

Traffic Optimization for Signalized Corridors (TOSCo) Phase 2

Functional Safety Concept and Hazard Analysis Final Report

www.its.dot.gov/index.htm

Final Report – June 30, 2022
FHWA-JPO-22-961



U.S. Department of Transportation
Federal Highway Administration

Produced by Crash Avoidance Metrics Partners LLC in response to Cooperative Agreement Number DTFH6114H00002.

U.S. Department of Transportation
Federal Highway Administration

Notice

This document is disseminated under the sponsorship of the U. S. Department of Transportation in the interest of information exchange. The U. S. Government assumes no liability for the use of the information contained in this document.

The U.S. Government does not endorse products or manufacturers. Trademarks or manufacturers' names appear in this only because they are considered essential to the objective of the document.

Technical Report Documentation Page

1. Report No. FHWA-JPO-22-961	2. Government Accession No.	3. Recipient's Catalog No.	
4. Title and Subtitle Traffic Optimization for Signalized Corridors (TOSCo) Corridor: Phase 2 Functional Safety Concept and Hazard Analysis Final Report		5. Report Date June 30, 2022	
7. Author(s) N. Das, K. Rosol, K. Madala, K. Balke, D. Florence, S. Hussain, V. Kumar, N. Probert, D. Tian, T. Yumak, R. Deering, R. Goudy		6. Performing Organization Code	
9. Performing Organization Name And Address Crash Avoidance Metrics Partners LLC (CAMP) on behalf of the Vehicle-to-Infrastructure (V2I) Consortium 27220 Haggerty Road, Suite D-1 Farmington Hills, MI 48331		8. Performing Organization Report No.	
12. Sponsoring Agency Name and Address US Department of Transportation, Federal Highway Administration 1200 New Jersey Avenue, SE West Building Washington, DC 20590		10. Work Unit No. (TR AIS)	
15. Supplementary Notes This work was performed under a cooperative agreement with the US Department of Transportation, Federal Highway Administration. The effort was conducted under the supervision of Govind Vadakpat, Federal Highway Administration.		11. Contract or Grant No. DTFH6114H00002	
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, which includes both vehicle and infrastructure components, 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. <ul style="list-style-type: none"> - 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) Analysis did not cover product design and integration. Functional requirements focused on technical implementation of specific TOSCo components at a system level which can be utilized for subsequent integration and implementation.		13. Type of Report and Period Covered Final Report	
17. Keywords ISO26262, Functional Safety, Hazard and Risk Analysis, Connected Automation, ASIL		18. Distribution Statement	
19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages 108	22. Price

Table of Contents

1	Introduction 1	
	TOSCo Description.....	1
	Background.....	1
	Purpose and Scope.....	1
2	TOSCo System Architecture.....	3
	TOSCo System Architecture Overview.....	3
	TOSCo Operating Modes and Boundary Diagram.....	4
	TOSCo Transitions.....	5
	Allowed TOSCo Transitions.....	7
	TOSCo Transitions Not Allowed.....	8
3	ISO 26262 Process Development.....	9
	Safety Lifecycle Process.....	9
	Safety Processes for TOSCo.....	10
4	Item Definition Development Process.....	11
	Item Boundary.....	11
	Functions of the Item.....	12
	Assumptions of Behavior of the Item.....	13
5	Hazard Analysis and Risk Assessment Development Process.....	15
	Hazard Analysis Operability (HAZOP) Study and Identification of Hazards.....	15
	Risk Assessment of Hazardous Events.....	26
	Safety Goals and Safe States.....	32
6	Functional Safety Concept.....	35
	Functional Safety Strategy.....	36
	Functional Safety Requirements.....	37
	Warning and Degradation Concept.....	37
	Actions of the Driver and Endangered Persons.....	37
	Arbitration of Multiple Requestors.....	37

7	Functional Safety Analysis.....	65
	Scope of Fault Tree Analysis for TOSCo	65
	Development of FTA.....	68
	Findings from the FTA	74
8	Conclusions and Summary.....	76
9	Future Actions.....	78
10	References and Input Documents	79
APPENDIX A.	Hazard Classification	80
	Exposure.....	80
	Severity	80
	Controllability	81
APPENDIX B.	Risk Mitigation for On-Road Testing.....	82
	Risk Mitigation Approach.....	82
	Impact on Functional Safety.....	83
APPENDIX C.	Traceability of TOSCo Functions, Hazards and Scenarios	85

List of Figures

- Figure 1. TOSCo System Architecture 3
- Figure 2. Preliminary Block Diagram of TOSCo Covered Under Functional Safety 4
- Figure 3. Allowable TOSCo Transitions 6
- Figure 4. Overview of ISO 26262..... 9
- Figure 5. Overview of ISO 26262..... 26
- Figure 6. Potential Vehicle Operational Situations..... 27
- Figure 7. ASIL Determination 29
- Figure 8. Fault Tolerant Time Interval 33
- Figure 9. Hierarchy of Safety Goals and Functional Safety Requirements 36
- Figure 10. Top-level FTA Events for the Excessive Acceleration Hazard of the TOSCo System 68
- Figure 11. Input Processing Failures for TOSCo Vehicle 69
- Figure 12. Input Processing Failures for TOSCo Infrastructure..... 70
- Figure 13. Control Strategy Failures in TOSCo Vehicle 71
- Figure 14. Control Strategy Failures in TOSCo Infrastructure 72
- Figure 15. Output Strategy Failures in TOSCo Vehicle..... 73
- Figure 16. Output Strategy Failures in TOSCo Vehicle..... 73
- Figure 17 – Risk Mitigation Speed Profile Approaching a Red Light..... 83

List of Tables

- Table 1. TOSCo Operating Modes Matrix 5
- Table 2. Allowable TOSCo Transitions..... 7
- Table 3. TOSCo Transitions Not Allowed..... 8
- Table 4. Primary Functions of TOSCo 12
- Table 5. HAZOP Study for TOSCo Vehicle Functions..... 16
- Table 6. HAZOP Study for TOSCo Infrastructure Functions..... 18
- Table 7. Identification of Hazards from TOSCo Vehicle Malfunctions 21
- Table 8. Identification of Hazards from TOSCo Infrastructure Malfunctions 23
- Table 9. Example of Driving Situation Catalog for TOSCo..... 28
- Table 10. Hazard Event Example for Excessive Acceleration “Scenario Evaluation” 30
- Table 11. Hazard Event Example for Excessive Acceleration “ASIL Identification” 30
- Table 12. ASIL D Malfunction Scenario A..... 31
- Table 13. ASIL D Malfunction Scenario B..... 31
- Table 14. Safety Goal and ASIL Determination..... 32
- Table 15. Requirements for Driver Confirmation to TOSCo Vehicle..... 38
- Table 16. Requirements for Communication with External Vehicle Inputs 40
- Table 17. Safety Requirements for Communication with Remote Vehicles..... 42
- Table 18. Safety Requirements for Receiving Communication from Infrastructure
(Enhanced SPaT and MAP)..... 43
- Table 19. Safety Requirements for GPS Reception for TOSCo Vehicles 44
- Table 20. Safety Requirements for Driver Take Over from TOSCo..... 45
- Table 21. Safety Requirements for Valid Trajectory Calculation for TOSCo Vehicles..... 46
- Table 22. Safety Requirements for Propulsion Commands from TOSCo Vehicle(s)..... 50
- Table 23. Safety Requirements for Providing Driver Take-over Requests or Warning 51
- Table 24. Safety Requirements for GPS Time Synchronization for Infrastructure 52

Table 25. Safety Requirements for RTCM Data and Security for Infrastructure.....	53
Table 26. Safety Requirements for Receiving SPaT Information to Infrastructure.....	55
Table 27. Safety Requirements for MAP Configuration for Infrastructure and MAP Messages Sent Between TOSCo Infrastructure and TOSCo Vehicle(s)	57
Table 28. Safety Requirements for Enhanced SPaT Message Generation	59
Table 29. Safety Requirements for Green Window Determination at TOSCo Infrastructure and Safety Requirements for Communicating Enhanced SPaT Message to TOSCo Vehicle(s)	60
Table 30. Assumptions for External Safety Measures	64
Table 31. Notations Used for Fault Tree Analysis	66
Table 32. Colored Notations used in Fault Trees	67
Table 33. Exposure Classes	80
Table 34. Severity Classes	80
Table 35. Controllability Classes	81
Table 36: Traceability with Item Function, Hazard and ASIL.....	85

List of Acronyms and Definitions

Acronym	Meaning
ABS	Anti-lock Braking System
ACC	Adaptive Cruise Control
AIS	Abbreviated Injury Scale
ASIL	Automotive Safety Integrity Level
BSM	Basic Safety Message
C	Controllability
CC	Cruise Control
CACC	Cooperative Adaptive Cruise Control
CAMP	Crash Avoidance Metrics Partners LLC
CSC	Coordinated Speed Control
E	Probability of Exposure
E/E	Electrical and/or electronic
Enhanced SPaT	Enhanced Signal Phase and Timing
FSC	Functional Safety Concept
FSR	Functional Safety Requirement
FTA	Fault Tree Analysis
FTTI	Fault Tolerant Time Interval
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GW	Green Window
HARA	Hazard Analysis and Risk Assessment
HAZOP	Hazard Analysis Operability
HDOP	Horizontal Dilution of Precision
HV	Host Vehicle
IEC	International Electrotechnical Commission
MAP	Map Data Message
OBE	On-board Equipment

Acronym	Meaning
QM	Quality Management
RSU	Roadside Units
RTCM	Radio Technical Commission for Maritime Services
S	Severity
SG	Safety Goal
SOTIF	Safety of the Intended Functionality
SPaT	Signal Phase and Timing
TCU	Traction Control Unit?
TIP	Traffic Infrastructure Processor
TSC	Traffic Signal Controller
TOSCo	Traffic Optimization for Signalized Corridors
USDOT	United States Department of Transportation
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle

Term	Definition
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
Malfunctioning Behavior	Failure or unintended behavior of an item with respect to its design intent
Operational Situation	Scenario that can occur during a vehicle's life
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
Work Product	Documentation resulting from one or more associated requirements of ISO 26262

Chapter 1. Introduction

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. Both passenger cars and trucks are assumed to be able to employ the TOSCo feature. For the purpose of this analysis, the scope of TOSCo application is limited to light duty passenger vehicles.

