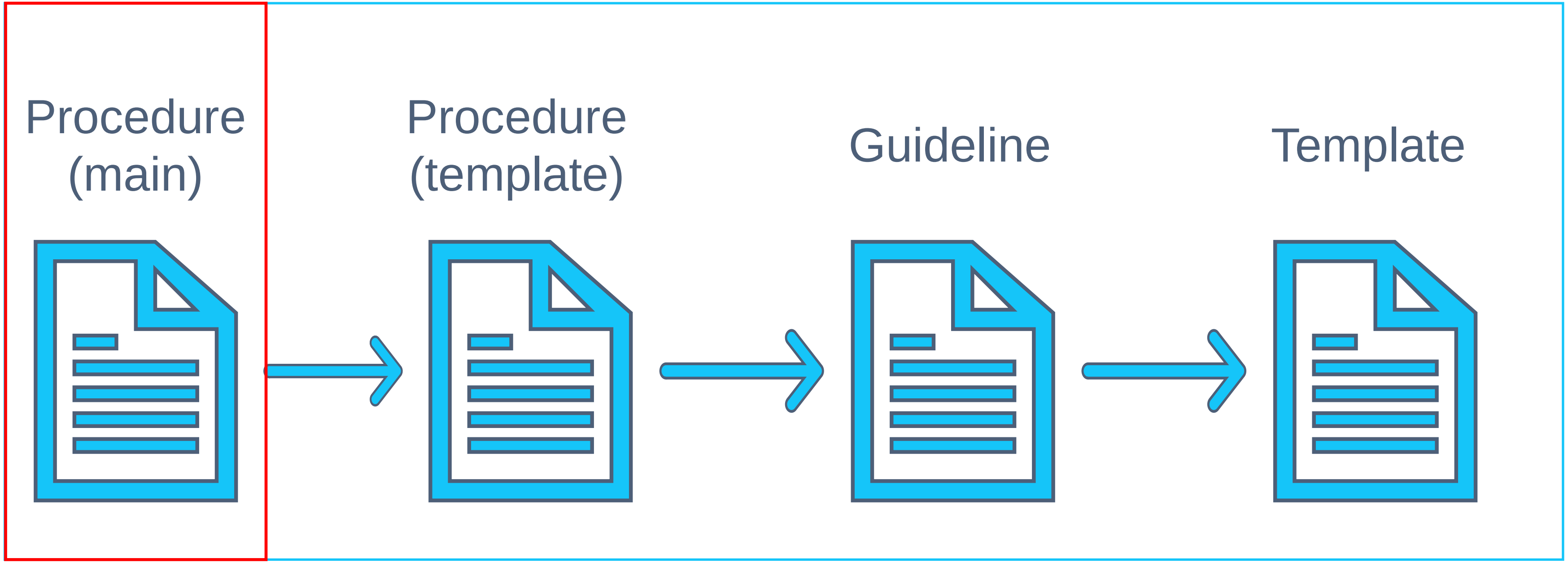


PhIM Inference Management

Table 6. Inputs and outputs of each step of the inference stage (related to Ph3, Ph4 and Ph5 of the traditional lifecycle)

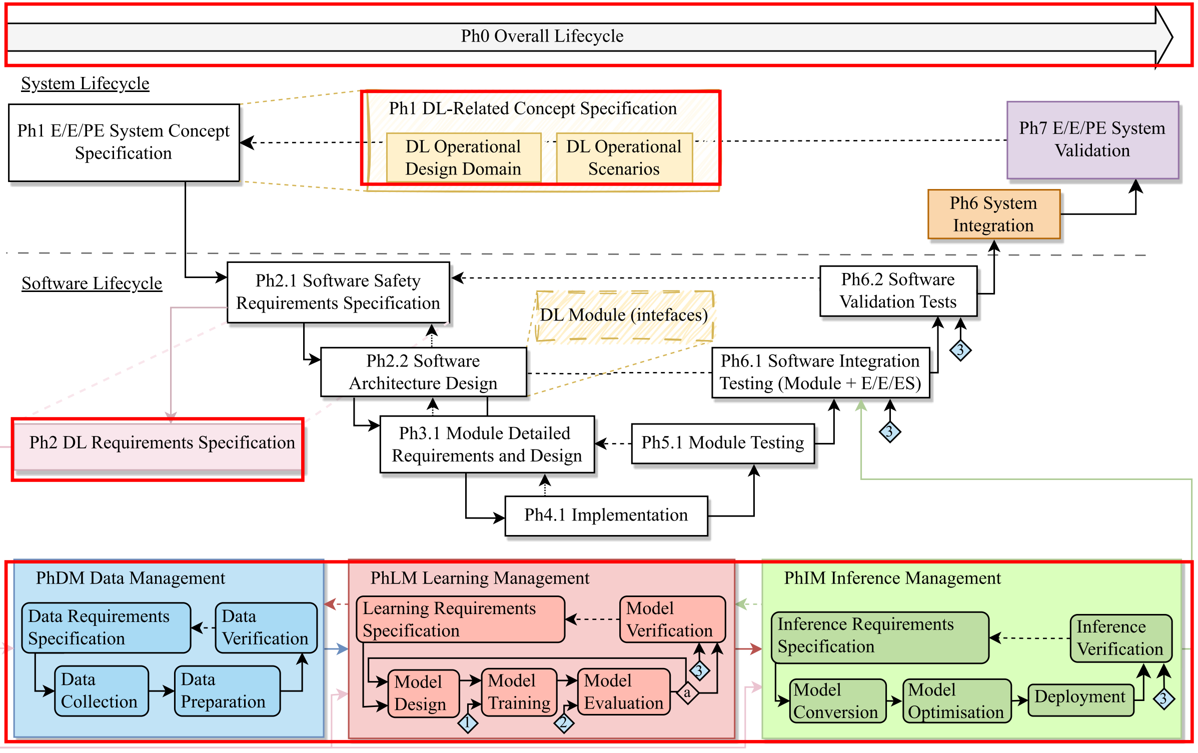
Phase	Step	Inputs	Outputs	Corresponding templates
PhIM Inference Management	*Inference Requirements Specifications*	REF_Ph2D0001_DL_Requirements_Specifications REF_PhLMD0001_Learning_Requirements_Specifications	REF_PhIMD0001_Inference_Requirements_Specifications REF_PhIMD0007_Inference_Requirements_Verification_Tests	PhIMT0001_Inference_Requirements_Specifications Ph0T0009_Test_definition_and_results_template
		REF_PhIMD0001_Inference_Requirements_Specifications REF_PhIMD0007_Inference_Requirements_Verification_Tests	REF_PhIMD0002_Inference_Requirements_Specifications_IR REF_PhIMD0008_Inference_Requirements_Verification_Tests_IR	REF_PhIMD0002_Inference_Requirements_Specifications_IR Ph0T0009_Test_definition_and_results_template_IR
	Model Conversion	REF_PhIMD0001_Inference_Requirements_Specifications Verified Learning Model	REF_PhIMD0003_Model_Conversion_Log Converted Model	PhIMT0002_Model_Conversion_Log
		REF_PhIMD0003_Model_Conversion_Log	REF_PhIMD0004_Model_Conversion_Log_IR	PhIMT0002_Model_Conversion_Log_IR
	Model Optimization	REF_PhIMD0001_Inference_Requirements_Specifications Converted Model	REF_PhIMD0005_Model_Optimization_Log Optimized Model	PhIMT0003_Model_Optimization_Log
		REF_PhIMD0005_Model_Optimization_Log	REF_PhIMD0006_Model_Optimization_Log_IR	PhIMT0003_Model_Optimization_Log_IR
	Inference Model Verification	REF_PhIMD0007_Inference_Requirements_Verification_Tests Optimized Model or Converted Model Verification dataset	REF_PhIMD0007_Inference_Requirements_Verification_Tests Verified Inference Model	*Document previously generated*

AI-FSM in-depth: Procedure (templ)



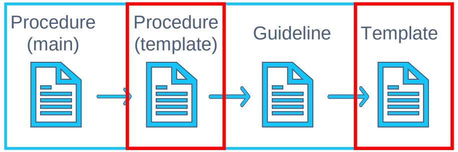
AI-FSM in-depth

- **Explanation order:**



SAFEXPLAIN

AI-FSM in-depth: Procedure (templ)



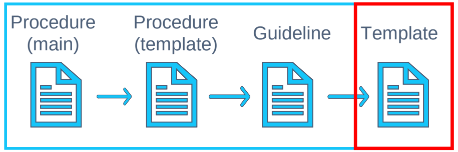
Overall Lifecycle – Phase 0 (Ph0)

- Definition activities:
  - Update the AI_Document_List
  - Complete the AI_Version_Tracking
  - Fulfill the AI_Organizational_Chart
  - Fulfill the AI_Tools_selection
  - Complete the AI_Traceability_Matrix
- Verification and validation activities:
  - Conduct the IRs

Table 1: Overall lifecycle - Phase 0 summary

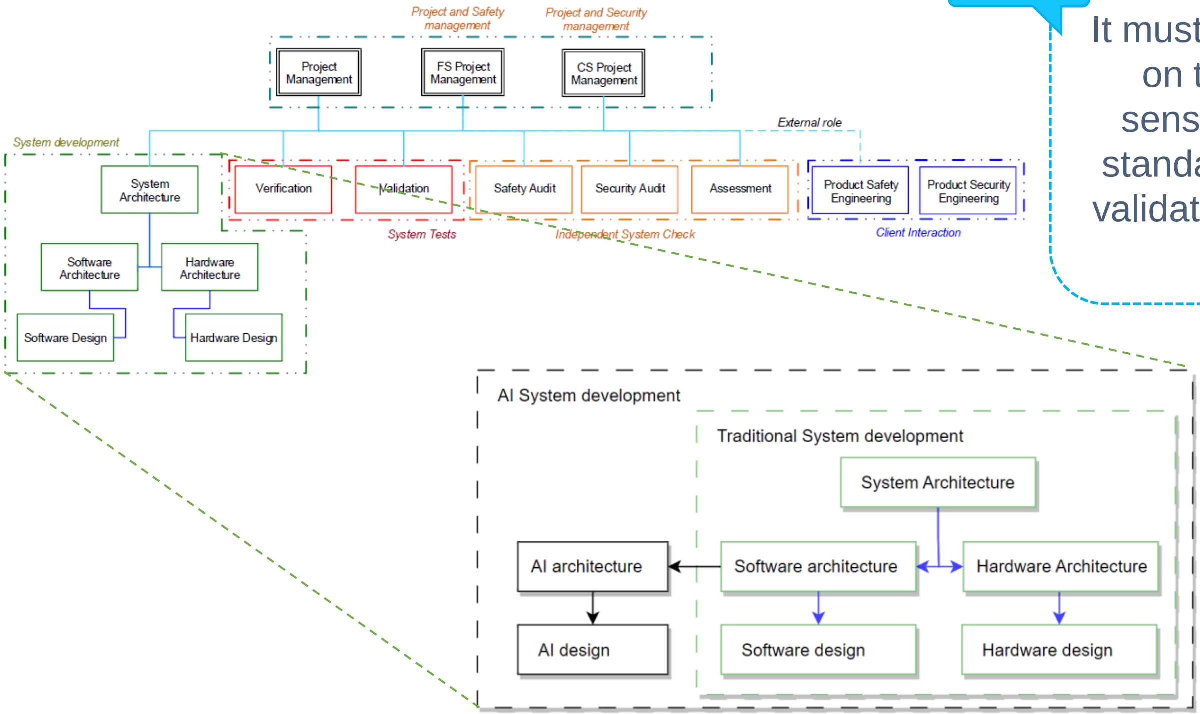
Phase	File input name	File output name	Responsible	Assessment
Ph0 AI Overall Lifecycle	• REF_FSM_Procedure • REF_Document_List • REF_Version_Tracking • REF_Organizational_Chart • REF_Traceability_Matrix	REF_Ph0D0001_AI-FSM_Procedure		
		REF_Ph0D0002_AI-FSM_Procedure_IR		
		REF_Ph0D0003_AI_Document_List		
		REF Ph0D0004_AI_Document_List_IR		
		REF_Ph0D0005_AI_Version_Tracking		
		REF Ph0D0006_AI_Version_Tracking_IR		
		REF_Ph0D0007_AI_Organizational_Chart		
		REF_Ph0D0008_AI_Organizational_Chart_IR		
		REF_Ph0D0009_AI_Log_of_Tests		
		REF_Ph0D0010_AI Log_of_Tests_IR		
		REF_Ph0D0011_AI_Tools_Selection		
		REF_Ph0D0012_AI_Tools_Selection_IR		
		REF_Ph0D0013_AI_Traceability_Matrix		
		REF_Ph0D0014_AI_Traceability_Matrix_IR		

AI-FSM in-depth: Organizational Chart template

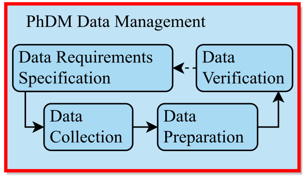


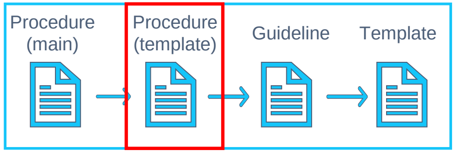
C2.1

It must be noted that the validation depicted on the figure is the validation in the AI sense, not in the sense of the EN 5012x standards. This must be clarified. Also, the validation (EN 50126) must be added to the organigram.



AI-FSM procedure template





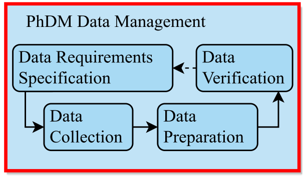
Data Management – Phase DM (PhDM)

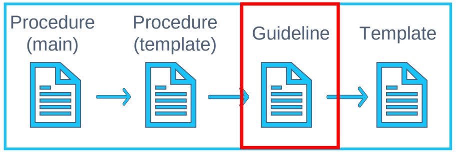
- Definition activities:
  - Collect data requirements
  - Define data req. verification tests
  - Data Collection
  - Data Prepation
  - Complete the Data Req. Verification Tests
- Verification & validation:
  - Implement data req. verification tests
  - Conduct the IRs
- Collect the tests in AI Log Test file
- Update the state of AI Document List

Table 4: Data Management - PhDM summary (related to Ph3, Ph4 and Ph5 of the traditional lifecycle)

Phase	File input name	File output name	Responsible	Assessment
PhDM: Data Management	• *REF_Ph2D0001_DL_Requirements_Specification* • *REF_Ph1D0001_DL_Operational Design Domain* • *REF_Ph1D0003_DL_Operational Scenarios*	*REF_PhDMD0001_Data_Requirements_Specification*		
		REF_PhDMD0007_Data_Requirements_Verification tests		
		REF_PhDMD0002_Data_Requirements_Specification_IR *REF_PhDMD0008_Data_Requirements_Verification Tests_IR*		
		REF_PhDMD0003_Data_Collection_Log Raw data files structured in datasets[1]		
		REF_PhDMD0004_Data_Collection_Log_IR		
		REF_PhDMD0005_Data_Preparation_Llog Prepared data structured in datasets[1]		
		REF_PhDMD0006_Data_Preparation_Log_IR		
		Verified datasets[1]		

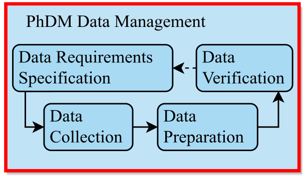
Data Management guideline

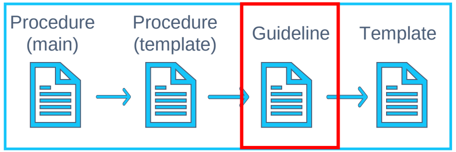




- The objective of this phase is the generation of:
  - Development dataset:
    - Training dataset.
    - Validation datasets.
  - Verification dataset.
- As previously mentioned, the following document should be generated:
  - REF_PhDMD0001_Data_Requirements_Specifications.docx. (+IR)
  - REF_PhDMD0003_Data_Collection_Log.docx. (+IR)
  - REF_PhDMD0005_Data_Preparation_Log.docx. (+IR)
  - REF_PhDMD0007_Data_Requirements_Verification_Tests. (+IR)
- All the documents should be stored in the "PhDM Data Management" folder.

Data Management guideline



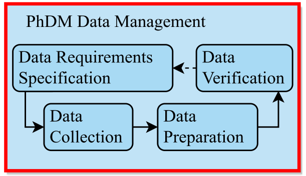


C2.1

In fact, three disjunct data sets are needed: for learning, for validation and for verification. Let`s discuss on this

- Development dataset:
  - Training dataset. It is employed to train the model.
  - Validation datasets (*). It evaluates if the model achieves a predefined performance and, in some cases, stops the training phase.
- Verification dataset. It expands upon the previous validation dataset to assess whether the model maintains its performance requirements with data not utilized during development. It must encompass sufficient information and data to ensure the appropriate behaviour of the DL constituent within the expected ODD and operational scenarios.

Data Management guideline



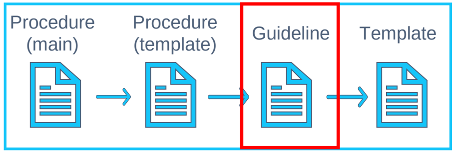
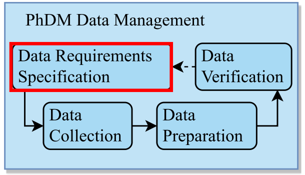


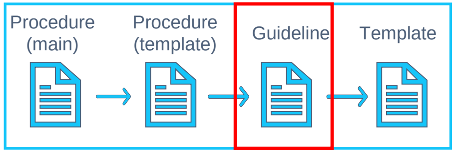
Table 1. Inputs and outputs of the Data Management phase

Phase	Step	Inputs	Outputs	Corresponding templates
PhDM Data Management	Data Requirements Specification	REF_Ph2D0001_DL_Requirements_Specifications REF_Ph1D0001_DL_Operational_Design_Domain REF_Ph1D0003_DL_Operational_Scenarios	REF_PhDMD0001_Data_Requirements_Specifications REF_PhDMD0007_Data_Requirements_Verification_Tests	PhDMT0001_Data_Requirements_Specifications_template Ph0T0009_Test_definition_and_results_template
		REF_PhDMD0001_Data_Requirements_Specifications REF_PhDMD0007_Data_Requirements_Verification_Tests	REF_PhDMD0002_Data_Requirements_Specifications_IR REF_PhDMD0008_Data_Requirements_Verification_Tests_IR	PhDMT0001_Data_Requirements_Specifications_template_IR Ph0T0009_Test_definition_and_results_template_IR
	Data Collection	REF_PhDMD0001_Data_Requirements_Specifications	REF_PhDMD0003_Data_Collection_Log Collected data structured in datasets(*)	PhDMT0002_Data_Collection_Log_template
		REF_PhDMD0003_Data_Collection_Log	REF_PhDMD0004_Data_Collection_Log_IR	PhDMT0002_Data_Collection_Log_template_IR
	Data Preparation	REF_PhDMD0001_Data_Requirements_Specifications REF_PhDMD0003_Data_Collection_Log Raw data files structured in datasets(*)	REF_PhDMD0005_Data_Preparation_Log Prepared data structured in datasets(*)	PhDMT0003_Data_Preparation_Log_template
		REF_PhDMD0005_Data_Preparation_Log	REF_PhDMD0006_Data_Preparation_Log_IR	PhDMT0003_Data_Preparation_Log_template_IR
	Data Verification	REF_PhDMD0001_Data_Requirements_Specifications REF_PhDMD0007_Data_Requirements_Verification_Tests Datasets(*)	REF_PhDMD0007_Data_Requirements_Verification_Tests Verified datasets(*)	*Document previously generated in data requirements specifications step*

(*) Datasets: i) Development (training and validation), ii) verification datasets.

Data Management guideline

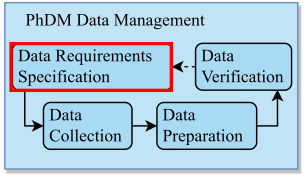


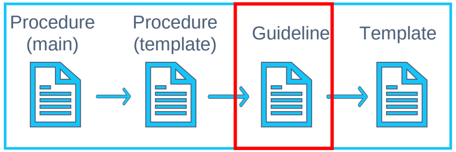


Data Requirements Specification step

- Define the data requirements:
  - Allocate DL requirements specification associated with the data requirement specification.
  - Refine those requirements and define additional ones.
  - Define the data notation policy.
  - This guideline proposes to decompose the requirements into two subcategories:
    - Dataset requirements specification.
    - Data requirements specification.
- Define the mechanisms or tests that must be carried out to check that the data meets the associated data requirements specification.
- Conduct the IRs

Data Management guideline





Data Requirements Specification step

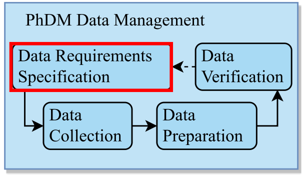
C2.3

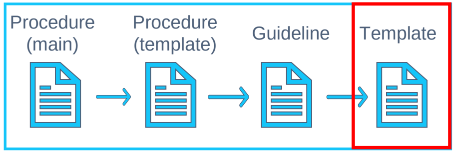
"Additionally, the dataset requirements should define the degree of differentiation between the datasets." – this is a very general requirement. It would be better to be more precise about the differences of the data sets.

Previous:

- Degree of differentiation between the datasets: Examples of such requirements may include training the model with real-world data and validating it with simulated data, introducing variations in the resolution of the inputs, or providing more extensive coverage for certain objects in the training dataset...

Data Requirements Specification template





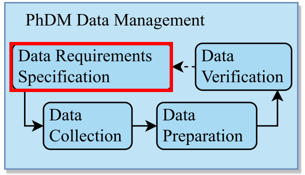
REF_PhDMD0001_Data_Requirements_Specification.docx

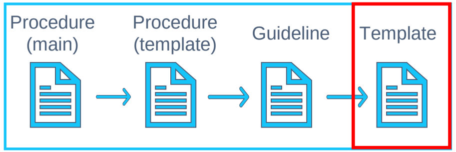
It includes:

- Example of definition of the filename policy: <Data_Procedence>_<ID_number>.<Data_Format>
    - <Data_Procedence>: Sensors (SENS), Synthetically generated data (SYNT), normalized data (NORM) …
    - <ID_number>: Identifier starting from 0 to N. Each <Data_Procedence> group starts at 0.
    - <Data_format>: I.e., resolution (1920x1080)
- Requirement Specification Table (common to all the phases)

<Identifier>	<Title>
Description	A brief description clearly and unambiguously defining the requirements in a couple of lines.
Source	The person, department, or source of relevant information associated with the description of the requirement.
Phase of the lifecycle	Data Management
Reference	References relevant to the requirement, i.e. documents, files,
Type	Mandatory/Desirable/Optional
Validation criteria	The requirement will have associated with at least one validation criterion: - Inspection - Analysis - Test
Date	Date of the definition of the requirements: Format YYYY/MM/DD
Version	The version has to follow a consecutive order

Data Requirements Specification template





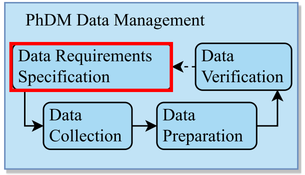
REF_PhDMD0001_Data_Requirements_Specification.docx

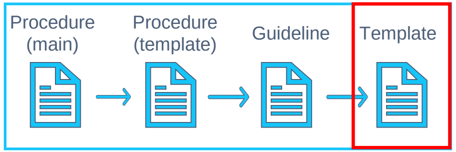
It proposes to decompose these reqs. to the following subgroups:

- Data reqs. specification (format, data characteristics)
- Dataset reqs. Specification
  - Completeness
  - Representativeness
  - Volume
  - Data origin
  - Degree of differentiation between the datasets.

SAFEXPLAIN

Data Requirements Specification template





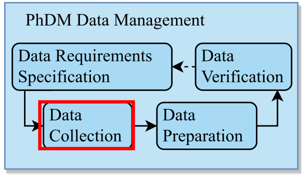
C13

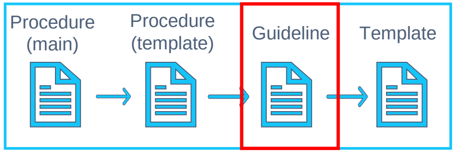
“Representativeness. Requirements associated with ensuring that data are representative of the Operational Design Domain (ODD). I.e., the definition of visual scenarios, viewpoints, lighting conditions, and object variations. Furthermore, the data must maintain representativeness throughout the intended usage period. If there are modifications to the ODD post-system deployment, a reanalysis of the Data Management phase is necessary” This is a very important point. OK

This makes it also very important, that the ODD is really complete in a way, that it covers all elements of the real operational world.

SAFEXPLAIN

Data Management guideline

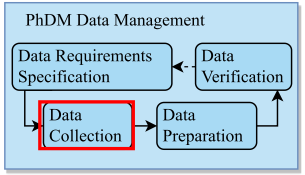


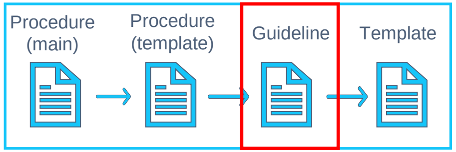


Data Collection step

- It can be decomposed into two substeps:
  - Data gathering: Referring to data directly obtained from sensors and datasets (before being prepared)
  - Data generation. New data that is synthetically generated, employing data augmentation techniques …
- All information relative to the data source and the process and decision made in the data gathering and generation shall be documented.
- Raw data files collected in each iteration of Data collection shall be stored in the “PhDM Data Management/Collected data” folder.
- Conduct the IR

Data Management guideline

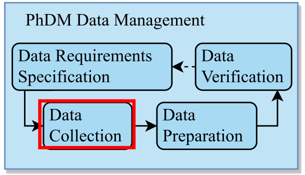


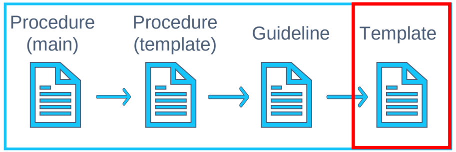


C2.2

By using synthetic data together with real world data, there must be ensured, that the AI doesn't get a biased during training to detect special cases just by from the synthetic data.

Data Collection template





REF_PhDMD0002_Data_Collection.docx

It includes

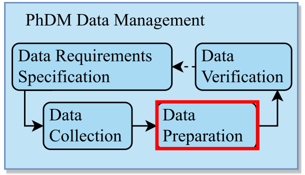
Table 1. Information related to the Data Gathering step

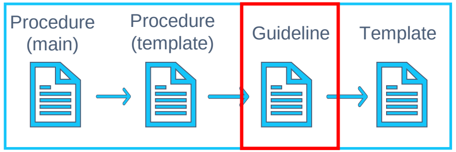
Data Gathering	
Date	Date of the collection: Format YYYY/MM/DD (Year/month/day)
Responsible	The person who collects the data
Phase of the lifecycle	Data Management
Description	Description of the data collection. It should include information of the data such as: • Format. • Guaranteeing of the data integrity. • Object collected (I.e., people (from kids to elderly), only blonde people, or people from different races).
Data source	Origin of the data, if they have been collected with cameras, sensors, or if it has been obtained from a public dataset (include the link in this case and additional information such as version), etc.
Tools (optional)	Description of the data storage tools employed. Include the required information to replicate their use from scratch.
Data Storage	Include the path to the folder/source where the data is stored.
Observations	Additional information. I.e., specify that it has not been possible to collect the required amount of data to meet the data requirements. Due to this limitation, it is necessary to generate new data.

Table 2. Information related to the Data Generation step

Data Generation			
Date	Date of the collection: Format YYYY/MM/DD (Year/month/day)		
Responsible	The person who generates new data		
Phase of the lifecycle	Data Management		
Description	Description of the data generation process. It has to include the methodology used to generate new data (data augmentation, synthetic data generation, etc.)		
Storage path to source data **(optional)**	Storage path of the data taken as the source in the generation of new data.		
Storage path to generated data	Include the path to the folder/source where the new data is stored.		
Tools of Data Generation	Tools/programs/frameworks used to generate new data. Include the necessary information for configuration and replicating their use from scratch.		
Description of the Data Generation	Information related to the amount of data generated, how it was generated, etc. It should include enough information to replicate the generation operation.		
Data IDs of Generated Data Traceability among the new data generated from raw or simulation data. It should include the ID of the newly generated data and the identification of the source data file.			
Previous IDs	Previous IDs	New IDs	Proposal. Rename the previous identifier by adding the subindex 'GEN_' at the beginning of the name.
Expected results	The set of expected results for data collection or the reason for generating data.		
Observations	Additional information. I.e., problems encountered during the collection.		

