Traffic Optimization for Signalized Corridors (TOSCo) Phase 1 Project

Functional Safety Concept and Hazard Analysis

Acknowledgement and Disclaimer

This material is based up on work supported by the U.S. Department of Transportation under Cooperative Agreement No. DTFH6114H00002.

Any opinions, findings and conclusions or recommendations expressed in this publications are those of the Author(s) and do not necessarily reflect the view of the U.S. Department of Transportation.

Technical Report Documentation Page

4. Title and Subtitle
Traffic Optimization for Signalized Corridors (TOSCo) Phase 1 Project
Functional Safety Concept and Hazard Analysis

5. Report Date
June 28, 2019

7. Author(s)
Das, Nabarun; George, Agish; Guenther, Hendrik-Joern; Hussain, Shah; Naes, Tyler; Probert, Neal; Vijaya Kumar, Vivek; Williams, Richard; Yoshida, Hiroyuki; Yumak, Tuncer; Deering, Richard; Goudy, Roy

9. Performing Organization Name And Address
Crash Avoidance Metrics Partners LLC
on behalf of the Vehicle-to-Infrastructure Consortium
27220 Haggerty Road, Suite D-1
Farmington Hills, MI 48331

16. Abstract
This report details a step-by-step framework developed in accordance with the process defined in ISO 26262 and provides a summary and findings of the functional safety analysis. The report begins with a review of the TOSCo system followed by an introduction of the ISO 26262 functional safety process. The report then provides details on the work products listed below, focusing on the concept phase for automotive applications.

- Item definition (identify the TOSCo boundary and its intended features and functions)
- Hazard Analysis and Risk Assessment (HARA) (determination of safety goals and Automotive Safety Integrity Levels (ASILs)
- Functional safety concept (provide requirements for functional safety management, design and implementation)

The analysis did not cover product design and integration. The functional requirements focused on technical implementation into specific TOSCo components at a system level which can be utilized for subsequent integration and implementation.

21. No. of Pages
47

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 TOSCo Description

Traffic Optimization for Signalized Corridors (TOSCo) is a system comprised of both in-vehicle and infrastructure-based equipment. The in-vehicle equipment employs data transmitted via wireless communications from Roadside Units (RSU) to optimize vehicle fuel economy, emissions reduction and traffic mobility along a signalized corridor equipped to provide information required for TOSCo to operate.

The primary function of TOSCo is to generate an optimal speed and acceleration profile to be able to pass through a green light at one or more traffic intersections or to decelerate to a stop and then launch in the most optimized manner per system design. The calculated targets are communicated to an in-vehicle longitudinal control system within the Host Vehicle (HV) to support partial automation. It is to be noted that in no situation would the driver set speed be exceeded by the longitudinal control system. Both passenger cars and trucks are assumed to be able to employ the TOSCo feature.

1.2 Background

ISO 26262 is the *state of the art* standard for functional safety of electrical and/or electronic (E/E) systems for passenger vehicles. It is closely tied to the automotive product development lifecycle and addresses all activities specific to management of functional safety. The ISO 26262 standard has been adapted from IEC 61508 and is tailored to the needs of the automotive industry. Product liability requires a burden of proof to be provided for development. The standard provides sufficient requirements and recommendations for the integration of a safe road worthy product throughout the development process, which is also accompanied with the appropriate documentation and work products. This provides sufficient evidence and confidence to use the ISO 26262 standard for initial development and analysis of the TOSCo feature. The second and latest edition of the standard now provides requirements for trucks and buses along with passenger vehicles, which sufficiently covers the intended scope of the TOSCo feature.

1.3 Purpose and Scope

ISO 26262 places significant emphasis towards development of safety in the early product lifecycle and provides comprehensive guidance on development of safety critical products running parallel to the overall development process. ISO 26262 addresses potential vehicle-level hazards and risks due to the failure or malfunction of electrical and/or electronic (E/E) safety relevant systems, including interaction of these systems.

For TOSCo, the need for functional safety is strengthened due to multiple E/E safety critical features and functions that are planned to support partial automation of the vehicle. V2V communication within the vehicle string and maintaining an optimal speed and acceleration profile throughout the TOSCo range is fully dependent on the proper operation of the TOSCo control system and its interfaces. Communication between the vehicle string and the infrastructure is key to proper operation of the TOSCo feature as well. Functional Safety operation would include maintaining a safe nominal path, monitoring and detection of faults, and mitigating hazards and failures to go to a safe vehicle state.

This requires safety relevant activities to be performed and described to show evidence for achievement of functional safety. For Phase 1 “Hazard Analysis” of the TOSCo feature, a step-by-step framework was developed with respect to ISO 26262. The work products developed focuses on the concept phase for automotive applications and includes:

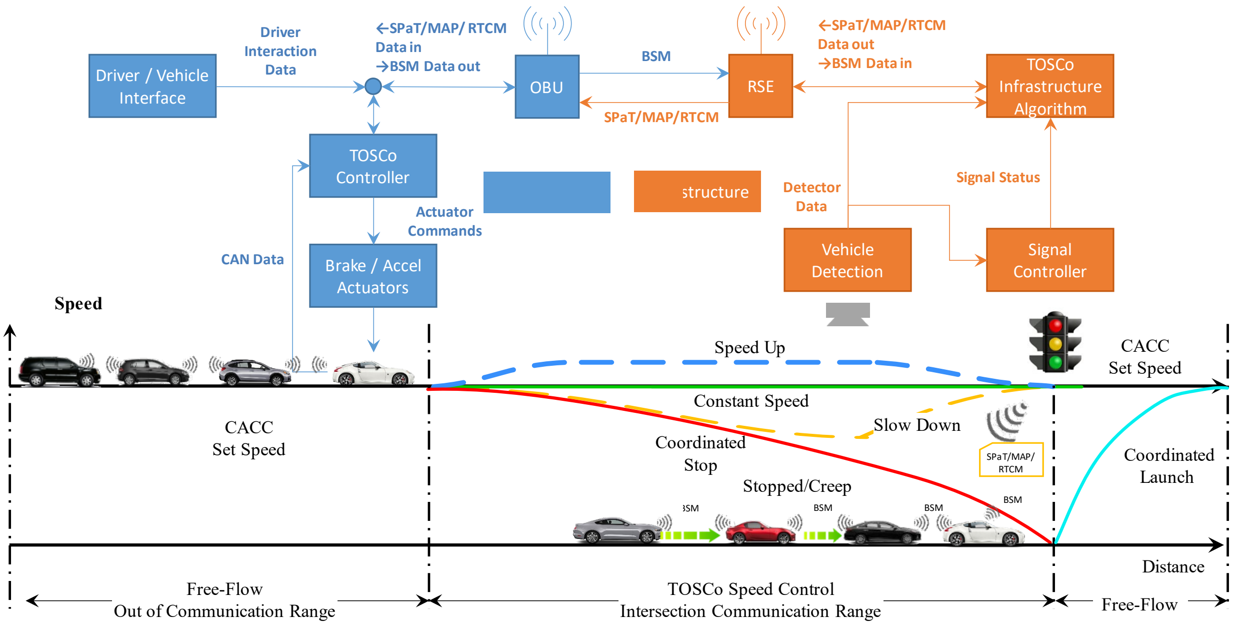
- Item definition (identify the TOSCo boundary and its intended features and functions)
- Hazard Analysis and Risk Assessment (HARA) (determination of safety goals and Automotive Safety Integrity Levels (ASILs)
- Functional safety concept (provide requirements for functional safety management, design and implementation)

This document shall provide a summary and findings of the above work products, which is intended to cover the concept phase of product development. The scope of this analysis will not cover product design and integration. However, the framework shall include recommendations and requirements to integrate functional safety activities into a company-specific development framework. The functional requirements shall focus on technical implementation into specific TOSCo components at a system level which can be utilized for subsequent integration and implementation. This entire development process shall follow the guidelines of ISO 26262.

2 TOSCo System Architecture

2.1 TOSCo System Architecture Overview

The figure below is a high-level illustration of the overall TOSCo system architecture derived from the TOSCo Vehicle System Specification.



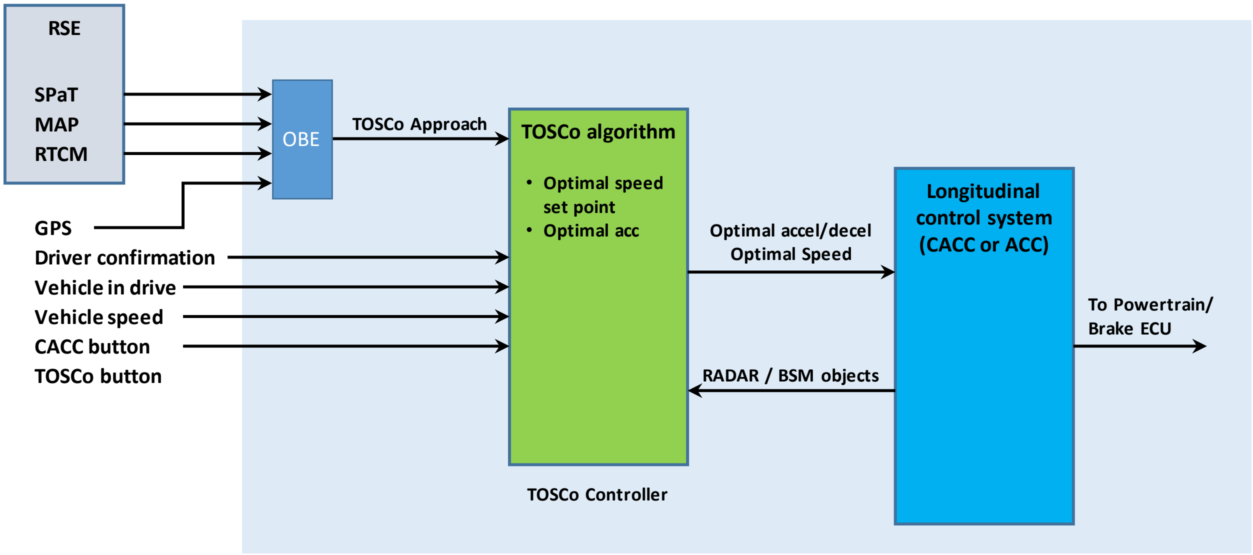
Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Figure 1: TOSCo System Architecture

The TOSCo feature uses a combination of infrastructure- and vehicle-based components and algorithms along with wireless data communications to position the equipped vehicle to arrive during the “green window” at specially designated signalized intersections. The vehicle side of the system (blue boxes) uses applications located in a vehicle to collect Signal Phase and Timing (SPaT), and MAP messages defined in SAE standard J2735 using Vehicle-to-Infrastructure (V2I) communications and data from nearby vehicles using Vehicle-to-Vehicle (V2V) communications. TOSCo also uses information broadcast in the SPaT, used to convey information about the “green window” to individual vehicles. The “green window”, computed by the infrastructure, is based on the estimated time that a queue will clear the intersection during the green interval. Upon receiving these messages, the individual vehicles perform calculations to determine a speed trajectory that is likely to either pass through the upcoming traffic signal on a green light, or to decelerate to a stop in an eco-friendly manner. This onboard speed trajectory plan is then sent to the onboard longitudinal vehicle control capabilities in the host vehicle to support partial automation. This vehicle control leverages previous work to develop Cooperative Adaptive Cruise Control (CACC) algorithms.

2.2 TOSCo Operating Modes and Boundary Diagram

Seven operating modes are defined under TOSCo. TOSCo is dependent upon CACC for vehicle control as shown in the figure below.



Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Figure 2: Preliminary Block Diagram of TOSCo Covered Under Functional Safety

The operating modes are defined as below. Each operating mode is identified to be safety critical, and safety requirements for accurate transition from each mode have been identified in the Functional Safety Concept.

Free Flow

If a TOSCo-equipped Host Vehicle (HV) is currently not receiving SPaT and MAP messages while the TOSCo feature is active, the equipped vehicles operate in speed/gap control under CACC. HV speed range in Free Flow is from zero to CACC Set Speed. Free Flow can also be considered as a safe state for TOSCo.

Coordinated Speed Control

A TOSCo-equipped Lead Vehicle (LV) enters this strategy when TOSCo is active, the LV is receiving SPaT and MAP messages from the nearest signalized intersection in the LV's path and there are no preceding vehicles in the path of the LV.

Coordinated Stop

The TOSCo-equipped LV enters this strategy when TOSCo is active and receiving SPaT and MAP messages from the intersection in the vehicle's path. LV speed range in Coordinated Stop mode is from a maximum allowed TOSCo speed range to a final speed of zero. If the LV determines that it will not pass the intersection, it plans a speed profile to come to a stop at the stop bar or end of a queue.