Background

ISO 26262 is the *state-of-the-art* standard for functional safety of electrical and/or electronic (E/E) systems that are installed in series production road vehicles, excluding mopeds. It is closely tied to the automotive product development lifecycle and addresses all activities specific to management of functional safety. The ISO 26262 standard was adapted from IEC 61508 (International Electrotechnical Commission) and is tailored to the needs of the road vehicle 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 latest edition of the standard written in 2018 now provides requirements for trucks, buses, and motorcycles along with typical passenger vehicles of cars, light-duty trucks, and sport utility vehicles which sufficiently covers the intended scope of the TOSCo feature.

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 E/E systems, including interaction of these systems.

For TOSCo, the need for functional safety is strengthened due to multiple E/E features and functions that are planned to support partial automation of the vehicle. Vehicle-to-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 the achievement of functional safety. The scope of the document includes a summary of the work products developed for implementation of the concept phase of the product development for automotive applications as per ISO 26262 and include the following:

- 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)
- Fault Tree Analysis (identification of failure modes and safety mechanisms through a systematic process)

The scope shall now cover Phase 2 of the development of the TOSCo Feature “Build and Test” and shall include the following changes compared to Phase 1 development “Modeling and Analysis:”

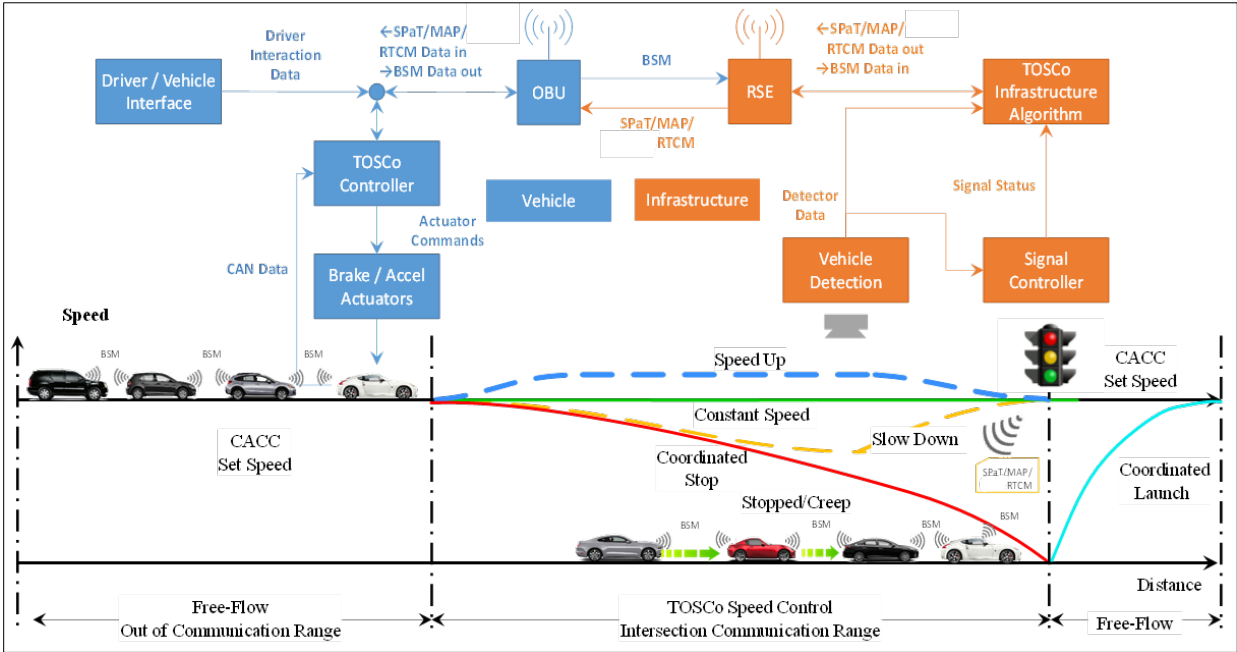
- Traffic Infrastructure processing and communication functionality with TOSCo Vehicle are now within TOSCo Item Boundary
- Influence from External functions to the Infrastructure and Vehicle components are considered in the hazard analysis

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 standard.

Chapter 2. TOSCo System Architecture

TOSCo System Architecture Overview

The Figure 1 below is a high-level illustration of the overall TOSCo system architecture derived from the TOSCo Vehicle System Specification.



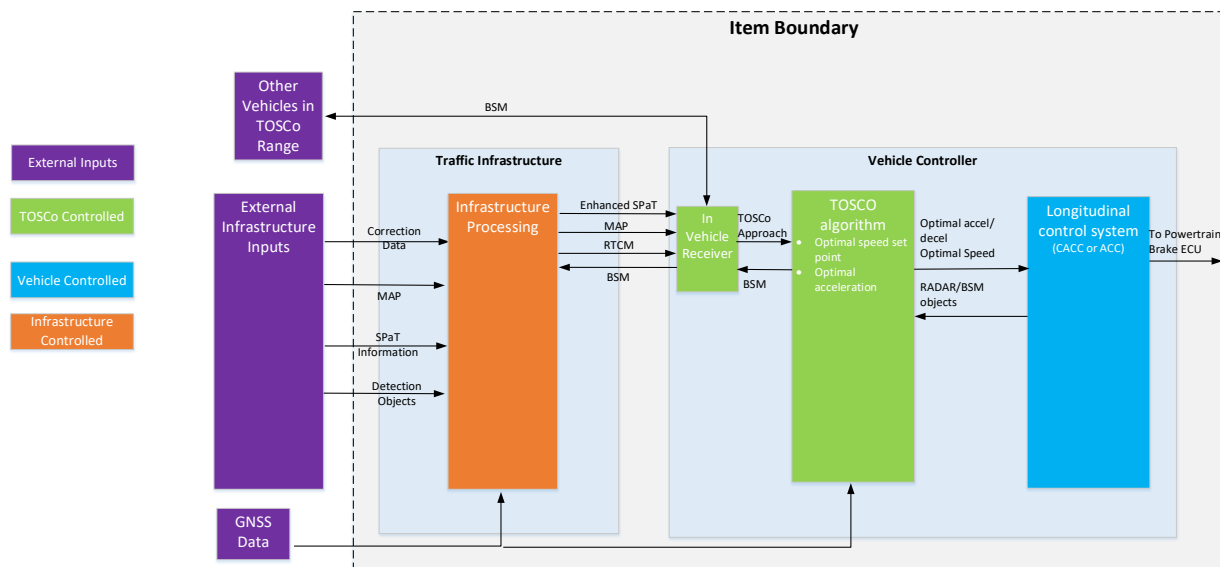
Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle to Infrastructure (V2I) Consortium, 2022

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 V2V communications. TOSCo also uses information broadcast in the Enhanced SPaT Message, which is computed on the infrastructure side, and is 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.

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, 2022

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

The above Figure 2 describes the architecture of the TOSCo Feature that is considered for functional safety requirements. This architecture and its control path, used to determine propulsion commands to the vehicle, are utilized as inputs to both the derivation of the Fault Tree Analysis and the Functional Safety Requirements.

A preliminary architecture allows the identification of the initial functions of the item, their boundaries and interfaces and includes the allocation of safety requirements to the relevant functions and components of the item. In this case, the item or the item boundary includes both the Infrastructure and TOSCo Vehicle Subsystem and considers the safety communication path associated with the Infrastructure and the TOSCo vehicle(s).

A detailed description of the functionality of each of the functions are provided in Section 4.1 of the Item Definition. Explanation of the elements within the architecture are provided in Section 5.1 of the Item Definition.

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

Free Flow

If a TOSCo-equipped Host Vehicle (HV) is in Free Flow mode while the TOSCo function 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.

Coordinated Speed Control

A TOSCo-equipped HV enters this strategy when TOSCo is active, the HV is receiving SPaT and MAP messages from the next signalized intersection in the HV's path and is matched to one of the intersections ingress lanes. The HV speed range in Coordinated Speed Control mode is from a minimum of V_{creep} to a maximum of the posted speed limit, V_{lim} .

- v_{lim} is the speed limit of ingress lane, typically 55 mph (88.5 km/h).
- v_{creep} is the Creep mode vehicle speed threshold, currently 6.0 m/s.

Coordinated Stop

A TOSCo-equipped HV enters this strategy when TOSCo is active, HV is cyclically receiving SPaT and MAP messages from the next signalized intersection in the HV’s path and is matched to one ingress lane of the intersection. HV speed range in Coordinated Stop mode is from a TOSCo speed range of v_{lim} , to a final speed of zero and the HV is transmitting a CSTOP flag through its Basic Safety Message (BSM).

Stopped

A TOSCo-equipped HV enters this strategy when the vehicle is stationary in TOSCo range and matched to an ingress lane either at the stop bar or in a queue. Any movement from this mode requires driver action.

Creep

The TOSCo-equipped vehicle is allowed to creep forward in direction towards the stop bar to fill gaps left by preceding vehicles if the gap is more than d_{creep} .

- d_{creep} : Creep distance threshold (gap between vehicles) that has to be exceeded to allow Creep mode, currently 7.0 m.