Data Management guideline

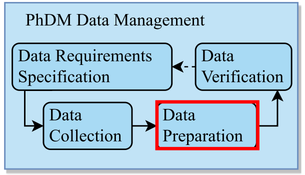


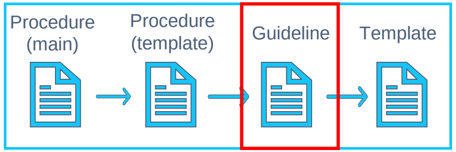


Data Preparation step

- Summarize the objective and the cases in which this step is necessary:
  - When the data need to be cleaned, processed or annotated.
  - All decisions made to prepare the data shall be documented
- All the documents should be stored in the "PhDM Data Management/Preparation" folder.
- Conduct the IRs

Data Management guideline



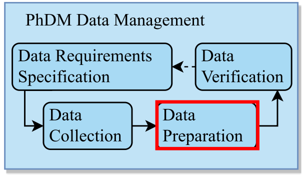


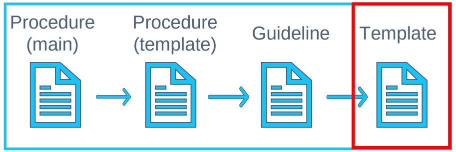
Data Preparation step

C4

"Data preparation is typically required when the raw data collected in the previous step has to be cleaned (i.e., removing anomalies), processed (perform normalization, scaling, feature selection…) or annotated (such as labelling) to match the defined input requirements of the model to be trained/verified." This is a very important statement. One can assume that in most cases the data sets for training, validation and verification need to undergo labelling to be used. Let's discuss on this

Data Preparation template





REF_PhDMD0003_Data_Preparation.docx

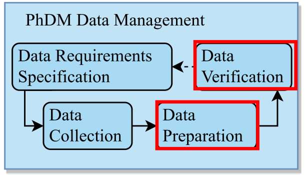
It includes:

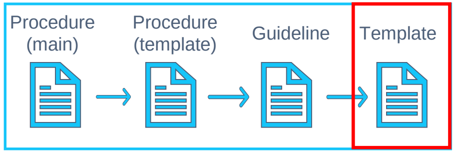
Table 1: Information related to the Data Preparation step

Data Preparation			
Date	Date of the preparation: Format YYYY/MM/DD (Year/month/day)		
Responsible	The person or team who annotates, cleans, preprocess, or structures the data.		
Lifecycle Phase	Data Management		
Description (technique used)	• *Data cleaning:* Removing anomalies using an anomaly detector, imputing missing values, etc or correcting erroneous values or standardizing values (e.g., cropping to remove irrelevant information from an image). • *Data processing:* Normalization (e.g., mi-max scaling, z-score normalization, robust scaling to reduce the sensibility to outliers...), scaling, feature Selection, dimensionality reduction, data Balance, fixing up formats through harmonising units (e.g., using consistent units), filling in missing values (different strategies can apply in this case, either removing the corresponding row in the dataset or filling missing data) ... • *Data annotation:* Manual annotation, Program-based annotation, etc.		
Reason for the Modification	Need to correct errors, improve data quality, adjust to new requirements, etc.		
Data ID of prepared data			
Previous IDs	Previous IDs:	News IDs	Proposal. Rename the previous identifier by adding the subindex 'PREP_' at the beginning of the name
Tools/Programs (optional)	Description of the tools and programs employed. Include the required information to replicate the preparation process from scratch. (I.e., Amazon Sage Maker Ground Truth)		
Details of the implementation (optional)	Details of the implementation (libraries, packages): • *Data annotation:* Annotate data using OpenCV. • *Data cleaning:* Removing anomalies using sklearn.svm.OneClassSVM. • *Data pre-processing:* Normalization of the data using sklearn.preprocessing.StandardScaler().		
Configuration of the environment	Package version, input parameters of the function used, etc. For example: train_test_split with parameters test_size=0.2 and random_state=0.		
Expected results	The set of expected results for the modification of the data applied.		
Observations	Additional information. I.e., specify that it has not been possible to collect the required amount of data to meet the data requirements and that for that reason it is necessary to generate new data.		

SAFEXPLAIN

Data Preparation template





REF_PhDMD0003_Data_Preparation.docx

C14.1

"Data cleaning" Be careful when cleaning: either use approved statistical methods or check, whether the data are really outside the ODD or really wrong" – Let's discuss this

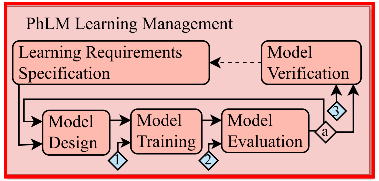
C14.2

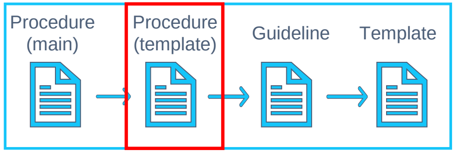
Inputing and Filling of missing data is listed under "data cleaning" and under "data processing"

Additional topics for discussion?

Break?

AI-FSM procedure template





Learning Management – Phase LM (PhLM)

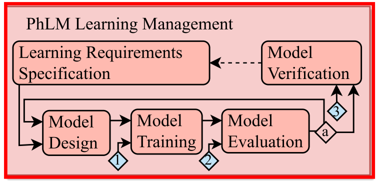
- Definition activities:
  - Collect learning requirements
  - Define learning req. evaluation tests & Learning req. verification tests
  - Design, train and evaluate the model
- Verification & validation:
  - Implement:
    - Learning req. evaluation tests
    - Learning req. verification tests
  - Conduct the Irs
  - Collect the tests in AI Log Test file
  - Update the state of AI Document List

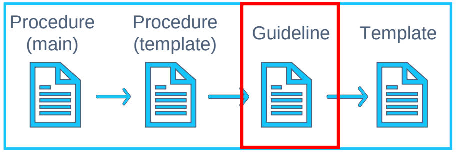
Table 5: Learning Management - PhLM summary (related to Ph3, Ph4 and Ph5 of the traditional lifecycle)

Phase	File input name	File output name	Responsible	Assessment
PhLM: Learning Management	*REF_Ph2D0001_DL_Requirements_Specifications*	*REF_PhLMD0001_Learning_Requirements_Specifications* *REF_PhLMD0005_Learning_Requirements_Evaluation_Tests* *REF_PhLMD0007_Learning_Requirements_Verification_Tests*		
		REF_PhLMD0002_Learning_Requirements_Specifications_IR *REF_PhLMD0006_Learning_Requirements_Evaluation_Tests_IR* *REF_PhLMD0008_Learning_Requirements_Verification_Tests_IR*		
		REF_PhLMD0003_Model_Election_Log		
		REF_PhLMD0004_Model_Election_Log_IR		
		Trained Model(s)		
		Evaluated Model(s)		
		Verified Learning Model(s)		

SAFEXPLAIN

Learning Management guideline



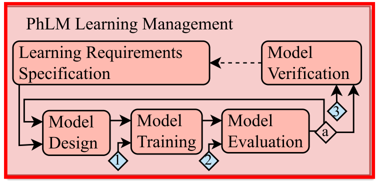


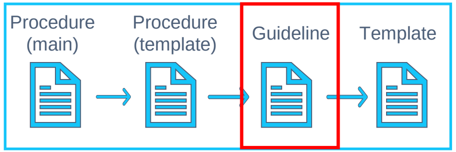
PhLM Learning Management

Table 5. Inputs and outputs of each step of the Learning Management phase (related to Ph3, Ph4 and Ph5 of the traditional lifecycle)

Phase	Step	Inputs	Outputs	Corresponding templates
PhLM Learning Management	Learning Requirements Specifications	REF_Ph2D0001_DL_Requirements_Specifications	REF_PhLMD0001_Learning_Requirements_Specifications REF_PhLMD0005_Learning_Requirements_Evaluation_Tests REF_PhLMD0007_Learning_Requirements_Verification_Tests	*PhLMT0001_Learning_Requirements_Specifications_template* *Ph0T0009_Test_definition_and_results_template* *Ph0T0009_Test_definition_and_results_template*
		REF_PhLMD0001_Learning_Requirements_Specifications REF_PhLMD0005_Learning_Requirements_Evaluation_Tests REF_PhLMD0007_Learning_Requirements_Verification_Tests	REF_PhLMD0002_Learning_Requirements_Specifications_IR REF_PhLMD0006_Learning_Requirements_Evaluation_Tests_IR REF_PhLMD0008_Learning_Requirements_Verification_Tests_IR	*PhLMT0001_Learning_Requirements_Specifications_template_IR* *Ph0T0009_Test_definition_and_results_template_IR* *Ph0T0009_Test_definition_and_results_template*
	Model Design	REF_PhLMD0001_Learning_Requirements_Specifications	REF_PhLMD0003_Model_Election_Log	*PhLMT0002_Model_Election_Log_template*
		REF_PhLMD0003_Model_Election_Log	REF_PhLMD0004_Model_Election_Log_IR	*PhLMT0002_Model_Election_Log_template_IR*
	Model Training	REF_PhLMD0003_Model_Election_Log Training dataset	Trained Model(s)	*There is not a template, it should be considered as an implementation.*
	Model Evaluation	REF_PhLMD0005_Learning_Requirements_Evaluation_Tests Trained Model(s) Validation dataset [2]	REF_PhLMD0005_Learning_Requirements_Evaluation_Tests Evaluated Model(s)	*Document previously generated*
	Learning Model Verification	REF_PhLMD0007_Learning_Requirements_Verification_Tests Evaluated Model(s) Verification dataset	REF_PhLMD0007_Learning_Requirements_Verification_Test Verified Learning Model(s)	*Document previously generated*

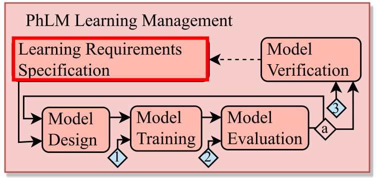
Learning Management guideline

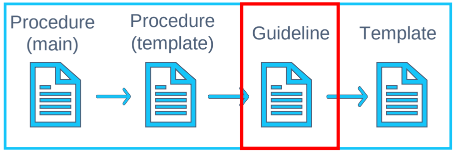




PhLM Learning Management

- The objective of this phase is the generation of:
    - Model trained
    - Model Evaluated
    - Learning model verified
- As previously mentioned, the following document should be generated:
    - REF_PhLMD0001_Learning_Requirements_Specifications.docx. (+IR)
    - REF_PhLMD0003_Model_Election_Log.docx. (+IR)
    - REF_PhLMD0005_Learning_Requirements_Evaluation_Tests.docx. (+IR)
    - REF_PhLMD0007_Learning_Requirements_Verification_Tests (+IR)
- All the documents should be stored in the “PhLM Learning Management” folder.





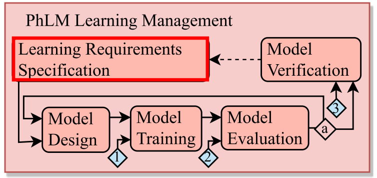
Learning Management guideline

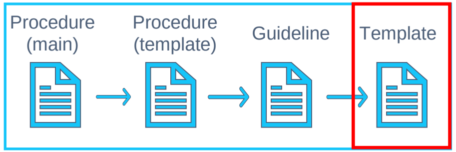
Learning requirements specification

- It directly addresses the safety designer to the learning reqs. specification template.
- Define the mechanisms or tests that must be carried out to check that the learning model meets the associated learning requirements specification:
  - Learning reqs. evaluation tests
  - Learning reqs. verification tests
- Conduct the IRs

IMP: These tests are not verification or validation tasks according to functional safety standards.

Learning Requirements Specification template





REF_PhLMD0001_Learning_Requirement_Specification.docx

It proposes decomposing the Learning reqs. into:

- Quantitative:
  - Model bias and variance boundaries -> focusing on avoiding underfitting and overfitting
  - Performance and robustness reqs. For ex: recall, precisión, **accuracy** or F1 score.
- Qualitative:
  - Methodology for searching the hyperparamenters

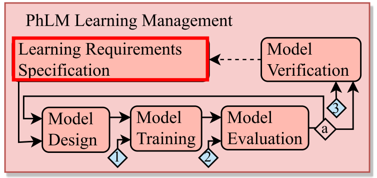
Define a Model Election criteria. For example:

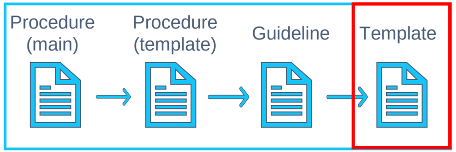
- Prioritizing classes accuracy
- Robustness regarding especific environments
- Emphasis on explainability

Table 1. Table of attributes for each requirement

<Identifier>	<Title>
Description	
Source	
Phase of the lifecycle	
Reference	
Type	
Validation criteria	
Date	
Version	

Learning Requirements Specification template





REF_PhLMD0001_Learning_Requirement_Specification.docx

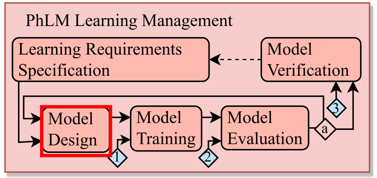
C16

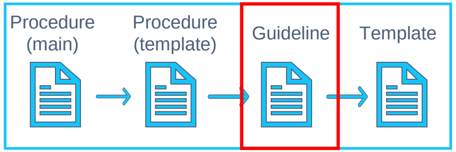
"Accuracy". Please note, that in fact during learning, the AI model statistically estimates the parameters it is defined by. These estimated parameters contain random influences. This is also part of the precision of the AI model and it can be estimated during verification. Let's discuss on this

C16

For the sake of robustness it is worthwhile to include corner cases for learning as well as for verification

Learning Management guideline

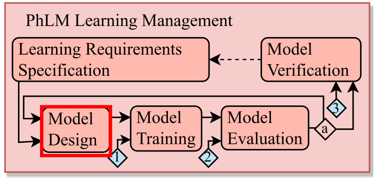


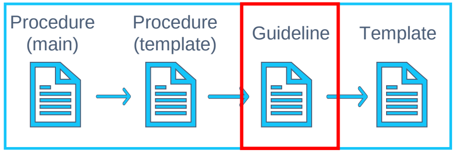


Model Design

- The objective of this step is to specificate a set of DL models that suits the application
- It explains aspects to be considered in the election of the DL such as:
  - Model Architecture
  - Pretrained Models
  - Hyperparameter tunning
  - …
- It finally addresses the user to the REF_PhLMD0003_Model_Election_Log.docx template.

Learning Management guideline





Model Design

C5

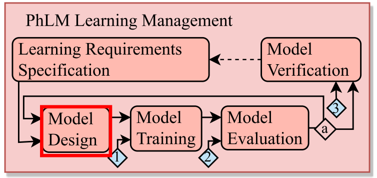
"The choice of the most appropriate model for the problem is often based on the designer's expertise." – This is a very general statement.
I miss a criterion for model selection. On the other hand, I understand that for such a general FSM system this might be impossible to define in a general manner. Let´s discuss on this.

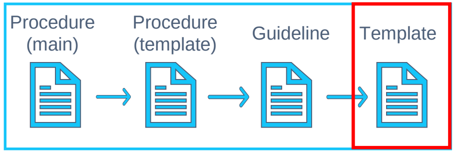
C6

Can you extend the list under the bullet point "Model architecture" (given after "For example" in line 3 from below)?

C7

The use of pre-trained models can be dangerous. In fact, the pooling of several samples is left here to the AI. "similar" data might be out of the ODD.....if they are inside the same ODD - then it is only logic to use them in a merged from in a normal manner. Let's discuss on this.





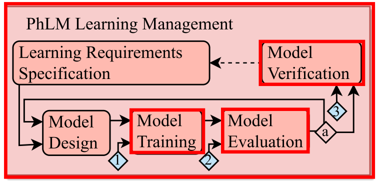
Model Election Log

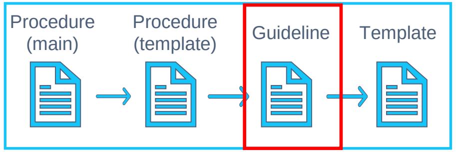
REF_PhLMD0003_Model_Election.docx

- It includes:

Model design	<Model_ID>_<version>
Date	Date of design: Format YYYY/MM/DD (Year/month/day)
Responsible	The person who designs the model
Phase of the lifecycle	Learning Management
Framework used	Specify the framework used to train the model: tensorflow, pytorch, keras, etc.
Model Format	Training model depends on the DL training framework employed: PyTorch (.pth), Keras (.h5), ONNX (.onnx)
Model Functionality	Specify the functionality of the model: detection, classification, etc.
Model Architecture	Specify the architecture of the model considered, including information such as the typology of layers (LSTM, CNN, RNN, Dropout, etc.)
Hyperparameters	Specify the hyperparameters used to train the model, including information such as: • Number of hidden layers, number of nodes per layer, etc. • Type of activation function of each layer: linear, tanh, relu, sigmoid, etc. • Learning rate: determines the step size at which the optimization algorithm updates the model´s parameters during training. • Type of loss function: Mean Squared Error (MSE), Mean Absolute Error (MAE), Huber Loss, Binary Cross-entropy, Multi-class Cross-entropy/categorical Cross-entropy… • Batch size: It refers to the number of training instances in the batch or the number of instances used per gradient update (each update equivalent to an iteration). • Epochs: number of times the model evaluates the entire training dataset • Optimizer: SGD, ADAM, RMSProp, etc.
Techniques used	If necessary, specify information about techniques that have been used to avoid overtraining or improve the generalizability of the model, such as: • Early Stopping: it stops training when no improvement in the validation metric is observed for a predefined number of epochs. In this case, specify the parameters used (patience, tolerance, etc.) • Regularization techniques: ○ L1 and L2 Regularization: These techniques add penalty terms to the loss function based on the magnitudes of model weights. They encourage smaller weights, reducing the risk of overfitting. ○ Dropout: During training, randomly set a fraction of the input units to zero at each update. This prevents the model from relying too heavily on any specific feature, promoting more robust representations. • Learning Rate Scheduling: ○ Learning Rate Annealing: Gradually reduce the learning rate during training. This can help the model converge more effectively and avoid overshooting minima. ○ Cyclical Learning Rates: Periodically increase and decrease the learning rate within certain bounds. This can help the model escape local minima and find better solutions.
Pretrained models	Specify if the model is trained from scratch or the source of the initial parameters. In the case of using pre-trained models, specify the path to the folder where they are stored.

Learning Management guideline





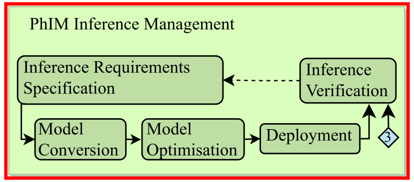
Model Training: In this step, the specified models are generated employing the training dataset

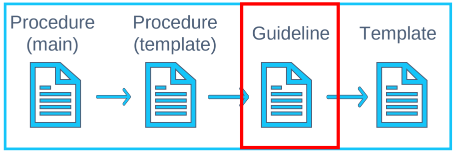
Model Evaluation: Once the model(s) are trained, they are evaluated employing the validation dataset:

- Explain the different situations that can arise:
  - None of the candidate models achieve the expected performance the:
    1. Iterative repeat the design, training and evaluating steps until meeting them
    2. If they are not meeting -> new iteration of the Data Management phase
  - Multiple candidates demonstrate the expected performance -> All will be evaluated in the next step

Model Verification: This phase not only evaluates the generalization capabilities and identifies potential issues using the verification dataset but also checks if the reqs. are met.

Inference Management guideline

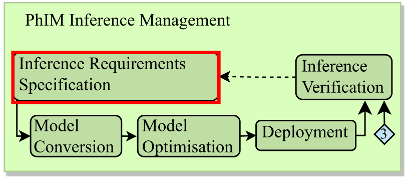


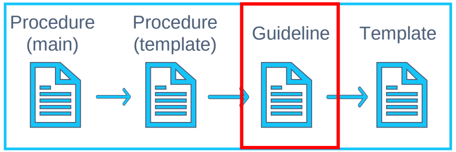


PhIM Inference Management

- The objective of this phase is the generation of:
  - Model converted
  - Model optimised
  - Inference model verified
- As previously mentioned, the following document should be generated:
  - REF_PhIMD0001_Inference_Requirements_Specifications.docx. (+IR)
  - REF_PhIMD0003_Model_Conversion_Log.docx. (+IR)
  - REF_PhIMD0005_Model_Optimization_Log.docx. (+IR)
  - REF_PhIMD0007_Inference_Requirements_Verification_Tests. (+IR)

Inference Management guideline

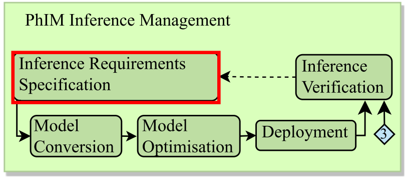


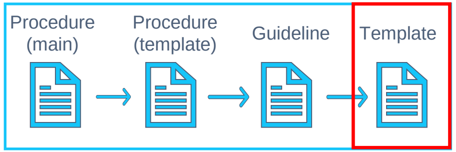


PhIM Inference reqs. specification

- Inference Management guidelines indicates that in this step:
  - The requirements and verification tests shall be defined
  - The IRs shall be conducted
- Inference management guideline directly addresses the user to the template.

Inference Requirements Specification template



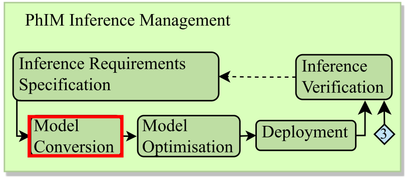


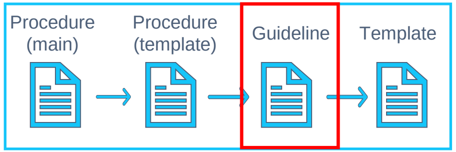
REF_PhIMD0001_Inference_Requirements_Specifications.docx

It proposes decomposing the Learning reqs. into:

- Reqs. associated with model conversion
  - Computer arithmetic
  - Software dependencies
- Rqs. associated with model optimization
  - Model quantization
  - Model pruning
- Reqs. associated with model deployment
  - Memory limitations
  - Execution time restrictions

Inference Management guideline

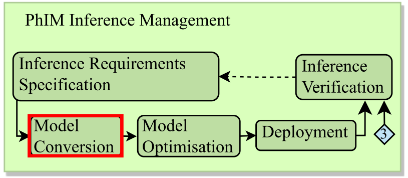


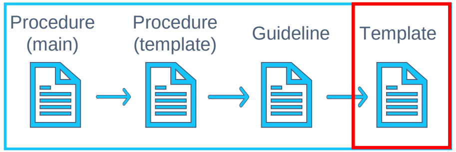


Model Conversion

- Inference Management Guideline includes:
  - Definition of the model conversión
  - Specifies that all the information of this step shall be documented in the associated template.Ex:
    - Training-specific operations removed
    - Loading and converting operations performed.
- Conduct the IR

Model Conversion template





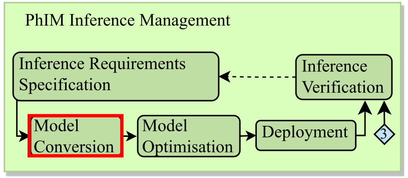
REF_PhIMD0003_Model_Conversion_Log.docx

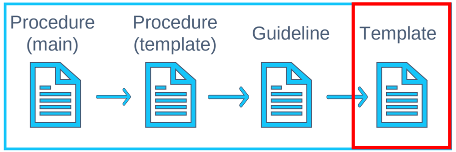
- It includes:

Table 1. Model conversion information

Model conversion	<Model_conversion_ID>
Date	Date of design: Format YYYY/MM/DD
Responsible	The person who converts the model
Phase of the lifecycle	Inference Management
Verified Learning Model	
Verified Learning Model ID	<Model_ID>_<Model_ID_version>
...	...
Elimination of Training-Specific Operations	
- Dropout - Batch Normalization - Gradient Clipping - Learning Rate Scheduling - Weight Regularization (L1,L2)	
Loading and Converting the Verified Learning Model	
Framework and version	Specify the framework used to convert the model and its version: TensorFlow, pytorch, keras, etc.
Packages and version	Tensorflow (keras, tensorflow), onnx-tf (onnx), torch (pythorch)...
Converter/model conversion script	In case of using tool for converting the model or separate scrips, it should be stored the configuration and its paragmeters. For example, the use of torch.onnx.export or tf2onnx functions/tools used in PyTorch and TensorFlow to export trained models to ONNX format
Environment information	Operation system or any additional information relevant to the conversion process

Model Conversion template



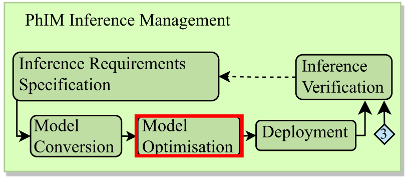


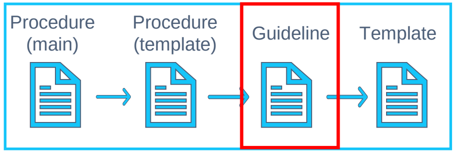
REF_PhIMD0003_Model_Conversion_Log.docx

C15

Model conversion must keep the essential properties of this model. Let's discuss on this.

Inference Management guideline





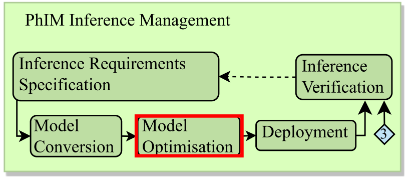
Model Optimisation:

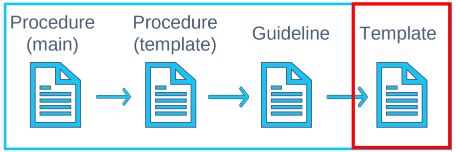
The guideline proposes completing the template with the information related to model optimization and outlines some information that shall be included in it:

- Calibration fundamental operations
- Post-training quantization specifications
- Pruning specifications
- Techniques to recover accuracy:

- Once finished, the IRs shall be carried out

Model Optimisation template





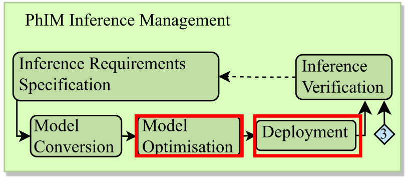
REF_PhIMD0005_Model_Optimization_Log.docx

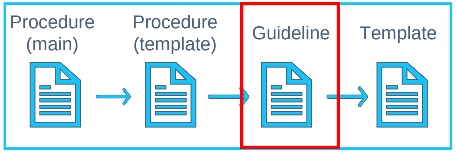
- It includes:

Model optimization	<Model_optimization_ID>
Date	Date of design: Format YYYY/MM/DD (year, moth, day)
Responsible	The person who converts the model
Phase of the lifecycle	Inference Management
Input Model Specifications	
Verified Learning Model ID or Model Conversion ID	<Model_ID>_<Model_ID_version> or, if the model have just been converted: <Model_conversion_ID>
Calibration fundamentals operations (preprocessing operations before post-quantization)	
Calibration	Set the range to a maximum absolute value seen during calibration, to a percentile of the distribution of absolute values, use specific methods such as the KL divergence method to obtain an entropy value...
Transformation function	For instance: $f(x)=s \cdot x$
Scale factor	I.e., $s= (2^b−1) / (\alpha−\beta)$
Post-training quantization specifications	
Framework and version	Specify the framework used to convert the model and its version: TensorFlow, pytorch, keras, etc.
Packages and version	Tensorflow (keras, tensorflow), onnx-tf (onnx), torch (pythorch)...
Quantization precision	Precision level for quantization: 8-bit (int8_t, uint8_t), int8, 16-bit (int16_t,uint16_t)
Quantization scheme	Symmetric/asymmetric
Quantization technique	Weight quantization, integer quantization...
Quantization granularity	Layerwise quantization, channelwise quantization, groupwise quantization... In case of being a particular quantization for each layer, group of layers... there would be specified configurations for each of the quantizations.
Additional configurations	Include here all the information that makes the quantization reproducible
Pruning specifications	
Framework and version	Specify the framework used to convert the model and its version: TensorFlow, pytorch, keras, etc.
Packages and version	Tensorflow (keras, tensorflow), onnx-tf (onnx), torch (pythorch)...
Pruning criteria	Weight magnitude, gradient magnitude, global or local threshold...
Pruning patterns	Element-wise, vector-wise, block-wise, group-wise...
Additional configurations	
Techniques to recover accuracy	
Partial quantization configurations	
Quantization-aware training configurations	
Learning quantization parameters configurations	

SAFEXPLAIN

Inference Management guideline





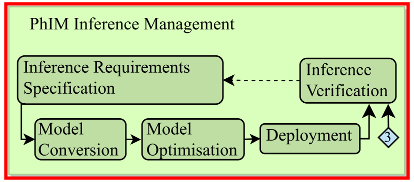
Deployment:

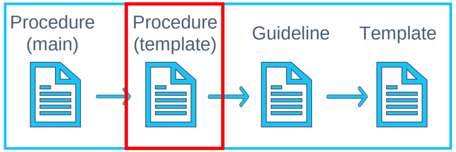
- This step entails the implementation of the model in the target platform.