Stopped

The TOSCo-equipped vehicle is stationary at the stop bar or in a queue. Vehicle speed range in Stopped mode is zero. The vehicle can move out of Stopped Mode only through driver action and provided all parameters to transition out of Stopped are met.

Creep

The TOSCo-equipped vehicle is allowed to creep forward with a defined limiting speed toward the stop bar to fill gaps left by vehicles that departed the lane during the red phase. Under these circumstances, the TOSCo-equipped vehicle would move forward to fill the gap created by the departing vehicle(s) but only after the driver acknowledges a prompt indicating it is possible to move forward in the queue.

Coordinated Launch

The TOSCo-equipped vehicle broadcasts a coordinated launch message as it launches upon the signal transition to the green phase but only after the driver acknowledges a prompt indicating the vehicle is prepared to launch.

Optimized Follow

Under Optimized Follow, a TOSCo-equipped vehicle operates predominately as a member of a string under CACC speed and gap control. The TOSCo-equipped vehicle also continually receives SPaT and MAP messages to calculate its optimized speed profile which could cause it to leave the string and become the TOSCo-equipped LV in a new string if the vehicle determines that remaining in the string will cause it to operate outside its range of optimized control.

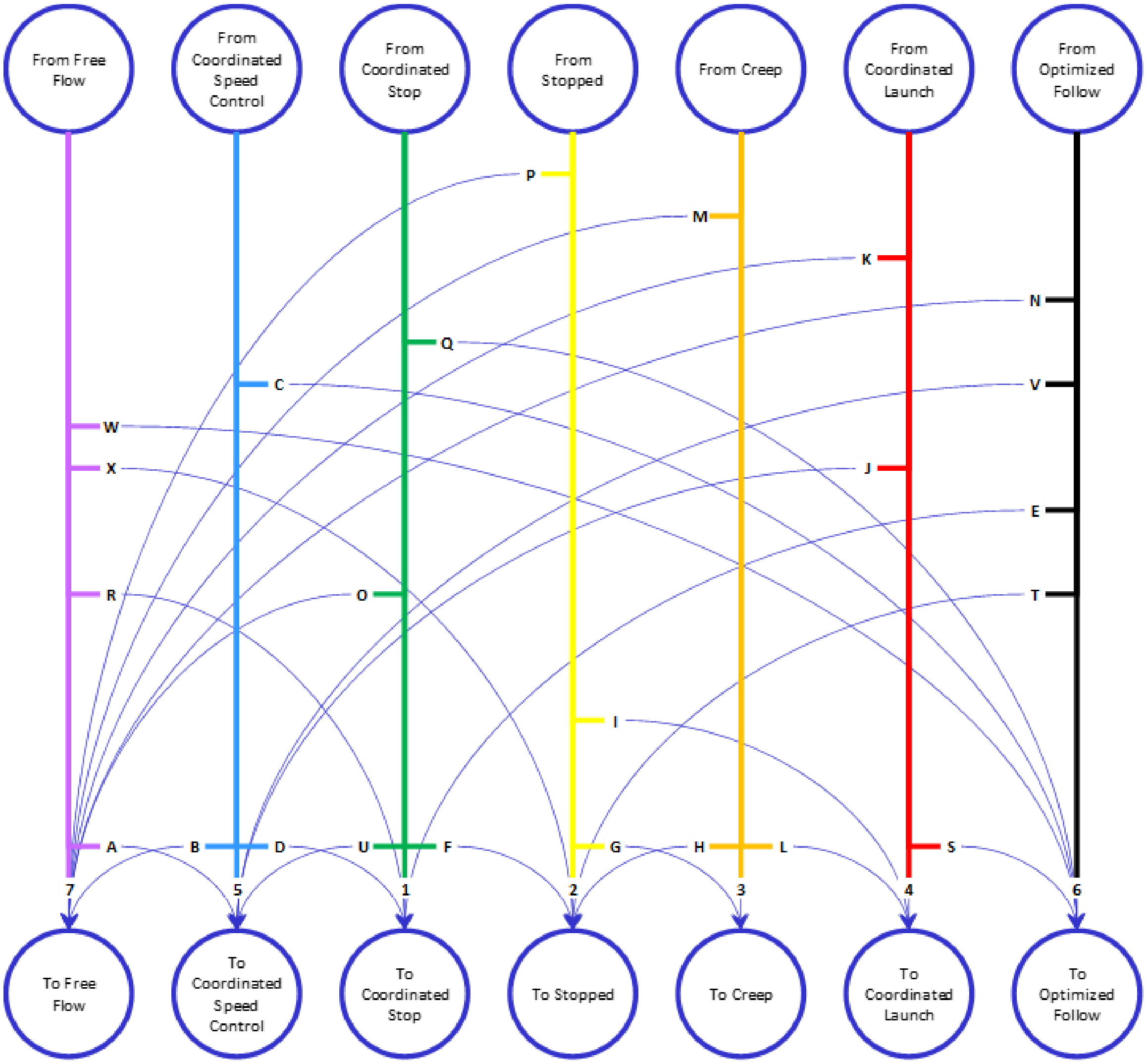
2.3 TOSCo Transitions

The numbers and capital letters in Table 1 below indicate transitions that are allowable while the lower-case Greek letters indicate transitions that are not allowed. Figure 3 below illustrates all allowable TOSCo transitions. This is as per the TOSCo Vehicle System Specification. Each transition from one mode to the other (including not allowed transitions) was analyzed with respect to functional safety. Functional Safety Requirements were developed based on potential safety critical transitions including defining all preconditions and scenarios to achieve a safe transition. Refer to Functional Safety Concept section for a detailed summary.

Table 1: TOSCo Operating Modes Matrix

		Current Mode						
		CStop	**Stopped**	**Creep**	**CLaunch**	**CSC**	**Opt Follow**	**Free Flow**
Previous Mode	CStop	**1**	**F**	ζ	λ	**U**	**Q**	**O**
	Stopped	α	**2**	**G**	**I**	o	ρ	**P**
	Creep	β	**H**	**3**	**L**	π	σ	**M**
	CLaunch	γ	δ	η	**4**	**J**	**S**	**K**
	CSC	**D**	ε	θ	μ	**5**	**C**	**B**
	Opt Follow	**E**	**T**	ι	ν	**V**	**6**	**N**
	Free Flow	**R**	**X**	κ	ξ	**A**	**W**	**7**

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium



Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Figure 3: Allowable TOSCo Transitions

The following sections describe transitions between the TOSCo operating modes that are allowed and the TOSCo operating modes that are not allowed.

2.3.1 Allowed TOSCo Transitions

Table 2 below identifies allowable transitions between TOSCo operating modes.

Table 2: Allowable TOSCo Transitions

Transition	Operating Mode Before Transition	Operating Mode After Transition
A	Free Flow	Coordinated Speed Control
B	Coordinated Speed Control	Free Flow
C	Coordinated Speed Control	Optimized Follow

Transition	Operating Mode Before Transition	Operating Mode After Transition
D	Coordinated Speed Control	Coordinated Stop
E	Optimized Follow	Coordinated Stop
F	Coordinated Stop	Stopped
G	Stopped	Creep
H	Creep	Stopped
I	Stopped	Coordinated Launch
J	Coordinated Launch	Coordinated Speed Control
K	Coordinated Launch	Free Flow
L	Creep	Coordinated Launch
M	Creep	Free Flow
N	Optimized Follow	Free Flow
O	Coordinated Stop	Free Flow
P	Stopped	Free Flow
Q	Coordinated Stop	Optimized Follow
R	Free Flow	Coordinated Stop
S	Coordinated Launch	Optimized Follow
T	Optimized Follow	Stopped
U	Coordinated Stop	Coordinated Speed Control
V	Optimized Follow	Coordinated Speed Control
W	Free Flow	Optimized Follow
X	Free Flow	Stopped
1	Coordinated Stop	Coordinated Stop
2	Stopped	Stopped
3	Creep	Creep
4	Coordinated Launch	Coordinated Launch
5	Coordinated Speed Control	Coordinated Speed Control
6	Optimized Follow	Optimized Follow
7	Free Flow	Free Flow

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

2.3.2 TOSCo Transitions Not Allowed

Table 3 below lists the transitions that are not allowed.

Table 3: TOSCo Transitions Not Allowed

Transition	Operating Mode Before Transition	Operating Mode After Transition
α	Stopped	Coordinated Stop
β	Creep	Coordinated Stop
γ	Coordinated Launch	Coordinated Stop
δ	Coordinated Launch	Stopped
ε	Coordinated Speed Control	Stopped
ζ	Coordinated Stop	Creep
η	Coordinated Launch	Creep

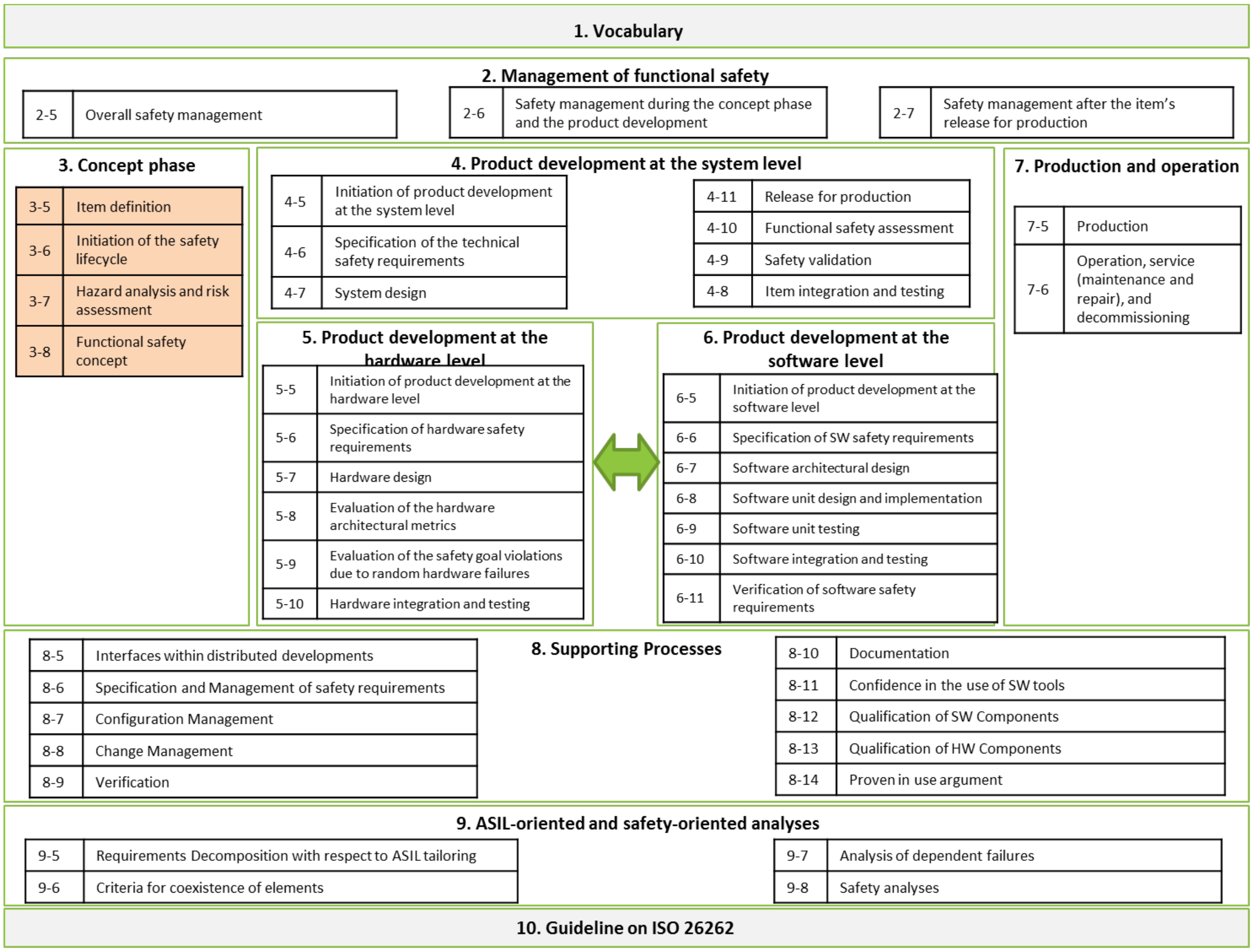
Transition	Operating Mode Before Transition	Operating Mode After Transition
θ	Coordinated Speed Control	Creep
ι	Optimized Follow	Creep
κ	Free Flow	Creep
λ	Coordinated Stop	Coordinated Launch
μ	Coordinated Speed Control	Coordinated Launch
ν	Optimized Follow	Coordinated Launch
ξ	Free Flow	Coordinated Launch
o	Stopped	Coordinated Speed Control
π	Creep	Coordinated Speed Control
ρ	Stopped	Optimized Follow
σ	Creep	Optimized Follow

3 ISO 26262 Process Development

This section provides an explanation of the overall structure of the ISO 26262 standard and the portions relevant to the scope of this project.