Coordinated Launch

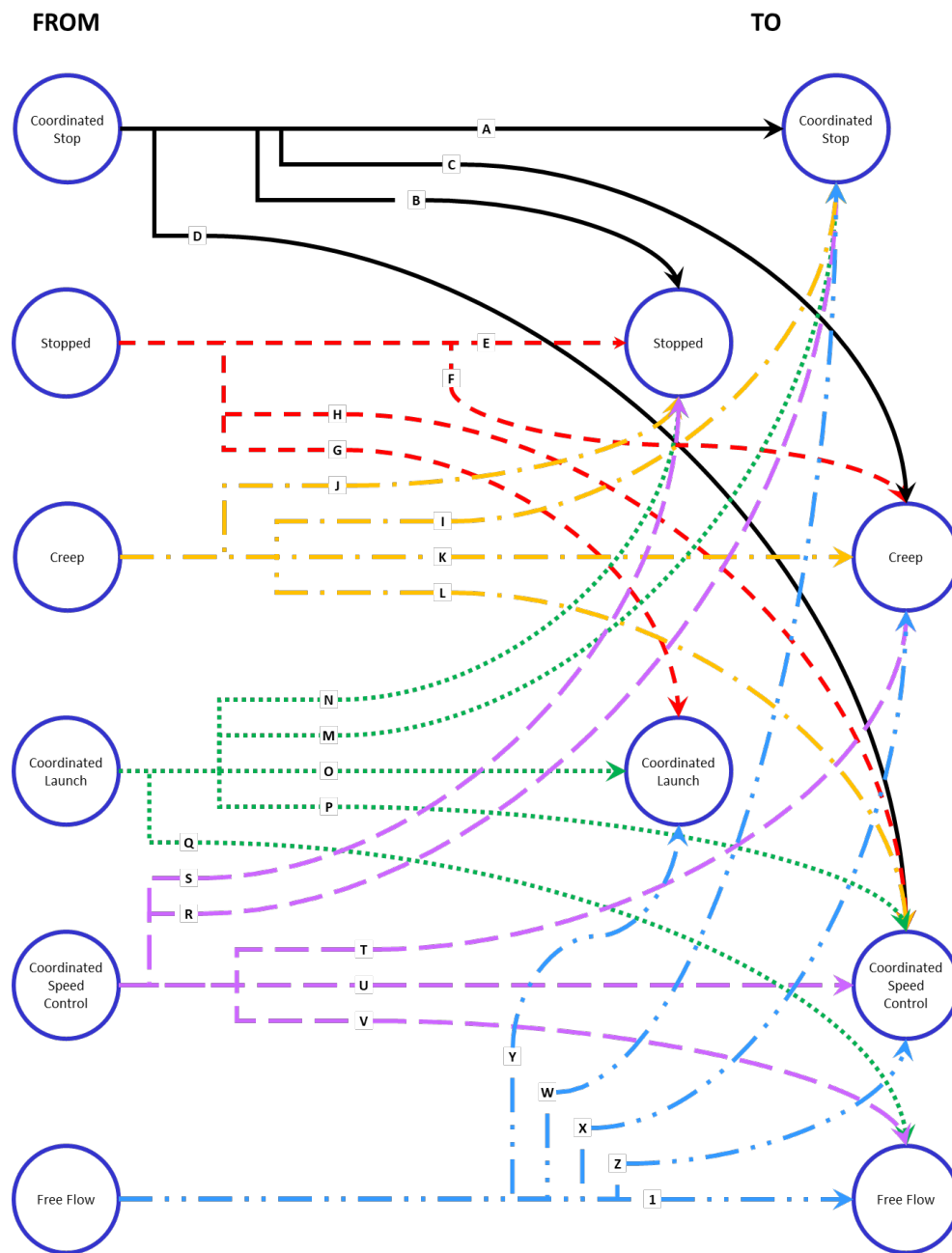
The TOSCo-equipped vehicle inside a TOSCo string broadcasts a Coordinated Launch message after the driver indicated readiness for launch during a STOPPED mode operation.

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

		To ↓	To ↓	To ↓	To ↓	To ↓	To ↓
	Operating Mode	CStop	Stopped	Creep	CLaunch	CSC	Free Flow
From →	CStop	A	B	C	α	D	β
From →	Stopped	γ	E	F	G	H (1-by-1 launch)	δ
From →	Creep	I	J	K	ϵ	L	ζ
From →	CLaunch	M	N	η	O	P	Q
From →	CSC	R	S	T	θ	U	V
From →	Free Flow	W	ι	X	Y (from standstill)	Z	1



Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle to Infrastructure (V2I) Consortium, 2022

Figure 3. Allowable TOSCo Transitions

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

Allowed TOSCo Transitions

The following table (Table 2) identifies allowable transitions between TOSCo operating modes.

Table 2. Allowable TOSCo Transitions

Transition	Operating Mode Before Transition	Operating Mode After Transition
A	Coordinated Stop	Coordinated Stop
B	Coordinated Stop	Stopped
C	Coordinated Stop	Creep
D	Coordinated Stop	Coordinated Speed Control
E	Stopped	Stopped
F	Stopped	Creep
G	Stopped	Coordinated Launch
H	Stopped	Coordinated Speed Control (1-by-1 launch)
I	Creep	Coordinated Stop
J	Creep	Stopped
K	Creep	Creep
L	Creep	Coordinated Speed Control
M	Coordinated Launch	Coordinated Stop
N	Coordinated Launch	Stopped
O	Coordinated Launch	Coordinated Launch
P	Coordinated Launch	Coordinated Speed Control
Q	Coordinated Launch	Free Flow
R	Coordinated Speed Control	Coordinated Stop
S	Coordinated Speed Control	Stopped
T	Coordinated Speed Control	Creep
U	Coordinated Speed Control	Coordinated Speed Control
V	Coordinated Speed Control	Free Flow
W	Free Flow	Coordinated Stop
X	Free Flow	Creep
Y	Free Flow	Coordinated Launch (from standstill)
Z	Free Flow	Coordinated Speed Control
1	Free Flow	Free Flow

TOSCo Transitions Not Allowed

Table 3 below lists the transitions that are not allowed.

Table 3. TOSCo Transitions Not Allowed

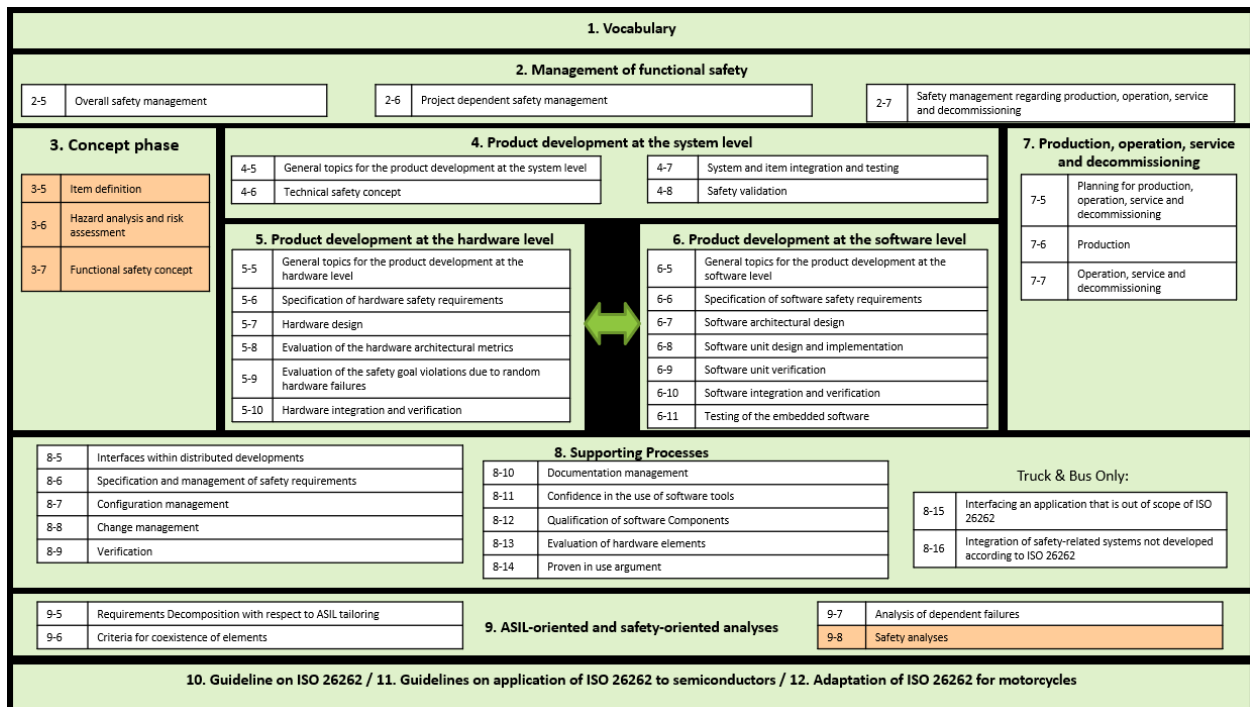
Transition	Operating Mode Before Transition	Operating Mode After Transition
α	Coordinated Stop	Coordinated Launch
β	Coordinated Stop	Free Flow
γ	Stopped	Coordinated Stop
δ	Stopped	Free Flow
ε	Creep	Coordinated Launch
ζ	Creep	Free Flow
η	Coordinated Launch	Creep
θ	Coordinated Speed Control	Coordinated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

Chapter 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.

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.



Source: kVA by UL Training Materials, 2022

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 vehicle implementation of TOSCo in the Concept Phase (highlighted in orange). For Phase 2 of the TOSCo Feature development, the focus of safety development was only on the infrastructure and vehicle implementations in the Concept Phase with a Safety Analysis of the entire TOSCo concept. The necessary work products were developed for the sections above highlighted in orange as part of the Phase 2 TOSCo development. These work products were considered and defined as per the requirements and recommendations of the latest ISO 26262 standard released in 2018.

U.S. Department of Transportation
Intelligent Transportation Systems Joint Program Office

During Phase 2, evaluation of TOSCo Infrastructure was added to the TOSCo Functional Safety Concept. This goes beyond the scope of a typical functional safety analysis to analyze the impacts of TOSCo infrastructure functionality on the vehicle.

Safety Processes for TOSCo

The following work products were created as required by the ISO 26262 standard to develop a concept phase version of the TOSCo feature that includes all the necessary functional safety attributes:

- Item Definition to define Safety Critical Functions_of the TOSCo System
- Hazard Analysis and Risk Assessment (HARA) to identify Vehicle-level Hazardous behavior caused by malfunctions
- Functional Safety Concept to specify safety requirements and achieve fault tolerance or mitigation of relevant faults

As a verification that the three items above were concise, complete, and sufficient, a Safety Analysis of the TOSCo feature was conducted. The safety analysis used in the Phase 2 TOSCo development was a qualitative Fault Tree Analysis.

The role and contribution of each of these work products are described in detail in the lower sections of this document. The Concept Phase (Part 3) of the ISO 26262 Standard follows the engineering V-model, hence each work product must be performed in sequential order as the next work product builds off the previous work product.

For the preparation of each work product, safety meetings and workshops were conducted with relevant TOSCo Project team participants, and all the pertinent information was documented. Multiple drafts of these safety documents were created for iterative reviews and references. Based on feedback and references from the concept versions of the TOSCo System Specification and TOSCo System Architecture, the safety relevant work products were updated, finalized, and subsequently released. As the iterative process continued for each work product, it was sometimes necessary to go back to the preceding work product and make revisions as follow-on work products discovered new findings ensuring the functional safety of the TOSCo feature

Chapter 4. Item Definition Development Process

The ISO 26262 Standard defines an 'item' as a system or combination of systems that implements a function at a vehicle-level to which functional safety processes of the standard must be applied. A 'vehicle function' is defined as a behavior of the vehicle that is implemented by one or more 'items' and is observable to the user. In this project, the TOSCo Feature is considered as an item that can contribute to the implementation of multiple vehicle functions.

The purpose of the Item Definition is to define and describe the item including its functionality and any dependencies on or interactions with the driver, environment, and other items at a vehicle-level. Also, the Item Definition is developed to provide an adequate understanding of the item so that the activities in subsequent safety lifecycle phases can be performed.

The Hazard Analysis and Risk Assessment is the follow-on step that utilizes the Item Definition to determine hazards, risks, and necessary Safety Goals prior to kicking off the Functional Safety Concept also derived from the Item Definition.