Inference verification.

- This step not only evaluates the generalization capabilities and identifies potential issues using the verification dataset but also checks if the reqs. are met.
  - If they are not meet, the inference model process shall be reiterated. If the inference model still does not meet the inference requirements specifications, further corrective actions or adjustments in the Data Management and the Learning Management may be required.
- Conduct the IR

AI-FSM procedure template





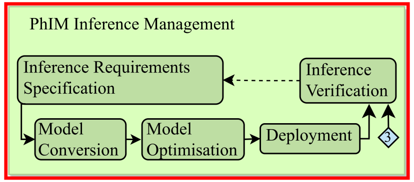
Inference Management – Phase IM (PhIM)

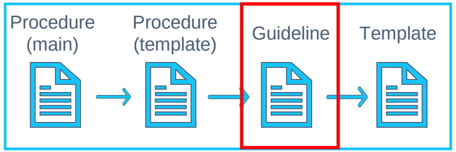
- Definition activities:
  - Collect inf. requirements
  - Define inf. req. verification tests
  - Convert the model
  - Optimise the model
- Verification & validation:
  - Implement inf. req. verification tests
  - Conduct the IRs

Table 6: Inference Management – PhIM summary (related to Ph3, Ph4 and Ph5 of the traditional lifecycle)

Phase	File input name	File output name	Responsible	Assessment
PhIM: Inference Management	REF_Ph2D0001_DL_Requirements_Specifications REF_PhLMD0001_Learning_Requirements_Specifications Verified Learning Model	REF_PhIMD0001_Inference_Requirements_Specifications REF_PhIMD0007_Inference_Requirements_Verification_Tests		
		REF_PhIMD0002_Inference_Requirements_Specifications_IR REF_PhIMD0008_Inference_Requirements_Verification_Tests_IR		
		REF_PhIMD0003_Model_Conversion_Log		
		Converted Model		
		REF_PhIMD0004_Model_Conversion_Log_IR		
		REF_PhIMD0005_Model_Optimization_Log		
		Optimized Model		
		REF_PhIMD0006_Model_Optimization_Log_IR		
		Verified Inference Model		

Inference Management guideline





PhIM Inference Management

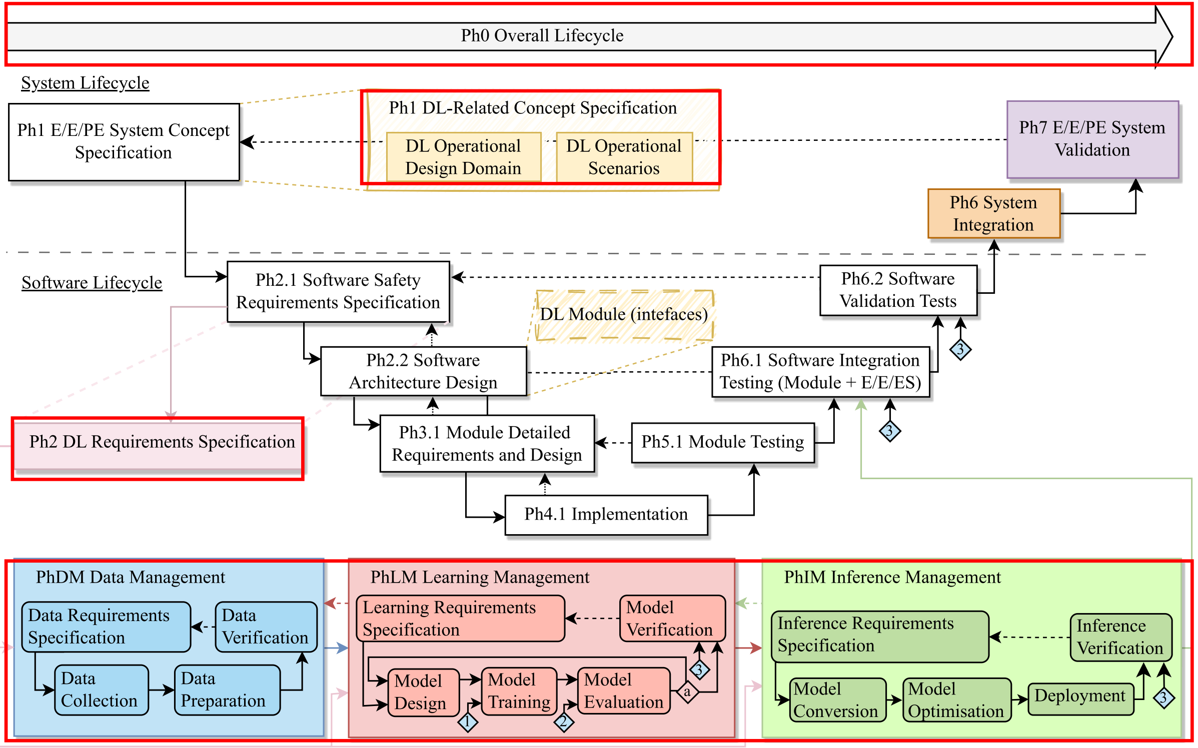
Table 6. Inputs and outputs of each step of the inference stage (related to Ph3, Ph4 and Ph5 of the traditional lifecycle)

Phase	Step	Inputs	Outputs	Corresponding templates
PhIM Inference Management	*Inference Requirements Specifications*	*REF_Ph2D0001_DL_Requirements_Specifications* *REF_PhLMD0001_Learning_Requirements_Specifications*	*REF_PhIMD0001_Inference_Requirements_Specifications* *REF_PhIMD0007_Inference_Requirements_Verification_Tests*	*PhIMT0001_Inference_Requirements_Specifications* *Ph0T0009_Test_definition_and_results_template*
		REF_PhIMD0001_Inference_Requirements_Specifications *REF_PhIMD0007_Inference_Requirements_Verification_Tests*	*REF_PhIMD0002_Inference_Requirements_Specifications_IR* *REF_PhIMD0008_Inference_Requirements_Verification_Tests_IR*	*REF_PhIMD0002_Inference_Requirements_Specifications_IR* *Ph0T0009_Test_definition_and_results_template_IR*
	Model Conversion	*REF_PhIMD0001_Inference_Requirements_Specifications* Verified Learning Model	*REF_PhIMD0003_Model_Conversion_Log* Converted Model	*PhIMT0002_Model_Conversion_Log*
		REF_PhIMD0003_Model_Conversion_Log	*REF_PhIMD0004_Model_Conversion_Log_IR*	*PhIMT0002_Model_Conversion_Log_IR*
	Model Optimization	*REF_PhIMD0001_Inference_Requirements_Specifications* Converted Model	*REF_PhIMD0005_Model_Optimization_Log* Optimized Model	*PhIMT0003_Model_Optimization_Log*
		REF_PhIMD0005_Model_Optimization_Log	*REF_PhIMD0006_Model_Optimization_Log_IR*	*PhIMT0003_Model_Optimization_Log_IR*
	Inference Model Verification	*REF_PhIMD0007_Inference_Requirements_Verification_Tests* Optimized Model or Converted Model Verification dataset	*REF_PhIMD0007_Inference_Requirements_Verification_Tests* Verified Inference Model	*Document previously generated*

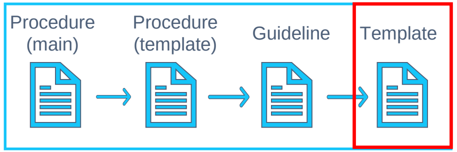
SAFEXPLAIN

AI-FSM in-depth

- **Explanation order:**



Ph1 DL-related concept specifications



REF_Ph1D0001_DL_Operational_Design_Domain.docx

- Purpose: Operating conditions under which a given overall system or feature is specifically designed to function (e.g., environmental restrictions, certain scenery characteristics, and dynamic elements surrounding the system).
  - Ph1T0001_DL_Operational_Design_Domain_template.docx
    - Categorization to describe the ODD, but customizable.

1) Scenery
   a) Physical infrastructure
   b) Operational constraints
   c) Zones
2) Environmental conditions
   a) Weather
   b) Particulate
   c) Illumination
   d) Connectivity
3) Dynamic elements
   a) Object types
   b) Object characteristics

- Scenery

Speed Limits	
Minimum Speed Limit	0 km/h
Maximum Speed Limit	90 km/h
Maximum Speed Limit entering station	30 km/h
Maximum Speed Limit exiting station	30 km/h
Minimum Speed Limit (standstill)	0 km/h

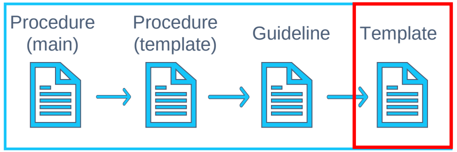
- Environmental conditions

Weather	
Rain	No
Fog	No
Sunny	Yes
Clear day	Yes
Cloudy	Yes

- Dynamic elements

Objects	
Animals	Cow, dog, bird
Person	Yes
Vehicles	Car
Others	Yes

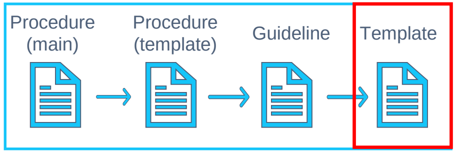
Ph1 DL-related concept specifications



C12.2

Overhead lines are not mentioned as elements of rail infrastructure environment (Ch. 4, p. 3)

Ph1 DL-related concept specifications



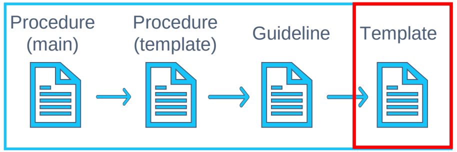
REF_Ph1D0002_DL_Operational_Scenarios.docx

- Objective: Specify operations, scenarios and environmental conditions for the system in which the system has to function according to the specification under the ODD. And must include standard situations but also challenging environments and cornerstone situations.
- Ph1T0002_DL_Operational_Scenarios_Template.docx
  - Gathers information of the specific scenario conditions

Operational Scenario 1	
With the conditions specified, the following operational scenario is described: A stopped object is parked, which is situated on the side of the track. The train is moving at a 50 km/h speed and accelerating 1m/s². The detected object must be analyzed if it is placed on the tracks or not, if it is a critical object or not, and the estimated distance where the object is located from the train. Depending on the results of these questions, the actions taken by the train will be different.	
Scenario Conditions:	
Scenery	
Maximum Speed Limit	90 km/h
Countryside	Yes
Multiple tracks	Yes
Distance threshold (warning)	[1001,1500] m
Distance threshold (warning & reduce)	[701, 1000] m
Distance threshold (breaking activation)	700 m
Environmental Conditions	
Sunny day	Yes
Daylight	[1200,15000] lm
Dynamic elements	
Vehicle	Car stopped

SAFEXPLAIN

Ph2 DL Requirements Specification



REF_Ph3D0001_DL_requirements_specification.docx

Objective: Allocate the SW reqs. Specification to the DL constituent and refine them.

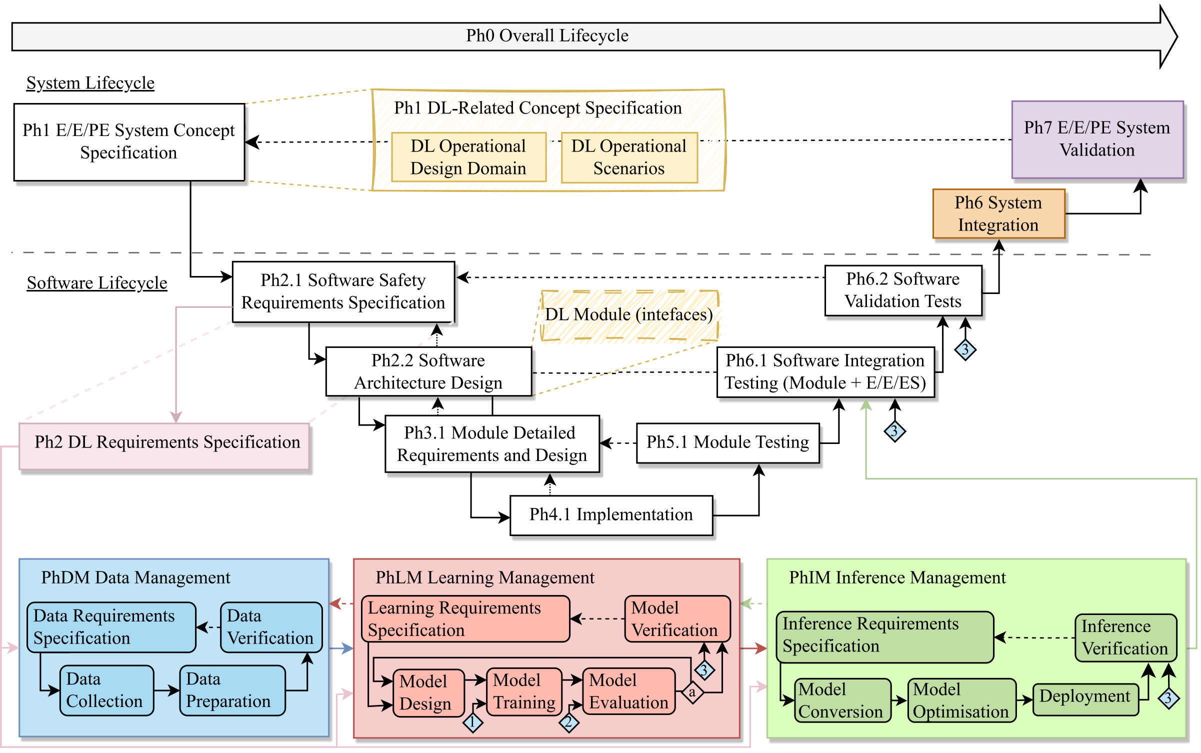
C12.2

"clear" makes use of "unambiguous" (wording; this concerns all requirements docs)

- **Unambiguous**. The requirements can be interpreted only one way.
- **Clear.** The requirement must be unambiguous and not misleading. The requirements are written in a way that allows them to be understood by all stakeholders in the project.

- **Clear.** The requirement must be **easy to understand** and not misleading. The requirements are written in a way that allows them to be understood by all stakeholders in the project.

AI-FSM in-depth

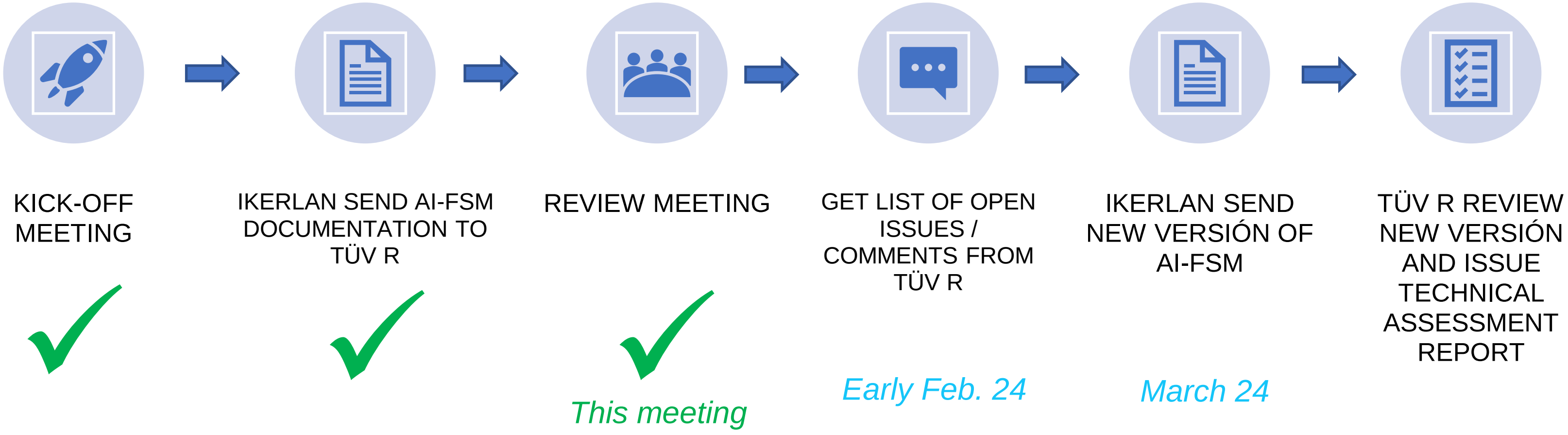


Additional topics for discussion?

Next steps

AI-FSM Activity planning

Activity 1: Review and assessment of the AI-FSM procedure w.r.t. IEC 61508 and ISO 5469 drafts	
WP 1.1	**Review** of the AI-FSM documentation (procedure, guidelines and templates), compilation of a draft list of comments and open issues
WP 1.2	Review **Workshop** in Arrasate-Mondragón (One day, two experts, online) including preparation and follow-up
WP 1.3	Issue of **Technical Note with open issues and comments** of the Review of the AI-FSM
WP 1.4	**Assessment** of revised AI-FSM, compilation of final Assessment Report including a general perception on the theoretical certifiability of such concepts



SAFEXPLAIN

Next steps

- Continue with Activity 1
  - IKR will address the changes suggested by TÜV R
  - IKR will modify and extend the current AI-FSM. Some potential areas for improvement include:
    - Hazard & Risk análisis + Failure & deficiency análisis -> Starting point: SOTIF
    - Adherence to the recently published IEC 5469 standard
    - Validation of the AI Systems / Safety assessment.
  - Send version 2.0 to TÜV R.

SAFEXPLAIN

Safe and Explainable
Critical Embedded Systems based on AI

Follow us on social media:

www.safexplain.eu

Funded by
the European Union

This project has received funding from the European Union's Horizon Europe programme under grant agreement number 101069595.

Scenarios catalogue
WP 2

gdallara@exida.com
carlo.donzella@exida-dev.com
francesca.guerrini@exida-eng.com
davide.cunial@exida-eng.com
giuseppe.nicosia@exida-dev.com
19/07/2023

V1R3

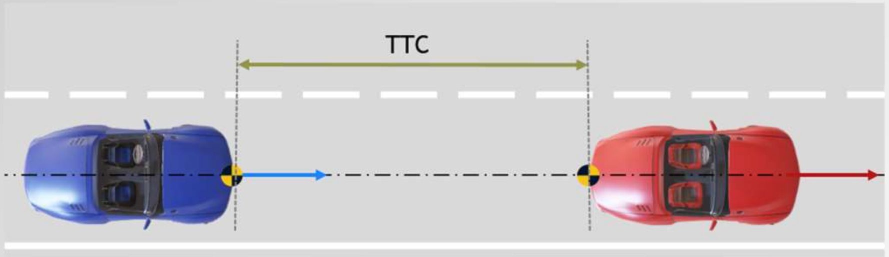
Scope and purpose

- The goal of this presentation is to shown the relevant driving scenario catalogue.
- For each driving scenarios is reported its probability of exposure (duration) (based on catalogue of manoeuvres, e.g., VDA-702) to allow the calculation of scenario weight.
- Both collision relevant and no collision relevant driving scenarios are reported in this presentation to analyse also False-positive detection by the intended functionality.

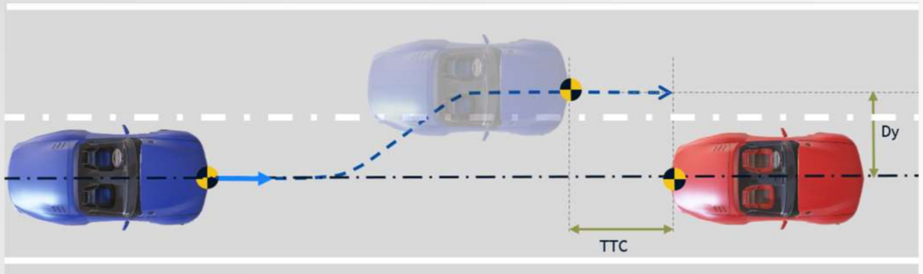
Scenarios catalogue summary 1/11

- The following list reports all the driving scenario contained in the driving scenario catalogue [with ID (e.g., DS-x) and title).
- For all the details on a given scenario, please refer to the dedicated scenario sheets.

- DS-1 – Driving following a target vehicle on highway

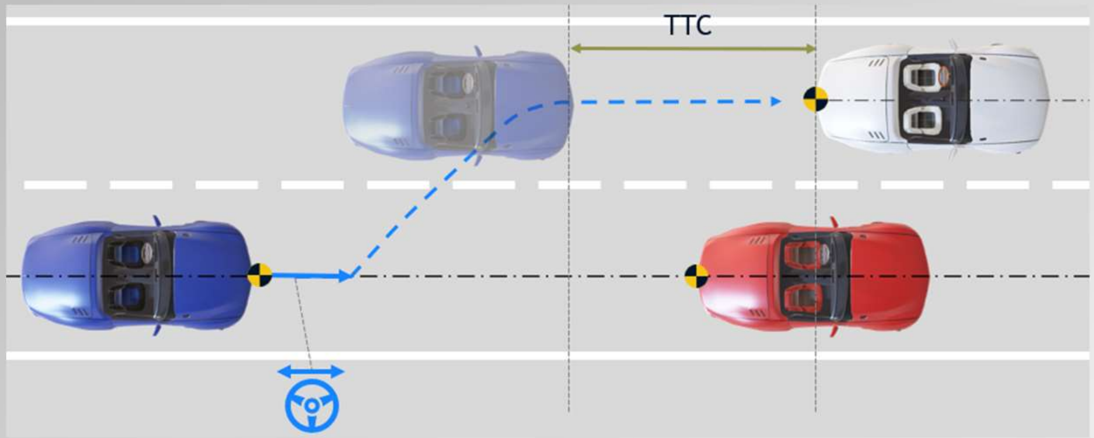


- DS-2 – Performing a lane change

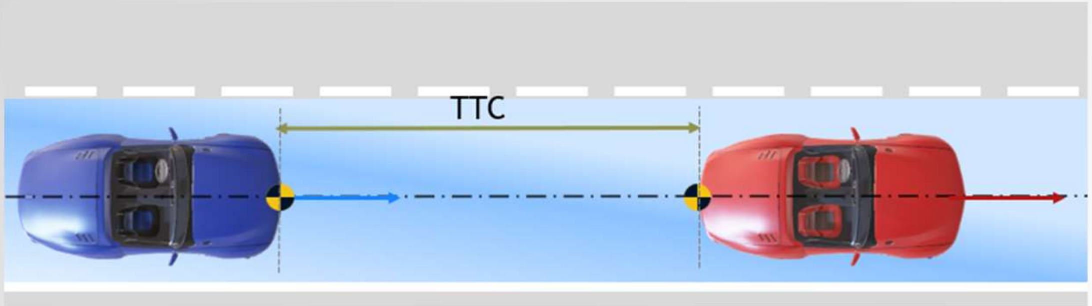


Scenarios catalogue summary 2/11

- DS-3 – Performing an overtaking and approaching a new target vehicle

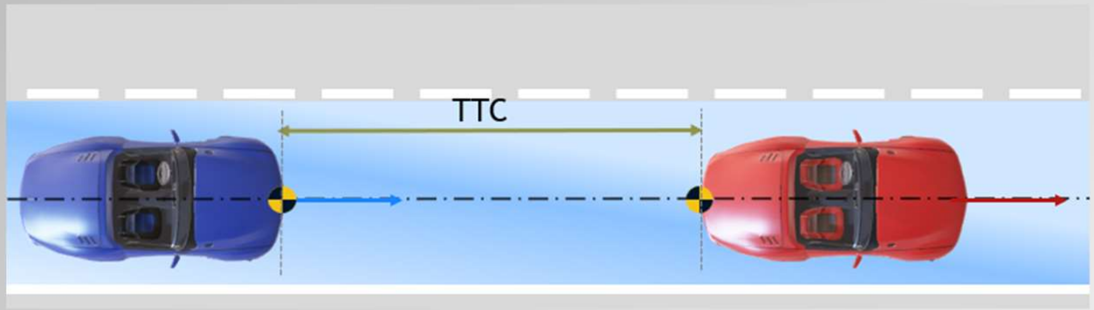


- DS-4 – Driving on road with reduced friction coefficient (μ < 0,8 ± -0,1)

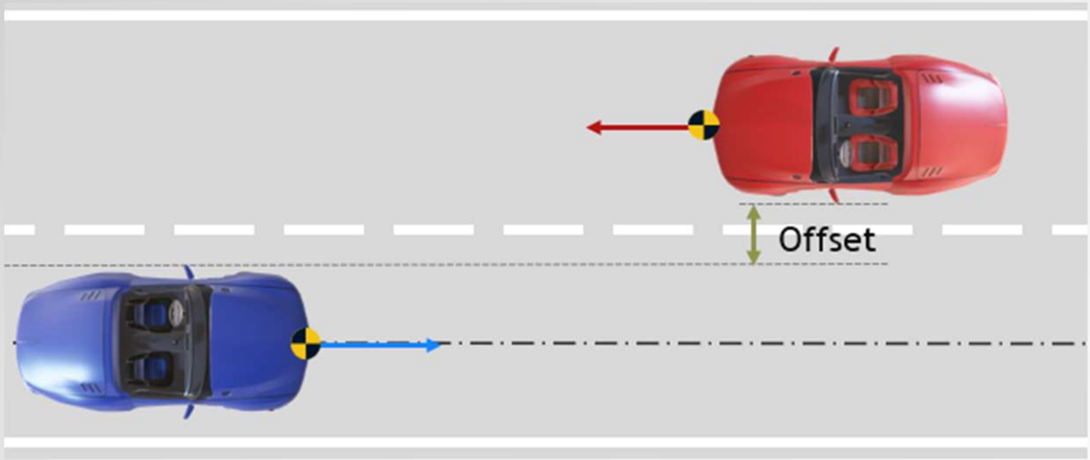


Scenarios catalogue summary 3/11

- DS-5 – Driving on road with low friction coefficient (μ < 0,5 ± -0,1 (e.g., snow, ice))