3.1 Safety Lifecycle Process

Figure 4 below provides the V-model for the different phases of product development and the work products required for implementation of functional safety throughout the development process.



1. Vocabulary

2. Management of functional safety

2-5	Overall safety management
2-6	Safety management during the concept phase and the product development
2-7	Safety management after the item's release for production

3. Concept phase

3-5	Item definition
3-6	Initiation of the safety lifecycle
3-7	Hazard analysis and risk assessment
3-8	Functional safety concept

4. Product development at the system level

4-5	Initiation of product development at the system level
4-6	Specification of the technical safety requirements
4-7	System design
4-11	Release for production
4-10	Functional safety assessment
4-9	Safety validation
4-8	Item integration and testing

7. Production and operation

7-5	Production
7-6	Operation, service (maintenance and repair), and decommissioning

5. Product development at the hardware level

5-5	Initiation of product development at the hardware level
5-6	Specification of hardware safety requirements
5-7	Hardware design
5-8	Evaluation of the hardware architectural metrics
5-9	Evaluation of the safety goal violations due to random hardware failures
5-10	Hardware integration and testing

6. Product development at the software level

6-5	Initiation of product development at the software level
6-6	Specification of SW safety requirements
6-7	Software architectural design
6-8	Software unit design and implementation
6-9	Software unit testing
6-10	Software integration and testing
6-11	Verification of software safety requirements

8. Supporting Processes

8-5	Interfaces within distributed developments
8-6	Specification and Management of safety requirements
8-7	Configuration Management
8-8	Change Management
8-9	Verification
8-10	Documentation
8-11	Confidence in the use of SW tools
8-12	Qualification of SW Components
8-13	Qualification of HW Components
8-14	Proven in use argument

9. ASIL-oriented and safety-oriented analyses

9-5	Requirements Decomposition with respect to ASIL tailoring
9-6	Criteria for coexistence of elements
9-7	Analysis of dependent failures
9-8	Safety analyses

10. Guideline on ISO 26262

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Figure 4: Overview of ISO 26262

The achievement of functional safety is influenced by the development and management process that includes an organization structure for management of functional safety, specification of requirements, design and implementation at various levels of development, integration of all systems and components of the product, and, finally, verification and validation. The V-model is closely linked with the common functional and operational activities for product development. For Phase 1 of the TOSCo Feature development, the focus of safety development was only on the Concept Phase. All work products mentioned under that section were considered and defined as per the requirements and recommendations of the standard.

3.2 Safety Processes for TOSCo

The following work products were created to meet the initial functional safety requirements of the TOSCo feature as per ISO 26262.

- Item Definition
- HARA
- Functional Safety Concept

The role and contribution of each of these work products are described in the lower sections. The Concept Phase (Part 3) of the standard also follows the V -model, hence each work product has to be performed in the order it is described.

For preparation of each work product, safety meetings and workshops were conducted with relevant CAMP participants and all information was documented. Multiple drafts of these safety documents were created for review and reference. Based on feedback and references from TOSCo System Specification and TOSCo System Architecture, the safety relevant work products were updated and subsequently released. A re-iterative process was followed for development of each work product, which allowed for changes to be incorporated in a previously created work product based on findings from the next subsequent phase.

4 Item Definition Process

As per ISO 26262, an item is a system or group of systems, to which functional safety processes are applied and that implements a function at a vehicle level. An implemented function influences the behavior of the vehicle that is observable to the user. In this project, the TOSCo Feature is considered as an item that is capable of implementing multiple vehicle functions.

The purpose of the Item Definition is to define and describe the item, its dependencies on, and interaction with, the environment and other items. Also, it is developed to provide an adequate understanding of the item so that the activities in subsequent safety lifecycle phases can be performed.

The HARA is carried out on the basis of the Item Definition, and the Functional Safety Concept is derived from the definition.

4.1 Item Boundary

Figure 2 specifies the boundary of the Item and its interaction with other components. The known system or item architecture (preliminary architecture), components, and interactions are shown at a high level. These provide a list of all elements, systems and interfaces within the boundary of the item. A brief high-level description of the elements and their scope for this item is provided below.

Roadside Equipment (RSE) : Infrastructure Device that allows the TOSCo Roadside Processor to communicate to TOSCo-enabled vehicles. The RSE manages all the communications between the infrastructure and equipped vehicles, including SPaT and MAP messages, containing TOSCo information elements. The RSE also contains the MAP artifact, which is the digital description of the intersection geometry and associated traffic control definitions.

On-board Equipment (OBE): The OBE establishes the operating environment ahead of the vehicle by receiving and using the respective decoders to decode SPaT and MAP and Global Positioning System (GPS) data from the Infrastructure. The OBE shall be used to determine the TOSCo approach.

TOSCo Algorithm (Intersection Longitudinal Controller): The TOSCo algorithm is part of the intersection longitudinal control and consists of the Operating Mode Selection, which is the strategy to transition between the TOSCo operating modes and provides an acceleration command based on appropriate speed control. The TOSCo algorithm shall receive multiple inputs from various sources (such as vehicle speed, driver confirmation, enabling/disabling of the CACC and TOSCo feature) to determine the appropriate strategy of operation of the TOSCo feature.

Longitudinal Controller: The Longitudinal Controller is under CACC or Adaptive Cruise Control (ACC) Gap control and provides an acceleration command based on Distance Calculation within the vehicle string.

4.2 Functions of the Item

The TOSCo feature is comprised of two functions: an infrastructure-side function and a vehicle-side function that cooperate with one another to implement a safe and controlled driving behavior of a vehicle string through a signalized corridor.

Below is the list of functions of the TOSCo Feature. These functions were utilized for identifying malfunctions and hazards at a vehicle level.

Table 4: Primary Functions of TOSCo

ID	NAME	DESCRIPTION
001	Acquire target remote vehicle(s)	Acquire a target vehicle to follow
002	Provide vehicle acceleration command	Provide the desired acceleration to the powertrain system
003	Provide vehicle deceleration command	Provide the desired deceleration to the brake system
004	Send/Receive communication from vehicle(s)	Send and receive BSM messages from other equipped vehicles in the vicinity
005	Receive communication from infrastructure (SPaT, MAP, Queue length)	Receive information from roadside equipment with respect to signal phase and timing, map and current queue length.
006	Provide driver take-over request/ warning	Request the driver to takeover longitudinal control
007	Allow driver take-over	Allow the driver to take over longitudinal control
008	Determine the Intersection approach/departure	Determine based on MAP and GPS information the geometry of the intersections and the relative position of the vehicle at the intersection
009	Determine the queue at the intersection	Determine the presence, length and activity of the queue at the intersection

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

4.3 Assumptions of Behavior of the Item

Some assumptions on how the performance, functionality and operation of the TOSCo item is influenced based on vehicle operating modes, weather and climate and environmental conditions are listed here. These assumptions have been considered for developing the HARA.

a) TOSCo works with only a level 1 longitudinal control system like CACC. It does not work when in ACC mode alone. In other words the driver is alert and ready to take control.

b) TOSCo works only with a CACC-equipped system. Maintaining sufficient distance gap is always the responsibility of CACC. Hence, CACC can act as a secondary safety measure to mitigate a failure of speed control from TOSCo.

c) TOSCo is intended for operation along appropriately equipped signalized arterials with posted speed limits of between 35 and 60 mph.

d) TOSCo functionality and safety concept are to be built assuming CACC is capable of safe operation (for which a safety analysis has already been accomplished).

e) Current TOSCo feature does not support lateral control. Scenarios for hazard evaluation are considered accordingly.

f) TOSCo needs to be individually activated by the driver and the driver is responsible for doing this. In other words, TOSCo will not be active unless driver exclusively activates it.

g) The analysis is focused on the host vehicle which is within communication range of a TOSCo-equipped intersection. All vehicles in the same vehicle string and the surrounding environment are also subject to the safety analysis.

h) The arbitration of control between the driver and the CACC system is performed by vehicle controllers such as the brake controller and/or engine controller as in a traditional ACC-equipped vehicle. Therefore, brake commands from the driver have priority over commands received from the CACC system.

5 Hazard Analysis Development Process

The purpose of the HARA is to identify and to categorize the potential vehicle-level hazards due to a malfunctioning behavior of the item and to formulate the safety goals related to the prevention or mitigation of the hazardous events in order to avoid unreasonable risk.

For this, the item is evaluated with regard to its potential hazardous events. Safety goals and their assigned ASIL are determined by a systematic evaluation of hazardous events. The ASIL is determined by considering the estimate of the impact factors, i.e., severity, probability of exposure and controllability.

The tasks comprising a HARA are:

- Situation analysis and hazard identification
- Classification of hazardous events (determination of severity, probability of exposure and controllability ratings)
- Determination of ASIL and related safety goals

The scope of this HARA is limited to the TOSCo feature.

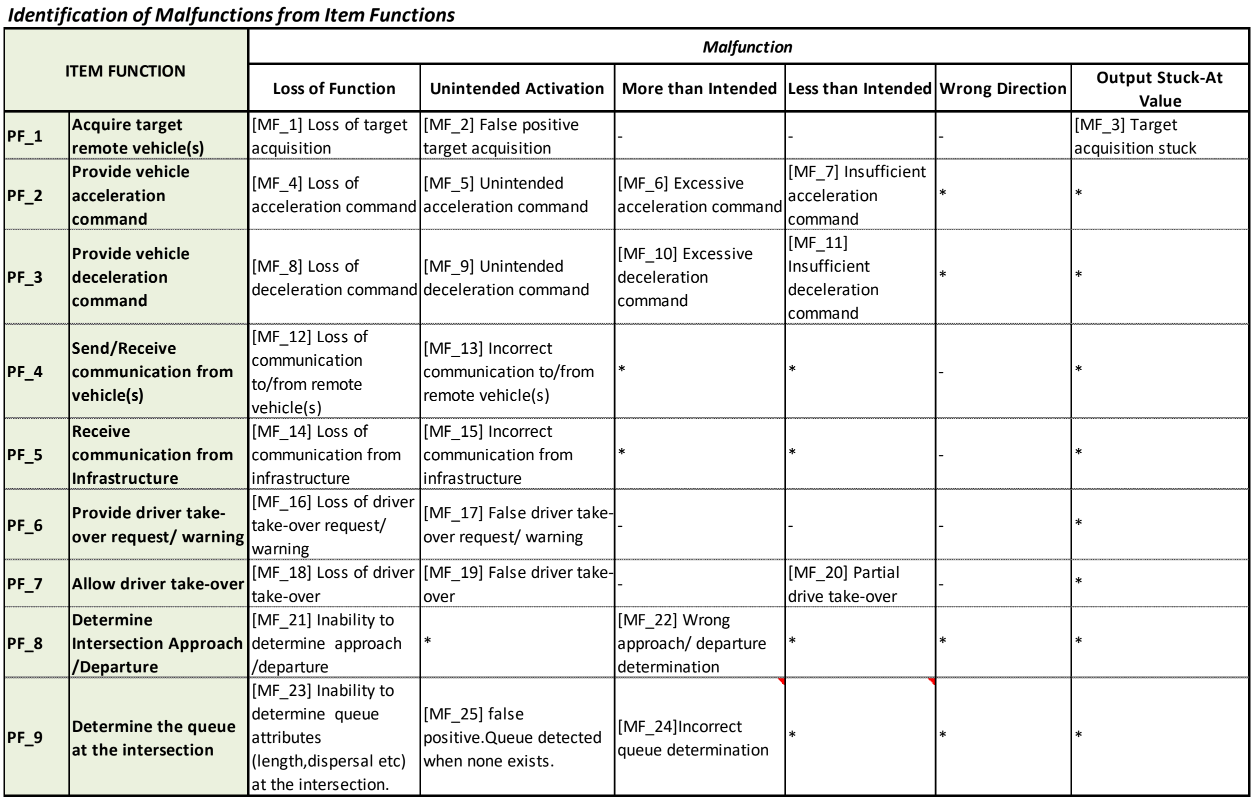
NOTE: This HARA (and its results) is only meant for research purposes. It is not intended, as is, to drive development of a TOSCo feature (or similar) in any series production vehicles in the present or in the future.