Item Boundary

Figure 2 in Section 2 of this document specifies the boundary of the TOSCo item and its interaction with other components of the vehicle and infrastructure. 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.

External Infrastructure Inputs: The External Infrastructure Inputs are outside the boundary of the TOSCo Feature and provide critical information to the Traffic Infrastructure system for accurate processing of the messages to the TOSCo vehicle(s). This includes a Detection System to detect and report vehicles at a TOSCo capable intersection, a traffic signal controller that provides SPaT data based on NTCIP protocol, a map that provides the necessary detail of the TOSCo capable intersection, and a correction station that provides Correction Data for Radio Technical Commission for Maritime Services (RTCM) correction information.

Traffic Infrastructure: Infrastructure device that allows the TOSCo Roadside Processor to communicate to TOSCo-enabled vehicles. The infrastructure provides Enhanced SPaT containing TOSCo information elements, intersection geometry (SAE J2735 MAP Data Message, or MAP) and position correction information to equipped vehicles.

In-vehicle Receiver: The On Board Equipment (OBE) of the TOSCo vehicle establishes the operating environment ahead of the vehicle by receiving and processing the enhanced SPaT data, MAP data, and RTCM corrections from the infrastructure as well as the BSM data from external sources.

TOSCo Algorithm: The TOSCo algorithm interfaces with the Longitudinal Control System and contains the Operating Mode Selection transition logic. The logic has the strategy to transition between the different TOSCo operating modes and provides acceleration commands based on optimal speed control. The TOSCo algorithm receives 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 Control System: The Longitudinal Controller uses CACC or Adaptive Cruise Control (ACC) gap control algorithms by utilizing acceleration and deceleration commands based on the distance calculations of an available vehicle string and the optimal vehicle speed for this intersection as determined by the TOSCo Feature.

Functions of the Item

The TOSCo Feature is comprised of functions from two different perspectives, the infrastructure-side perspective and the vehicle-side perspective. Both are utilized together to implement a safe and controlled driving behavior as part of both individual vehicle and a vehicle string through a connected and TOSCo-equipped 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

Vehicle Functions		
ID	NAME	DESCRIPTION
TOSCO_Veh_01	Acquire target remote vehicle(s)	Acquire a target vehicle to follow
TOSCO_Veh_02	Provide vehicle acceleration command	Provide the desired acceleration to the powertrain system
TOSCO_Veh_03	Provide vehicle deceleration command	Provide the desired deceleration to the powertrain and brake systems
TOSCO_Veh_04	Send/Receive communication between vehicle(s)	Send and receive BSM messages with CACC extension to/from other equipped vehicles within the communication range
TOSCO_Veh_05	Receive communication from Infrastructure	Receive information from roadside equipment with respect to signal phase and timing, including queue and Green Window information
		Receive information from roadside equipment with respect to map
		Receive information from roadside equipment with respect to position correction data
		Receive information from roadside equipment with respect to data security validation credentials
TOSCO_Veh_06	Provide driver take-over request/warning	Request the driver to takeover longitudinal control
TOSCO_Veh_07	Allow driver take-over	Allow the driver to take over longitudinal control
TOSCO_Veh_08	Provide the trajectory based on Queue, Green Window and stop bar	Determine based on Green Window provided by the Infrastructure, vehicle speed, and queue length
TOSCO_Veh_09	Receive GNSS Data for TOSCo Vehicle (s)	Use GNSS Data along with MAP and RTCM to perform map matching and vehicle localization
Infrastructure Functions		
ID	NAME	DESCRIPTION
TOSCO_Inf_01	Collect BSM information from connected vehicles(s) when available	Receive BSM messages from TOSCo-equipped vehicles in the vicinity and distribute the information within the infrastructure components
	NOTE: Not safety critical functionality	
TOSCO_Inf_02	Provide information to TOSCo vehicle(s) (Enhanced SPaT, MAP, RTCM, Security Credentials)	Information from roadside equipment with respect to signal phase and timing, map, and current queue length
TOSCO_Inf_03	Determine queue at the intersection	Determine the presence, length, and activity of the queue at the intersection
	NOTE: Queue detections are not safety critical	

Vehicle Functions		
ID	NAME	DESCRIPTION
TOSCO_Inf_04	Determine Green Window prediction based on queue information	Determine the Green Window based on information from intersection approach, traffic signal system, and queue detection system queue length to predict the duration of the Green Window
TOSCO_Inf_05	Establish communication with external infrastructure elements	Establish communications with infrastructure objects that provide queue and map information needed for the infrastructure to calculate the Green Window
TOSCO_Inf_06	Receive GPS Data for TOSCo infrastructure	Receive the GPS clock data needed by the TOSCo infrastructure to perform time synchronization

Assumptions of Behavior of the Item

The following assumptions of behavior were generated by considering these conditions:

- TOSCo performance and behavior under different operational modes and operational states
- TOSCo behavior under different vehicle scenarios, environmental and roadway conditions, and external influences
- Expectation of TOSCo's behavior during maintenance, decommissioning, and repair
- TOSCo's behavior while entering or recovering from a safe state
- Interactions of TOSCo with other elements and items on-board the vehicle
- Interactions of other elements and components within the TOSCO item boundary

The assumptions of behavior of the TOSCo Feature under various conditions and situations are detailed below:

- TOSCo works with only a level one 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. Maintaining enough headway/gap from the lead vehicle is always the responsibility of CACC. Hence, CACC can act as a secondary safety measure to mitigate a failure of speed control commands generated by the TOSCo Feature.
- TOSCo is intended for operation along appropriately equipped signalized arterials with posted speed limits of between 35 mph (56.3 km/h) and 60 mph (96.6 km/h).
- TOSCo equipped intersections are assumed to be intended for longitudinal controlled driving only, and TOSCo driven system is expected to follow the profile of the road curvature. TOSCo is not meant to support lateral control at this point.
- The driver must activate the TOSCo feature to gain TOSCo efficiencies. TOSCo provides feedback to the driver of the current active/inactive state of the TOSCo Feature.
- The Green Window estimation is calculated by the infrastructure using the signal timing and queue information from the intersection and sent to a TOSCo vehicle when within the appropriate range of the intersection to determine the appropriate speed trajectories to improve the efficiency of the vehicles contained within a string.
- The infrastructure utilizes a queue detection system along with SPaT to estimate the Green Window.
- An Enhanced SPaT message from the infrastructure is used by the TOSCo vehicles to improve trajectory estimation.
- GNSS position correction data from the infrastructure is used by the TOSCo vehicles to improve map matching.
- The infrastructure shall stop broadcasting regional extension data (queue length, Green Window) in the Enhanced SPaT message when the TOSCo Feature is not intended to be available at a given intersection or in the event of a failure in the infrastructure equipment.

NOTE: Further assumptions of behavior for the vehicle and infrastructure are covered in the Hazard Analysis Report and the Functional Safety Concept Report.

Chapter 5. Hazard Analysis and Risk Assessment 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:

- a. Situation analysis and hazard identification
- b. Classification of hazardous events (determination of severity, probability of exposure and controllability ratings)
- c. 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.

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 and Table 6 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 Vehicle Functions

Based on SAE standard J2980 for scenario development to support Hazard Analysis and Risk Assessment
<i>An asterisk "*" indicates that the hazard is covered elsewhere in the table</i>
<i>A dash '-' indicates that no new hazard is found for the HAZOP-structured malfunction.</i>
<i>An "X" indicates that no malfunctions are applicable for that particular cell in the table</i>
<i>Patterned cells are not malfunctions as they are deemed to be non-safety critical</i>

Identification of Malfunctions from Item Functions							
ITEM FUNCTION		Malfunction					
		Loss of Function	Unintended Activation	More than Intended	Less than Intended	Incorrect or Wrong (State)	Output Stuck-At Value
TOSCO_Veh_01	Acquire target remote vehicle(s)	[MF_1] Loss of target acquisition	[MF_2] False positive target acquisition	-	-	-	[MF_3] Target acquisition stuck
TOSCO_Veh_02	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	*	*
TOSCO_Veh_03	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	*	*
TOSCO_Veh_04	Send/Receive communication between vehicle(s)	[MF_12] Loss of communication between remote vehicle(s)	[MF_13] Incorrect communication between remote vehicle(s)	*	*	-	*
TOSCO_Veh_05	Receive communication from Infrastructure	[MF_14] Loss of communication from infrastructure	[MF_15] Incorrect communication from infrastructure	*	*	-	*
TOSCO_Veh_06	Provide driver take-over request/ warning	[MF_16] Loss of driver take-over request/ warning	[MF_17] False driver take-over request/ warning	-	-	-	*
TOSCO_Veh_07	Allow driver take-over	[MF_18] Loss of driver take-over	[MF_19] False driver take-over	-	[MF_20] Partial drive take-over	-	*
TOSCO_Veh_08	Provide the trajectory	[MF_21] Inability to follow	[MF_22] Unintended	*	*	[MF_23] Wrong	*

Identification of Malfunctions from Item Functions							
ITEM FUNCTION		Malfunction					
		Loss of Function	Unintended Activation	More than Intended	Less than Intended	Incorrect or Wrong (State)	Output Stuck-At Value
	based on Queue, Green Window and Stop Bar	trajectory leading to loss of determining approach /departure	Activation leading to significant speed differential between vehicles in queue			approach/ departure determination	
		Inability to determine queue attributes (length, dispersal etc.) at the intersection. Inability to determine approach /departure	Queue detected when none exists.	Incorrect queue determination	*	Wrong approach/ departure determination	*
TOSCO_Veh_09	Receive GPS Data for TOSCo Vehicle (s)	[MF_25] Inability to determine vehicle location and time values	X	X	X	[MF_26] Incorrect GPS Data leading to incorrect determination of vehicle location and time values	-