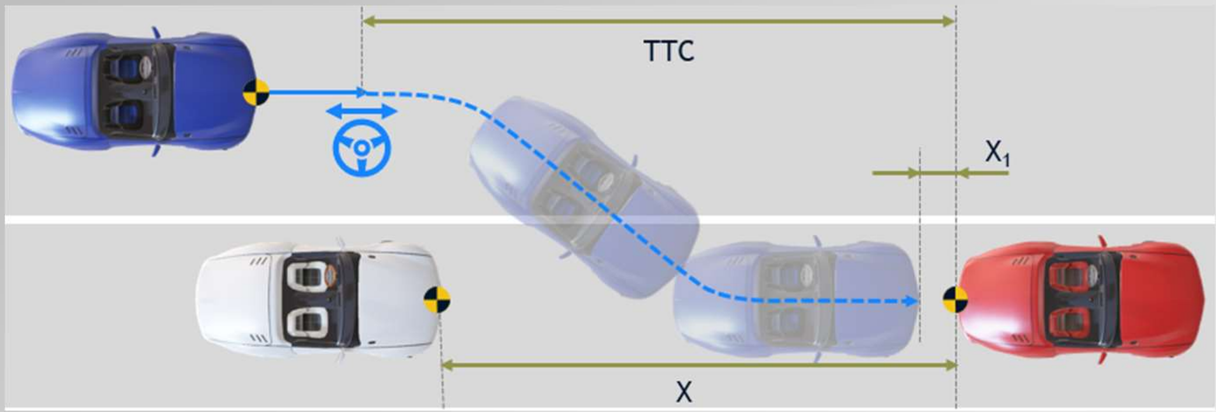


- DS-6 – Driving with a target vehicle coming from opposite direction

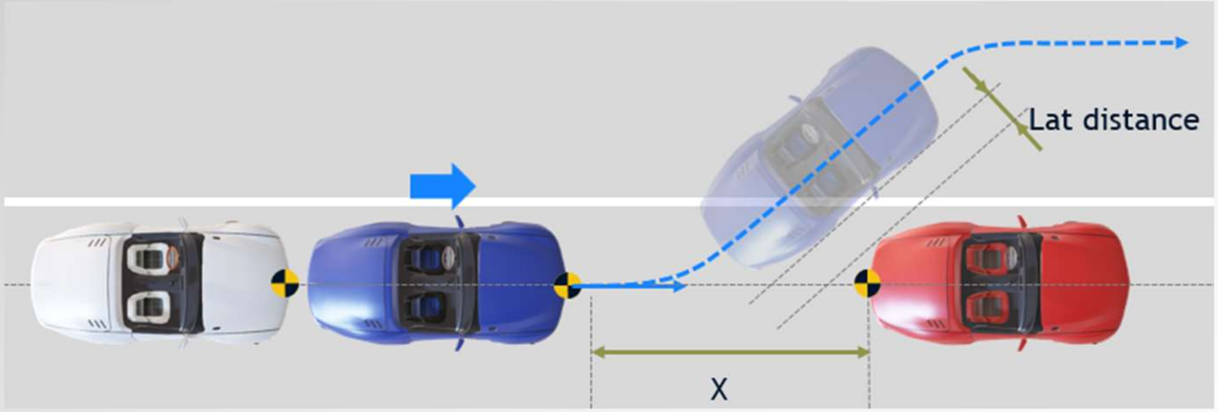


Scenarios catalogue summary 4/11

- DS-7 – Enter in a parking space in longitudinal direction

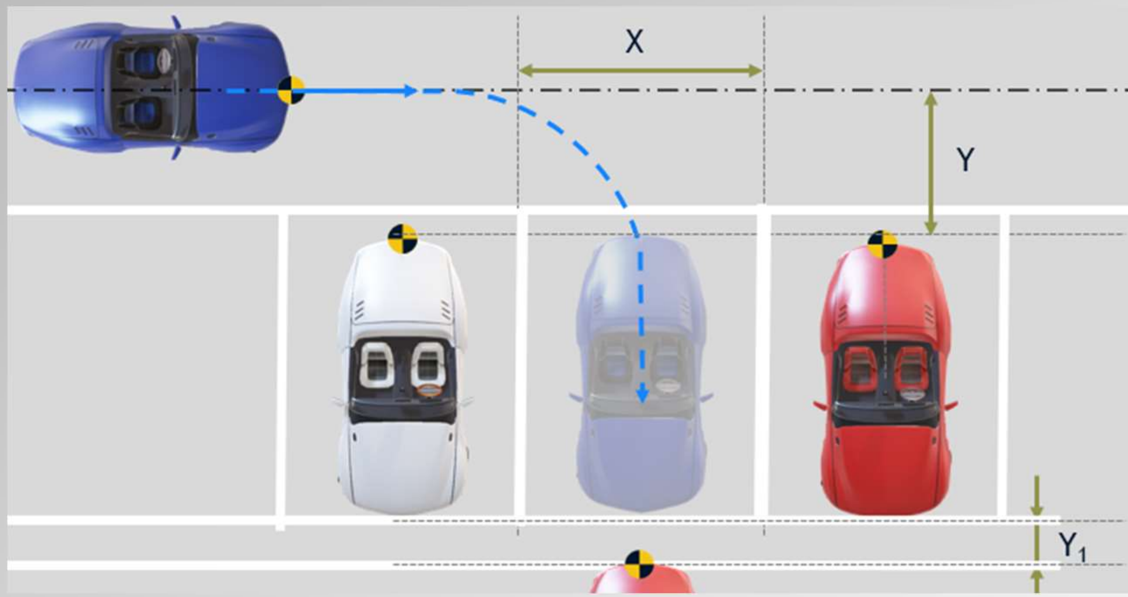


- DS-8 – Exit from a parking space in longitudinal direction



Scenarios catalogue summary 5/11

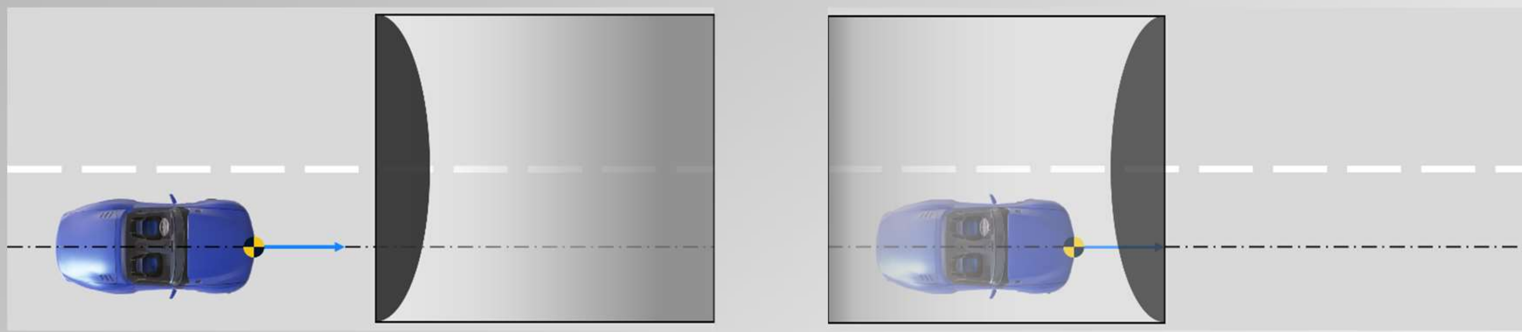
- DS-9 – Enter in a parking space in cross direction



- DS-10 – Driving with trailer attached

Scenarios catalogue summary 6/11

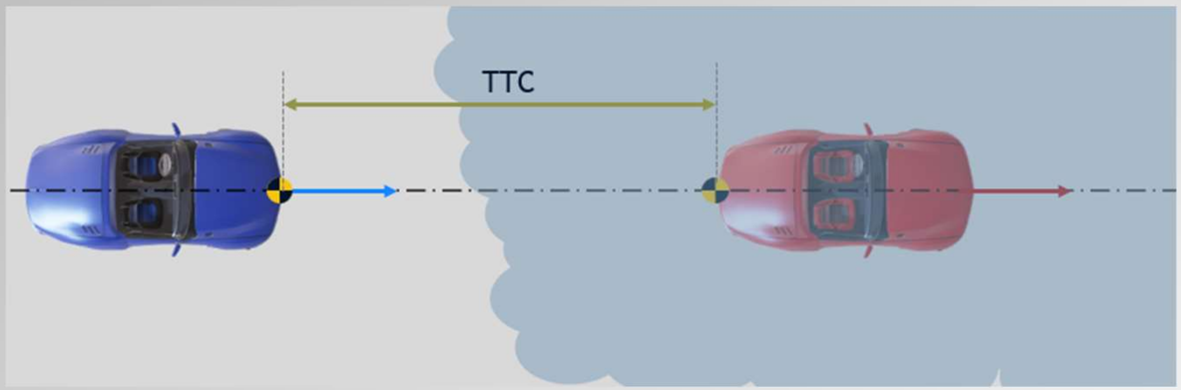
- DS-11 – Driving in a tunnel



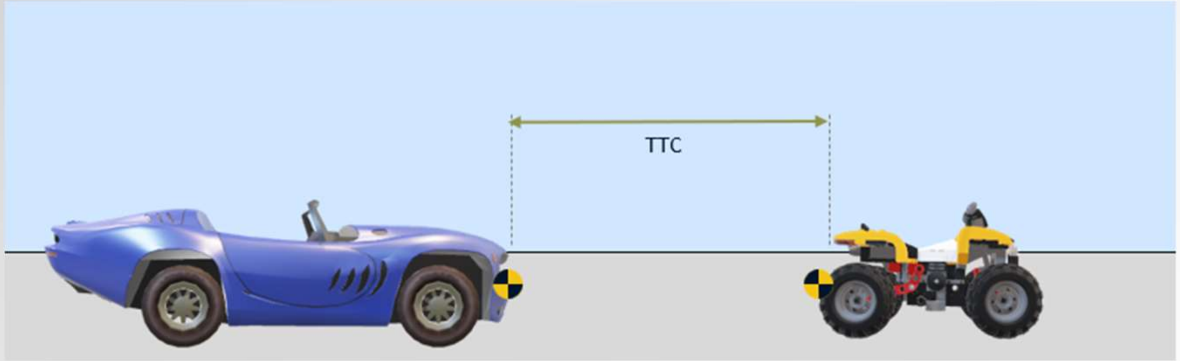
- DS-12 – Passing a crossroads

Scenarios catalogue summary 7/11

- DS-13 – Driving with low visibility (fog)

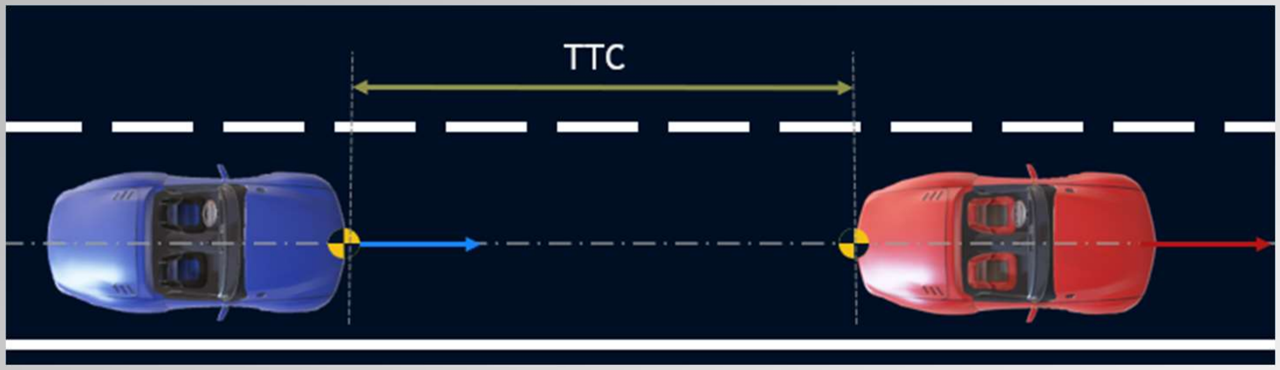


- DS-14 – Driving following a target vehicle (no normal configuration)

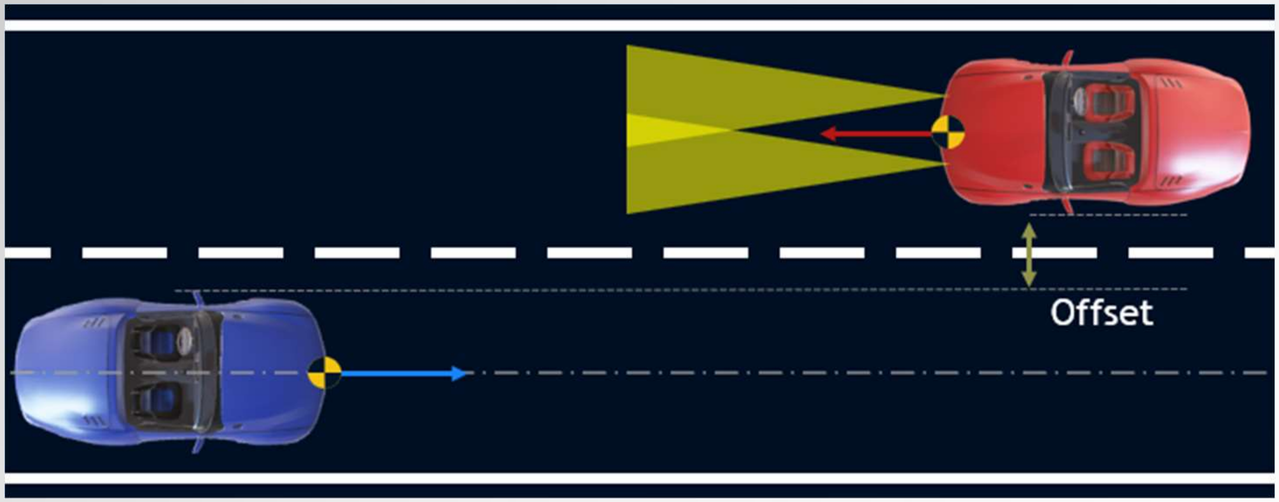


Scenarios catalogue summary 8/11

- DS-15 – Driving at darkness without remaining light

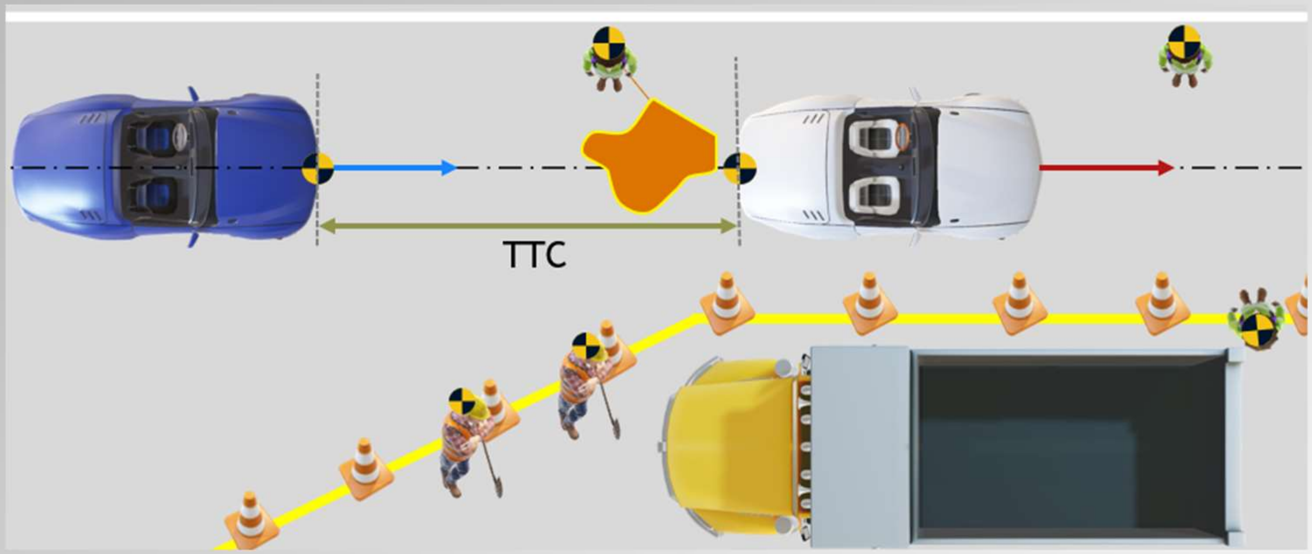


- DS-16 – Driving at darkness with an oncoming vehicle with headlights on

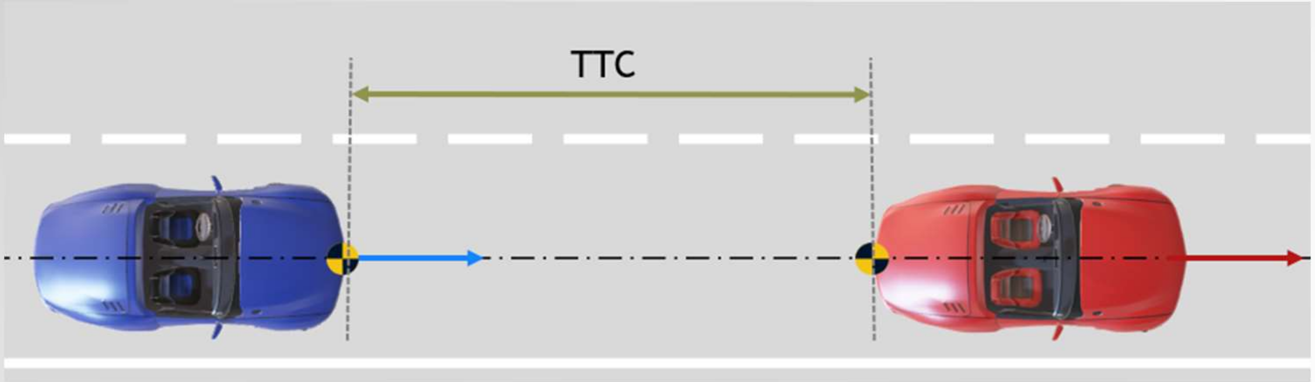


Scenarios catalogue summary 9/11

- DS-17 – Driving in road construction works site

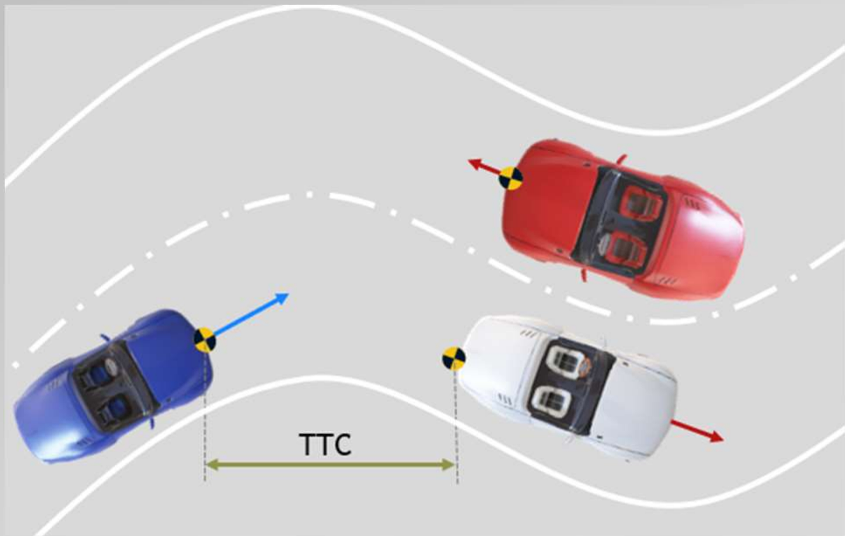


- DS-18 – Driving with longitudinal acceleration above 4 m/s^2

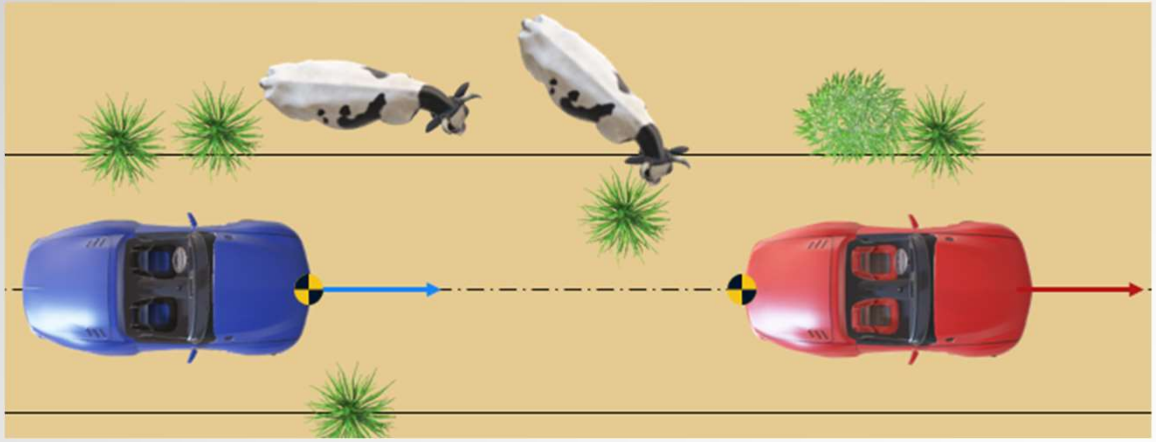


Scenarios catalogue summary 10/11

- DS-19 – Driving on mountain pass

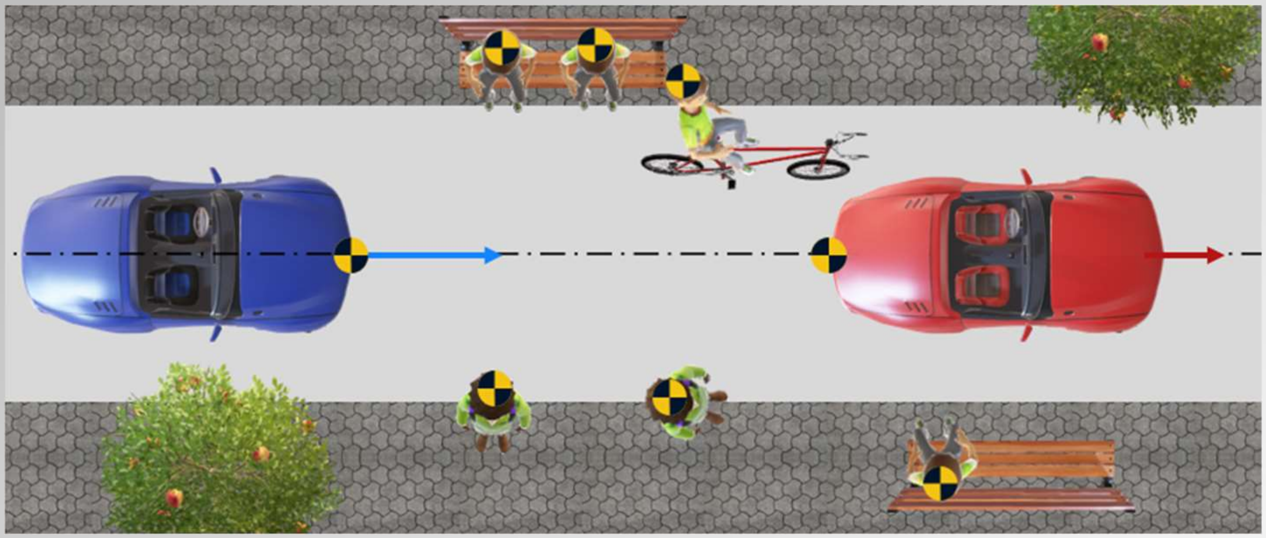


- DS-20 – Driving on country road



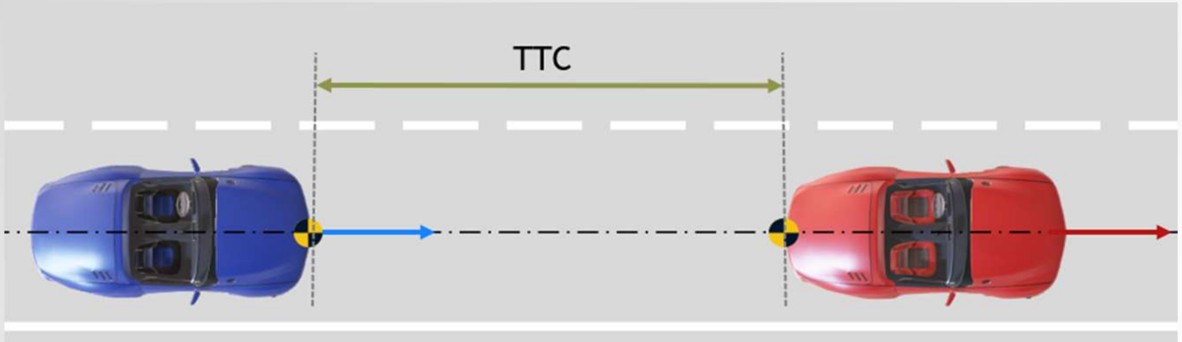
Scenarios catalogue summary 11/11

- DS-21 – Driving in the city (shared space with pedestrians and vehicle)



DS-1 – Driving following a target vehicle on highway – 1/2 Back

- When the distance with the target vehicle decreases so that the driver is in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle.
- The probability of exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Driving with normal longitudinal acceleration (<2m/s2) – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Driving in Highway– E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h



DS-1 – Driving following a target vehicle on highway – 2/2

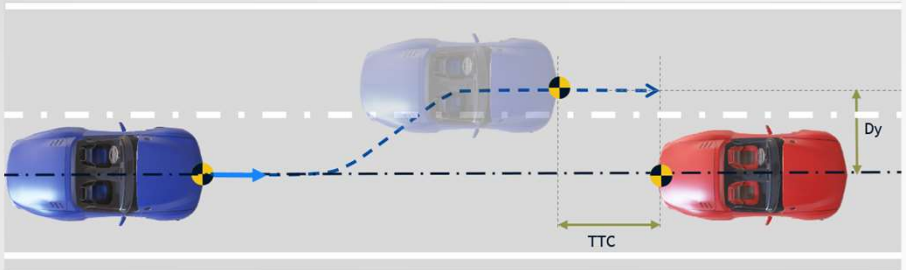
- The scenario conditions/constraints are the following:
  - The Ego vehicle drives with a longitudinal acceleration higher than $2m/s^2$ towards a moving target vehicle and is at a distance corresponding to a Time To Collision (TTC) of at least 4 s.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The target vehicle drive at 80 km/h
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be respected:
    - both vehicles shall keep steady speed and path and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

"Ego vehicle" definition: Connected and/or automated vehicle, the behaviour of which is of primary interest in testing, trialling or operational scenarios [Ego vehicle - CAV Vocabulary | BSI (bsigroup.com)]

DS-2 – Performing a lane change 1/2

Back

- While the Ego vehicle is performing a lane change and the distance with the target vehicle decreases so that the driver is in dangerous zone (possible collision) and the lateral offset is not greater than **lat_offset**, the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle.
- The probability of Exposure (duration) of these scenario conditions is E3, considering the following combinations:
  - Performing a lane change (the Ego vehicle is not completely on one lane only) – E3 (1% to 10% of average operating time)
    - E.g., from 80 h to 800 h
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h



DS-2 – Performing a lane change 2/2

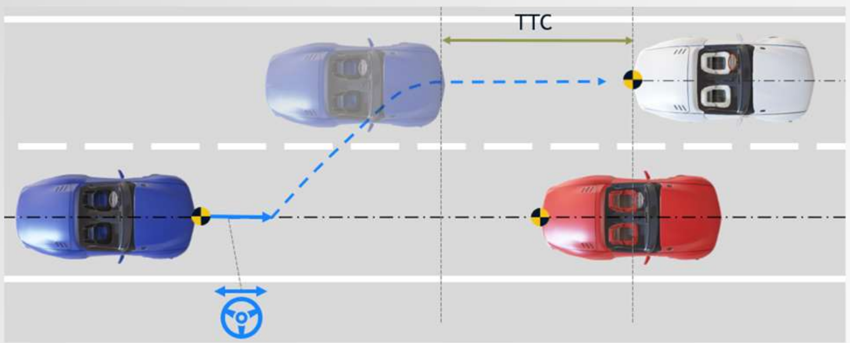
- The scenario conditions/constraints are the following:
  - The Ego vehicle drives at constant speed in highway towards a moving target vehicle, positioned with a lateral offset with respect to the Ego vehicle trajectory.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The target vehicle drive at 80 km/h
  - The **lat_offset** (Y) is from 0,5 m to -0,5 m
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be respected:
    - both vehicles shall keep steady speed and path and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

DS-3 – Performing an overtaking and approaching a new target vehicle – 1/2

Back

- While Ego vehicle is performing an overtaking maneuver approaching a new target vehicle and the distance with it decreases so that the driver is in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle.