5.1 Hazard Analysis Operability (HAZOP) Study and Identification of Hazards

The primary functions from the item definition for the TOSCo feature and the initial estimate of the malfunctions and hazards from item definition are utilized to initiate a Hazard Analysis Operability (HAZOP) Study. The HAZOP is an explorative type of analysis where applicable guidewords are applied to each of the functions of an item to postulate malfunctioning behaviors.

Shown below in Table 5 is the HAZOP Study performed for the TOSCo feature. Here a matrix is created between the primary functions of the TOSCo feature (identified from the Item definition) and a probable list of guidewords, which are then utilized to identify potential malfunctions of the system. The malfunctions and failure modes identified from the Item definition could also be used to populate the table.

Table 5: HAZOP Study for TOSCo



Identification of Malfunctions from Item Functions

ITEM FUNCTION		Malfunction					
		Loss of Function	**Unintended Activation**	**More than Intended**	**Less than Intended**	**Wrong Direction**	**Output Stuck-At Value**
PF_1	**Acquire target remote vehicle(s)**	[MF_1] Loss of target acquisition	[MF_2] False positive target acquisition	-	-	-	[MF_3] Target acquisition stuck
PF_2	**Provide vehicle acceleration command**	[MF_4] Loss of acceleration command	[MF_5] Unintended acceleration command	[MF_6] Excessive acceleration command	[MF_7] Insufficient acceleration command	*	*
PF_3	**Provide vehicle deceleration command**	[MF_8] Loss of deceleration command	[MF_9] Unintended deceleration command	[MF_10] Excessive deceleration command	[MF_11] Insufficient deceleration command	*	*
PF_4	**Send/Receive communication from vehicle(s)**	[MF_12] Loss of communication to/from remote vehicle(s)	[MF_13] Incorrect communication to/from remote vehicle(s)	*	*	-	*
PF_5	**Receive communication from Infrastructure**	[MF_14] Loss of communication from infrastructure	[MF_15] Incorrect communication from infrastructure	*	*	-	*
PF_6	**Provide driver take-over request/ warning**	[MF_16] Loss of driver take-over request/ warning	[MF_17] False driver take-over request/ warning	-	-	-	*
PF_7	**Allow driver take-over**	[MF_18] Loss of driver take-over	[MF_19] False driver take-over	-	[MF_20] Partial drive take-over	-	*
PF_8	**Determine Intersection Approach /Departure**	[MF_21] Inability to determine approach /departure	*	[MF_22] Wrong approach/ departure determination	*	*	*
PF_9	**Determine the queue at the intersection**	[MF_23] Inability to determine queue attributes (length,dispersal etc) at the intersection.	[MF_25] false positive.Queue detected when none exists.	[MF_24]Incorrect queue determination	*	*	*

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

It is recommended to revisit the HARA process during the next phase of TOSCo development. Considering identification of different vehicle operating scenarios and change in life cycle phases, it may be possible that new functions may arise leading to additional potential malfunctions and their associated vehicle hazards.

The malfunctioning behaviors identified for the vehicle functions in Figure 5 are mapped to vehicle hazards in Figure 6. The mapping varies with the driving situations considered for the various malfunctioning behaviors

Table 6: Identification of Hazards from Malfunctions

ITEM FUNCTION	Malfunctions	Malfunction Note	Hazard
Acquire Remote Vehicles	[MF_1] Loss of target	Remote vehicle target is lost/ missed	[H_1] Excessive Acceleration [H_2] Insufficient Deceleration
	[MF_2] False positive target acquisition	Remote vehicle target is acquired when there is none	[H_3] Excessive deceleration [H_4] Insufficient acceleration
	[MF_3] Target acquisition stuck	Target acquisition is stuck at 'missing' or 'false positive'	All hazards
Provide Acceleration Commands	[MF_4] Loss of acceleration command	Missing acceleration command, provided target acquisition and communication functions are working correctly	[H_4]

ITEM FUNCTION	Malfunctions	Malfunction Note	Hazard
	[MF_5] Unintended acceleration command	Unintended acceleration command, provided target acquisition and communication functions are working correctly	[H_1] and [H_4]
	[MF_6] Excessive acceleration command	Excessive acceleration command, provided target acquisition and communication functions are working correctly	[H_1]
	[MF_7] Insufficient acceleration command	Insufficient acceleration command, provided target acquisition and communication functions are working correctly	[H_4]
Provide Deceleration Commands	[MF_8] Loss of deceleration command	Missing deceleration command, provided target acquisition and communication functions are working correctly	[H_2]
	[MF_9] Unintended deceleration command	Unintended deceleration command, provided target acquisition and communication functions are working correctly	[H_2] and [H_3]
	[MF_10] Excessive deceleration command	Excessive deceleration command, provided target acquisition and communication functions are working correctly	[H_3]
	[MF_11] Insufficient deceleration command	Insufficient deceleration command, provided target acquisition and communication functions are working correctly	[H_2]
Communicate with other Remote Vehicles	[MF_12] Loss of Communication with remote vehicle(s)	Communication from remote leading vehicle is lost provided other functions are working correctly	[H_1] and [H_2]
	[MF_13] Incorrect Communication with remote vehicle(s)	Communication from remote leading vehicle is misleading/ corrupt provided other functions are working correctly	All hazards
Communicate with Infrastructure	[MF_14] Loss of communication with infrastructure	Communication from infrastructure is lost provided other functions are working correctly	All hazards
	[MF_15] Incorrect communication with remote vehicle(s)	Communication from infrastructure is misleading/ corrupt provided other functions are working correctly	All hazards
Prove Driver Take-over Request/ Warning	[MF_16] Loss of driver take-over request/ warning	System operating in an unsafe state without notifying the driver	All hazards
	[MF_17] False driver take-over request/ warning	System requests driver to take-over/ provides warning without an error	No hazard - Driver is asked to take over manual control when not required. This is inherently safe.
Provide Driver Take-Over	[MF_18] Loss of driver take-over	System is stuck in TOSCo, CACC, ACC or CC operating state without letting driver take-over	All hazards
	[MF_19] False driver take-over	System hands back control to the driver without warning/ driver take-over command	System falsely provides warning to the driver who then takes over controls - this is a reliability issue and not a safety issue

ITEM FUNCTION	Malfunctions	Malfunction Note	Hazard
	[MF_20] Partial driver take-over	System partially hands back control to driver i.e., acceleration or braking takeover is provided but not both. Partial take-over is considered equally hazardous as loss of take-over	All hazards
Determine the Intersection Approach/Departure	[MF_21] Inability to determine approach /departure	TOSCo cannot determine where it is relative to the geometry or timing of the intersection. This could result in the vehicle wrongly determining that it should cross the intersection when it should come to a stop or vice versa	All hazards
	[MF_22] Wrong approach /departure determination	TOSCo cannot determine where it is relative to the geometry or timing of the intersection. This could result in the vehicle wrongly determining that it should cross the intersection or come to a stop.	All hazards: - [H_1] Excessive Acceleration [H_2] Insufficient Deceleration [H_3] Excessive deceleration [H_4] Insufficient acceleration
Determine the Queue at the Intersection	[MF_23] Inability to determine queue attributes (length, dispersal etc.) at the intersection.	TOSCo is blind to the presence of a queue and a collision may become inevitable	[H_1] Excessive Acceleration
	[MF_24] Incorrect queue determination	TOSCo thinks the back of the queue is closer or farther than it actually is	All hazards: - [H_1] Excessive Acceleration [H_2] Insufficient Deceleration [H_3] Excessive deceleration [H_4] Insufficient acceleration

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

The following hazards were identified from the HAZOP study:

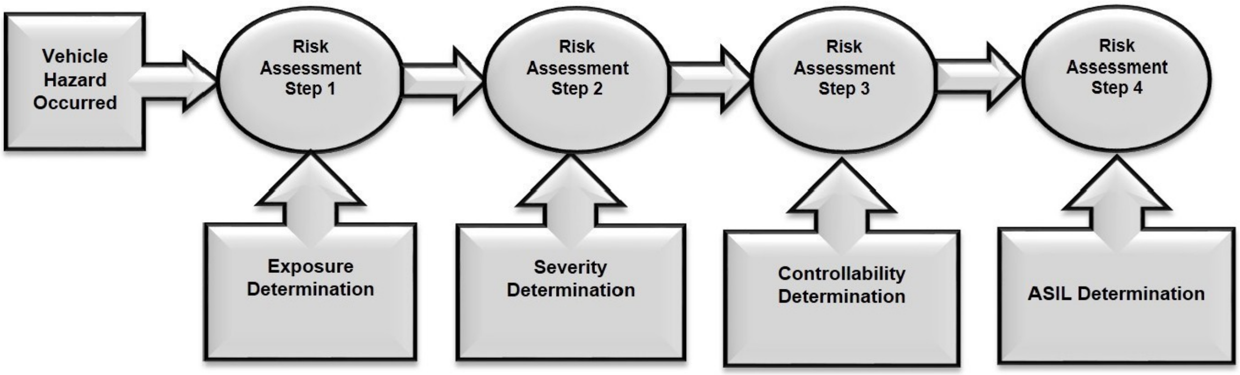
1. Excessive Acceleration
2. Insufficient Deceleration
3. Insufficient Acceleration
4. Excessive Deceleration

Now a HARA can be performed for each of these four unique hazards. This procedure is explained in the next step.

5.2 Risk Assessment of Hazardous Events

The HARA is an analysis procedure that identifies potential hazards, develops a set of specific hazardous events, and assesses the risk of each hazardous event to determine the ASIL and the safety goal. Based on Figure 5, a HARA would be performed for each of the 4 identified hazards.

Step 1: As a first step for identification of the list of hazardous events, all the safety critical TOSCo vehicle driving or operating scenarios need to be considered. For each such operating scenario, the likelihood of Exposure to that scenario is then determined. The method to determine the “Exposure Rating” and assignment of Exposure Rating to a vehicle operational situation is explained in APPENDIX A.

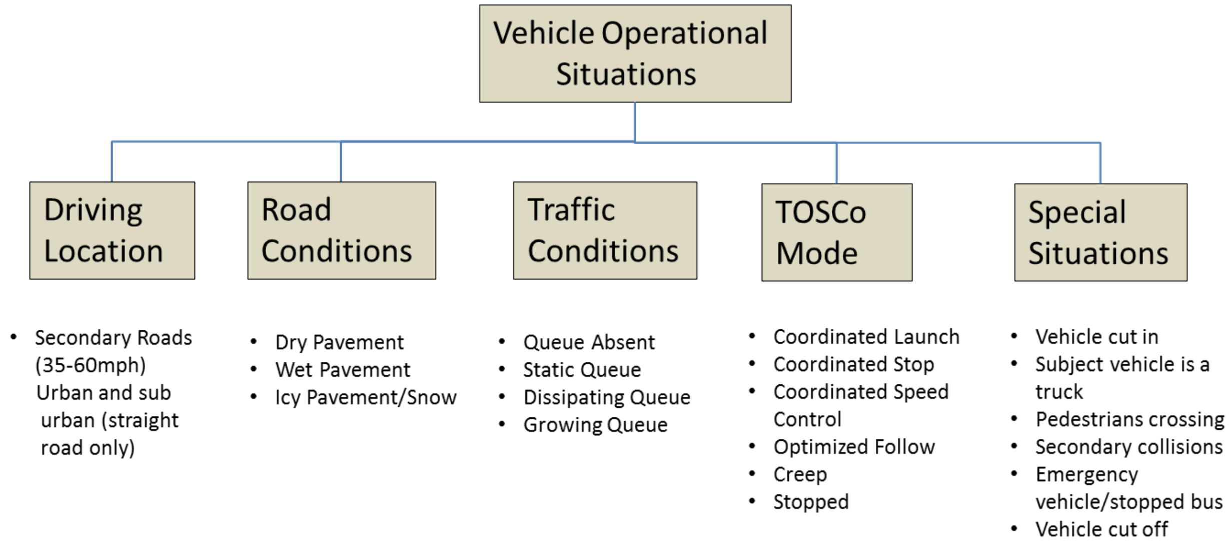


Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Figure 5: Overview of ISO 26262

Vehicle Situation Analysis

Figure 6 below shows a list of all vehicle situations that can be used to identify hazardous events for the TOSCo feature. These operating situations can be used to populate the HARA worksheet for analysis.



Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Figure 6: Potential Vehicle Operational Situations

Free Flow is not considered as a scenario as the vehicle would already be in Safe State or CACC Gap Control. Based on the operational scenarios a driving situation catalog can be derived which is common to all four different hazards. Table 7 shows a snapshot of the driving situation catalog along with its properties created for the TOSCo Project. An exhaustive list of potential hazardous events has been identified. For the TOSCo, a total of 54 different safety critical scenarios and events were identified.

Table 7: Example of Driving Situation Catalog for TOSCo

DRIVING SITUATION CATALOG					
Scenario				Exposure Probability	
Location	Road Conditions	Traffic Conditions	Vehicle Operation	Exposure Probability	E – note
Secondary Roads (35 mph < posted speed limit < 60 mph – urban and suburban)	Dry pavement	Queue absent	Coordinated Stop	E4	Based on a frequency-based approach, it is conservatively assumed that the TOSCo-equipped vehicle will be at a secondary road intersection at least once every driving cycle
Secondary Roads (35 mph < posted speed limit < 60 mph – urban and suburban)	Dry pavement	Queue absent	Coordinated Speed Control	E4	Based on a frequency-based approach, it is conservatively assumed that the TOSCo-equipped vehicle will be at a secondary road intersection at least once every driving cycle
Secondary Roads (35 mph < posted speed limit < 60 mph – urban and suburban)	Dry pavement	Queue absent	Coordinated Launch	E4	Based on a frequency-based approach, it is conservatively assumed that the TOSCo-equipped vehicle will be at a secondary road intersection at least once every driving cycle
Secondary Roads (35 mph < posted speed limit < 60 mph – urban and suburban)	Dry pavement	Static queue	Coordinated Stop	E4	Based on a frequency-based approach, it is conservatively assumed that the TOSCo-equipped vehicle will be at a secondary road intersection at least once every driving cycle
Secondary Roads (35 mph < posted speed limit < 60 mph - urban and sub-urban)	Wet pavement	Queue Absent	Coordinated Speed Control	E2	Based on a duration-based approach, immediate vehicle slowing down on a secondary road in wet conditions is <1% operating time
Secondary Roads (35 mph < posted speed limit < 60 mph – urban and suburban)	Dry pavement	Target vehicle left queue OR Dissipating Queue (other vehicles still in front)	Creep	E4	Highly likely that traffic signal will turn from red to green and vehicles ahead move out of the intersection

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

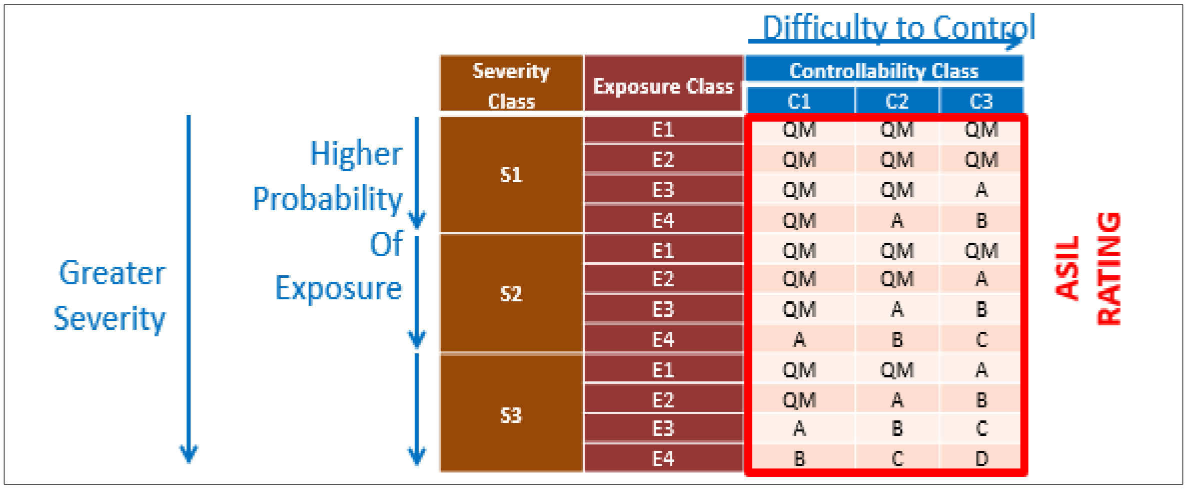
Step 2 and Step 3:

For each hazardous event based on the driving situation catalog, the Severity and the Controllability ratings are each assigned following the guidelines provided in APPENDIX A. For a given hazardous event, this procedure is repeated for reasonable and foreseeable operating scenarios of the vehicle containing the item.

The results of the risk assessment are dependent upon the item, the vehicle and the availability of data. The item functions, operating environment and vehicle characteristics will affect the specification of the resulting scenarios, as well as the class and rationale for the E, S, and C parameters. The analyst along with expert judgment needs to take these factors into account and create a thorough output with reasonable assumptions relevant to the system scope.

Step 4:

After all three ratings of "Severity," "probability of Exposure" and "Controllability" are identified, an ASIL is determined for each hazardous event utilizing these three parameters. The matrix shown in Figure 7 below defines the method to determine ASIL based on the ratings from each line item of the HARA.


Difficulty to Control
Greater Severity
Higher Probability Of Exposure
ASIL RATING

Severity Class	Exposure Class	Controllability Class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Figure 7: ASIL Determination

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

A HARA was performed for each hazard in a spreadsheet template for functional safety, after identification of the safety relevant scenarios and operational situations. The completed Hazardous event analysis was able to determine the “Severity,” “Exposure,” “Controllability” and the ASIL classification with appropriate rationale for each hazardous event. The highest ASIL identified from all hazardous events for each vehicle level hazard became the overall ASIL requirement for the particular hazard. The safety goals were identified based on the hazard analysis and is covered in Section 5.3.

Each of the 54 scenarios were evaluated as one-line item for a potential hazardous event and repeated for every other hazard. Here is an example of one hazardous event for Excessive Acceleration. The hazard event is separated into two sections “Scenario Evaluation” and “ASIL Identification.”

Table 8: Hazard Event Example for Excessive Acceleration “Scenario Evaluation”

Hazardous Event ID	Hazard	*SCENARIO*				
		Location	Road Conditions	Traffic Conditions at intersection	Vehicle Operation	Scenario Notes
HE_1_001	[H_1] Excessive Acceleration	Secondary Roads (35mph<V<60mph - urban and sub-urban)	Dry pavement	Queue Absent	Coordinated Stop	No vehicle in front

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Table 9: Hazard Event Example for Excessive Acceleration "ASIL Identification"

Exposure Probability		*Severity*		*Controllability*		ASIL
Exposure Probability	E - note	Severity	S - note	Controllability	C-Note	
E4	Based on a frequency-based approach, it is conservatively assumed that the TOSCo equipped vehicle will be at a secondary road intersection at least once every driving cycle	S3	Collision (side impact) is possible with cross traffic as this is a situation where a stop was being attempted. As this happens during a coordinated stop and cross traffic may already be present the delta V can be > 20 mph. Hence severe injuries possible and survival is questionable	C2	The driver of the host vehicle potentially has sufficient time to apply brakes and/or steering in the case of unintended acceleration. The driver is approaching an intersection and we are assuming this is the first vehicle at the stop bar as there is no queue. Most drivers should be able to reasonably estimate if the vehicle would be able to come to a stop at the stop bar or not. A controllability of C2 is assigned	C

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

5.3 Safety Goals and Safe States

After completion of the HARA, the output is a set of safety goals and safe states to ensure safe operation of the item. The highest ASIL identified from the hazardous events for each hazard becomes the ASIL allocated to that particular hazard. Safe states and related safety measures are specified in the functional safety concept, as appropriate, to achieve the safety goals in case of faults within the item. Each safety goal becomes the top-level safety requirement for all modules of the TOSCo Feature associated with the relevant hazard.

Table 10: Safety Goal and ASIL Determination

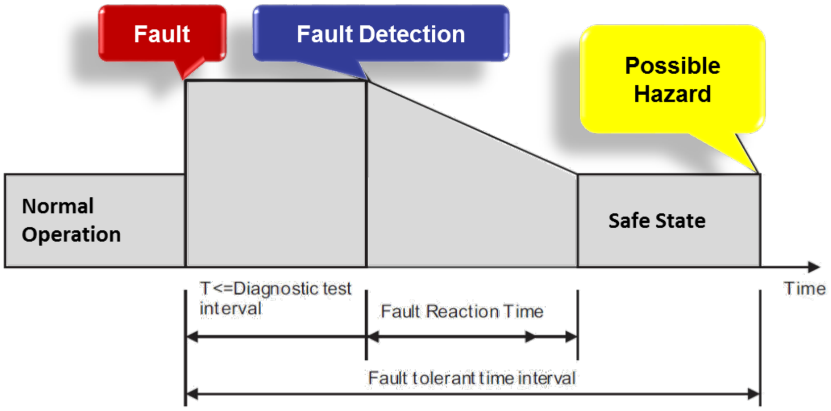
SAFETY GOAL ID	ASSOCIATED HAZARD	SAFETY GOAL TITLE	SAFE STATE	HIGHSEST ASIL	FTTI
SG01	Excessive Acceleration	Prevent Excessive Acceleration due to malfunctions in TOSCo	Disable TOSCo operation	C	400ms
SG02	Insufficient Deceleration	Prevent Insufficient Deceleration due to malfunctions in TOSCo	Disable TOSCo operation	C	400ms
SG03	Excessive Deceleration	Prevent Excessive Deceleration due to malfunctions in TOSCo	Disable TOSCo operation	B	200ms
SG04	Insufficient Acceleration	Prevent Insufficient Acceleration due to malfunctions in TOSCo	NA	QM	NA

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Quality Management (QM) and not safety relevant. No safety goal is written for 'QM' rated item-level hazards.

The ASIL rating for safety goals are assigned based on the maximum ASIL of the relevant item-level hazards.

Fault Tolerant Time Interval (FTTI) was defined for each safety goal which is the minimum time-span from the occurrence of a fault in an item to a possible occurrence of a hazardous event, in the absence of a safety mechanism. Based on FTTI assumed for the CACC Safety Analysis, a slightly relaxed value is considered due to lower vehicle speeds in TOSCo and minimum time gap being only 600ms.



Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

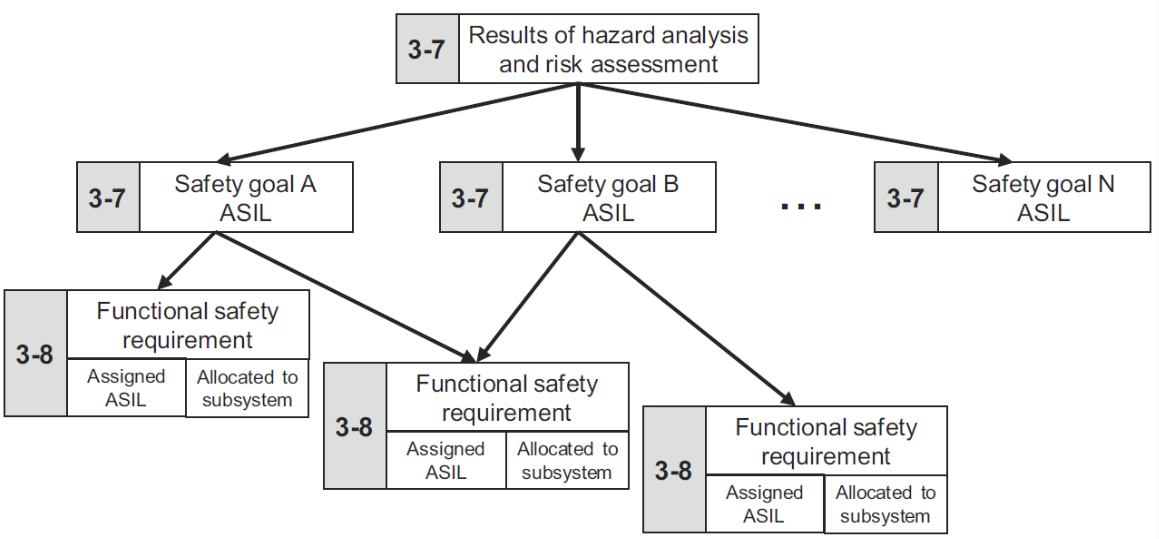
Figure 8: Fault Tolerant Time Interval

6 Functional Safety Concept

The purpose of the functional safety concept is to derive the functional safety requirements, from the safety goals, and to allocate them to the preliminary architectural elements of the item, or to external measures.