Table 6. HAZOP Study for TOSCo Infrastructure Functions

Identification of Malfunctions from Item Functions							
ITEM FUNCTION		Malfunction					
		Loss of Function	Unintended Activation	More than Intended	Less than Intended	Incorrect or Wrong (State)	Output Stuck-At Value
TOSCO_Inf_02	Provide information to TOSCo vehicle(s) (Enhanced SPaT)	[MF_28] Inability to perform trajectory planning as the TOSCo Vehicle(s) cannot receive a Green Window	[MF_29] Inadvertent activation of the TOSCo during the wrong scenario(s) due to unintended TOSCo information from the infrastructure	[MF_30] Vehicle unable to determine speed trajectory due to excessive SPaT information from Infrastructure	-	[MF_31] Incorrect Enhanced SPaT information leading to wrong trajectory planning	-
	Provide information to TOSCo vehicle(s) (MAP)	[MF_33] Inability to provide MAP data to TOSCo Vehicle(s)	X	X	X	[MF_34] Incorrect MAP data to TOSCo Vehicle(s) leading to inaccurate TOSCo Approach determination	-
	Provide information to TOSCo vehicle(s) (RTCM)	Potential dual point failure Loss of correction data to Vehicle (Vehicle needs to utilize internal GPS data to calculate location)	X	X	X	[MF_36] Wrong RTCM Message leading to inability to calculate vehicle position	-
	Provide information to TOSCo vehicle(s) (Security Credentials)	Potential dual point failure Loss of security credentials	X	X	X	Potential dual point failure Incorrect Security credentials	X
TOSCO_Inf_03	Determine queue at the intersection NOTE: Queue detections are not safety critical	[MF_38] Inability to determine queue attributes (length, dispersal etc.) at the intersection.	[MF_39] false positive. Queue detected when none exists. [MF_40] false negative -- no queue detected when one exists.	-	-	[MF_41] Incorrect queue determination	-

Identification of Malfunctions from Item Functions							
ITEM FUNCTION		Malfunction					
		Loss of Function	Unintended Activation	More than Intended	Less than Intended	Incorrect or Wrong (State)	Output Stuck-At Value
TOSCO_Inf_04	Determine Green window prediction based on queue information	[MF_42] Inability to determine Green Window leading to inability to plan vehicle trajectory	[MF_43] false positive. Provide Green Window when not intended	[MF_44] Determine Green Window more often than necessary, leading to inhibiting Enhanced SPaT transmission	[MF_45] Determine Green Window less frequently, leading to inaccurate determination of the trajectory planning	[MF_46] Incorrect Green Window prediction a) behind the intersection or the opposite direction of the intersection b) Receive Green Window from the wrong lane	-
TOSCO_Inf_05	Establish communication with external infrastructure elements	[MF_50] Loss of Correction Data leading to loss of RTCM at a vehicle level	X	-	-	[MF_51] Receive corrupted data (or data not updated/updated data not utilized) leading to incorrect determination of vehicle location	-
		[MF_53] Loss of queue objects leading to inability to predict Green Window	X	-	-	[MF_54] Incorrect Queue objects received leading to incorrect queue determination (Covered in MF_39)	-
		[MF_56] Loss of MAP Data leading to loss of TOSCo functionality (<i>Reliability concern</i>)	X	X	X	[MF_57] Incorrect MAP Data leading to wrong calculation of TOSCo functionality	X
TOSCO_Inf_06	Receive GPS Data for TOSCo infrastructure	[MF_58] Inability to determine Clock Data leading to inaccurate time values to TOSCo vehicle(s)	X	X	X	[MF_59] Incorrect Clock Data leading to inaccurate time	X

Identification of Malfunctions from Item Functions						
ITEM FUNCTION		Malfunction				
		Loss of Function	Unintended Activation	More than Intended	Less than Intended	Incorrect or Wrong (State)
						values to TOSCo vehicle(s)

It is recommended to revisit the HARA process during every phase of TOSCo development. Vehicle operating scenarios and conditions may change, and it is possible that new functions may arise leading to additional potential malfunctions and their associated vehicle hazards.

The malfunctioning behaviors identified above are then mapped to the vehicle functions identified in Table 4. The process below is intended to identify vehicle-level hazards for the TOSCo Feature as shown in Table 7 for vehicle malfunctions and Table 8 for infrastructure malfunctions. The mapping varies with the driving situations considered for the various malfunctioning behaviors.

Table 7. Identification of Hazards from TOSCo Vehicle 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
Acquire Remote Vehicles	[MF_2] False positive target acquisition	Remote vehicle target is acquired when there is none.	[H_3] Excessive deceleration [H_4] Insufficient acceleration
Acquire Remote Vehicles	[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]
Provide Acceleration Commands	[MF_5] Unintended acceleration command	Unintended acceleration command, provided target acquisition and communication functions are working correctly.	[H_1] and [H_4]
Provide Acceleration Commands	[MF_6] Excessive acceleration command	Excessive acceleration command, provided target acquisition and communication functions are working correctly.	[H_1]
Provide Acceleration Commands	[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]
Provide Deceleration Commands	[MF_9] Unintended deceleration command	Unintended deceleration command, provided target acquisition and communication functions are working correctly.	[H_2] and [H_3]
Provide Deceleration Commands	[MF_10] Excessive deceleration command	Excessive deceleration command, provided target acquisition and communication functions are working correctly.	[H_3]
Provide Deceleration Commands	[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]
Communicate with other Remote Vehicles	[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
Communicate with Infrastructure	[MF_15] Incorrect communication with remote vehicle(s)	Communication from infrastructure is misleading/corrupt provided other functions are working correctly.	All hazards

ITEM FUNCTION	Malfunctions	Malfunction Note	Hazard
Provide 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
Provide Driver Take-over Request/Warning	[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.
Allow 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
Allow Driver Take-over	[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
Allow Driver Take-over	[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
Provide the Trajectory based on Queue, Green Window and stop bar	[MF_21] Inability to follow trajectory leading to loss of determining 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
Provide the Trajectory based on Queue, Green Window and Stop Bar	[MF_22] Unintended Activation leading to significant speed differential between vehicles in queue	Inadvertent activation of the TOSCo Feature (within the TOSCo Range) in the vehicle string; leading to a sudden slow down or acceleration of the vehicle.	[H_1] Excessive vehicle Acceleration [H_3] Excessive vehicle deceleration
Provide the Trajectory based on Queue, Green Window and Stop Bar	[MF_23] 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 (i.e., it can result in incorrect trajectory).	All hazards
Provide the Trajectory based on Queue, Green Window and Stop Bar	[MF_24] Intermittent TOSCo Approach based on trajectory calculation	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
Receive GPS Data for TOSCo Vehicle(s)	[MF_25] Inability to determine vehicle location and time values	Assumption that TOSCo shuts off (system goes to CACC). NOTE: Functional Safety requirement to warn the driver of GPS loss is required.	All hazards
Receive GPS Data for TOSCo Vehicle(s)	[MF_26] Incorrect GPS Data leading to incorrect determination of vehicle location and time values	Unable to perform accurate path planning of vehicle due to wrong or sudden change in GPS values.	All hazards
Receive GPS Data for TOSCo Vehicle(s)	[MF_27] Unstable GPS Data leading to incorrect determination of vehicle location and time values	Receive erratic location data leading to intermittent change in vehicle speed.	All hazards

Table 8. Identification of Hazards from TOSCo Infrastructure Malfunctions

ITEM FUNCTION	Malfunctions	Malfunction Note	Hazard
Provide Information to TOSCo Vehicle(s) (Enhanced SPaT)	[MF_28] Inability to perform trajectory planning as the TOSCo Vehicle(s) cannot receive a Green Window	If vehicle is approaching TOSCo Range or outside TOSCo Range, may not be safety critical as vehicle continues motion in CACC. Already in TOSCo Range - All hazards could occur-TOSCo will be shut off.	All hazards
Provide Information to TOSCo Vehicle(s) (Enhanced SPaT)	[MF_29] Inadvertent activation of the TOSCo during the wrong scenario(s) due to unintended TOSCo information from the infrastructure	Provide Enhanced SPaT during a time or situation when not intended or when TOSCo was not supposed to be active. OR Change of intersection status due to external influence (changes the status of the traffic signal controller). - Should not lead to a safety concern.	
Provide Information to TOSCo Vehicle(s) (Enhanced SPaT)	[MF_30] Vehicle unable to determine speed trajectory due to excessive SPaT information from Infrastructure	Update comment: Too many TOSCo messages received affecting TOSCo resources resulting in vehicle unable to determine speed trajectories and leading to TOSCo shutoff. NOTE: CSTOP Scenario (unintended acceleration)	All hazards
Provide Information to TOSCo Vehicle(s) (Enhanced SPaT)	[MF_31] Incorrect or Stuck-At Enhanced SPaT information leading to wrong trajectory planning	Receive incorrect SPaT messages from the infrastructure leading to wrong trajectory planning.	All propulsion-based hazards
Provide Information to TOSCo Vehicle(s) (Enhanced SPaT)	[MF_32] Intermittent Enhanced SPaT information	TOSCo Shut ON and OFF (All propulsion-based hazards based on the vehicle operating mode). <i>NOTE: Intermittent Enhanced SPaT can be classified as:</i> <i>a) Erratic behavior of Green Window inside the SPaT message (while the reception of the SPaT message is still consistent) This leads to “jerky” drive scenarios and simulation studies and filed date have found this to be safety critical.</i> <i>b) Green Window (GW) information is consistent but the reception of the SPaT message itself is intermittent / erratic. This would lead to TOSCo ON and OFF.</i>	Potentially lead to all hazards if TOSCo OFF close to intersection (mitigated by other collision avoidance systems or by driver)
Provide Information to TOSCo Vehicle(s) (MAP)	[MF_33] Inability to provide MAP data to TOSCo Vehicle(s)	A) Vehicle never received MAP: Assume TOSCo is not available or TOSCo gets shut off. B) Vehicle received a MAP and then didn't receive any other MAP messages as it traverses through the intersection -> Vehicle would still use the original MAP message. Not a safety concern. <i>NOTE: TOSCo should not be active on a corridor for dynamic changes in the MAP based on the time of the day (STOP sending Enhanced SPaT messages before entering TOSCo Range).</i>	Not a safety concern