- The probability of Exposure (duration) of these scenario conditions is E2, considering the following:
  - Vehicle performs an over taking maneuver – E2 (<1 % of average operating time)
    - E.g., lower than 80 h
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h



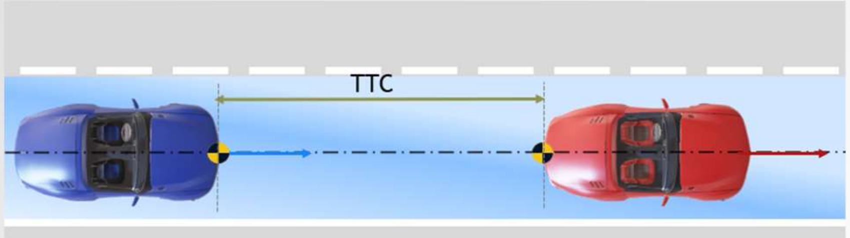
DS-3 – Performing an overtaking and approaching a new target vehicle – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives at constant speed in highway and performs a lane change. In the new lane approaches a moving target vehicle and is at a distance corresponding to a Time To Collision (TTC) of at least 4 s.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The target vehicle drive at 20 km/h
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be met:
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

DS-4 – Driving following a target vehicle with reduce friction coefficient (µ < 0,8 ± -0,1) – 1/2

Back

- When the distance with the target vehicle decreases so that the driver is in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle , except in cases where the stability control functions (e.g., ABS, ESC, …) are providing their intervention.
- The probability of Exposure (duration) of these scenario conditions is E3, considering the following combinations:
  - Driving with reduced friction coefficient in the range of µ < 0,8 ± -0,1 (e.g., snow, ice) – E3 (1% to 10% of average operating time)
    - E.g., from 80 h to 800 h
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h



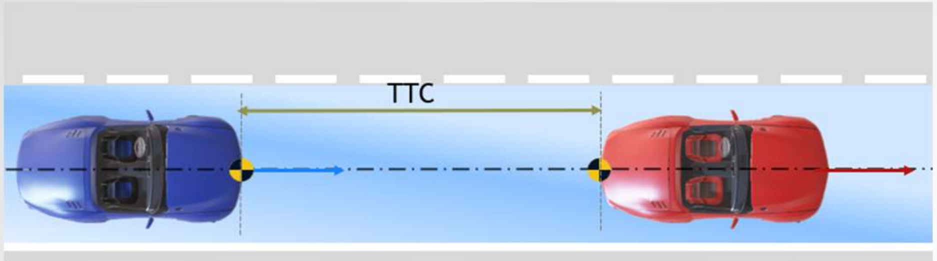
DS-4 – Driving following a target vehicle with reduce friction coefficient (μ < 0,8 ± -0,1) – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives at constant speed in highway towards a moving target vehicle with reduced road grip conditions and is at a distance corresponding to a Time To Collision (TTC) of at least 4 s.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The target vehicle drive at 20 km/h
  - The following environmental conditions shall be present:
    - Wet surface and daylight with minimum 1000 lux and Sun angle >15° to horizon
  - Road condition with reduced grip condition, with μ < 0.8
  - The following Pre-conditions shall be respected:
    - both vehicles shall keep steady speed and path and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold
    - ABS, ESC are available

DS-5 – Driving following a target vehicle with reduce friction coefficient (µ < 0,5 ± -0,1 (e.g., snow, ice)) – 1/2

Back

- When the distance with the target vehicle decreases so that the driver is in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle, except in cases where the stability control functions (e.g., ABS, ESC, …) are providing their intervention.
- The probability of Exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - Driving with low friction coefficient in the range of µ < 0,5 ± -0,1 (e.g., snow, ice) – E2 (<1% of average operating time)
    - E.g., lower than 80 h
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h



DS-5 – Driving following a target vehicle with reduce friction coefficient (μ < 0,5 ± -0,1 (e.g., snow, ice)) – 2/2

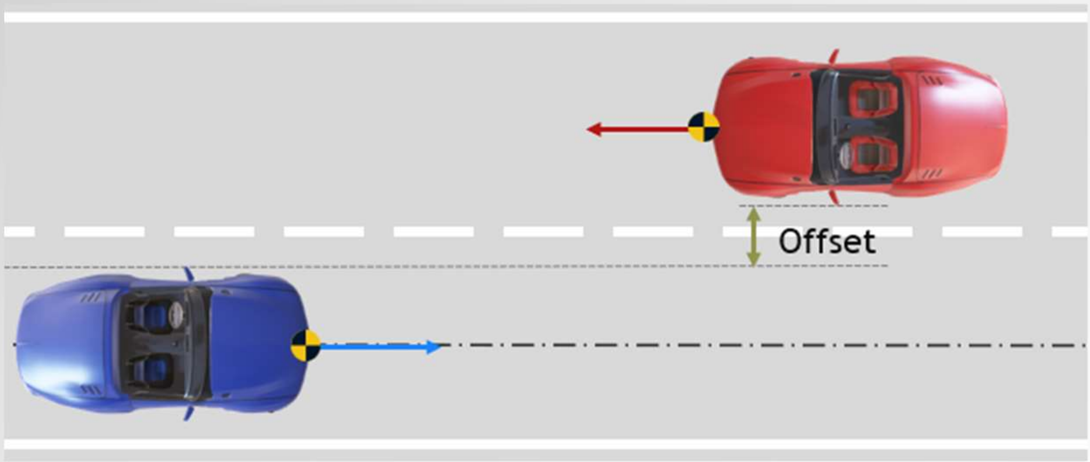
- The scenario conditions/constraints are the following:
  - The Ego vehicle drives at constant speed towards a moving target vehicle with low-μ conditions and is at a distance corresponding to a Time To Collision (TTC) of at least 4 s.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The target vehicle drive at 20 km/h
  - The following environmental conditions shall be present:
    - Wet surface and daylight with minimum 1000 lux and Sun angle >15° to horizon
  - Road condition with reduced grip condition, with μ < 0,5 ± -0,1
  - The following Pre-conditions shall be respected:
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold
    - ABS, ESC are available

DS-6 – Driving with a target vehicle coming from opposite direction – 1/2

Back

- When the distance with the target vehicle (from opposite direction) decreases but the driver is not in dangerous zone (no possible collision) the intended functionality shall neither warn the driver nor decelerate the vehicle.

- The probability of Exposure (duration) of these scenario conditions is E4, considering the following combinations:
  - Driving with opposite traffic within in visibility range – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h

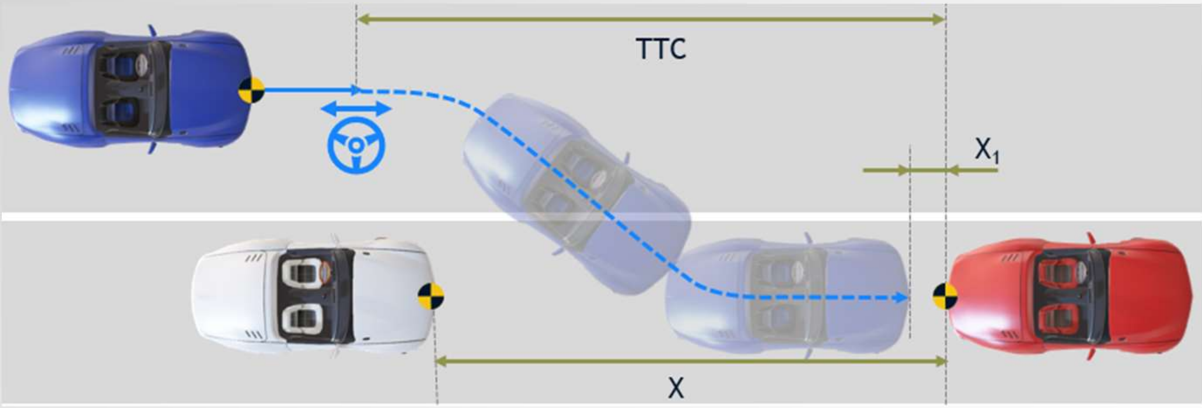


DS-6 – Driving with a target vehicle coming from opposite direction – 2/2

- The scenario conditions/constraints are the following:
  - The Ego-vehicle drives at a constant speed towards a target vehicle coming from the opposite direction.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The target vehicle drive from 10 to 30 km/h
  - The offset between the vehicles is 1,5 m
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be respected:
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

- While the Ego vehicle is entering in a parking space even in case the distance with the target vehicle decreases so that could be considered as collision relevant, the intended functionality shall neither warn the driver or decelerate the vehicle.

- The probability of Exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - In to and out of parking space in longitudinal direction – E2 (<1% of average operating time)
    - E.g., lower than 80 h



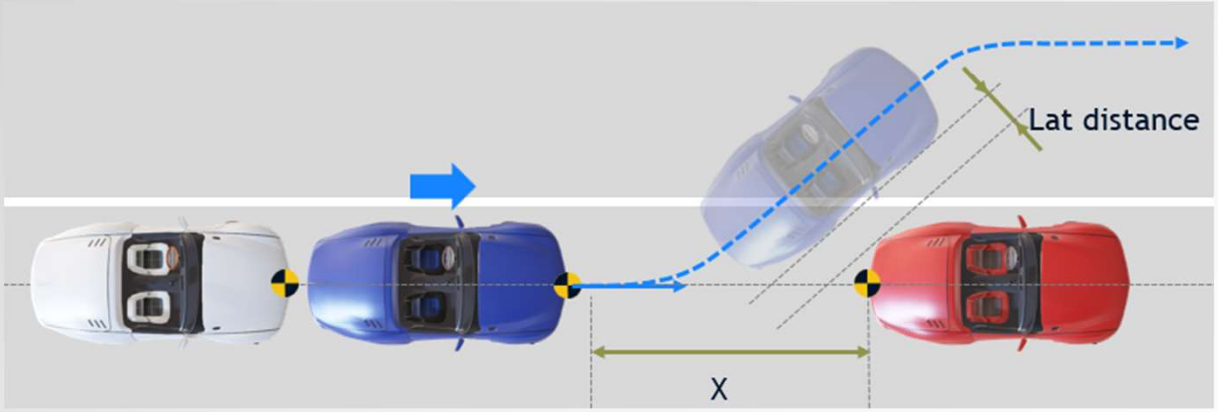
DS-7 – Enter in a parking space in longitudinal direction – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle performs a lane change and decelerates to park, between two target vehicles parked on the road edge.
  - The Ego vehicle speed range is [10 km/h, 30 km/h]
  - The Ego vehicle deceleration is 2,5 m/s^2 (± 0,5 m/s^2)
  - The space beetween the parked vehicles (X) is from 10 m to 20 m
  - The final distance (X_1) with the parked target vehicle at the end of the manoeuvre is 1 m with a tolerance of ± 0,25 m
  - The Ego vehicle shall perform the parking manoeuvre according the following:
    - TTC at lane change: from 5s to 4s
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete

DS-8 – Exit from a parking space in longitudinal direction – 1/2

Back

- While the Ego vehicle is leaving a parking space even in case the distance with the target vehicle decreases so that could be considered as collision relevant, the intended functionality shall neither warn the driver or decelerate the vehicle.
- The probability of Exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - In to and out of parking space in longitudinal direction – E2 (<1% of average operating time)
    - E.g., lower than 80 h



DS-8 – Exit from a parking space in longitudinal direction – 2/2

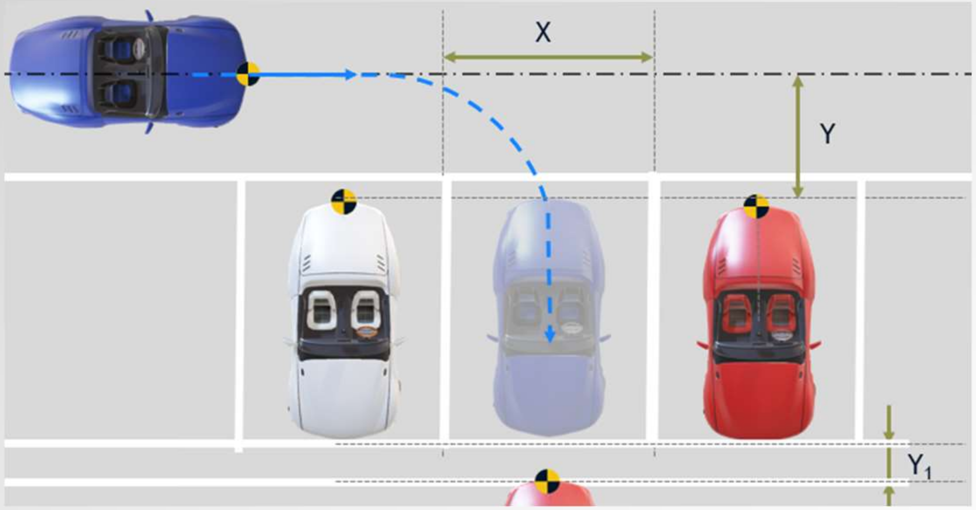
- The scenario conditions/constraints are the following:
  - The Ego vehicle is parked between two vehicles, at a defined distance with the vehicle in front, and starts a lane change to exit from the park.
  - The Ego vehicle speed range is [0 km/h, 25 km/h]
  - The Ego vehicle acceleration is 1,5 m/s^2 (± 0,5 m/s^2)
  - The distance (X) with the parked target vehicle in front is from 10 m to 5 m
  - The lateral distance with target vehicle in front during lane change is 1 m (± 0,5 m)
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete

DS-9 – Enter in a parking space in cross direction – 1/2

Back

- While the Ego vehicle is entering in a parking space even in case the distance with the target vehicle decreases so that could be considered as collision relevant, the intended functionality shall neither warn the driver or decelerate the vehicle.

- The probability of Exposure (duration) of these scenario conditions is E3, considering the following combinations:
  - In to and out of parking space in cross direction – E3 (1% to 10% of average operating time)
    - E.g., from 80 h to 800 h



DS-9 – Enter in a parking space in cross direction – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle starts a manoeuvre to park between two target vehicles and behind a third target vehicle.
  - The Ego vehicle speed range is [10 km/h, 30 km/h]
  - The Ego vehicle deceleration is 2,5 m/s^2 (± 0,5 m/s^2)
  - The space beetween the parked vehicles (X) is from 3 m to 4 m
  - The final distance (Y_1), at the end of the manoeuvre, with the parked target vehicle in front is 1,5 m with a tolerance of ± 0,5m
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete

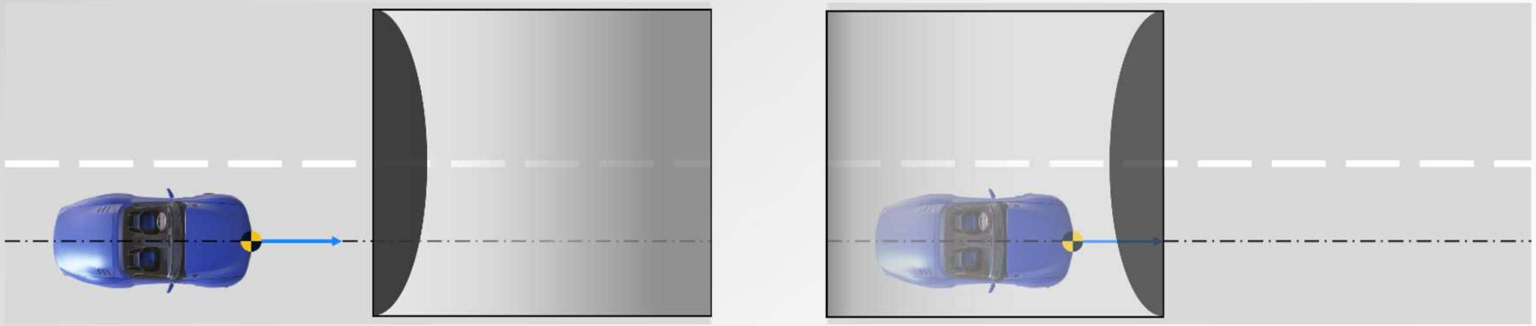
- When due to the high load in the rear, the camera performance are affected, so that the FOV angle goes out of the accepted range, the indented functionality shall warn the driver about the failure (FOV out of the range), deactivate the function but shall not decelerate the vehicle.
- The probability of Exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - Driving with trailer attached – E2 (<1% of average operating time)
    - E.g., lower than 80 h

DS-10 – Driving with trailer attached – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives at constant speed with high load at the rear axle.
  - The Ego vehicle speed range is [5 km/h, 80 km/h]
  - The rear axle load exceeds the allowed weight
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete

DS-11 – Driving in a tunnel – 1/2

- While entering in or leaving a tunnel, the sudden light intensity differences could affect the camera performance leading to a False positive. When light differences are detected, the indented functionality shall warn the driver about the failure (camera performance affected), deactivate the function but shall not provide vehicle deceleration.
- The probability of Exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - Driving in tunnel – E2 (<1% of average operating time)
    - E.g., lower than 80 h



DS-11 – Driving in a tunnel – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives from a very illuminated area to a poorly illuminated area or from a poorly illuminated area to a very illuminated area.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete

DS-12 – Driving with pedestrians within danger zone – 1/2 Back

- When the distance with vulnerable users (e.g., pedestrian, cyclist) decreases so that the driver or vulnerable users are in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle.

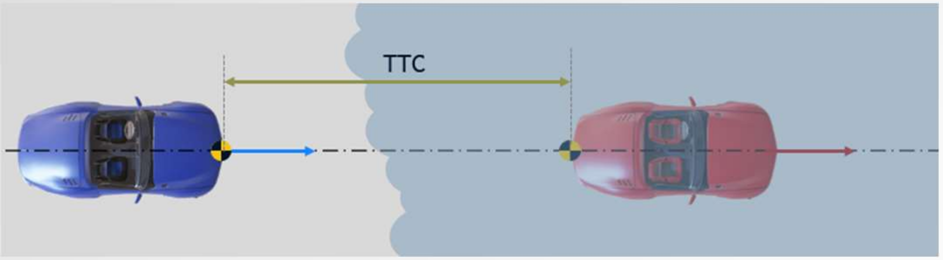
- The probability of Exposure (duration) of these scenario conditions is E3, considering the following combinations:
  - Driving in a city– E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Persons within danger zone (ca. 1 vehicle lenght in front of vehicle) – E3 (1% to 10% of average operating time)
    - E.g., from 80 h to 800 h

DS-12 – Driving with pedestrians within danger zone – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives in urban roads towards a pedestrian crossing the road perpendicular to the Ego vehicle's direction.
  - The Ego vehicle speed range is [5 km/h, 50 km/h]
  - The pedestrian crosses the road at 5 km/h (± 0,1 km/h)
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be respected:
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

DS-13 – Driving with low visibility – 1/2

- The heavy fog condition could affect the camera performance leading to a False negative. The indented functionality shall warn the driver about the failure (camera performance affected, or target suddenly lost), deactivates the function but shall not provide vehicle deceleration.
- The probability of Exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - Driving at low visibility (visibility range below 50 m) – E2 (<1% of average operating time)
    - E.g., lower than 80 h
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h



DS-13 – Driving with low visibility – 2/2

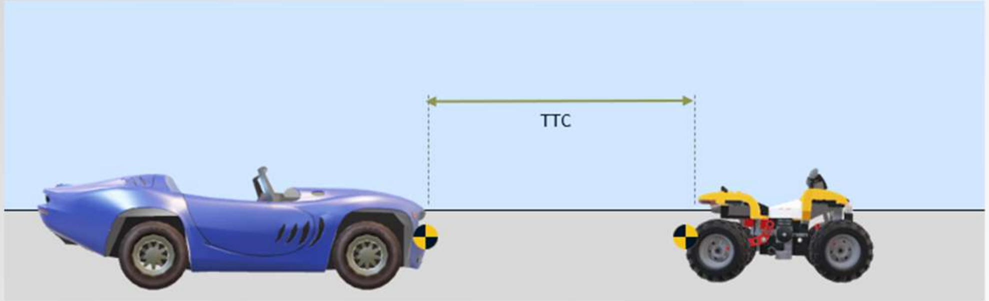
- The scenario conditions/constraints are the following:
  - The Ego vehicle drives behind another vehicle with reduced visibility due to heavy fog condition.
  - The Ego vehicle speed range is [5 km/h, 50 km/h]
  - The distance (TTC) with the target vehicle is from 4s to 3s.
  - The following environmental conditions shall be present:
    - Fog and daylight
    - Fog and night
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be respected:
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

DS-14 – Driving following a target vehicle (no normal configuration) – 1/2

Back

- When the distance with the target vehicle decreases so that the driver is in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle.
- The target vehicle is not a traditional target (different vehicle configuration with respect to conventional vehicle, e.g. trailer attached, ATV) so that could be difficult to be classifiable by the algorithm.

- The probability of Exposure (duration) of these scenario conditions is E4, considering the following combinations:
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h



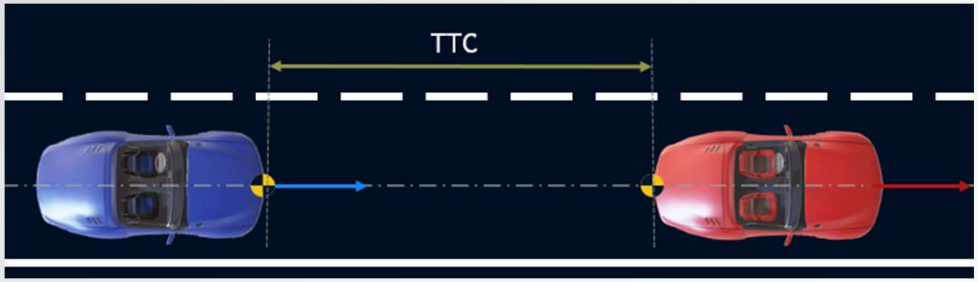
DS-14 – Driving following a target vehicle (no normal configuration) – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives towards a moving object difficult to classify by the system.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The target vehicle drive at 20 km/h
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be respected:
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

DS-15 – Driving at darkness without remaining light – 1/2 Back

- When the distance with the target vehicle decreases so that the driver is in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle .

- The probability of Exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Driving in the dark without residual light (no streetlights, no moon, no lights by other road users) – E3 (1% to 10% of average operating time)
    - E.g., from 80 h to 800 h



DS-15 – Driving at darkness without remaining light – 2/2

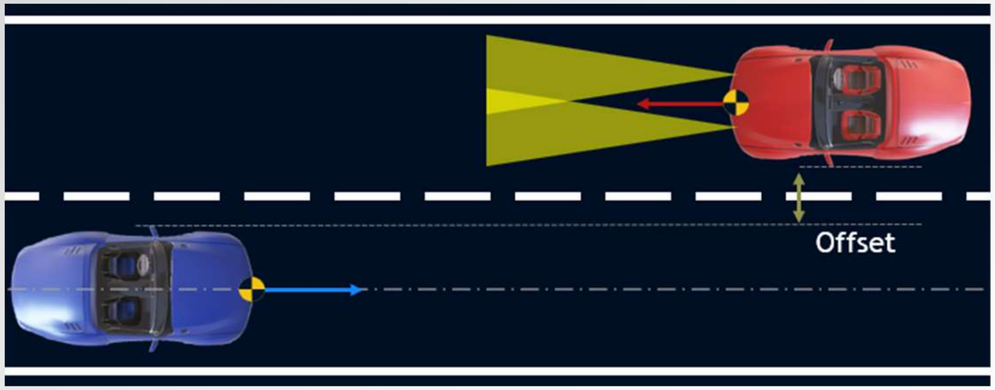
- The scenario conditions/constraints are the following:
  - The vehicle drives in the darkness without residual light (no streetlights, no moon, no lights by other road users) towards a moving target vehicle and is at a distance corresponding to a Time To Collision (TTC) of at least 4 s.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The target vehicle drive at 20 km/h
  - The following environmental conditions shall be present:
    - Dry and night with lower than 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be met:
    - Low beam or high beam switched off
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

DS-16 – Driving at darkness with an oncoming vehicle with headlights on – 1/2

Back

- When the distance with the target vehicle (from opposite direction) decreases but the driver is not in dangerous zone (no possible collision) the intended functionality shall neither warn the driver nor decelerate the vehicle.

- The probability of Exposure (duration) of these scenario conditions is E3, considering the following combinations:
  - Driving with opposite traffic within in visibility range – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Driving in the dark with residual light – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h

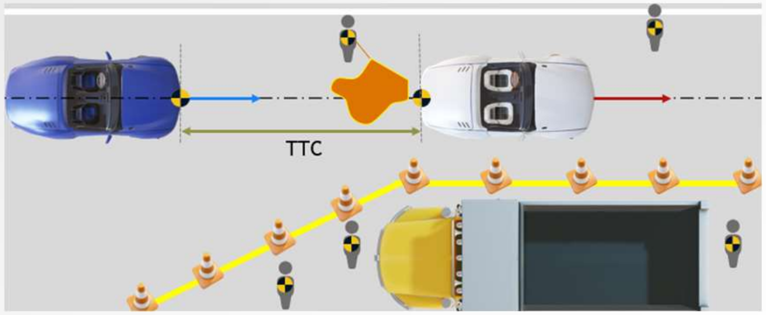


DS-16 – Driving at darkness with an oncoming vehicle with headlights on – 2/2

- The scenario conditions/constraints are the following:
  - The vehicle drives in the darkness with lights on towards an oncoming target vehicle from the opposite direction with headlights on.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The target vehicle drive at 20 km/h
  - The following environmental conditions shall be present:
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be met:
    - Low beam or high beam switched on
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

- When the distance with the target vehicle, operators or temporary road structures decreases so that the driver is in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle.

- The probability of Exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Driving in road construction works – E2 (<1% of average operating time)
    - E.g., lower than 80 h
  - Persons within danger zone (ca. 1 vehicle lenght in front of vehicle) – E3 (1% to 10% of average operating time)
    - E.g., from 80 h to 800 h



DS-17 – Driving in road construction works site – 2/2

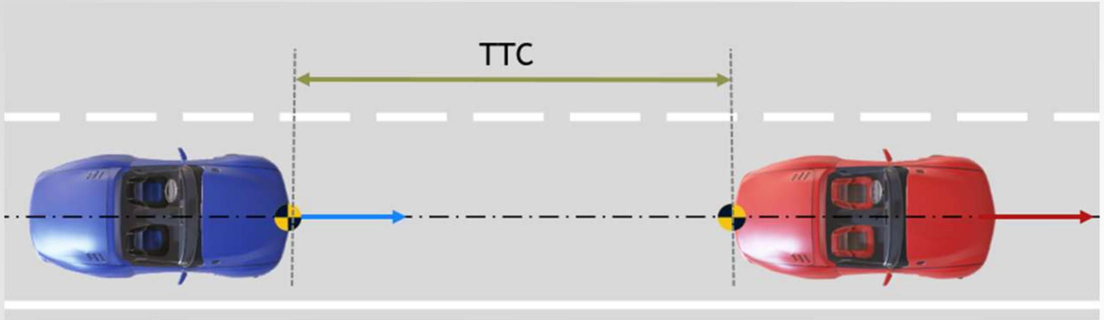
- The scenario conditions/constraints are the following:
  - The Ego vehicle drives at constant speed in road construction works towards a moving target vehicle and is at a distance corresponding to a Time To Collision (TTC) of at least 4 s. Operators and temporary road structures are also present near the ego vehicle.
  - The Ego vehicle speed range is [50 km/h, 80 km/h]
  - The target vehicle drive at 20 km/h
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be met:
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

DS-18 – Driving with longitudinal acceleration above 4 m/s2 – 1/2

Back

- When the distance with the target vehicle decreases so that the driver is in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle.

- The probability of Exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Driving with normal longitudinal acceleration (>4m/s^2) – E2 (<1% of average operating time)
    - E.g., lower than 80 h



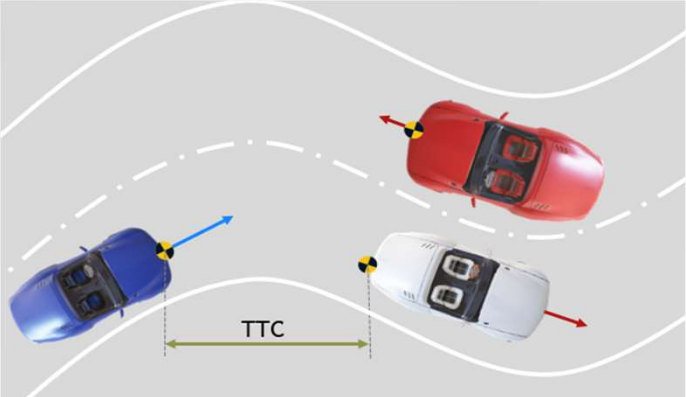
DS-18 – Driving with longitudinal acceleration above 4 m/s2 – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives with a longitudinal acceleration higher than $4 m/s^2$ towards a moving target vehicle and is at a distance corresponding to a Time To Collision (TTC) of at least 4 s.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The target vehicle drive at 20 km/h
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be met:
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

DS-19 – Driving on mountain pass – 1/2

- When the distance with the target vehicle decreases so that the driver is in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle. No reaction shall be provided for target vehicle coming from opposite direction.