The functional safety concept addresses:

a) Fault detection and failure mitigation
b) Transitioning to a safe state
c) Fault tolerance mechanisms, where a fault does not lead directly to the violation of the safety goal(s) and which maintains the item in a safe state (with or without degradation)
d) Fault detection and driver warning in order to reduce the risk exposure time to an acceptable interval (e.g., engine malfunction indicator lamp, ABS fault warning lamp)
e) Arbitration logic to select the most appropriate control request from multiple requests generated simultaneously by different functions



Source ISO 26262: 2011- Part 3, Clause 7.2, Figure 2)

Figure 9: Hierarchy of Safety Goals and Functional Safety Requirements

6.1 Functional Safety Concept Overview

The TOSCo feature shall be able to detect faults both internal and external that could cause an incorrect longitudinal acceleration or deceleration. At the concept level, most of these requirements tend to be common across the 3 individual safety goals. The strategy is to identify single point fault and dual point faults that could cause the TOSCo feature to generate an incorrect longitudinal acceleration. Examples of external faults are data corruption of SPaT, MAP or incorrect vehicle speeds. Internal faults are pertinent to the controller on which the TOSCo feature is hosted. An example of a dual point fault that can cause the hazard are incorrect SPaT messages. An incorrect SPaT message itself may not result in the hazard but that along with an incorrect RADAR/fused object could result in the TOSCo feature not being able to detect the back of the queue. Hence the SPaT fault is referred to as a dual point fault as it can cause the hazard only with an independent fault in the system.

6.1.1 Safety Strategy

As part of the functional safety strategy for TOSCo, there is a need to be able to identify those inputs that can cause the TOSCo feature to cause the hazard (incorrect longitudinal acceleration). Such inputs include SPaT, MAP, RADAR or fused objects, BSM objects, GPS, vehicle speed, TOSCo activation button, driver confirmation and vehicle drivetrain status.

Incorrect SPaT & MAP Information:
The SPaT and MAP information is transmitted by the RSE. The OBE should communicate with the RSE with end to end protection. This shall ensure that faults like data corruption, data arriving in wrong order, loss of signal etc., are detected. Additionally, if the RSE detects faults internally, whereby it cannot provide a highly assured signal (accurate and correct), it should indicate the same with a flag. Additionally, the OBE should authenticate that it is receiving information from an authorized RSE and not from a malicious source. The SPaT and MAP information configured by human operators shall be assured by some process framework that can assure the integrity of the data.

Incorrect RADAR/Fused Objects:
The RADAR objects and/or fused objects can be provided by any external source. An incorrect object can result in a wrong determination of the back of the queue or just the distance to the preceding vehicle and thereby result in the hazard. The objects provided to the TOSCo feature from any external source (e.g., CACC) shall be at ASIL C integrity.

Incorrect BSM Objects:
An incorrect BSM object can affect TOSCo approach and Estimated Time of Arrival (ETA) at the intersection or back of queue. The external control source of the BSM (e.g., CACC) shall ensure that the objects provided to the TOSCo feature are of ASIL C integrity.

Incorrect GPS Signals:
The OBE is responsible for receiving GPS information. Poor quality or malicious information can result in incorrect TOSCo approach determination.

Incorrect Vehicle Speed:
An incorrect vehicle speed can result in the TOSCo feature calculating a higher or lower acceleration/deceleration than required. The vehicle speed may be received from a separate external vehicle module (such as the ABS). If the information is received from an external module like the ABS, the communication should be end-to-end protected (checksum, counters etc.) to be able to detect faults like data corruption, messages coming out of sequence etc.). The TOSCo feature shall use the information only after checking the integrity of the data received. In case the sending module cannot assure the information to ASIL C integrity, it shall indicate it with a flag.

Incorrect TOSCo Button Activation or Driver Confirmation:
If the TOSCo button is stuck ON (detection depends on the technology used), then TOSCo operation should not be permitted until repair. The same applies for the driver confirmation and would apply for all faults of that status.

Incorrect Vehicle Drive Train:
In case the vehicle drive train status cannot be judged by the CACC controller with high integrity, then TOSCo shall be disabled.

6.1.2 Functional Safety Requirements

Based on the above safety strategy and the requirements of the standard, functional safety requirements were derived for each of the safety critical modules of the TOSCo Feature. These safety requirements were allocated to the modules based on a preliminary architectural design. The requirements focus on a more generic approach to the capabilities of the TOSCo feature, such that the interfaces defined can be integrated with any TOSCo-enabled vehicle system. It will be up to the vehicle integrator to interpret the interfaces and utilize the capabilities of the vehicle system, external measures available and the safety requirements defined for TOSCo for actual implementation.

Note: For requirements where an explicit safe state may not be applicable, the corresponding cell in the table is left blank.

Table 11: Safety Requirements Assigned to the Infrastructure (RSE)

FSR ID	Requirement	Safe State
TOSCO_001	RSE shall always send the correct information (SPaT, MAP)	Broadcast no information Safe state shall be ensured by vehicle controller in case no RSE information is obtained
TOSCO_002	RSE shall be configured with the correct information by the human operator	Broadcast no information Safe state shall be ensured by vehicle controller in case no RSE information is obtained
TOSCO_003	RSE shall broadcast no information (SPaT, MAP) and set a non-availability flag when it cannot assure a correct signal (including during transitions from one pattern to another)	Disable TOSCo Transition to CACC (FREE FLOW) Safe state shall be ensured by vehicle controller in case no RSE information is obtained
TOSCO_004	OBE shall communicate with the RSE over an end to end protected channel	Disable TOSCo Transition to CACC (FREE FLOW) Safe state shall be ensured by vehicle controller in case no RSE information is obtained

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Table 12: Safety Requirements Assigned to the Rest of the Vehicle System to Support TOSCo

FSR ID	Requirement	Safe State
TOSCO_007	Correct vehicle speed shall be sent out to the TOSCO	Depends on vehicle design and behavior
TOSCO_008	Vehicle system shall set an invalidity flag if the vehicle speed cannot be assured to be correct	Depends on vehicle design and behavior
TOSCO_009	TOSCo feature shall communicate with the external vehicle system for vehicle speed over an end-to-end protected channel	Depends on vehicle design and behavior
TOSCO_016	Correct BSM objects to the TOSCo feature shall be sent out by the external vehicle controller	Depends on vehicle design and behavior
TOSCO_017	External vehicle controller shall indicate if the BSM objects are faulty	Disable TOSCo Transition to CACC (FREE FLOW)
TOSCO_018	External vehicle controller shall send the correct RADAR and Fused objects to the TOSCo feature	Depends on vehicle design and behavior
TOSCO_019	External vehicle controller shall indicate if the RADAR or Fused objects are faulty	Disable TOSCo Transition to CACC (FREE FLOW)

FSR ID	Requirement	Safe State
TOSCO_034	A central arbitration control system shall process the correct acceleration / deceleration values to be sent out from both the TOSCo and the CACC controller	Disable TOSCo and if required CACC operation

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Table 13: Safety Requirements Assigned to TOSCo Controller

FSR ID	Requirement	Safe State
TOSCO_010	TOSCo feature shall use the received vehicle speed information only if communication channel errors (data errors, out of order messages, time out, masquerading etc.) are absent	Disable TOSCo Transition to Manual mode (FREE FLOW)
TOSCO_011	TOSCo feature shall be able to detect faulty vehicle level inputs like vehicle transmission lever (PRNDL shifter) status (vehicle in DRIVE)	Disable TOSCo
TOSCO_012	TOSCo feature shall detect a TOSCo activation input that is STUCK ON	Disable TOSCo Transition to CACC (FREE FLOW)
TOSCO_013	TOSCo shall be able to verify the integrity of the "Driver Confirmation"	Disable TOSCo Transition to CACC (FREE FLOW)
TOSCO_031	TOSCo modes shall be allowed only when the driver has enabled both the CACC and TOSCo button	TOSCo disabled until driver confirmation
TOSCO_032	TOSCO controller shall ensure that the TOSCo Longitudinal Control algorithm converts the optimized speed setpoint to the correct acceleration/deceleration command	Disable TOSCo operation
TOSCO_036	"Creep" function shall be able to request an acceleration of not more than CREEP_MAX_ACC m/s2	Transition to STOPPED
TOSCO_037	Vehicle shall not be allowed to exceed maximum creep speed during CREEP mode (CREEP_MAX_SPD m/s)	Transition to STOPPED
TOSCO_038	TOSCo shall not allow vehicle movement beyond the stop line when in Coordinated Stop or Creeping mode	Maintain current STOPPED state
TOSCO_039	TOSCo shall cede control (transition to manual mode in CACC) on driver input (e.g., accelerator pedal, brake, gear in neutral etc.)	Disable TOSCo operation
TOSCO_040	TOSCo feature shall not request an acceleration as long as vehicle needs to remain in "STOPPED" mode	Maintain STOPPED mode
TOSCO_041	TOSCo feature shall not enter "Coordinated Launch" or "CREEP" without correct Driver confirmation	Disable TOSCo operation (Transition to FREE_FLOW)
TOSCO_042	"Safety monitor" shall be able to detect all internal single point faults that can cause an incorrect acceleration / deceleration (e.g., microcontroller faults like Random-Access Memory (RAM) corruption, Arithmetic Logic Unit (ALU) errors, peripheral faults, clock errors etc.)	Disable TOSCo operation
TOSCO_046	TOSCo controller shall ensure that the correct TOSCo vehicle speed setpoint is calculated during TOSCo operation	Transition to FREE_FLOW
TOSCO_047	TOSCo Mode selection shall allow exit from STOPPED mode only after a correct driver authorization is received	Maintain STOPPED condition
TOSCO_049	TOSCo controller shall ensure that the Intersection Longitudinal Controller calculates the correct brake command	Transition to FREE_FLOW

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Table 14: Safety Requirements Assigned to OBE

FSR ID	Requirement	Safe State
TOSCO_014	OBE shall be able to authenticate received GPS information	Disable TOSCo Transition to Manual mode (FREE FLOW)
TOSCO_015	OBE shall be able to detect poor GPS quality	Handover control to driver and warn the driver (only if in coordinated stop) Note: GPS critical only during coordinated stop
TOSCO_043	OBE shall detect all internal single point faults that can cause an incorrect TOSCo approach calculation (e.g., microcontroller faults like RAM corruption, ALU errors, peripheral faults etc.)	Disable TOSCo Transition to Manual mode (FREE FLOW)
TOSCO_044	OBE shall ensure that it sends the correct TOSCo approach at all times	Disable TOSCo Transition to Manual mode (FREE FLOW)

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Table 15: Safety Requirements Assigned to TOSCo Controller Based on Operating Mode Transitions

FSR ID	Requirement	Safe State
TOSCO_020	In case the TOSCo feature is unable to TRANSITION TO FREE FLOW (TOSCo disabled), if faults with Driver Confirmation information is detected, TOSCo shall still be able to warn the driver to take over	Provide Driver warning
TOSCO_021	TOSCo feature shall ensure TRANSITION TO FREE FLOW if unauthorized communication is detected	Transition to FREE FLOW and Provide Driver Warning Disable CACC operation (transition to Manual Mode) if cannot transition to FREE FLOW
TOSCO_022	TOSCo feature shall ensure TRANSITION TO FREE FLOW if incorrect information (SPaT, MAP) from the RSE is detected	Transition to FREE FLOW and Provide Driver Warning Disable CACC operation (transition to Manual Mode) if cannot transition to FREE FLOW
TOSCO_023	TOSCo feature shall ensure TRANSITION TO FREE FLOW if incorrect vehicle speed is detected	Transition to FREE FLOW and Provide Driver Warning Disable CACC operation (transition to Manual Mode) if cannot transition to FREE FLOW
TOSCO_024	TOSCo feature shall ensure TRANSITION TO FREE FLOW if faulty BSM object is detected	Transition to FREE FLOW and Provide Driver Warning Disable CACC operation (transition to Manual Mode) if cannot transition to FREE FLOW
TOSCO_025	TOSCo feature shall ensure TRANSITION TO FREE FLOW if poor GPS information is detected when in TOSCo COORDINATED STOP	Transition to FREE FLOW and Provide Driver Warning Disable CACC operation (transition to Manual Mode) if cannot transition to FREE FLOW
TOSCO_026	TOSCo feature shall ensure TRANSITION TO FREE FLOW if incorrect RADAR or Fused objects is detected	Transition to FREE FLOW and Provide Driver Warning Disable CACC operation (transition to Manual Mode) if cannot transition to FREE FLOW