ITEM FUNCTION	Malfunctions	Malfunction Note	Hazard
Provide Information to TOSCo vehicle(s) (MAP)	[MF_34] Incorrect MAP data to TOSCo Vehicle(s) leading to inaccurate TOSCo Approach determination	Wrong vehicle location and data leading to all propulsion-based hazards.	All hazards
Provide Information to TOSCo Vehicle(s) (MAP)	[MF_35] Delayed MAP Data to TOSCo Vehicle(s) leading to inability to calculate trajectory planning	Could get too close to the intersection to calculate trajectory thereby leading to collision with traffic.	All hazards
Provide Information to TOSCo Vehicle(s) (RTCM)	[MF_36] Wrong RTCM Message leading to inability to calculate vehicle position	Inaccurate processing of the RTCM message due to old version of correction data on the CORS station.	All hazards
Provide Information to TOSCo Vehicle(s) (RTCM)	[MF_37] Delayed or Expired RTCM message leading to inability to determine vehicle position	Inaccurate processing of the RTCM message due to old version of correction data on the CORS station.	All hazards
Determine the Queue at the Intersection	This is not a safety concern.	This is not a safety concern.	This is not a safety concern.
Determine Green Window Prediction based on Queue Information	[MF_42] Inability to determine green window leading to inability to plan vehicle trajectory	Same as MF_28	All hazards
Determine Green Window Prediction based on Queue Information	[MF_43] Provide Green Window when not intended	Unintended green window (but accurate) would not be a vehicle level hazard.	
Determine Green Window Prediction based on Queue Information	[MF_44] Determine green window more often than necessary, leading to inhibit Enhanced SPaT transmission	Same as [MF_30]	All hazards
Determine Green Window Prediction based on Queue Information	[MF_45] Determine green window less frequently, leading to inaccurate determination of the trajectory planning	Unstable Green Window leading to incorrect trajectory planning	All hazards
Determine Green Window Prediction based on Queue Information	[MF_46] Incorrect or Stuck Green Window prediction (behind the intersection or the opposite direction of the intersection)	<p>Incorrect Green Window prediction leading to incorrect trajectory planning.</p> <p>Determining the start or close of the Green Window earlier in the cycle than where it really exists.</p> <p>Start too early: Vehicle can be targeting to arrive at the stop bar before the queue has cleared. This is not a safety concern based on simulation and field testing.</p> <p>Close too early: inefficiencies and unnecessary stops (not a safety concern).</p> <p>Inability to act on the planned trajectory close to the intersection.</p> <p>Start too late: inefficiencies in the signal operations -- wasted capacity.</p> <p>Close too late: Runs a red light.</p>	All hazards

ITEM FUNCTION	Malfunctions	Malfunction Note	Hazard
Determine Green Window Prediction based on Queue Information	[MF_47] Determine Green Window too early, leading to inaccurate determination of the trajectory planning	Too early determination of Green Window does not lead to a safety concern as long as the message is valid.	Not a safety concern
Determine Green Window Prediction based on Queue Information	[MF_48] Determine Green Window too late, leading to inaccurate determination of the trajectory planning	IF Green Window is determined too late, the Enhanced SPaT cannot be broadcasted. TOSCo will STOP functioning. Similar to [MF28].	All hazards
Determine Green Window Prediction based on Queue Information	[MF_49.1] Determine Green Window intermittently, leading to inaccurate determination of the trajectory planning [MF_49.2] Sudden change in Green Window prediction leading to a sudden change in TOSCo trajectory causing a vehicle hazard [This is not safety critical]	Need to re-calculate Green Window continuously. Leads to TOSCo switch ON and OFF. Green Window still available for driver to maintain trajectory. Corner Case: Close to the intersection in case of a Green Window "OPEN" when supposed to be "CLOSED," could led to a hazard. Intermittent SPaT information: This could pose as a hazard if SPaT information is processed incorrectly before the next Green Window.	All hazards
Establish Communication with External Infrastructure Elements - Receive Queue Objects	[MF_53] Loss of queue objects leading to inability to predict Green Window	TOSCo does not activate.	All hazards
Establish Communication with External Infrastructure Elements - Receive Queue Objects	[MF_54] Incorrect Queue objects received leading to incorrect queue determination	If queue objects are determined at an incorrect location, potentially vehicle could SPEED_UP to reach to queue quickly.	All hazards
Establish Communication with External Infrastructure Elements - Receive Queue Objects	[MF_55] Intermittent Queue objects received	Lead to intermittent SPaT Message transmission. Same as [MF32]	Potentially lead to all hazards if TOSCo OFF close to intersection (mitigated by other collision avoidance systems or by driver)
Establish Communication with External Infrastructure Element - Configure MAP Data	[MF_56] Loss of MAP Data leading to loss of TOSCo functionality	Reliability Concern only	
Establish Communication with External Infrastructure Element - Configure MAP Data	[MF_57] Incorrect MAP Data leading to wrong calculation of TOSCo functionality	Wrong vehicle location and data leading to all propulsion-based hazards.	All hazards
Receive GPS Clock Data for TOSCo Infrastructure	[MF_58] Inability to determine Clock Data leading to inaccurate time values to TOSCo vehicle(s)	Leads to incorrect processing of data leading to incorrect trajectory planning.	All hazards
Receive GPS Clock Data for TOSCo Infrastructure	[MF_59] Incorrect Clock Data leading to inaccurate time values to TOSCo vehicle(s)	Leads to incorrect processing of data leading to incorrect trajectory planning.	All hazards

The following hazards were identified from the HAZOP study:

- Excessive Acceleration
- Insufficient Deceleration
- Insufficient Acceleration
- Excessive Deceleration

For Phase 2, Hazardous behavior of Input Processing of Infrastructure, Control Logic and Communication from Infrastructure to TOSCo Vehicle were evaluated. Following observations are recorded from the HAZOP Study.

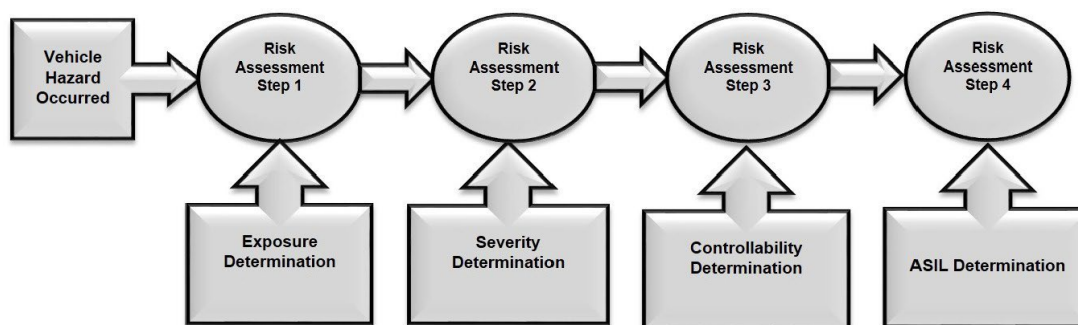
- Infrastructure failure(s) usually lead to all hazards except for certain cases in queue length determination.
- Failure due to Enhanced SPaT (Green Window determination) and MAP have severe safety critical impacts from the infrastructure.

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

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 the Exposure Rating to a vehicle operational situation is explained in APPENDIX A.

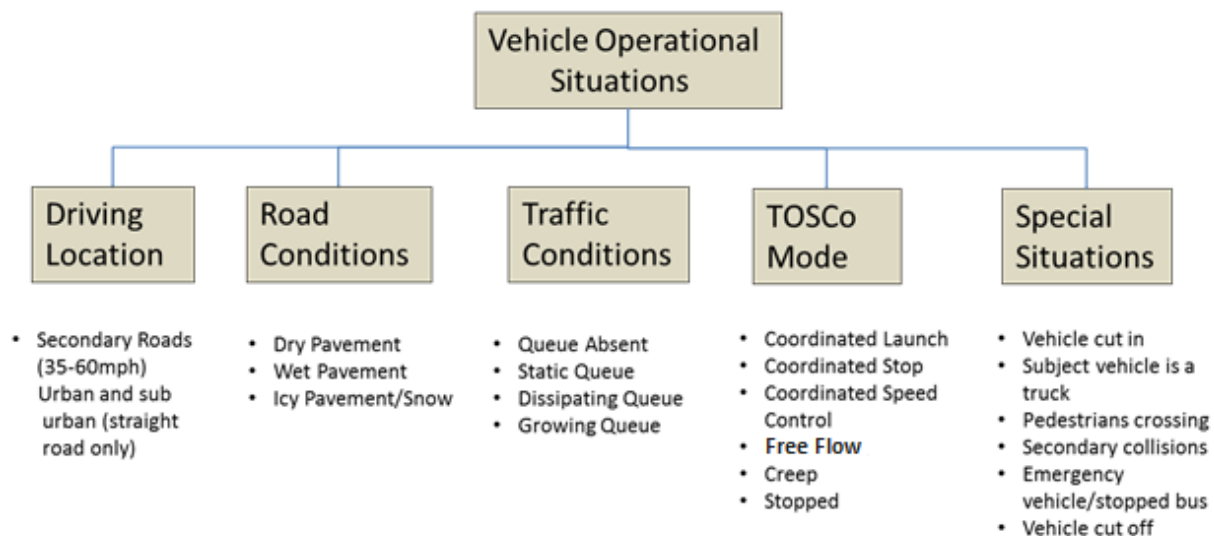


Source: kVA by UL Training Materials, 2022

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, 2022

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 8 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. Hypothetically for the TOSCo Project, a total of 151 situation combinations can be identified. However, for the sake of analysis only certain safety critical scenarios and events were considered.

Table 9. 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.

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.

The matrix is titled "Difficulty to Control" and "ASIL RATING". It shows the relationship between Severity Class, Exposure Class, and Controllability Class. The Controllability Class is further divided into C1, C2, and C3. The ASIL Rating is determined by the combination of these three factors. The matrix is as follows:

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: kVA by UL Training Materials, 2022

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 Hazard Analysis and Risk Assessment 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 hazard. The Safety goals were identified based on the hazard analysis and is covered in Section 5.3.

Each of the safety critical 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 10. 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

Table 11. Hazard Event Example for Excessive Acceleration “ASIL Identification”

Exposure Probability		Severity		Controllability		ASIL
Exposure	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

Updated HARA Study for Phase 2. Identification of ASIL D Risk

During Phase 1, the above analysis was valid and identifies an ASIL C criterion for the TOSCo feature for excessive acceleration. During Phase 2 analysis, certain corner case scenarios were identified.

Scenario A: Vehicle is in TOSCo Mode, queue is absent, and no vehicle is in front. This is a Coordinated Stop. Vehicle Stopping on a RED light and further out of the intersection.

Analysis: The driver may not be able to distinguish between an unintended acceleration and intended acceleration as, from the driver's perspective, an unintended acceleration may be identical to the Speed Up case in Coordinated Speed Control (CSC) Mode. It will be too late for the driver to react towards the end of the intersection. General driver expectations of change in acceleration during a RED light including reaction times need to be evaluated.

Table 12. ASIL D Malfunction Scenario A

Hazard	Scenario	S	Comment for Severity	E	Comment for Exposure	C	Comment for Controllability	ASIL
Excessive Acceleration	Coordinated Stop Vehicle Stopping on a RED light and further out of the intersection No vehicle in front	S3	Collision (side impact) is possible with cross traffic delta V can be > 20	E4	Based on a frequency-based approach, TOSCo-equipped vehicle will be at a secondary road intersection at least once every driving cycle	C3	Too late for the driver to react towards the end of the intersection	D

Scenario B: Vehicle is in TOSCo Mode, queue is absent, and no vehicle is in front. This is in a Coordinated Speed Control. Vehicle Slow Down on a RED light.