- The probability of Exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Driving with opposite traffic within in visibility range – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Driving on mountain pass – E2 (<1% of average operating time)
    - E.g., lower than 80 h



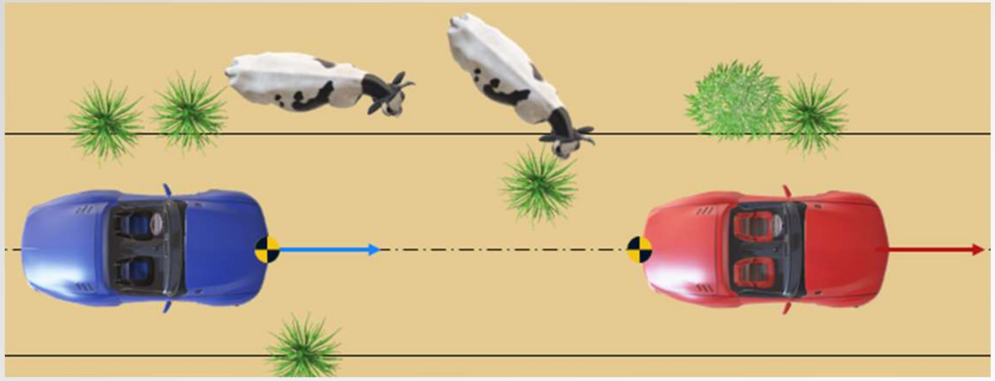
DS-19 – Driving on mountain pass – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives at constant speed on mountain pass towards a moving target vehicle and is at a distance corresponding to a Time To Collision (TTC) of at least 4 s, and with a target vehicle coming from opposite direction.
  - The Ego vehicle speed range is [30 km/h, 60 km/h]
  - The target vehicle drive at 20 km/h
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be met:
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

DS-20 – Driving on country road – 1/2

Back

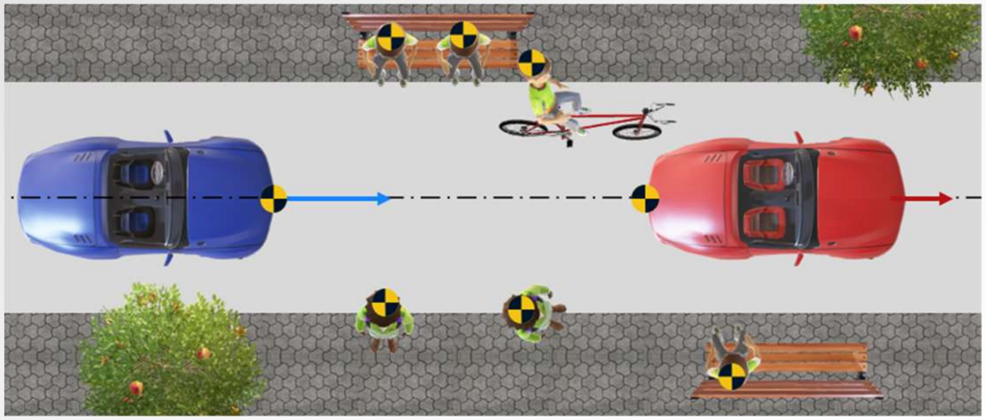
- When the distance with the target vehicle or animals decreases so that the driver is in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle.
- The probability of Exposure (duration) of these scenario conditions is E3, considering the following combinations:
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Driving on country road – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h



DS-20 – Driving on country road – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives at constant speed on country roads towards a moving target vehicle and is at a distance corresponding to a Time To Collision (TTC) of at least 4 s. Considering the environment cannot be excluded the presence of animals on the road.
  - The Ego vehicle speed range is [50 km/h, 80 km/h]
  - The target vehicle drive at 20 km/h
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be met:
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

- When the distance with the target vehicle or vulnerable users decreases so that the driver or the vulnerable users are in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle.
- The probability of Exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Driving in the city – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Persons within danger zone (ca. 1 vehicle lenght in front of vehicle) – E3 (1% to 10% of average operating time)
    - E.g., from 80 h to 800 h



DS-21 – Driving in the city (shared space with pedestrians and vehicle) – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives at constant speed in the city towards both moving target vehicle and VRUs (pedestrians and/or cyclist).
  - The Ego vehicle speed range is [5 km/h, 50 km/h]
  - The target vehicle drive at 20 km/h
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be met:
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

Author	G. Dallara, C. Donzella, F. Guerrini, D. Cunial, G. Nicosia
Company	Exida Development
Version	1.3
File name	Scenario catalogue
Status	Release

Document Change History			
Date	**Version**	**Changed by**	**Change Description**
08/05/2023	1.0	G. Dallara, C. Donzella, F. Guerrini, D. Cunial, G. Nicosia	First emission
09/05/2023	1.1	G. Nicosia	Minor format fix
26/05/2023	1.2	G. Nicosia	Updated of resulting exposure value of DS-1, DS-15, DS-20 and DS-21 scenarios. Replaced "probability of occurrence" with "probability of Exposure (duration)" within the document.
19/07/2023	1.3	G. Nicosia	Updated picture and text of "DS-2 – Performing a lane change"

exida DEVELOPMENT

excellence in dependable automation

Many Thanks for your Attention

V&V Strategy application for Scenarios catalogue Tailored WP 2

gdallara@exida.com
carlo.donzella@exida-dev.com
francesca.guerrini@exida-eng.com
giuseppe.nicosia@exida-dev.com

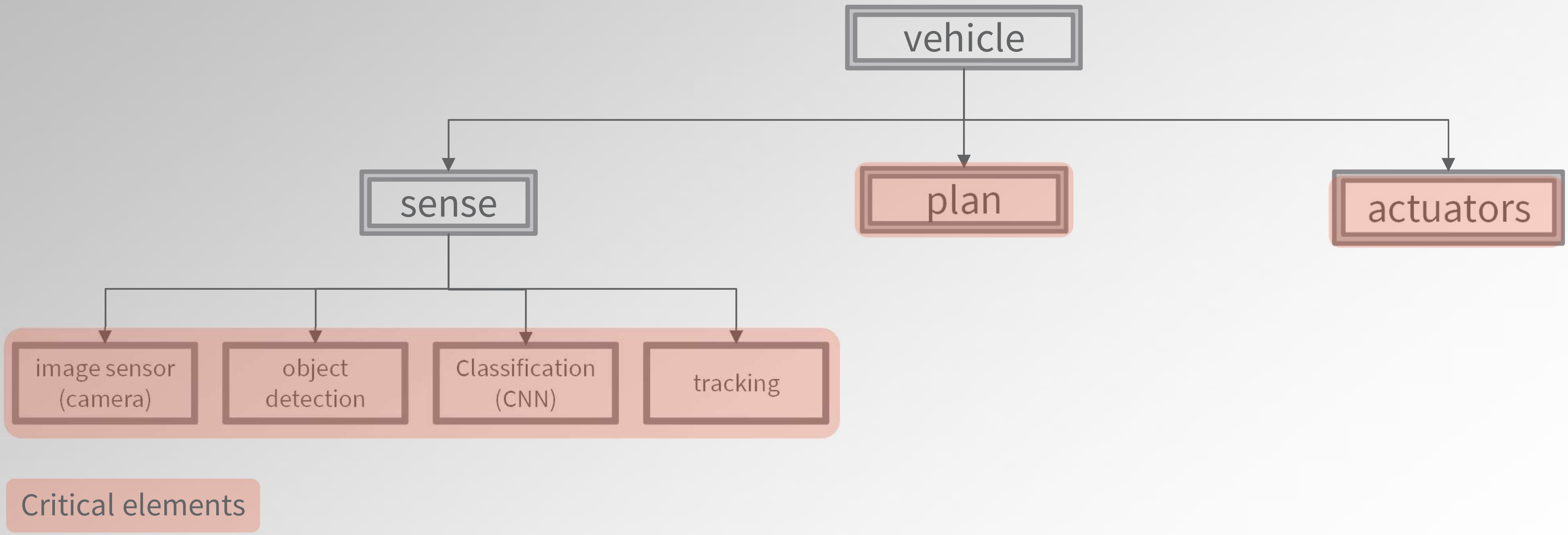
07/08/2024

Draft

V1R1

Scope and purpose

- The goal of this presentation is to show the relevant driving scenario catalogue, adapted for the automotive use case, and the application of the defined V&V strategy among the different Architectural levels (reported below).
- Starting from the relevant driving scenario catalogue test cases at vehicle, sensor, algorithm and actuator level shall be derived.



V&V strategy at vehicle level

- At vehicle level the strategy is based on the following steps:
  - Definition of driving situation catalogue
  - Creation of stage scenes on test track
  - Execution of driving situation to count how often and how long the ego-vehicle is entering in the dangerous zone
  - Execute a Root cause analysis to identify the component(s) whose failures or inadequacy bring to enter in the dangerous zone
  - Identification of improvements/mitigations to reduce the risk

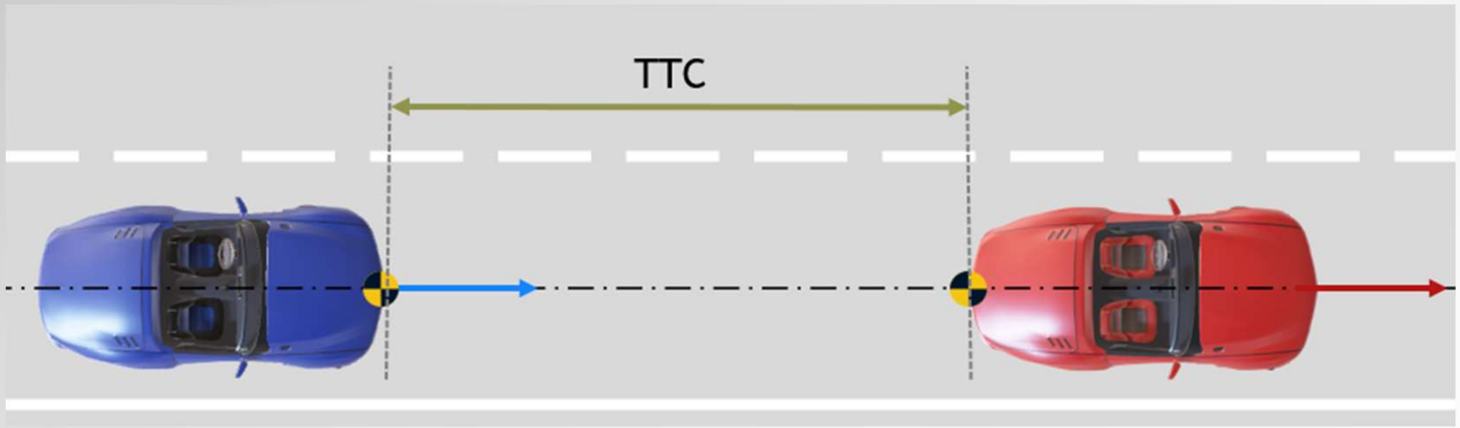
V&V strategy at element level

- At element level the strategy is based on the following steps:
  - Evaluate overall design to find out the most critical elements
  - Evaluate where fault can be injected and analyze the results to identify the system weakness.
  - Evaluate the testing results, after fault injection.

Scenarios catalogue summary 1/11

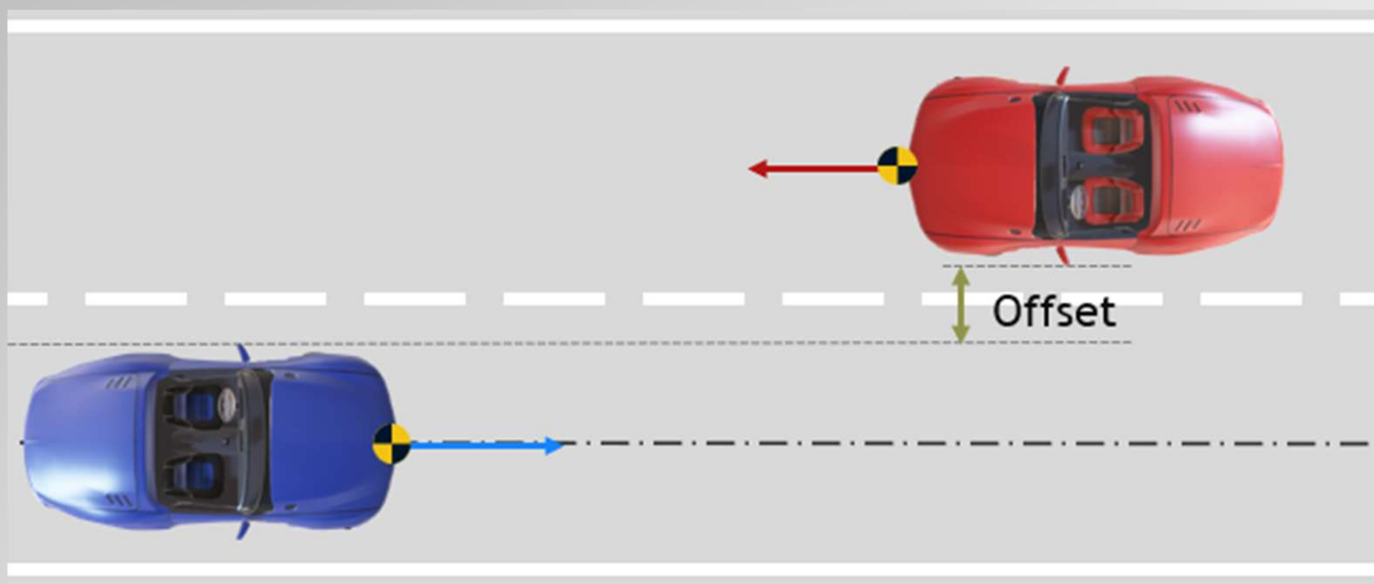
- The following list reports all the driving scenario contained in the driving scenario catalogue [with ID (e.g., DS-x) and title).
- For all the details on a given scenario, please refer to the dedicated scenario sheets.

- DS-1 – Driving following a target vehicle on highway



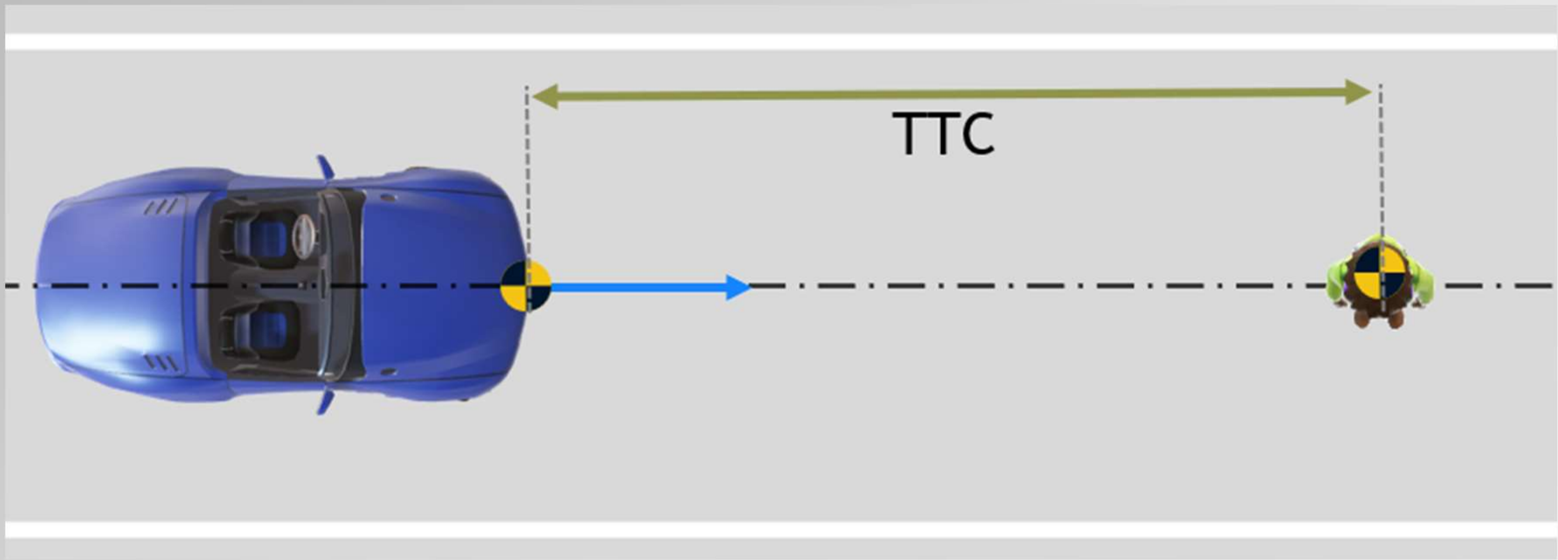
Scenarios catalogue summary 2/11

- DS-2 – Driving with a target vehicle coming from opposite direction



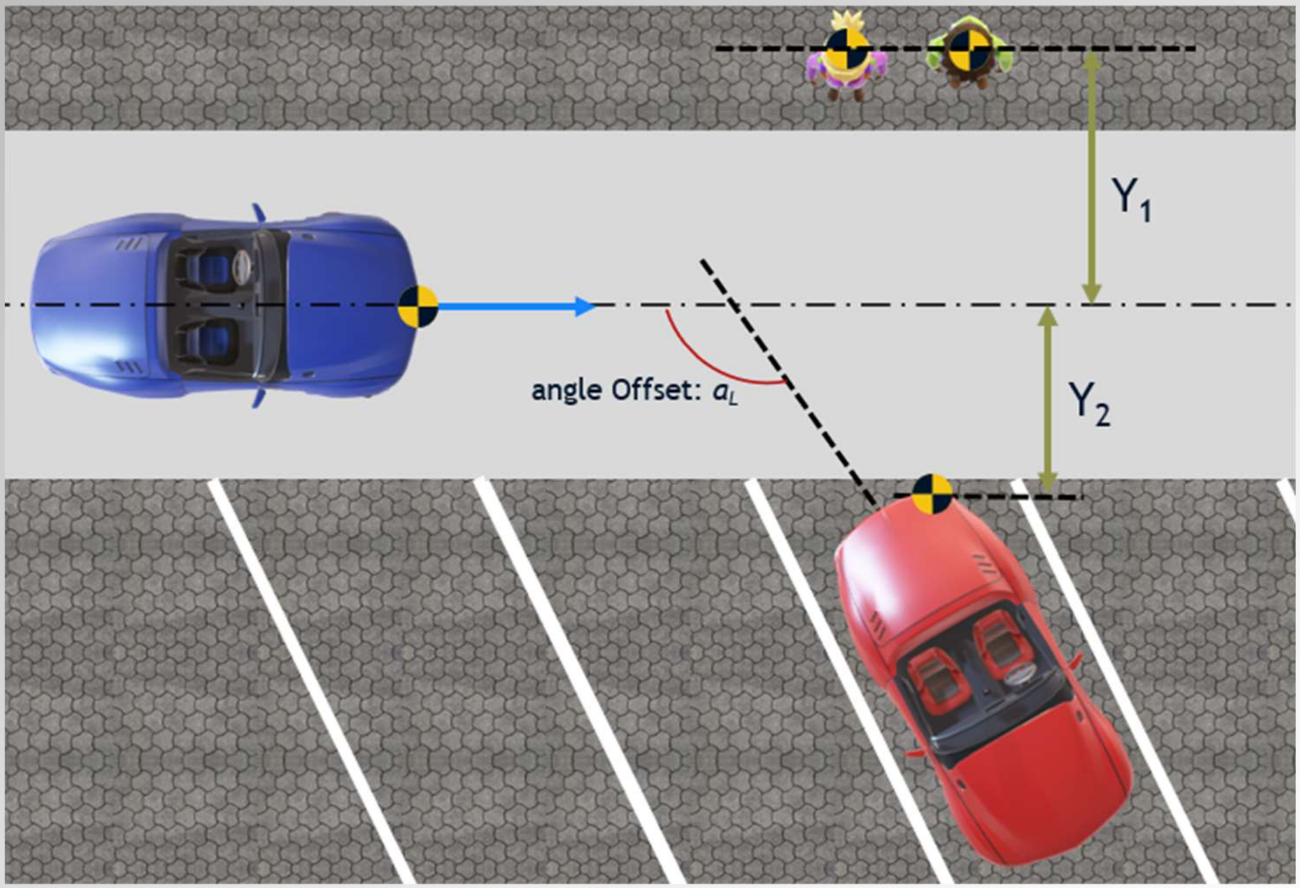
Scenarios catalogue summary 3/11

- DS-3 – Drive towards a pedestrian



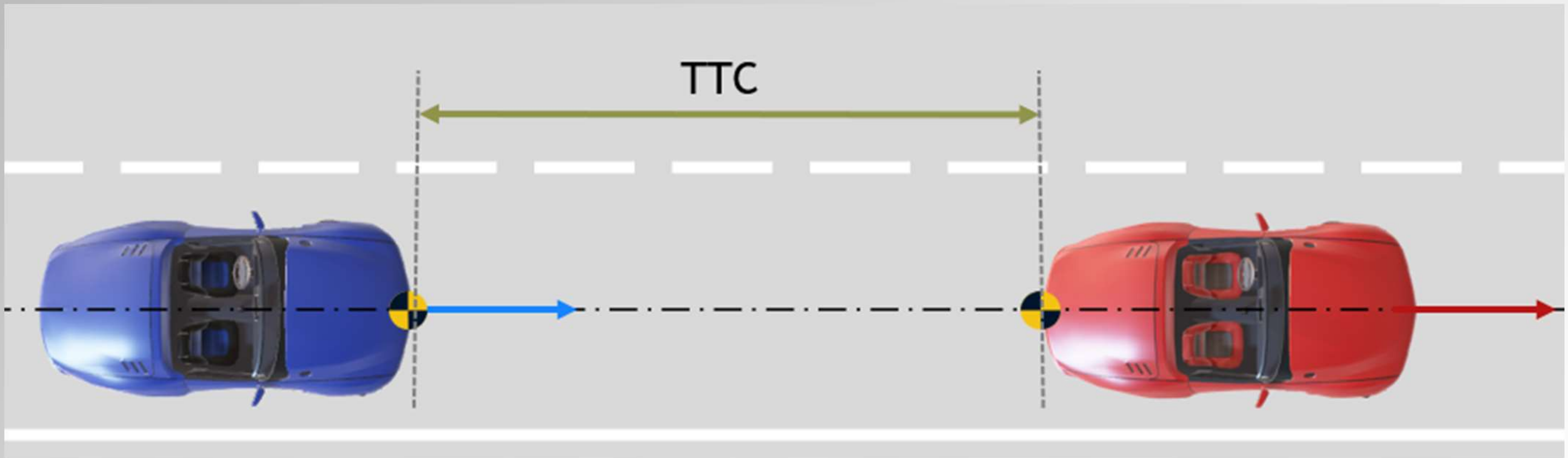
Scenarios catalogue summary 4/11

- DS-4 – Drive towards parked cars and pedestrians on sidewalk



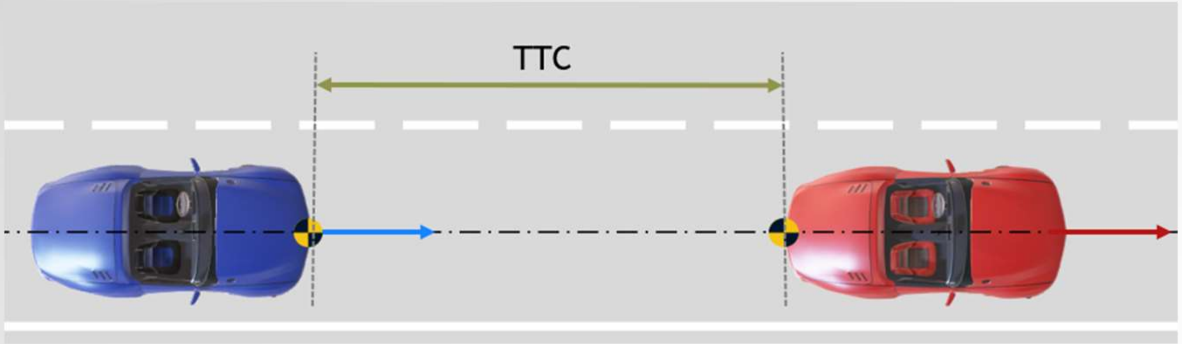
DS-1 Scenario

- DS-1 – Driving following a target vehicle on highway



DS-1 – Driving following a target vehicle on highway – 1/2

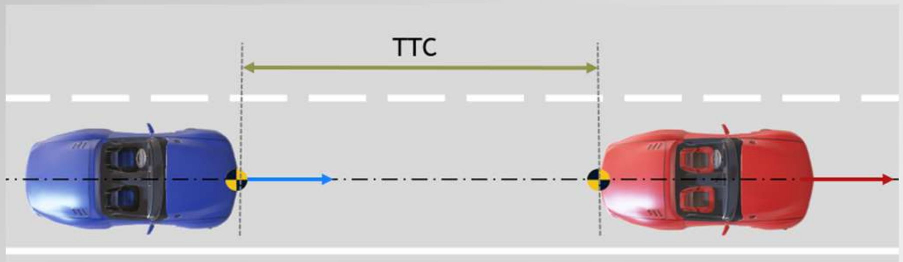
- When the distance with the target vehicle decreases so that the driver is in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle.
- The probability of exposure (duration) of these scenario conditions is E2, considering the following combinations:
  - Driving behind other vehicle with normal distance – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Driving with normal longitudinal acceleration (<2m/s2) – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Driving in Highway– E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h



DS-1 – Driving following a target vehicle on highway – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives with a longitudinal acceleration lower than $2m/s^2$ towards a moving target vehicle and is at a distance corresponding to a Time To Collision (TTC) of at least 4 s.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The target vehicle drive at 80 km/h
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be respected:
    - both vehicles shall keep steady speed and path and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

DS-1 – Test case specification



- Test case at vehicle level – ID: TCDS_1
  - For the DS-1 scenario, the following intended functionality capabilities shall be demonstrated:
    - (Step 1) Track the red target vehicle and evaluate it as no-collision relevant
    - (Step 2) When the distance, between the ego vehicle and the red target vehicle, is equal to the Time To Warning (TTW), the intended functionality shall evaluate the red target vehicle as collision relevant and provide at least 0,8 s before the start of the emergency braking the visual and audible warning to the driver (UN Regulation N° 152 clause 5.2.1.1, 5.5.1).
    - (Step 3) When the distance, between the ego vehicle and the red target vehicle, is equal to the Time To Collision AEB (TTC AEB), the intended functionality shall ,if no driver reaction occurs, shall decelerate the vehicle providing at least 5.0 m/s2 (UN Regulation N° 152 clause 5.2.1.2).

