CONIGITAL
CONNECTED DIGITAL

D7.1_SAVOR_Get_Safe_Recommendation_Report.docx

SAVOR

D7.1 Get Safe Recommendations Report

Conigital.com   info@conigital.com   +44 (0) 843 289 0874

SAVOR D7.1 Get Safe Recommendation Report

Author: Prashanth Dhurjati

Date: 13/0/2022

Filename: D7.1 – Get Safe Recommendation Report.docx

Doc Version: 2

Status: ISSUED

Classification: PUBLIC

Intended Audience: No Restrictions

Rev	Description	Date
1	Initial Draft to share for Review	07/04/2022
2	For Release	13/05/2022

Table 1 Revision History

Contents

Tables

1 Introduction

This deliverable provides recommendations for defining the Minimum Risk Conditions (MRCs) for Automated Driving Systems (ADS) where the occupants of the vehicle do not take the role of Dynamic Driving Task (DDT) fallback.

The strategy for MRC selection is defined considering various architectures of the autonomous vehicle (with and without redundancies). It can be applied to vehicles that drive on urban roads, inter-urban roads and highways.

1.1 Key definitions

The following definitions (Source: ISO 26262, SAE J3016, IDIADA internal development) are used in the MRC strategy:

- **Element:** system, components (hardware or software), hardware parts, or software units.
- **Event:** Any condition that affects the same behaviour of the ADS. Even could be an internal event such as a malfunction or an external event such as encountering a SOTIF triggering event.
- **Failure:** Termination of an intended behaviour of an element or an item due to a fault manifestation.
- **Item:** System or combination of systems, to which ISO 26262 is applied, that implements a function or part of a function at the vehicle level.
- **Redundancy:** Existence of means in addition to the means that would be sufficient to perform a required function or to represent information. Duplicated functional components can be an instance of redundancy for the purpose of increasing availability.
- **Primary element:** Element that supports the provision of the intended function under non-faulty conditions (nominal performance).
- **Redundant element:** Duplicated element that provides the intended function when the primary element is unavailable due to malfunction.
- **Operational function:** Lateral and longitudinal vehicle motion control functions are defined as operational functions.
- **Tactical function:** Functions including manoeuvre planning based on objects and events detection and functions that enhance conspicuity via lighting, sounding the horn, signalling, gesturing, etc form part of the tactical functions.
- **Strategic function:** High level functions like route and destination timing and selection form part of the strategic functions.

2 Approach for defining the MRCs

The SAVOR project defines the MRCs as a function of the risk posed by the current unsafe event and the current location of the vehicle.

$MRC = f(Risk, location)$

2.1 Risk estimation

Risk posed by an unsafe event is based on the category of driving function affected by the malfunction and the availability of the redundant elements to assume the task of the affected function(s).

The table below defines the overall approach for risk classification:

Risk Level	Unsafe Event
High	Failure of a redundant element or the only available element (absence of redundant elements) supporting the operational and tactical functions.
Medium	Failure of a primary element supporting operational and tactical functions (whilst redundant elements are available) or failure of the only available element supporting strategic function (absence of redundant elements).
Low	Failure of a primary element supporting strategic functions (whilst redundant elements are available)

TABLE 1 - RISK CLASSIFICATION

2.2 Location categories

Apart from the risk associated with unsafe event, the MRC also depend on the current location of the autonomous vehicle. This is to address the following two concerns:

- Same MRC might not be achievable in all locations (e.g. stopping at a parking spot might not be feasible on a highway, but easier in inter-urban scenarios)
- Same MRC might not be safe in all the locations (e.g. On highways moving to low speed lanes and then stopping might be safer than stopping in the current lane which is fine while driving in low speed urban roads)

The current strategy assumes that the vehicle is used in any of the following 3 types of roads:

- High speed roads (Motorways and A-roads)
- Inter-urban roads (B and C-roads)
- Urban roads (Roads within cities, towns, and villages)

2.3 Minimum Risk Condition (MRC) assignment

The following procedure is used to assign MRC for each of the detected unsafe event on the autonomous vehicle:

1. Identify the **risk level** of the unsafe event based on the Table 1 - Risk Classification provided in section 2.1 Risk estimation.
2. Identify the current **location category** of the autonomous vehicle based on the criteria defined in section 2.2 Location categories.
3. Assign the MRC based on the Table 2 - Assignment of MRCs provided in the section 2.3 Minimum Risk Condition (MRC) assignment.

The table below assigns MRCs based on the risk level of the unsafe event and the location of the autonomous vehicle:

Location Risk Level	Highspeed roads	Inter -urban road	Urban road
High	Stop in lane	Stop in lane	Stop in lane
Medium	Move away from active lanes of traffic and stop at the next available hard shoulder	Stop at the closest available parking spot adjacent to the lane	Stop at the closest parking spot
Low	Exit the highway and stop at a designated highway parking area or depot	Stop at the closest parking area or depot	Stop at the closest parking spot or depot

TABLE 2 - ASSIGNMENT OF MRCS

Rationale for the assignments:

- **High risk events:** Stopping in lane is the safest condition to achieve (irrespective of the location category) when safe operation of the operational and tactical functions cannot be guaranteed. This can happen either due to lack of redundant elements or due to failure of the redundant elements that are being utilised due to prior conditions (e.g. pre-existing independent unsafe event).