Analysis: If the vehicle is in SLOW DOWN and vehicle accelerates, driver will not be sure if it intended SPEED UP or unintended acceleration until the vehicle is too close to the intersection, which will be difficult to avoid.

Table 13. ASIL D Malfunction Scenario B

Hazard	Scenario	S	Comment for Severity	E	Comment for Exposure	C	Comment for Controllability	ASIL
Excessive Acceleration	Coordinated Speed Control Vehicle Slowing on a RED light No vehicle in front	S3	Collision (side impact) is possible with cross traffic delta V can be > 20	E4	Based on a frequency-based approach, TOSCo-equipped vehicle will be at a secondary road intersection at least once every driving cycle	C3	Driver will not be sure if TOSCo intended SPEED UP or unintended acceleration until the vehicle is too close to the intersection	D

Normal operation of TOSCo ‘trains’ the driver to trust the system that the traffic signal will be green when the vehicle arrives at the intersection regardless of the traffic signal state while approaching the intersection. Requirements specifically assigned as ASIL D are due to a scenario where the applicable failure (such as faulty Enhanced SPaT, MAP, or propulsion command) occurs and the hazardous situation of the vehicle being “too close to the intersection” with no queue present and the traffic signal is red. The hazard is determined at a location that does not allow the driver sufficient time to control the vehicle before running the red traffic signal and hence ASIL D is allocated to such faults and their corresponding safety mechanisms. For Phase 2 of the TOSCo Feature, the TOSCo controller and related safety critical components at the Vehicle and Infrastructure shall be considered at ASIL D integrity.

Risk Mitigation Strategy

To ensure that risk to the driver and the surrounding environment is mitigated for the above circumstances, safety mechanisms must be implemented within the TOSCo Controller, Traffic Infrastructure Controllers and other vehicle controllers that send critical vehicle data to the TOSCo controller. This could utilize a safe state strategy to slow down or stop the vehicle before the vehicle can cross the intersection due to a fault. Other measures could include a combination of some or all of the following methods.

- Continuous warning strategy to the driver to slow or stop the vehicle much ahead of the intersection
- Reduce capability of the operating design domain of the TOSCo Range by slowing down the vehicle while approaching the intersection
- Provide ability to differentiate between a TOSCo controlled safe operation versus a faulty operation to control a hazard by the driver
- Remove driver in loop while implementing safe state due to a TOSCo failure

Section 6 of this document provides safety requirements for TOSCo that need to be implemented to mitigate such a risk. Appendix B describes an interim risk mitigation strategy during the current Build and Test project to protect drivers and the surrounding environment in case of a TOSCo failure. Note that this risk mitigation strategy has been implemented only for test purposes using trained drivers fully aware of the potential hazards.

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 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.

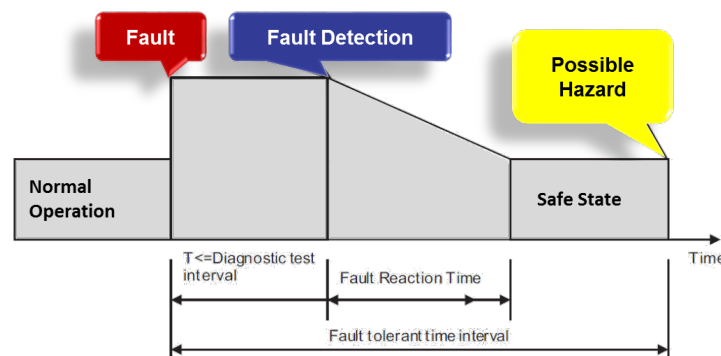
Table 14. Safety Goal and ASIL Determination

SAFETY GOAL ID	ASSOCIATED HAZARD	SAFETY GOAL TITLE	SAFE STATE	HIGHEST ASIL	FTTI	NOTES
SG01	Excessive Acceleration	Prevent Excessive Acceleration due to malfunctions in TOSCo	<ul style="list-style-type: none"> • If the vehicle is in CSC and the traffic light is green, the vehicle transitions to ACC when a lead vehicle is present or Manual mode is no lead vehicle is present. • If the vehicle is in CSC with Risk Mitigation Strategy (zero queue length reported) and the traffic light is red, the vehicle will remain in CSC Fallback and come to a stop at the stop bar. • If the vehicle is in CSTOP or CREEP, remain in TOSCo 	D	400ms	ASIL D: No vehicle in the front (No queue) (Too close to the intersection) ASIL C: For all other situations

U.S. Department of Transportation
Intelligent Transportation Systems Joint Program Office

SAFETY GOAL ID	ASSOCIATED HAZARD	SAFETY GOAL TITLE	SAFE STATE	HIGHEST ASIL	FTTI	NOTES
			and transition to CSTOP Fallback or CREEP Fallback.			
SG02	Insufficient Deceleration	Prevent Insufficient Deceleration due to malfunctions in TOSCo	Disable TOSCo Transition to ACC when a lead vehicle is present or Manual mode is no lead vehicle is present	D	400ms	ASIL D: No vehicle in the front (No queue) (Too close to the intersection) ASIL C: For all other situations
SG03	Excessive Deceleration	Prevent Excessive Deceleration due to malfunctions in TOSCo	Disable TOSCo Transition to ACC when a lead vehicle is present or Manual mode is no lead vehicle is present	B	200ms	
SG04	Insufficient Acceleration	Prevent Insufficient Acceleration due to malfunctions in TOSCo	NA	QM	NA	

No safety goal is written for Quality Management (QM) rated item-level hazards as these are not considered safety relevant. 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 timespan from the occurrence of a fault in an item to a possible occurrence of a hazardous event, in the absence of a safety mechanism as shown in Figure 8. Based on FTTI, assumed for the CACC Safety Analysis, a slightly relaxed value is considered due to relatively lower vehicle speeds in TOSCo compared to standalone CACC analysis and minimum time gap being only 600ms.



Source: kVA by UL Training Materials, 2022

Figure 8. Fault Tolerant Time Interval

For SG01, SG02 and SG03, the highest ASIL is associated with the worst-case scenario and the appropriate malfunctions associated to the hazard. It is possible that for a malfunction or failure mode associated to the hazard and for a specific scenario, the ASIL may be different. It is necessary to evaluate each such failure

mode separately and identify the appropriate ASIL from the HAZOP performed in the hazard analysis. The goal is not to over design the system with more complexity by allocating the highest ASIL to a very safety component in the architecture. Like most safety relevant automotive systems in the industry, the TOSCo Feature can be designed with a mix of multiple ASILs allocated to various components and elements. A mapping of each function, driving scenario and hazard to address these above issues is provided in Annex C of this document.

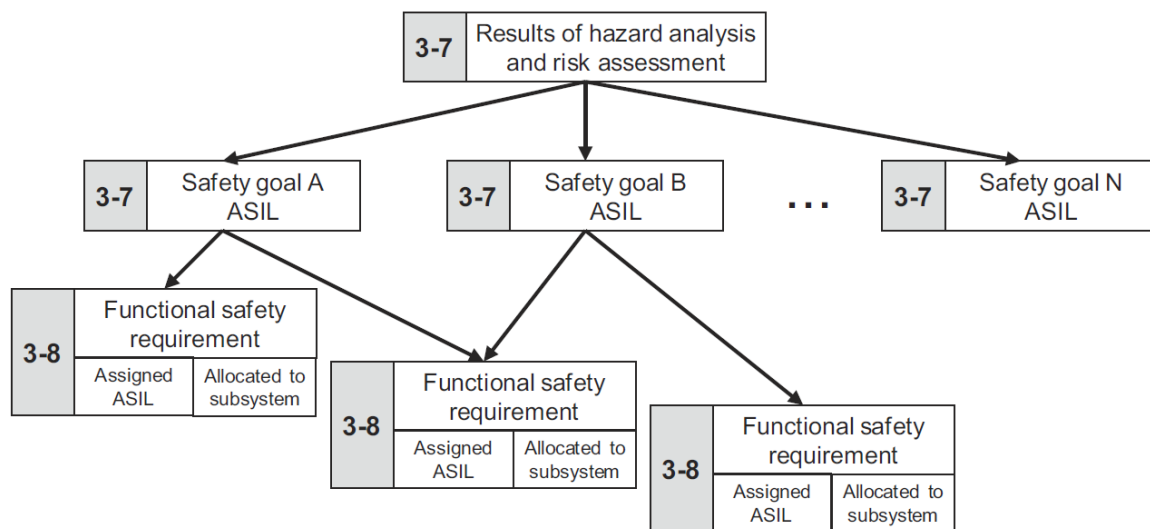
Chapter 6. Functional Safety Concept

The purpose of the Functional Safety Concept (FSC) is to derive the functional safety requirements from the safety goals and allocate them to the preliminary architectural elements of the item, or to external measures. To comply with the safety goals, the FSC contains safety measures, including the safety mechanisms, to be implemented in the item's architectural elements and specified in the functional safety requirements.

The functional safety concept addresses the following:

- Occurrence of fault and degradation of functionality when fault has occurred
- At vehicle level how the timing requirements are met, i.e., how the fault tolerant time interval shall be met by defining a fault handling time interval
- In case of occurrence of fault, the driver warnings needed to increase the controllability by the driver
- In case of occurrence of fault, the warnings that the driver should get for reduction of the risk exposure time to acceptable duration
- Fault detection and failure mitigation
- Transitioning to a safe state, if applicable from a safe state
- Fault avoidance and 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)
- Fault detection and driver warning in order to reduce the risk of exposure time to an acceptable interval
- Arbitration logic to select the most appropriate control requires from multiple requests generated simultaneously by different functions

The FSC continues along the hierarchical approach illustrated in Figure 9 by which the safety goals were determined as a result of the hazard analysis and risk assessment. Likewise, in this document, the functional safety requirements are now derived from the safety goals. The Functional Safety Requirements (FSRs) specify the basic safety mechanisms and safety measures which are then allocated to the elements of the preliminary system architecture. Per ISO 26262, the focus of this document is not on the safety of the intended function, but instead is focused on mitigating potential hazards due to malfunctions in the system.