DS-1 – Test case specification

- TCDS_1 - Step 1
  - Ego vehicle status:
    - Kl.15 = on;
    - Gear position = "D"
    - Intended functionality state: active
  - Initial ego vehicle speed:
    - 50 (+/- 2) km/h
    - 80 (+/- 2) km/h
    - 100 (+/- 2) km/h
  - Driver Input:
    - Steering wheel angle: < SWA_Threshold
    - Acceleration = constant
    - Brake = not present
  - Initial target vehicle speed (red):
    - 80 (+/- 2) km/h

DS-1 – Test case specification

- TCDS_1 - Step 1
  - Initial longitudinal offset = TTC > TTW or TTC_{AEB}
  - Environmental conditions:
    - Light
      - Day: > LuxDay_Threshold
      - Night: ≤ LuxNight_Threshold
      - Test surface = solid and dry
  - Expected result:
    - Warning = Not present
    - Braking = Not present

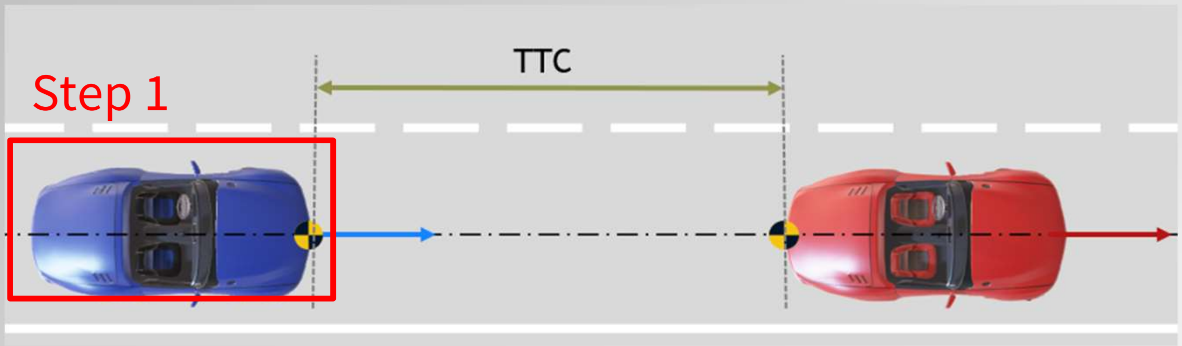
DS-1 – Test case specification

- TCDS_1 - Step 2
  - Ego vehicle status:
    - Kl.15 = on;
    - Gear position = "D"
    - Distance between Ego vehicle position and target vehicle = TTC == TTW
    - Intended functionality state: active intervening
  - ego vehicle speed = constant according to initial speed
  - target vehicle speed = 80 (+/- 2) km/h
  - Driver Input:
    - Steering wheel angle: < SWA_Threshold
  - Environmental conditions:
    - Light
      - Day: > LuxDay_Threshold
      - Night: ≤ LuxNight_Threshold
      - Test surface = solid and dry
  - Expected result:
    - Warning = Present
    - Braking = Not present

DS-1 – Test case specification

- TCDS_1 - Step 3
  - Ego vehicle status:
    - Kl.15 = on;
    - Gear position = "D"
    - Distance between Ego vehicle position and target vehicle = TTC == TTC AEB
    - Intended functionality state: active intervening
  - ego vehicle speed = constant according to initial speed
  - target vehicle speed = 80 (+/- 2) km/h
  - Driver Input:
    - Steering wheel angle: < SWA_Threshold
  - Environmental conditions:
    - Light
      - Day: > LuxDay_Threshold
      - Night: ≤ LuxNight_Threshold
      - Test surface = solid and dry
  - Expected result:
    - Warning = Present
    - Braking = Present

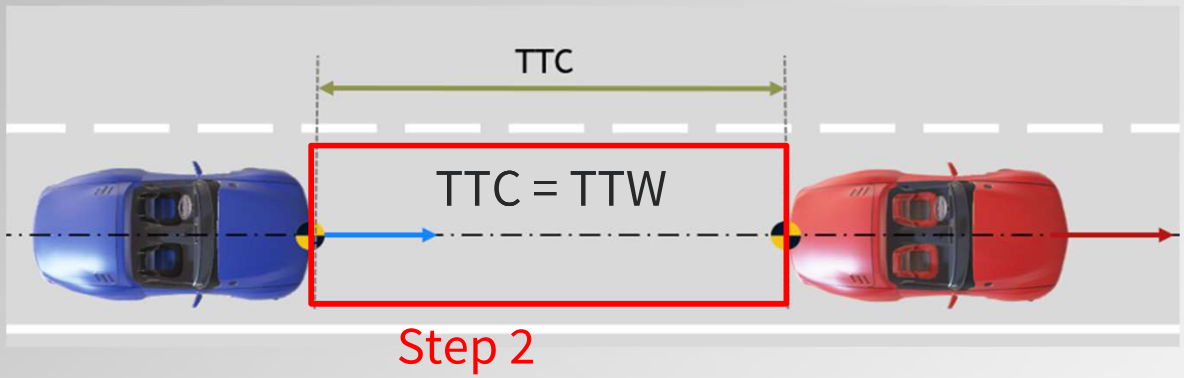
DS-1 – Test case Break-down



- TCDS_1 - Step 1 – Vehicle
  - Expected result:
    - Warning = Not present
    - Braking = Not present
- TCDS_1 – Step 1 – Sense
  - Expected result:
    - Object detected
    - Object classified as “car”
      - Evaluate outputs of sensors to evaluate the expected results (e.g. detected objects, object classification)
- TCDS_1 – Step 1 – Logic
  - Expected result:
    - Object evaluated as “no-collision” relevant
      - Evaluate outputs of Logic to evaluate the expected results (e.g. request to the actuator)
- TCDS_1 – Step 1 – Actuator
  - Expected result:
    - No warning
    - No braking actuated

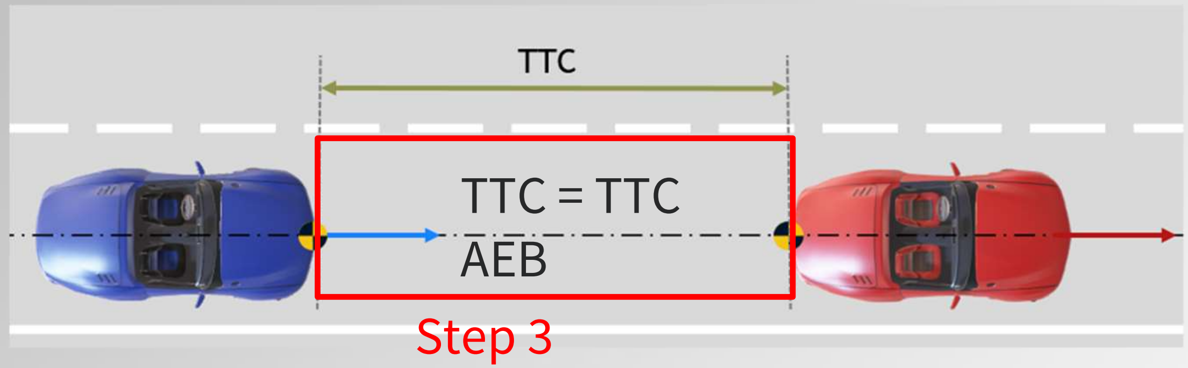
DS-1 – Test case Break-down

- TCDS_1 - Step 2 – Vehicle
  - Expected result:
    - Warning = Present
    - Braking = Not present
- TCDS_1 – Step 2 – Sense
  - Expected result:
    - Object detected
    - Object classified as “car”
      - Evaluate outputs of sensors to evaluate the expected results (e.g. detected objects, object classification)
- TCDS_1 – Step 2 – Logic
  - Expected result:
    - Object evaluated as “collision” relevant because TTC == TTW
      - Evaluate outputs of Logic to evaluate the expected results (e.g. request to the actuator, Item state*)
- TCDS_1 – Step 2 – Actuator
  - Expected result:
    - Warning provided (visual and audible warning according to N 152)
    - No braking actuated



*: the function state shall be moved to Active – intervention, since it is providing the warning

DS-1 – Test case Break-down

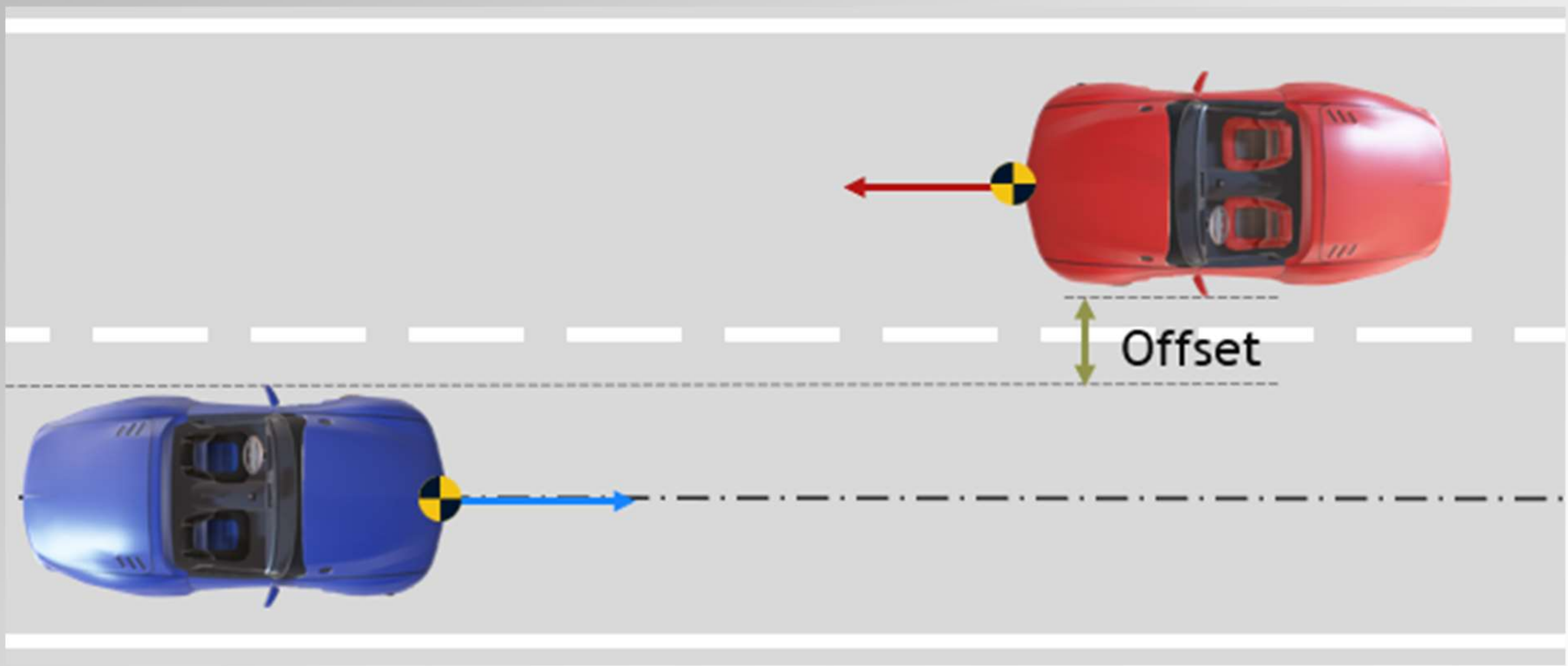


- TCDS_1 - Step 3 – Vehicle
  - Expected result:
    - Warning = present
    - Braking = present
- TCDS_1 – Step 3 – Sense
  - Expected result:
    - Object detected
    - Object classified as "car"
      - Evaluate outputs of sensors to evaluate the expected results (e.g. detected objects, object classification)
- TCDS_1 – Step 3 – Logic
  - Expected result:
    - Object evaluated as "collision" relevant because TTC == TTC AEB
      - Evaluate outputs of Logic to evaluate the expected results (e.g. request to the actuator, Item state*)
- TCDS_1 – Step 3 – Actuator
  - Expected result:
    - Warning provided (visual and audible warning according to N 152)
    - Braking provided (deceleration of at least 5 m/s^2 according to N 152)

*: the function state shall be moved to Active – intervention, since it is providing both the warning and the braking

DS-2 Scenario

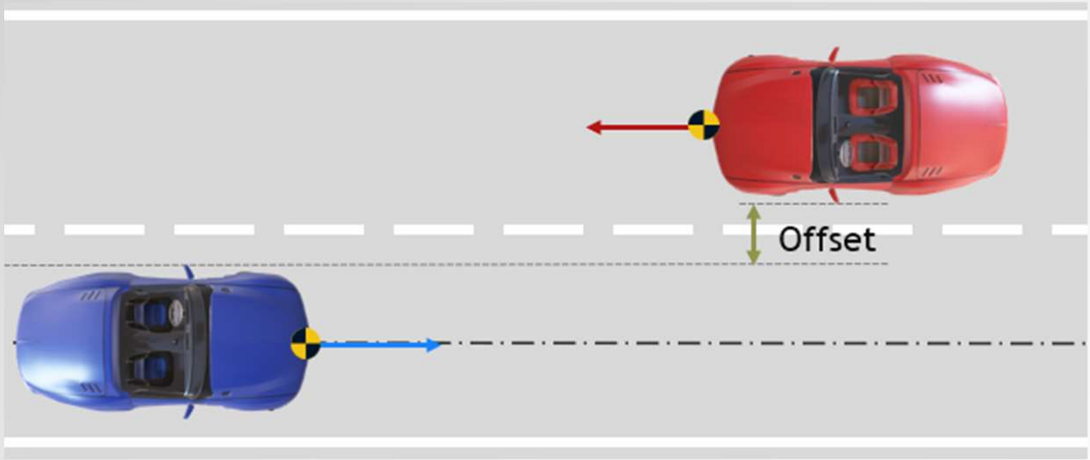
- DS-2 – Driving with a target vehicle coming from opposite direction



DS-2 – Driving with a target vehicle coming from opposite direction – 1/2

- When the distance with the target vehicle (from opposite direction) decreases but the driver is not in dangerous zone (no possible collision) the intended functionality shall neither warn the driver nor decelerate the vehicle.

- The probability of Exposure (duration) of these scenario conditions is E4, considering the following combinations:
  - Driving with opposite traffic within in visibility range – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h

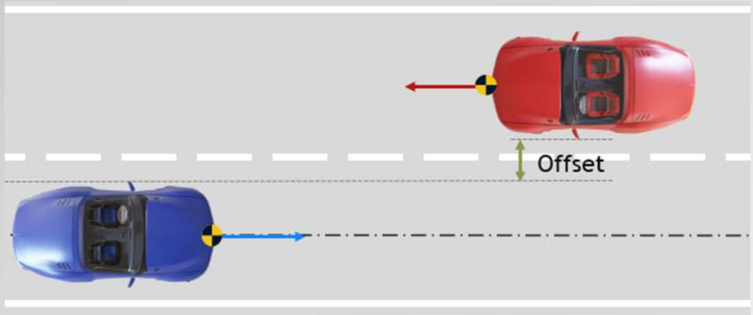


DS-2 – Driving with a target vehicle coming from opposite direction – 2/2

- The scenario conditions/constraints are the following:
  - The Ego-vehicle drives at a constant speed towards a target vehicle coming from the opposite direction.
  - The Ego vehicle speed range is [50 km/h, 130 km/h]
  - The target vehicle drive from 10 to 30 km/h
  - The offset between the vehicles is 1,5 m
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be respected:
    - both vehicles shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

DS-2– Test case specification

- Test case at vehicle level – ID: TCDS_2
  - For the DS-2 scenario, the following intended functionality capabilities shall be demonstrated:



- (Step 1) Track the red target vehicle and evaluate it as no-collision relevant
- (Step 2) When the distance, between the ego vehicle and the red target vehicle, is equal to the Time To Warning (TTW) but the lateral offset is > **lat_offset** , the intended functionality shall evaluate the red target vehicle as no-collision relevant and shall not provide at the visual and audible warning to the driver.
- (Step 3) When the distance, between the ego vehicle and the red target vehicle, is equal to the Time To Collision AEB (TTC AEB) but the lateral offset is > **lat_offset** , the intended functionality shall evaluate the red target vehicle as no-collision relevant shall not decelerate the vehicle.

DS-2 – Test case specification

- TCDS_2 - Step 1
  - Ego vehicle status:
    - Kl.15 = on;
    - Gear position = "D"
    - Intended functionality state: active
  - Initial ego vehicle speed:
    - 50 (+/- 2) km/h
    - 80 (+/- 2) km/h
    - 100 (+/- 2) km/h
  - Driver Input:
    - Steering wheel angle: < SWA_Threshold
    - Acceleration = constant
    - Brake = not present
  - Initial target vehicle speed (red):
    - 10 (+/- 2) km/h
    - 20 (+/- 2) km/h
    - 30 (+/- 2) km/h

DS-2 – Test case specification

- TCDS_2 - Step 1
  - Initial longitudinal offset = TTC > TTW or TTC_{AEB}
  - Environmental conditions:
    - Light
      - Day: > LuxDay_Threshold
      - Night: <= LuxNight_Threshold
      - Test surface = solid and dry
  - Expected result:
    - Warning = Not present
    - Braking = Not present

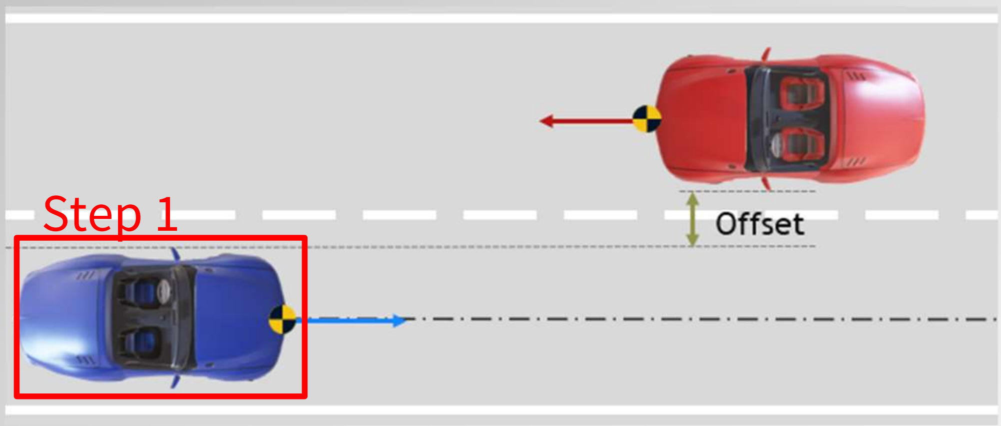
DS-2 – Test case specification

- TCDS_2 – Step 2
  - Ego vehicle status:
    - Kl.15 = on;
    - Gear position = "D"
    - Distance between Ego vehicle position and target vehicle = TTC == TTW
    - Intended functionality state: active
    - lateral offset > **lat_offset**
  - ego vehicle speed = constant according to initial speed
  - target vehicle speed = constant
  - Driver Input:
    - Steering wheel angle: < SWA_Threshold
  - Environmental conditions:
    - Light
      - Day: > LuxDay_Threshold
      - Night: <= LuxNight_Threshold
      - Test surface = solid and dry
  - Expected result:
    - Warning = Not present
    - Braking = Not present

DS-2 – Test case specification

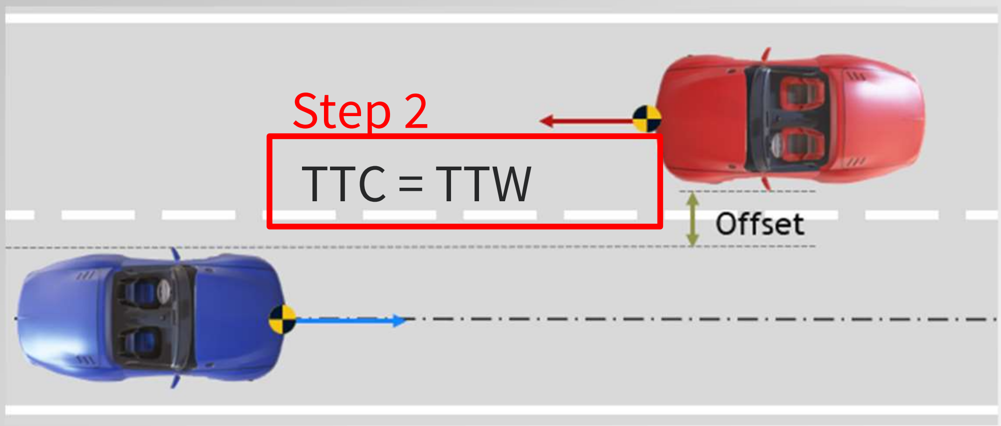
- TCDS_2 - Step 3
  - Ego vehicle status:
    - Kl.15 = on;
    - Gear position = "D"
    - Distance between Ego vehicle position and target vehicle = TTC == TTC AEB
    - Intended functionality state: active
    - lateral offset > **lat_offset**
  - ego vehicle speed = constant according to initial speed
  - target vehicle speed = constant
  - Driver Input:
    - Steering wheel angle: < SWA_Threshold
  - Environmental conditions:
    - Light
      - Day: > LuxDay_Threshold
      - Night: <= LuxNight_Threshold
      - Test surface = solid and dry
  - Expected result:
    - Warning = Not present
    - Braking = Not present

DS-2 – Test case Break-down



- TCDS_2 - Step 1 – Vehicle
  - Expected result:
    - Warning = Not present
    - Braking = Not present
- TCDS_2 – Step 1 – Sense
  - Expected result:
    - Object detected
    - Object classified as "car"
      - Evaluate outputs of sensors to evaluate the expected results (e.g. detected objects, object classification)
- TCDS_2 – Step 1 – Logic
  - Expected result:
    - Object evaluated as "no-collision" relevant
      - Evaluate outputs of Logic to evaluate the expected results (e.g. request to the actuator)
- TCDS_2 – Step 1 – Actuator
  - Expected result:
    - No warning
    - No braking actuated

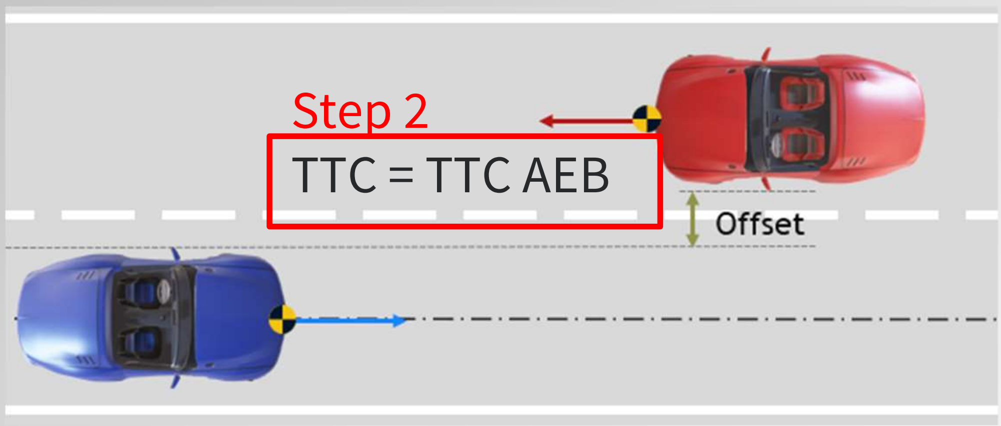
DS-2 – Test case Break-down



- TCDS_2 - Step 2 – Vehicle
  - Expected result:
    - Warning = Not present
    - Braking = Not present
- TCDS_2 – Step 2 – Sense
  - Expected result:
    - Object detected
    - Object classified as "car"
      - Evaluate outputs of sensors to evaluate the expected results (e.g. detected objects, object classification)
- TCDS_2 – Step 2 – Logic
  - Expected result:
    - Object evaluated as "no-collision" relevant because lateral offset is higher than lat_Offset
      - Evaluate outputs of Logic to evaluate the expected results (e.g. request to the actuator, Item state*)
- TCDS_2 – Step 2 – Actuator
  - Expected result:
    - No warning
    - No braking actuated

*: the function state shall be Active

DS-2 – Test case Break-down

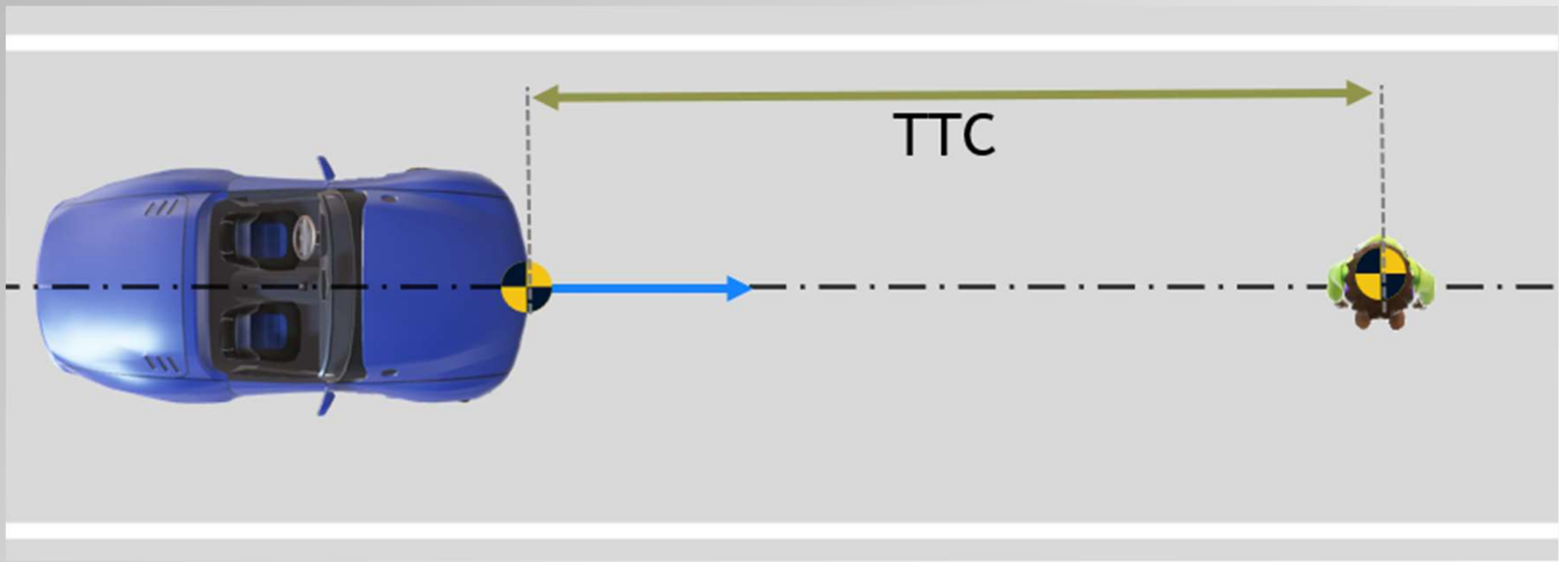


- TCDS_2 - Step 3 – Vehicle
  - Expected result:
    - Warning = Not present
    - Braking = Not present
- TCDS_2 - Step 3 – Sense
  - Expected result:
    - Object detected
    - Object classified as "car"
      - Evaluate outputs of sensors to evaluate the expected results (e.g. detected objects, object classification)
- TCDS_2 - Step 3 – Logic
  - Expected result:
    - Object evaluated as "no-collision" relevant because lateral offset is higher than lat_Offset
      - Evaluate outputs of Logic to evaluate the expected results (e.g. request to the actuator, Item state*)
- TCDS_2 - Step 3 – Actuator
  - Expected result:
    - No warning
    - No braking actuated

*: the function state shall be Active

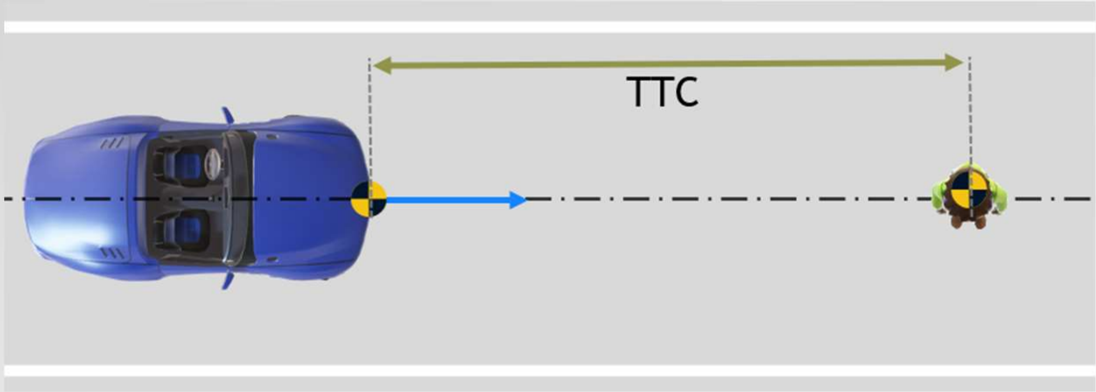
DS-3 Scenario

- DS-3 – Drive towards a pedestrian



DS-3 – Drive towards a pedestrian – 1/2

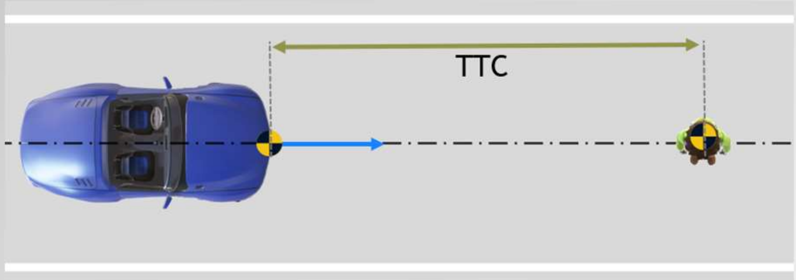
- When the distance with vulnerable users (e.g., pedestrian, cyclist) decreases so that the driver or vulnerable users are in dangerous zone (possible collision) the intended functionality shall warn the driver and, if no driver reaction occurs and the collision is imminent, shall decelerate the vehicle.
- The probability of Exposure (duration) of these scenario conditions is E3, considering the following combinations:
  - Driving in a city– E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Persons within danger zone (ca. 1 vehicle lenght in front of vehicle) – E3 (1% to 10% of average operating time)
    - E.g., from 80 h to 800 h



DS-3 – Drive towards a pedestrian – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives in urban roads towards vulnerable users (e.g., pedestrian, cyclist) crossing the road perpendicular to the Ego vehicle's direction.
  - The Ego vehicle speed range is [5 km/h, 50 km/h]
  - The pedestrian crosses the road at 5 km/h (± 0,1 km/h)
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be respected:
    - Ego vehicle shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold

DS-3 – Test case specification



- Test case at vehicle level – ID: TCDS_3
  - For the DS-3 scenario, the following intended functionality capabilities shall be demonstrated:
    - (Step 1) The ego vehicle is approaching the vulnerable users (e.g., pedestrian, cyclist)
    - (Step 2) When the distance, between the ego vehicle and the VRUs, is equal to the Time To Warning (TTW), the intended functionality shall evaluate the VRUs as collision relevant and provide at least 0,8 s before the start of the emergency braking the visual and audible warning to the driver (UN Regulation N° 152 clause 5.2.1.1, 5.5.1).
    - (Step 3) When the distance, between the ego vehicle and VRUs, is equal to the Time To Collision AEB (TTC AEB), the intended functionality shall ,if no driver reaction occurs, shall decelerate the vehicle providing at least 5.0 m/s2 (UN Regulation N° 152 clause 5.2.1.2).