  E.g. loss of OEDR function, loss of steering control, loss of visibility due to extreme fog, etc.

- **Medium risk events:** Due to the presence of redundant systems, no DDT (Dynamic Driving Task) functions are compromised by these unsafe events. But further failures or unsafe events can result in hazardous events. Therefore, when medium risk events occur, the vehicle shall find a suitable place to stop without compromising the safety of the other road users. It is assumed that the integrity of the redundant systems is high enough to complete the task safely. The same strategy is used when redundant systems supporting strategic functions are lost. In this case, the autonomous system cannot change its current route, therefore it has to find the closed available parking spot on its current route and stop.

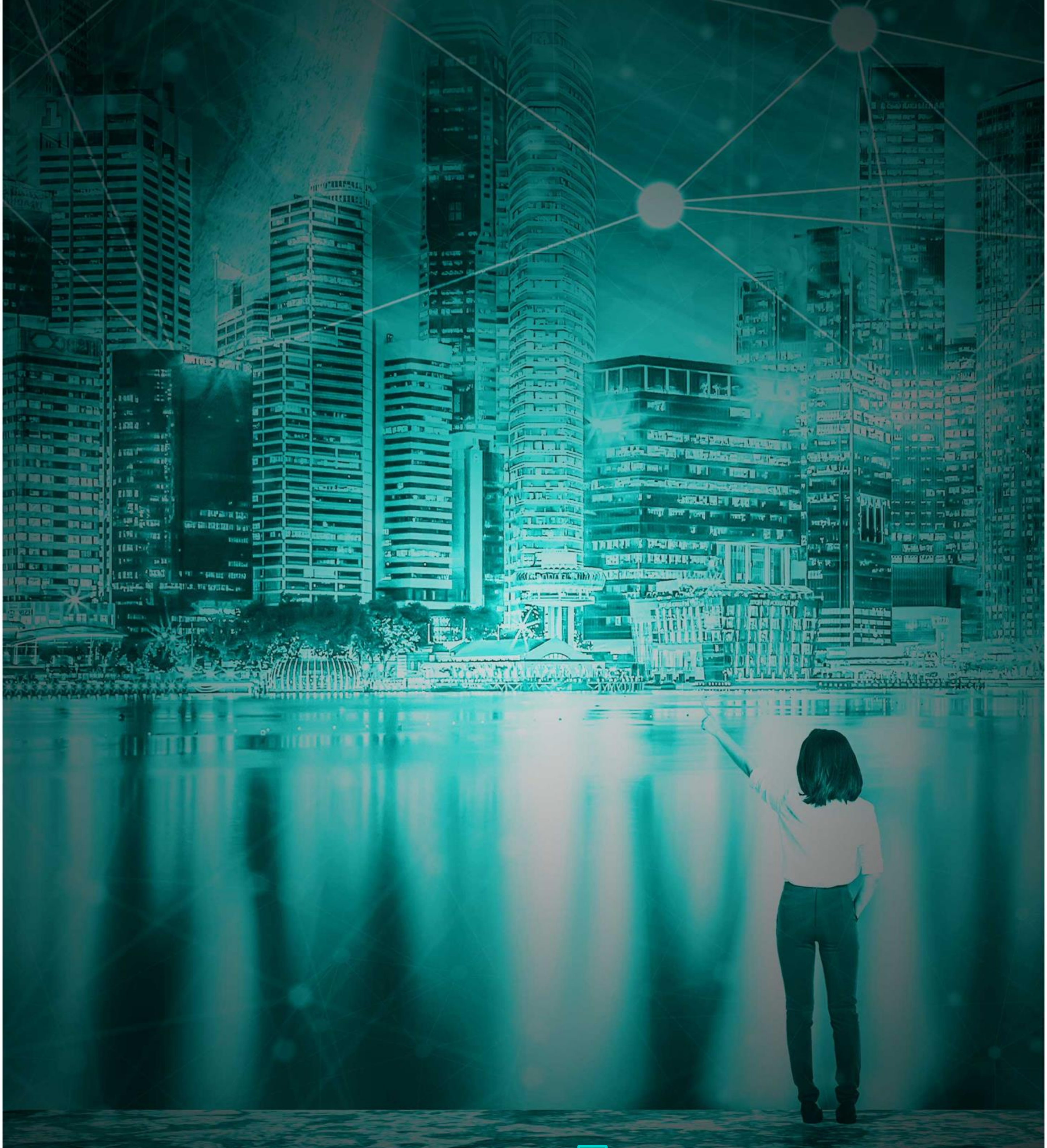
- **Low risk events:** Low risk events do not compromise the DDT tasks nor the strategic functions of the autonomous vehicle. Therefore, it gives the system the opportunity to find a parking area or go back to the depot.

3 Conclusions

The SAVOR project defined a strategy for assigning Minimum Risk Conditions (MRCs) for autonomous vehicles based on the risk associated with the current unsafe event and the current location of the vehicle.

A method was defined to assign risk levels to the current unsafe event based on the functions being affected by the malfunction/event (operational functions, tactical functions or strategic functions) and the availability of redundant elements in the vehicle architecture.

An on-board safety driver shall be mandatory for autonomous vehicles that do not incorporate redundant elements for the operational and tactical function.



SAVOR

D7.1 Get Safe Recommendations Report

Conigital.com
info@conigital.com
☎ +44 (0) 843 289 0874