FSR ID	Requirement	Safe State
TOSCO_027	TOSCo feature shall ensure TRANSITION TO FREE FLOW if vehicle gear lever is detected to be not in DRIVE OR if vehicle gear lever information is faulty	Transition to FREE FLOW and Provide Driver Warning Disable CACC operation (transition to Manual Mode) if cannot transition to FREE FLOW
TOSCO_028	TOSCo feature shall ensure the driver is warned whenever there is a TRANSITION TO FREE FLOW due to a detected fault	Transition to FREE FLOW and Provide Driver Warning Disable CACC operation (transition to Manual Mode) if cannot transition to FREE FLOW
TOSCO_029	TOSCo feature shall limit the maximum acceleration and deceleration requests to CACC to TOSCo_MAX_ACCEL or TOSCo_MAX_DECEL (e.g., +/-0.3*g)	Transition to FREE FLOW
TOSCO_030	TOSCo feature shall be disabled in case the vehicle speed goes above TOSCO_SPEED_LIMIT mph (e.g., 55 mph) inside the TOSCo range.	Transition to FREE FLOW
TOSCO_045	If a forbidden state transition is attempted, then TOSCo shall warn the driver and transition to FREE_FLOW	Transition to FREE FLOW and Provide Driver Warning Disable CACC operation (transition to Manual Mode) if cannot transition to FREE FLOW
TOSCO_048	Before entering CLAUNCH on a valid GREEN window, if a driver authorization is not received when in CREEP mode, the TOSCo controller shall transition to STOPPED within: a) Minimum stop distance if a preceding vehicle is present b) Minimum stop distance of stop bar if no preceding vehicle is present	Transition to FREE_FLOW
TOSCO_050	TOSCo controller shall allow transition to CREEP only when vehicle is stationary	Transition to STOPPED

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

6.1.3 Warning and Degradation Concept

Whenever the TOSCo controller detects a fault which does not allow normal TOSCo operation, it will transition to free flow and warn the driver through visual and audio aids. TOSCo operation will be disabled if the fault persists.

6.1.4 Actions of the Driver and Endangered Persons

The driver would need to be appropriately warned to take over control and maintain appropriate distance gaps with preceding vehicles.

6.1.5 Arbitration of Multiple Requestors

An independent arbitration control mechanism is responsible for arbitrating the correct acceleration / deceleration values from the Intersection longitudinal controller (TOSCo) and the CACC.

6.2 Fault Tree Analysis

Fault Tree Analysis (FTA) is a deductive (top-down) analysis used to:

- Systematically evaluate potential failures in a design or process
- Identify effects of failure modes, including safety-related effects
- Classify failures based on their effects and/or risks
- Calculate/estimate probabilities of safety-related events

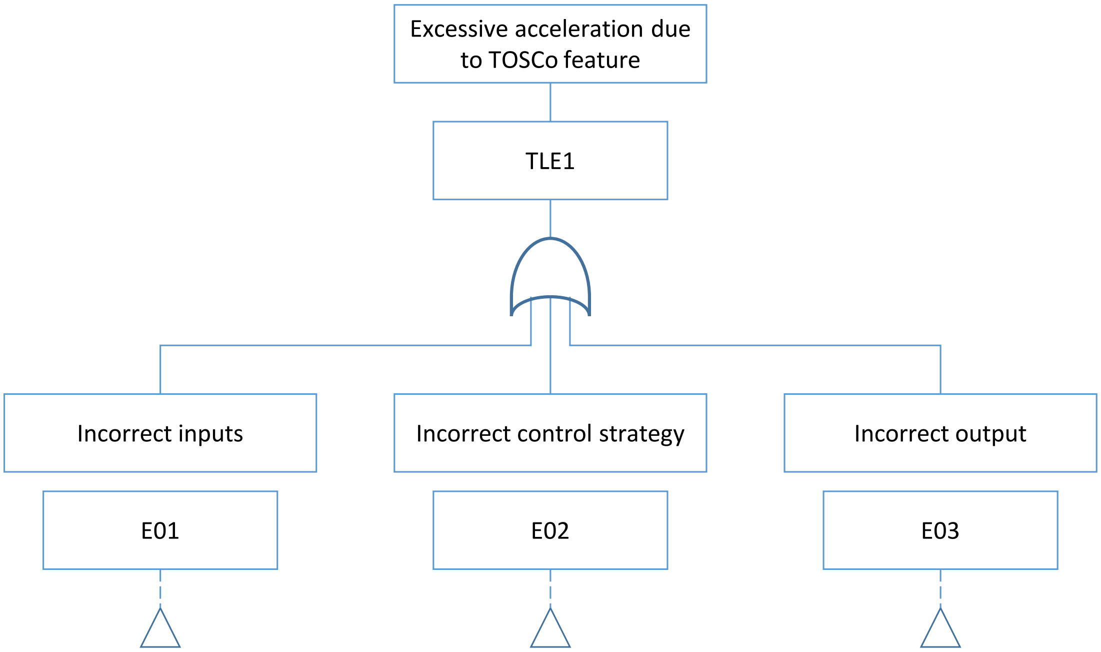
FTA is a logical combination of intermediate events and basic events, which can be assembled using AND / OR logical operators to analyze the effects of component faults on system failures. In safety, the FTA typically begins with a top-level event representing a major hazardous event, and/or the violation of a safety goal or Functional Safety Requirement, as defined in ISO 26262. Figure 10 illustrates excessive acceleration which is one of the four top-level TOSCo hazards identified earlier. The analysis is then performed by deducing what conditions or events would lead to the top-level event and in what logical combination. Excessive acceleration is broken down into the events and causes through a deductive analysis. The failure modes leading to the hazard are grouped by

a) Input Processing

b) Output Processing

c) Control Strategy

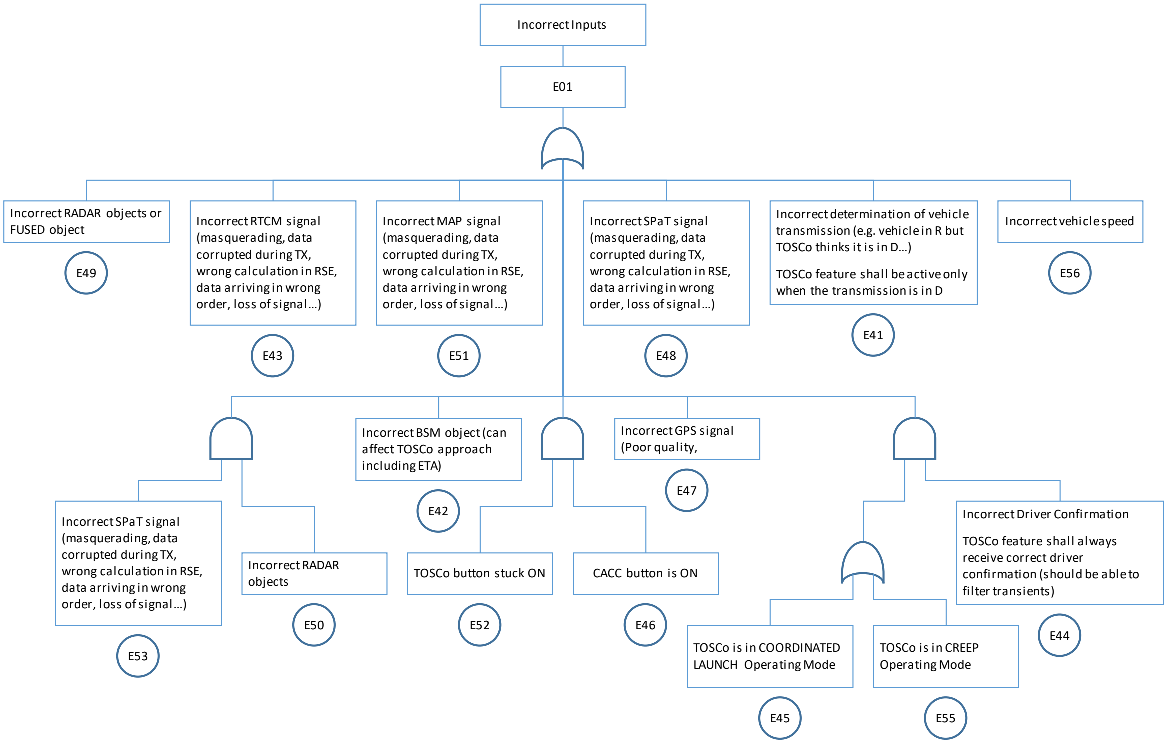
These failure modes are illustrated in Figure 11, Figure 12 and Figure 13.


Excessive acceleration due to TOSCo feature
TLE1
Incorrect inputs
Incorrect control strategy
Incorrect output
E01
E02
E03

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Figure 10: Excessive Acceleration Fault Tree Analysis

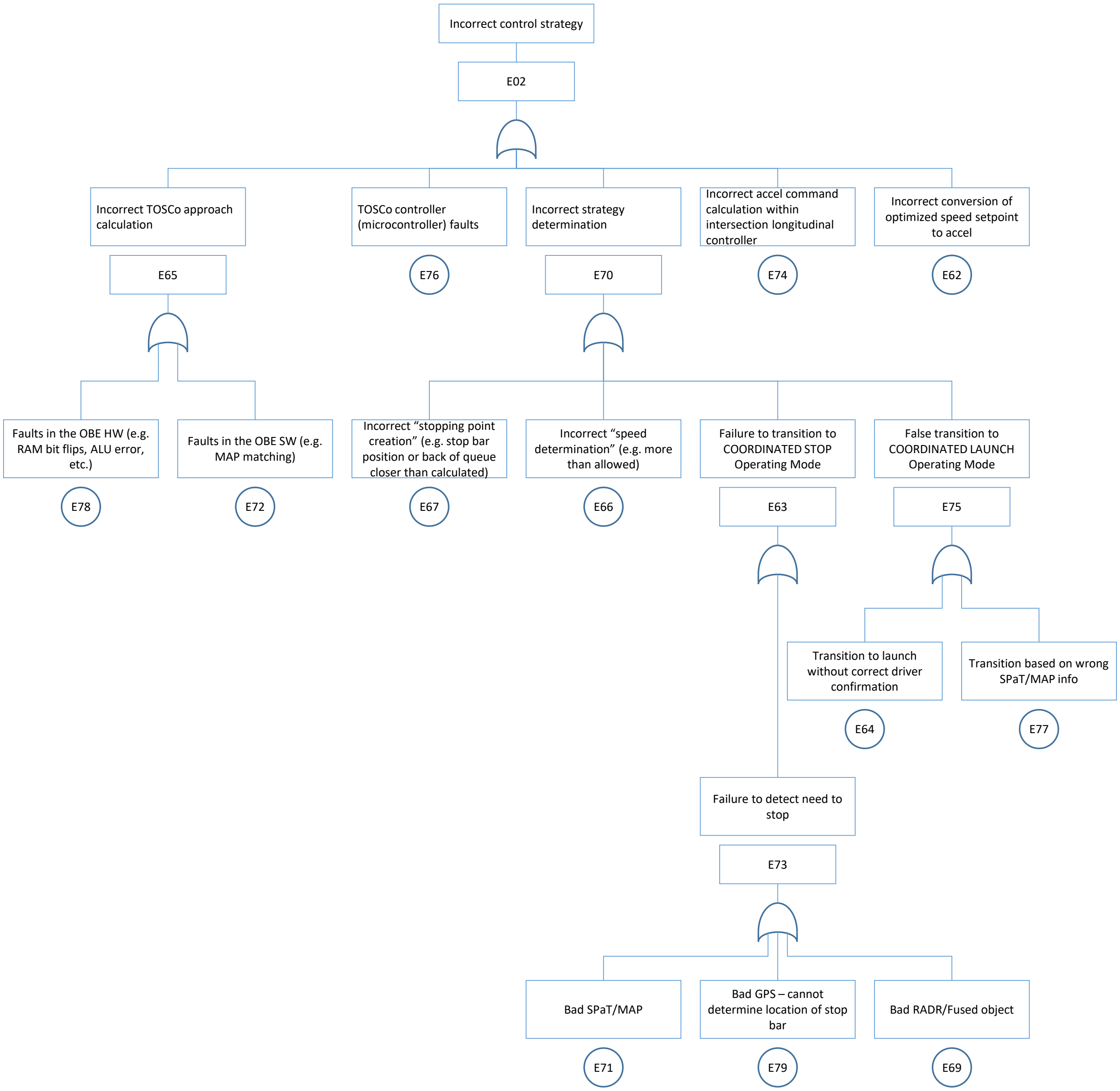
A) Input Processing Failures (E01)