DS-3 – Test case specification

TCDS_3 - Step 1

- Ego vehicle status:
  - Kl.15 = On;
  - Gear position = D;
  - Intended functionality state: Active
- Initial ego vehicle speed:
  - 10 (+/- 2) km/h
  - 30 (+/- 2) km/h
  - 50 (+/- 2) km/h
- Driver Input:
  - Steering wheel angle: < SWA_Threshold
  - Acceleration = constant
  - Brake = not present
- Environmental conditions:
  - Light
    - Day: > LuxDay_Threshold
    - Night: ≤ LuxNight_Threshold
    - Test surface = solid and dry
- Initial longitudinal offset = TTC > TTW or TTC_{AEB}
- Expected result:
  - Warning = Not present
  - Braking = Not present

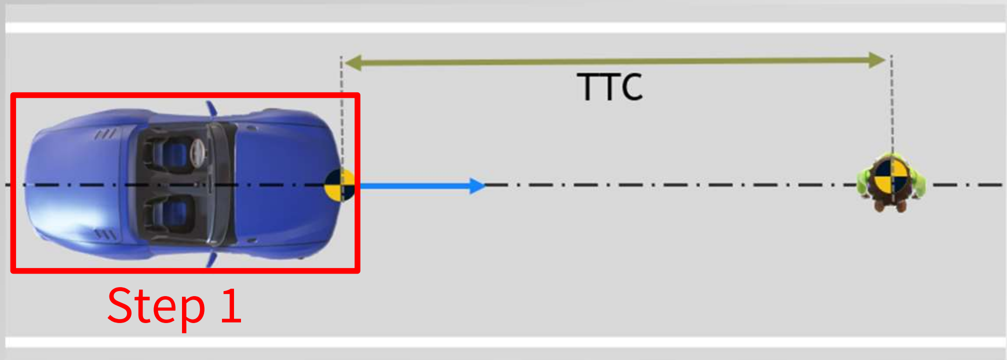
DS-3 – Test case specification

- TCDS_3 - Step 2
  - Ego vehicle status:
    - Kl.15 = On;
    - Gear position = D;
    - Intended functionality state: Active intervening
  - Ego vehicle speed: constant according to initial speed
  - Driver Input:
    - Steering wheel angle: < SWA_Threshold
    - Acceleration = constant
    - Brake = not present
  - Environmental conditions:
    - Light
      - Day: > LuxDay_Threshold
      - Night: ≤ LuxNight_Threshold
      - Test surface = solid and dry
  - Distance between Ego vehicle position and target vehicle = TTC == TTW
  - Expected result:
    - Warning = Present
    - Braking = Not present

DS-3 – Test case specification

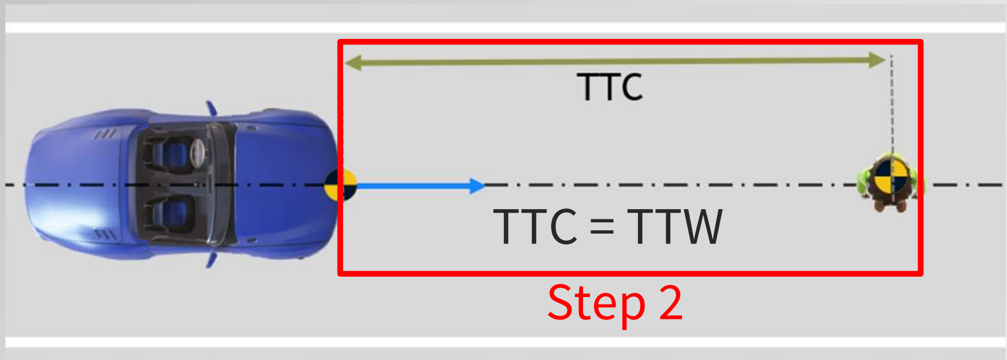
- TCDS_3 - Step 3
  - Ego vehicle status:
    - Kl.15 = On;
    - Gear position = D;
    - Intended functionality state: Active intervening
  - Ego vehicle speed: constant according to initial speed
  - Driver Input:
    - Steering wheel angle: < SWA_Threshold
    - Acceleration = constant
    - Brake = not present
  - Environmental conditions:
    - Light
      - Day: > LuxDay_Threshold
      - Night: ≤ LuxNight_Threshold
      - Test surface = solid and dry
  - Distance between Ego vehicle position and target vehicle = TTC == TTC_{AEB}
  - Expected result:
    - Warning = Present
    - Braking = Present

DS-3 – Test case Break-down



- TCDS_3 - Step 1 – Vehicle
  - Expected result:
    - Warning = Not Present
    - Braking = Not Present
- TCDS_ 3 – Step 1 – Sense
  - Expected result:
    - Object detected
    - Object classified as "pedestrian"
      - Evaluate outputs of sensors to evaluate the expected results (e.g. detected objects, object classification)
- TCDS_3 – Step 1 – Logic
  - Expected result:
    - Object evaluated as "no-collision" relevant
      - Evaluate outputs of Logic to evaluate the expected results (e.g. request to the actuator)
- TCDS_3 – Step 1 – Actuator
  - Expected result:
    - No warning
    - No braking actuated

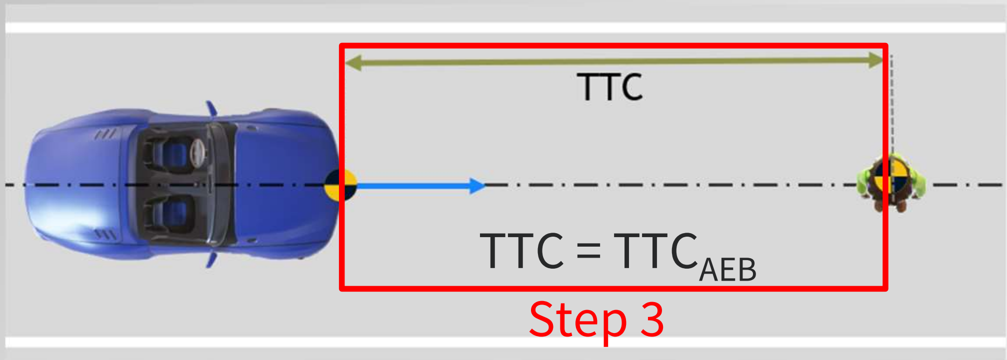
DS-3 – Test case Break-down



- TCDS_3 - Step 2 – Vehicle
  - Expected result:
    - Warning = Present
    - Braking = Not Present
- TCDS_3 – Step 2 – Sense
  - Expected result:
    - Object detected
    - Object classified as "pedestrian"
      - Evaluate outputs of sensors to evaluate the expected results (e.g. detected objects, object classification)
- TCDS_3 – Step 2 – Logic
  - Expected result:
    - Object evaluated as "collision" relevant because TTC == TTW
      - Evaluate outputs of Logic to evaluate the expected results (e.g. request to the actuator, Item state*)
- TCDS_3 – Step 2 – Actuator
  - Expected result:
    - Warning provided (visual and audible warning according to N 152
    - No braking actuated

*: the function state shall be moved to Active – intervention, since it is providing the warning

DS-3 – Test case Break-down

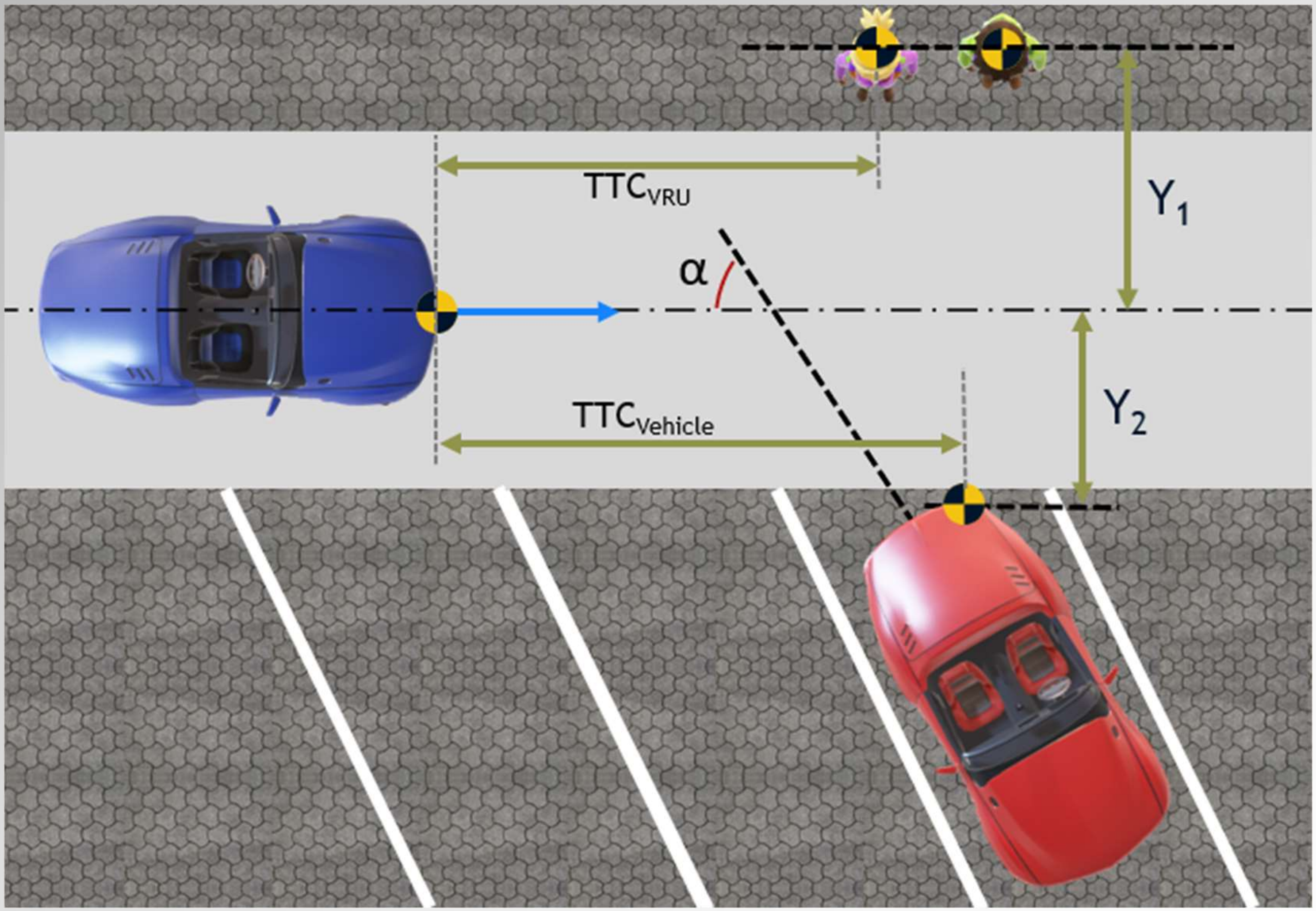


- TCDS_3 - Step 3 – Vehicle
  - Expected result:
    - Warning = Present
    - Braking = Present
- TCDS_3 – Step 3 – Sense
  - Expected result:
    - Object detected
    - Object classified as "pedestrian"
      - Evaluate outputs of sensors to evaluate the expected results (e.g. detected objects, object classification)
- TCDS_3 – Step 3 – Logic
  - Expected result:
    - Object evaluated as "collision" relevant because TTC == TTC_{AEB}
      - Evaluate outputs of Logic to evaluate the expected results (e.g. request to the actuator, Item state*)
- TCDS_3 – Step 3 – Actuator
  - Expected result:
    - Warning provided (visual and audible warning according to N 152)
    - Braking provided (deceleration of at least 5 m/s^2 according to N 152)

*: the function state shall be moved to Active – intervention, since it is providing the warning

DS-4 Scenario

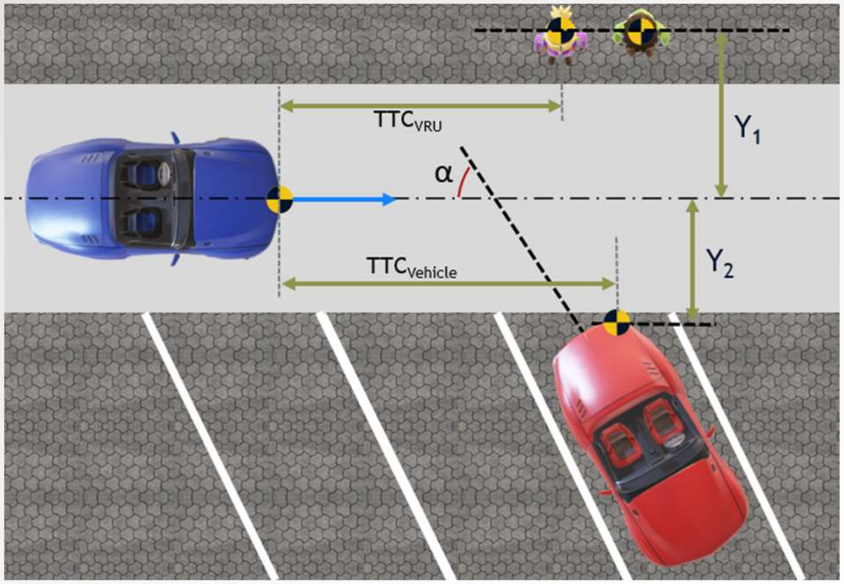
- DS-4 – Drive towards parked cars and pedestrians on sidewalk



DS-4 – Drive towards parked cars and pedestrians on sidewalk) – 1/2

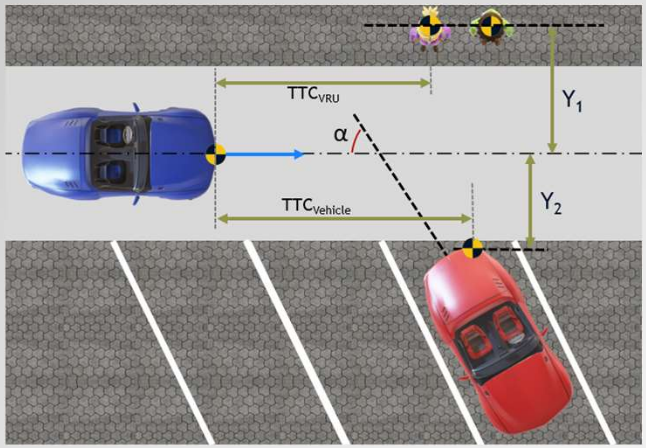
Back

- When the distance with the parked target vehicle and the VRUs on sidewalk decreases but the driver is not in dangerous zone (no possible collision) the intended functionality shall neither warn the driver nor decelerate the vehicle.
- The probability of Exposure (duration) of these scenario conditions is E3, considering the following combinations:
  - Driving in the city – E4 (>10 % of average operating time)
    - E.g., 10% of 8000h = 800 h
  - Persons within danger zone (ca. 1 vehicle lenght in front of vehicle) – E3 (1% to 10% of average operating time)
    - E.g., from 80 h to 800 h



DS-4 – Drive towards parked cars and pedestrians on sidewalk) – 2/2

- The scenario conditions/constraints are the following:
  - The Ego vehicle drives at constant speed in the city towards a parked target vehicle (positioned with an angle offset with respect to the trajectory) and VRUs (pedestrians and/or cyclist) on sidewalk.
  - The Ego vehicle speed range is [5 km/h, 50 km/h]
  - The parked target vehicle has an angle offset (α) from x ° and z °
  - The offset between the ego vehicle and parked vehicle (Y_1) is at least 1,5 m
  - The offset between the ego vehicle and VRUs (Y_2) is at least 1,5 m
  - The following environmental conditions shall be present:
    - Dry and daylight with minimum 1000 lux and Sun angle >15° to horizon
    - Dry and night with maximum 10 lux
  - Road surface is asphalt or concrete
  - The following Pre-conditions shall be met:
    - Ego vehicle shall keep steady speed and path
    - steering angle shall be lower than the override threshold
    - yaw rate shall be lower than the override threshold



- Test case at vehicle level – ID: TCDS_4
  - For the DS-4 scenario, the following intended functionality capabilities shall be demonstrated:
    - (Step 1) Track the parked target vehicle and the VRUs and evaluate them as no-collision relevant.
    - (Step 2) When the distance, between the ego vehicle and parked red target vehicle or VRUs, is equal to the Time To Warning (TTW) but both Y1 lateral offset and Y2 lateral offset are > lat_offset, the intended functionality shall evaluate the target vehicle and the VRUS as no-collision relevant and shall not provide at the visual and audible warning to the driver.
    - (Step 3) When the distance, between the ego vehicle and parked red target vehicle or VRUs, is equal to the Time To Collision AEB (TTC AEB) but both Y1 lateral offset and Y2 lateral offset are > lat_offset, the intended functionality shall evaluate the target vehicle and the VRUS as no-collision relevant and shall not decelerate the vehicle.

DS-4 – Test case specification

- TCDS_4 - Step 1
  - Ego vehicle status:
    - Kl.15 = on;
    - Gear position = "D"
    - Intended functionality state: active
  - Initial ego vehicle speed:
    - 20 (+/- 2) km/h
    - 25 (+/- 2) km/h
    - 50 (+/- 2) km/h
  - Driver Input:
    - Steering wheel angle: < SWA_Threshold
    - Acceleration = constant
    - Brake = not present
  - Initial longitudinal offset = TTC_{VRU} and $TTC_{Vehicle}$(4s) > TTW or TTC_{AEB}
  - Parked vehicle Angle offset (α) from x ° and z °

DS-4 – Test case specification

- TCDS_4 - Step 1
  - VRUs lateral offset $(Y_1) \geq 1{,}5$ m
  - Parked vehicle lateral offset $(Y_2) \geq 1{,}5$ m
  - Environmental conditions:
    - Light
      - Day: > 1000 lux
      - Sun angle > 15° to horizon
      - Night: <= 10 lux
      - Test surface = solid and dry
  - Expected result:
    - Warning = Not present
    - Braking = Not present

DS-4 – Test case specification

- TCDS_4 - Step 2
  - Ego vehicle status:
    - Kl.15 = on;
    - Gear position = "D"
    - Distance between Ego vehicle position and parked vehicle = $TTC_{Vehicle}$ == TTW
    - Distance between Ego vehicle position and VRUs = TTC_{VRU} == TTW
    - Intended functionality state: active
  - ego vehicle speed = constant according to initial speed
  - Driver Input:
    - Steering wheel angle: < SWA_Threshold
    - Acceleration = constant
    - Brake = not present
  - Parked vehicle Angle offset (α) from x ° and z °
  - VRUs lateral offset (Y1) ≥ 1,5 m
  - Parked vehicle lateral offset (Y2) ≥ 1,5 m

DS-4 – Test case specification

- TCDS_4 - Step 2
  - Environmental conditions:
    - Light
      - Day: > 1000 lux
      - Sun angle > 15° to horizon
      - Night: <= 10 lux
      - Test surface = solid and dry
  - Expected result:
    - Warning = Not present
    - Braking = Not present

DS-4 – Test case specification

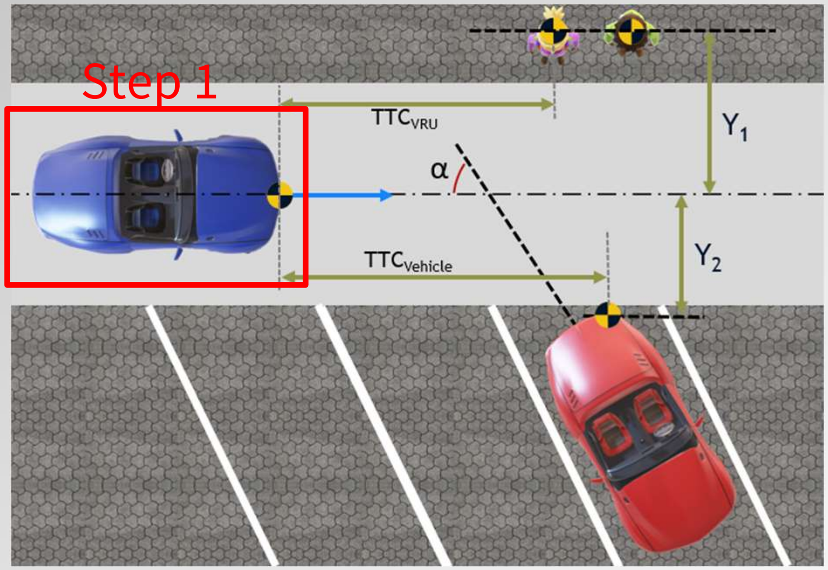
- TCDS_4 - Step 3
  - Ego vehicle status:
    - Kl.15 = on;
    - Gear position = "D"
    - Distance between Ego vehicle position and parked vehicle = $TTC_{Vehicle}$ == TTC AEB
    - Distance between Ego vehicle position and VRUs = TTC_{VRU} == TTC AEB
    - Intended functionality state: active
  - ego vehicle speed = constant according to initial speed
  - Driver Input:
    - Steering wheel angle: < SWA_Threshold
    - Acceleration = constant
    - Brake = not present
  - Parked vehicle Angle offset (α) from x ° and z °
  - VRUs lateral offset (Y1) ≥ 1,5 m
  - Parked vehicle lateral offset (Y2) ≥ 1,5 m

DS-4 – Test case specification

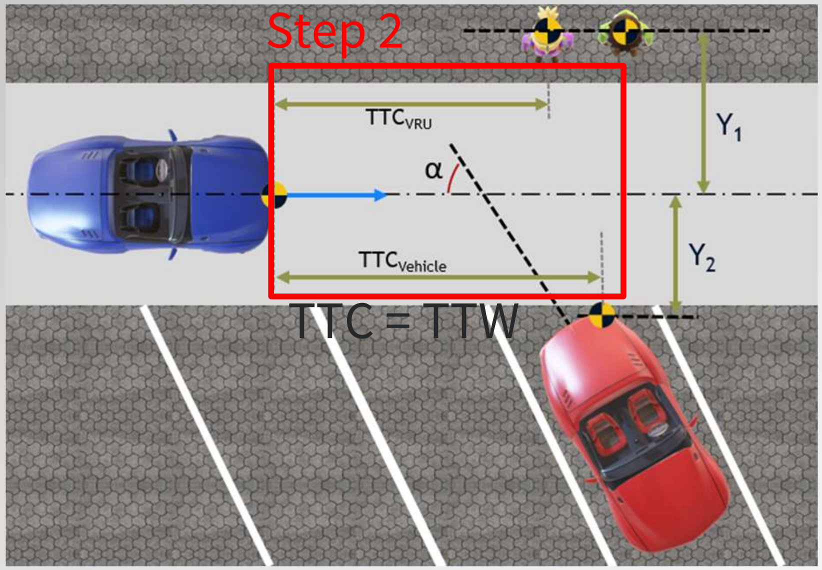
- TCDS_4 - Step 3
  - Environmental conditions:
    - Light
      - Day: > 1000 lux
      - Sun angle > 15° to horizon
      - Night: <= 10 lux
      - Test surface = solid and dry
  - Expected result:
    - Warning = Not present
    - Braking = Not present

DS-4 – Test case Break-down

- TCDS_4 - Step 1 – Vehicle
  - Expected result:
    - Warning = Not present
    - Braking = Not present
- TCDS_4 – Step 1 – Sense
  - Expected result:
    - Objects detected
    - Objects classified as “car” or “pedestrian”
      - Evaluate outputs of sensors to evaluate the expected results (e.g. detected objects, object classification)
- TCDS_4 – Step 1 – Logic
  - Expected result:
    - Objects evaluated as “no-collision” relevant
      - Evaluate outputs of Logic to evaluate the expected results (e.g. request to the actuator)
- TCDS_4 – Step 1 – Actuator
  - Expected result:
    - No warning
    - No braking actuated



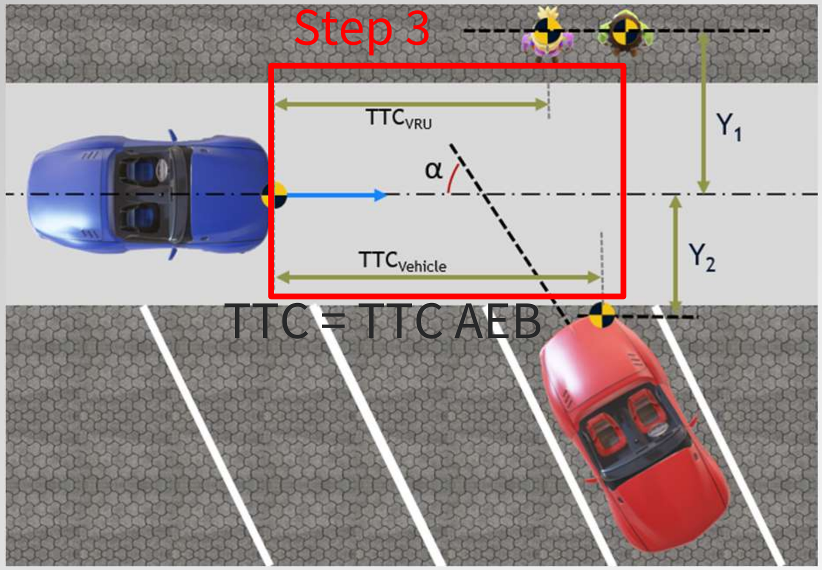
DS-4 – Test case Break-down



- TCDS_4 - Step 2 – Vehicle
  - Expected result:
    - Warning = Not present
    - Braking = Not present
- TCDS_4 – Step 2 – Sense
  - Expected result:
    - Objects detected
    - Objects classified as “car” or “pedestrian”
      - Evaluate outputs of sensors to evaluate the expected results (e.g. detected objects, object classification)
- TCDS_4 – Step 2 – Logic
  - Expected result:
    - Object evaluated as “no-collision” relevant because lateral offsets (Y_1 and Y_2) are higher than lat_Offset
      - Evaluate outputs of Logic to evaluate the expected results (e.g. request to the actuator, Item state*)
- TCDS_4 – Step 2 – Actuator
  - Expected result:
    - No warning
    - No braking actuated

*: the function state shall be active

DS-4 – Test case Break-down



- TCDS_4 - Step 3 – Vehicle
  - Expected result:
    - Warning = Not present
    - Braking = Not present
- TCDS_4 – Step 3 – Sense
  - Expected result:
    - Objects detected
    - Objects classified as “car” or “pedestrian”
      - Evaluate outputs of sensors to evaluate the expected results (e.g. detected objects, object classification)
- TCDS_4 – Step 3 – Logic
  - Expected result:
    - Object evaluated as “no-collision” relevant because lateral offsets (Y_1 and Y_2) are higher than lat_Offset
      - Evaluate outputs of Logic to evaluate the expected results (e.g. request to the actuator, Item state*)
- TCDS_4 – Step 3 – Actuator
  - Expected result:
    - No warning
    - No braking actuated

*: the function state shall be active

UN Regulation No. [152]

Back

5.2.	Specific Requirements
5.2.1.	Car to car scenario
5.2.1.1.	Collision warning

When a collision with a preceding vehicle of Category M_1, in the same lane with a relative speed above that speed up to which the subject vehicle is able to avoid the collision, is imminent, a collision warning shall be provided as specified in paragraph 5.5.1., and shall be triggered at the latest 0.8 seconds before the start of emergency braking.

However, in case the collision cannot be anticipated in time to give a collision warning 0.8 seconds ahead of an emergency braking a collision warning shall be provided as specified in paragraph 5.5.1. and shall be provided no later than the start of emergency braking intervention.

The collision warning may be aborted if the conditions prevailing a collision are no longer present.

This shall be tested according to paragraphs 6.4. and 6.5.

UN Regulation No. [152]

Back

5.5.	Warning Indication
5.5.1.	The collision warning referred to in paragraphs 5.2.1.1. and 5.2.2.1. shall be provided by at least two modes selected from acoustic, haptic or optical.

5.2.1.2.	Emergency braking
	When the system has detected the possibility of an imminent collision, there shall be a braking demand of at least 5.0 m/s² to the service braking system of the vehicle.
	The emergency braking may be aborted if the conditions prevailing a collision are no longer present.
	This shall be tested in accordance with paragraphs 6.4. and 6.5. of this Regulation.

Author	G. Nicosia
Company	Exida Development
Version	1.0
File name	Scenarios catalogue Tailored
Status	Draft

Document Change History			
Date	**Version**	**Changed by**	**Change Description**
12/01/2024	1.0	G. Nicosia	First Draft creation
07/08/2024	1.1	G. Nicosia	Update of Scope and purpose page

exida DEVELOPMENT

excellence in dependable automation

Many Thanks for your Attention