Incorrect Inputs
E01
Incorrect RADAR objects or FUSED object
E49
Incorrect RTCM signal (masquerading, data corrupted during TX, wrong calculation in RSE, data arriving in wrong order, loss of signal…)
E43
Incorrect MAP signal (masquerading, data corrupted during TX, wrong calculation in RSE, data arriving in wrong order, loss of signal…)
E51
Incorrect SPaT signal (masquerading, data corrupted during TX, wrong calculation in RSE, data arriving in wrong order, loss of signal…)
E48
Incorrect determination of vehicle transmission (e.g. vehicle in R but TOSCo thinks it is in D…)
TOSCo feature shall be active only when the transmission is in D
E41
Incorrect vehicle speed
E56
Incorrect BSM object (can affect TOSCo approach including ETA)
E42
Incorrect GPS signal (Poor quality,
E47
Incorrect SPaT signal (masquerading, data corrupted during TX, wrong calculation in RSE, data arriving in wrong order, loss of signal…)
E53
Incorrect RADAR objects
E50
TOSCo button stuck ON
E52
CACC button is ON
E46
Incorrect Driver Confirmation
TOSCo feature shall always receive correct driver confirmation (should be able to filter transients)
E44
TOSCo is in COORDINATED LAUNCH Operating Mode
E45
TOSCo is in CREEP Operating Mode
E55

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Figure 11: Input Processing Failures (Refer to E01 in Figure 10)

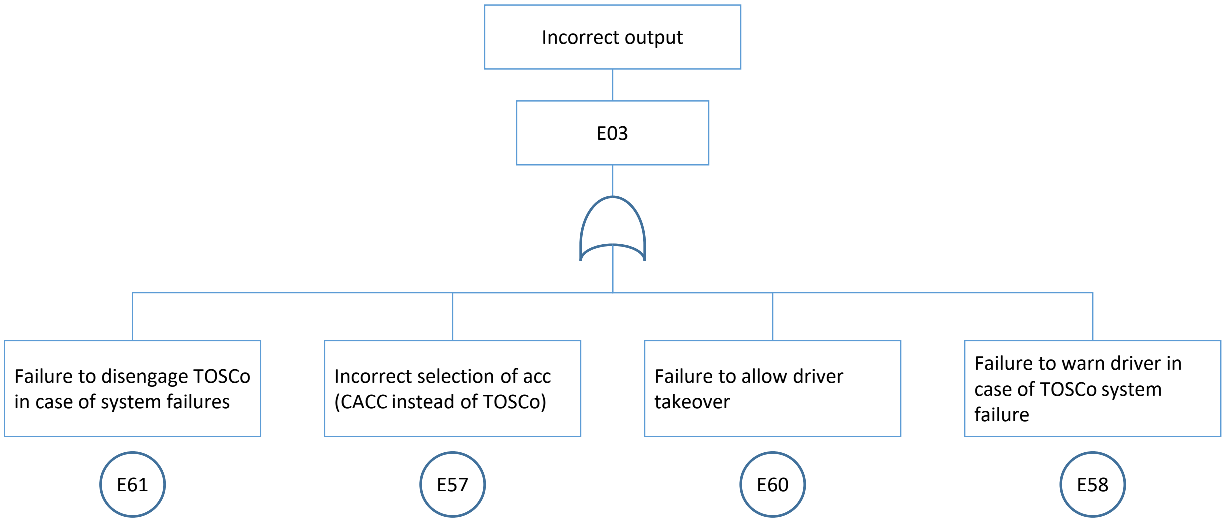
B) Control Strategy Failures (E02)


Incorrect control strategy
E02
Incorrect TOSCo approach calculation
E65
TOSCo controller (microcontroller) faults
E76
Incorrect strategy determination
E70
Incorrect accel command calculation within intersection longitudinal controller
E74
Incorrect conversion of optimized speed setpoint to accel
E62
Faults in the OBE HW (e.g. RAM bit flips, ALU error, etc.)
E78
Faults in the OBE SW (e.g. MAP matching)
E72
Incorrect “stopping point creation” (e.g. stop bar position or back of queue closer than calculated)
E67
Incorrect “speed determination” (e.g. more than allowed)
E66
Failure to transition to COORDINATED STOP Operating Mode
E63
False transition to COORDINATED LAUNCH Operating Mode
E75
Transition to launch without correct driver confirmation
E64
Transition based on wrong SPaT/MAP info
E77
Failure to detect need to stop
E73
Bad SPaT/MAP
E71
Bad GPS – cannot determine location of stop bar
E79
Bad RADR/Fused object
E69

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Figure 12: Control Strategy Failures (Refer to E02 in Figure 10)

C) Output Strategy Failures (E03)


Incorrect output
E03
Failure to disengage TOSCo in case of system failures
Incorrect selection of acc (CACC instead of TOSCo)
Failure to allow driver takeover
Failure to warn driver in case of TOSCo system failure
E61
E57
E60
E58

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

Figure 13: Output Strategy Failures (Refer to E03 in Figure 10)

D) Complete FTA

The complete fault tree for the excessive acceleration hazard only is obtained by putting together the fault tree segments illustrated in Figure 10, Figure 11, Figure 12 and Figure 13 where the section illustrated in Figure 10 is the top of the fault tree. To obtain a complete fault tree for the entire TOSCo feature, the same approach can be utilized to obtain fault trees for each of the three remaining hazards.

Based on the findings from the FTA, safety measures and diagnostic coverages can be implemented in the system design to mitigate such failure modes.

7 Conclusions and Summary

An introduction to the technical scope of the TOSCo feature was provided along with a background of the ISO 26262 processes for functional safety. The applicable safety relevant work products for ISO 26262 specific to the TOSCo Project included only the conceptual phase requirements. That included creating an Item boundary surrounding the features and functions of TOSCo.

An Item Definition was created which considered assumptions of behavior of the system and listed out vehicle level functions to be performed by the system. The Safety development followed closely to the V-model of product development and was linked to the TOSCo System Specification and the System Architecture.

A hazard analysis was completed that included identification of malfunctions from the TOSCo feature and then identification of vehicle level hazards. Four vehicle level hazards were identified which underwent a thorough hazard analysis processes by looking at multiple vehicle operational situations. The Hazard classification methods of ISO 26262 was utilized to determine the "ASIL" level for each hazard, which resulted in creating safety goals or top-level safety requirements for the TOSCo system.

The final step was preparing a functional safety concept that utilized the parameters and guidelines of ISO 26262 to develop safety requirements and allocate them to the respective safety critical modules of the TOSCo feature. ASILs were assigned to each functional requirement along with identification of safe states, in case of a potential failure. These requirements focused on only one TOSCo boundary and its operating environment. The vehicle parameters that could be integrated to TOSCo were left generic in nature and could be applicable for any potential interface.

The functional safety requirements can be refined for more technical detail when the preliminary system design physical architecture is available. Safety mechanisms for the system components, requirements for the actual elements and interfaces and the fault handling capabilities would be defined in the technical safety requirements during system design and implementation. A System Safety Analysis either through a Failure Modes & Effects Analysis (FMEA) or FTA is also recommended to be performed for the overall physical system along with its external interfaces to verify the effectiveness of the safety mechanisms based on identified causes of faults and the effects of failures.

8 References and Input Documents

[1] ISO 26262:2018, *Road Vehicles - Functional Safety*, International Organisation for Standardisation, Second edition.

[2] Considerations for ISO 26262 ASIL Hazard Classification, SAE J2980, May 2015.

[3] Guenther, Hendrik-Joern; Williams, Richard; Yoshida, Hiroyuki; Yumak, Tuncer; Moradi-Pari, Ehsan; Hussain, Shah; Naes, Tyler; Vijaya Kumar, Vivek; Probert, Neal; Sommerwerk, Kay; Bondarenko, Dennis; Wu, Guoyuan; Deering, Richard; Goudy, Roy, *Traffic Optimization for Signalized Corridors (TOSCo) Phase 1 Project – Interim Report on Vehicle System Requirements and Architecture Specification*, 2019, publication in process (2019).

APPENDIX A. List of Acronyms and Definitions

Acronym	Definition
ABS	Anti-lock Braking System
ACC	Adaptive Cruise Control
AIS	Abbreviated Injury Scale
ALU	Arithmetic Logic Unit
ASIL	Automotive Safety Integrity Level
BSM	Basic Safety Message
C	Controllability
CACC	Cooperative Adaptive Cruise Control
CAMP	Crash Avoidance Metrics Partners LLC
E	Probability of Exposure
E/E	Electrical and/or electronic
ETA	Estimated Time of Arrival
FTTI	Fault Tolerant Time Interval
FTA	Fault Tree Analysis
FMEA	Failure Mode & Effects Analysis
GID	Geometry Messages
GPS	Global Positioning System
HARA	Hazard Analysis and Risk Assessment
HAZOP	Hazard Analysis Operability
HV	Host Vehicle
LV	Lead Vehicle
MAP	MapData Message
OBE	On-board Equipment
OBU	On-board Unit
RAM	Random-Access Memory
RSE	Roadside Equipment
RSU	Roadside Units

Acronym	Definition
RTCM	Radio Technical Commission for Maritime Services
S	Severity
SG	Safety Goal
SPaT	Signal Phase and Timing
TOSCo	Traffic Optimization for Signalized Corridors
USDOT	United States Department of Transportation
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle

Term	Definition
Work Product	Documentation resulting from one or more associated requirements of ISO 26262
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
Operational Situation	Scenario that can occur during a vehicle's life
Malfunctioning Behavior	Failure or unintended behavior of an item with respect to its design intent
Safe State	Operating mode, in case of a failure, of an item without an unreasonable level of risk
Safety Critical	A function, element or component is safety critical if in its absence, has the potential to lead to a hazard
Safety Goal	Top-level safety requirement as a result of the Hazard Analysis and Risk Assessment at the vehicle level

APPENDIX B. Hazard Classification

The hazard classification scheme comprises the determination of the severity, the probability of exposure, and the controllability associated with the hazardous events of the item. The severity represents an estimate of the potential harm in a particular driving situation, while the probability of exposure is determined by the corresponding situation. The controllability rates how easy or difficult it is for the driver or other road traffic participant to avoid the considered accident type in the considered operational situation. For each hazard, depending on the number of related hazardous events, the classification will result in one or more combinations of severity, probability of exposure, and controllability.

B.1 Exposure

Exposure to a vehicle operational situation is based on one of the five levels as shown in Table 16 below. The objective in the Exposure determination is to comprehend realistic situations including normal driving conditions and adverse driving conditions. However, it should be noted that different traffic rules, environmental conditions, etc., influence the situations under consideration and may lead to a different Exposure.

Table 16: Exposure Classes

Class	Description	Informative Criteria for Exposure Based on Frequency	Informative Criteria for Exposure Based on Duration
E0*	Incredible	Not specified	Not specified
E1	Very low probability	Occurs less often than once a year for the great majority of drivers	Not specified
E2	Low probability	Occurs a few times a year for the great majority of drivers	<1 % of average operating time
E3	Medium probability	Occurs once a month or more often for an average driver	1 % to 10 % of average operating time
E4	High probability	Occurs during almost every drive on average	>10 % of average operating time

* No ASIL is assigned for E0

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

B.2 Severity

To describe the severity, the Abbreviated Injury Scale (AIS) classification is used. The AIS represents a classification of the severity of injuries The Severity class will be assigned to a given hazardous event based on a representative hazardous event scenario. The Severity class of the potential harm caused by a particular hazardous event is assigned to one of four levels as shown in Table 17 below.

Table 17: Severity Classes

Class	Description	Reference for Single Injuries (from AIS Scale)
S0*	No Injuries	AIS 0 and less than 10 % probability of AIS 1-6; or damage that cannot be classified safety-related
S1	Light & Moderate Injuries	More than 10 % probability of AIS 1-6 (and not S2 or S3)
S2	Severe and Life-threatening Injuries, Survival Probable	More than 10 % probability of AIS 3-6 (and not S3)
S3	Life-threatening Injuries (Survival Uncertain), Fatal Injuries	More than 10 % probability of AIS 5-6

* No ASIL is assigned for S0

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium

B.3 Controllability

To determine the controllability class for a given hazard, an estimation of the probability that the representative driver or other persons involved can influence the situation in order to avoid harm is made. The Controllability of a hazardous event is assigned to one of four levels as shown in Table 18 below.

Table 18: Controllability Classes

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

* No ASIL is assigned for C0

Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle-to-Infrastructure (V2I) Consortium