Source: kVA by UL Training Materials, 2022

Figure 9. Hierarchy of Safety Goals and Functional Safety Requirements
(From ISO 26262: 2011- Part 3, Clause 7.2, Figure 2)

Functional Safety Strategy

The TOSCo Feature Functional Safety Strategy shall consider the Traffic Infrastructure portion, the communication path to the TOSCo Vehicle(s) and the TOSCo Algorithm within the TOSCo Vehicle(s). The Safety Strategy shall also include external inputs to the Infrastructure and the TOSCo Vehicle(s) that are responsible to ensure a safe TOSCo trajectory when the TOSCo Vehicle is within range of the TOSCo intersection. Inputs from the Item Definition and the Hazard Analysis are considered to refine the preliminary safety architecture and develop functional safety requirements for both the Infrastructure and the Vehicle portion, including the safety communication path between the two control systems. The Functional Safety Requirements were derived based on a Fault Tree Safety Analysis performed at a feature level for the TOSCo Feature. A traceability structure has been established between the Fault Tree Analysis and the Functional Safety Requirements where the Fault Tree events have been associated to the requirements. This provides the ability to derive safety requirements from the identified malfunctions and failure modes from the Hazard Analysis as well as from the safety measures identified from the Fault Tree Analysis.

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.

All safety requirements derived during Phase 1 have been either modified or replaced with new requirements based on verification reviews and updated architecture. Tables are identified below that consist of functional safety requirements for both the TOSCo Vehicle and TOSCo Infrastructure.

Note: Safety Requirements labeled as TOSCO_Veh_{ID} are allocated only to the TOSCo vehicle(s) and their relevant components. The diagnostics and the safety measures described within the requirements shall also be mitigated by the software and hardware components within the TOSCo Vehicle.

Note: Safety Requirements labeled as TOSCO_Inf_{ID} are allocated only to the TOSCo Infrastructure and their relevant components. Such requirements shall provide the relevant hazardous failure modes of the infrastructure components and the corresponding detection and mitigation strategy within the TOSCo Infrastructure.

Note: Safety Requirements labeled as TOSCO_Inf_Veh {ID} are allocated to both the TOSCo vehicle(s) and the Infrastructure. Such requirements are defined for scenarios where a hazardous infrastructure failure needs to be detected and mitigated by the TOSCo Vehicle(s) or safe state needs to be achieved by both Infrastructure and Vehicle components. This is usually for cases where a fault is detected by the Infrastructure, the fault status is communicated to the vehicle, and the vehicle algorithm mitigates or prevents the fault by taking appropriate action.

Warning and Degradation Concept

Whenever the TOSCo controller detects a fault which does not allow normal TOSCo operation, it will transition to ACC when a lead vehicle is present or Manual mode if no lead vehicle is present. Depending on the failure mode and operating mode, the system will warn the driver through visual and audio aids. TOSCo operation will be disabled if the fault persists.

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.

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 controller.

Table 15. Requirements for Driver Confirmation to TOSCo Vehicle

<i>ID</i>	<i>Description</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated to</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Note</i>
TOSCO_Veh_01.1	The TOSCo Algorithm shall utilize redundant input processing to identify driver input for activation and deactivation transitions. NOTE: A validity check between the two redundant inputs may be performed to detect faulty transition.	Detect unintended transition to TOSCo activation or deactivation due to faulty driver confirmation input.	C	[SG_001]	TOSCo Algorithm	NA	[E351] [E296]	Example relevant operating mode: TOSCo feature shall not activate or deactivate without correct driver confirmation input.
TOSCO_Veh_01.2	The TOSCo Algorithm shall utilize redundant input processing to identify driver confirmation input for transition to the Coordinated Launch and Creep operating modes. NOTE: A validity check between the two redundant inputs may be performed to detect faulty transition.	Detect unintended transition to CREEP or CLAUNCH due to faulty driver confirmation.	C	[SG_001]	TOSCo Algorithm	NA	[E351] [E296]	Example relevant operating mode: TOSCo feature shall not enter "Coordinated Launch" or "CREEP" without correct Driver confirmation input.

ID	Description	Rationale	ASIL	Safety Goals	Allocated to	Safe State	FTA_Event(s)	Note
TOSCO_Veh_01.3	<p>The longitudinal control system (TOSCo and CACC) shall cede control to the driver on driver intervention (such as accelerator pedal or brake pedal input).</p> <p>Note: Accelerator pedal input provides temporary overrides that revert to automated control when removed.</p> <p>Brake inputs deactivate the automated longitudinal control reverting to Manual mode.</p>	React to Driver takeover input	C	[SG_001]	Longitudinal Control System (TOSCo and CACC control Algorithm)	Revert to Manual Control	[E296]	
TOSCO_Veh_01.4	If the TOSCo algorithm identifies a faulty driver confirmation to activate TOSCo, then TOSCo function shall be disabled.	Prevent unintended activation of TOSCo	C	[SG_001]	TOSCo Algorithm	TOSCo does not activate until valid driver confirmation	[E351] [E296]	
TOSCO_Veh_01.5	In case the TOSCo feature is unable to transition to Free Flow when a lead vehicle is present and TOSCo disables due to the detection of a Driver Confirmation fault, TOSCo shall still be able to warn the driver to take over.	Emergency operation on inability to disable TOSCo	C	[SG_001]	TOSCo Algorithm	Provide driver warning	[E351] [E296]	

<i>ID</i>	<i>Description</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated to</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Note</i>
TOSCO_Veh_01.6	In case the TOSCo feature is unable to transition to Manual mode when no lead vehicle is present and TOSCo disables due to the detection of a Driver Confirmation fault, TOSCo shall still be able to warn the driver to take over.	Emergency operation on inability to disable TOSCo	C	[SG_001]	TOSCo Algorithm	Provide driver warning	[E351] [E296]	

Table 16. Requirements for Communication with External Vehicle Inputs

<i>ID</i>	<i>Description</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Notes</i>
TOSCO_Veh_02.1	<p>TOSCo feature shall communicate with the external vehicle controllers (such as ABS, TCU) for safety critical inputs over an end-to-end protected channel.</p> <p>NOTE: Relevant Safety critical inputs from the external vehicle controller(s) to the TOSCo Algorithm include:</p> <p>a) Vehicle Speed b) Vehicle Transmission (PRNDL) State c) Vehicle Gear State d) Accelerator Pedal or Brake Pedal Input</p>	Detect faulty safety critical inputs from external controllers	D	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	<p>External Vehicle System</p> <p>TOSCo Feature</p>	NA	<ul style="list-style-type: none"> • [E341] • [E295] • [E292] 	<p>ASIL D: Faulty Input too close to the intersection, leading to faulty acceleration command.</p> <p>External vehicle controllers are outside the TOSCo boundary and are responsible to generate and transmit accurate inputs with the appropriate safety integrity.</p>

ID	Description	Rationale	ASIL	Safety Goals	Allocated To	Safe State	FTA_Event(s)	Notes
TOSCO_Veh_02.2	If the TOSCo feature determines that an external safety critical vehicle input to TOSCo is invalid due to communication channel errors (data errors, out of order messages, time out, masquerading etc.), then the TOSCo Algorithm shall disable the TOSCo function and transition to ACC when a lead vehicle is present or Manual mode is no lead vehicle is present depending on the failure mode.	React to faulty External Vehicle Inputs to TOSCo	D	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	External Vehicle System TOSCo Feature	Disable TOSCo Transition to ACC when a lead vehicle is present or Manual mode is no lead vehicle is present. Vehicle System Sets invalidity flag.	<ul style="list-style-type: none"> • [E295] • [E341] 	
TOSCO_Veh_02.3	TOSCo feature shall disable TOSCo function if it detects a TOSCo activation input that is STUCK ON.	React to faulty TOSCo activation input	C	<ul style="list-style-type: none"> • [SG_001] 	TOSCo Algorithm	Disable TOSCo Transition to ACC when a lead vehicle is present or Manual mode if no lead vehicle is present.	<ul style="list-style-type: none"> • [E287] • [E289] • [E429] 	

Table 17. Safety Requirements for Communication with Remote Vehicles

<i>ID</i>	<i>Description</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Notes</i>
TOSCO_Veh_03.1	The TOSCo Vehicle algorithm shall identify faulty elements in the BSM information corresponding to plausibility issues with remote target vehicles that could compromise string stability by comparing received BSM inputs and Sensor Data.	Detect invalid BSM information based on plausibility between remote target vehicles	C	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	TOSCo algorithm\controller	NA	<ul style="list-style-type: none"> • [E352] • [E336] • [E337] • [E364] • [E365] • [E366] • [E368] 	
TOSCO_Veh_03.2	The OBE of the TOSCo Vehicle shall incorporate End-to End protection to ensure valid BSM Messages are communicated between remote target vehicle(s).	Implement End-to-End protection on BSM Messages	C	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	OBE	NA	<ul style="list-style-type: none"> • [E365] 	
TOSCO_Veh_03.3	If the TOSCo Algorithm determined invalid BSM information corresponding to remote target vehicles, the TOSCo algorithm shall revert to ACC when a lead vehicle is present or Manual mode if no lead vehicle is present depending on the failure mode.	Mitigate invalid BSM information between remote target vehicles	C	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	TOSCo Algorithm	Revert to ACC / Manual	<ul style="list-style-type: none"> • [E352] • [E336] • [E337] • [E338] • [E339] • [E368] • [E364] 	

Table 18. Safety Requirements for Receiving Communication from Infrastructure (Enhanced SPaT and MAP)

<i>ID</i>	<i>Description</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated to</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Notes</i>
TOSCO_Veh_04.1	The TOSCo Vehicle OBE shall receive Enhanced SPaT messages to the vehicle over an End-to-End protection channel. NOTE: The end-to-end protected channel shall diagnose data errors, repeated or aged data, time out.	Detect invalid Enhanced SPaT communication from infrastructure	D	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	OBE	NA	<ul style="list-style-type: none"> • [E354] • [E244] • [E243] 	
TOSCO_Veh_04.2	The OBE on the TOSCo vehicle shall be capable to receive updated MAP data from the Infrastructure over an End-to- End protected channel. NOTE: The end-to-end protected channel shall diagnose data errors, repeated or aged data, time out.	Detect incorrect MAP communication on TOSCo Vehicle	D	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	OBE	NA	<ul style="list-style-type: none"> • [E354] • [E244] • [E243] 	

Table 19. Safety Requirements for GPS Reception for TOSCo Vehicles

<i>ID</i>	<i>Description</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Notes</i>
TOSCO_Veh_05.1	If the TOSCo Algorithm determines that the HDOP (Horizontal Dilution of Precision) measurement for GPS position exceeds a specified threshold where vehicle location cannot be determined accurately, the TOSCo feature shall be turned OFF and driver shall be notified.	Prevent incorrect localization of the vehicle due to incorrect GPS	D	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	OBE (GPS Receiver) TOSCo Algorithm	Disable TOSCo Feature. Provide Driver Warning	<ul style="list-style-type: none"> • [E349] • [E269] 	ASIL D: Incorrect GPS received too close to the intersection
TOSCO_Veh_05.2	If the TOSCo vehicle receives unstable GPS or cannot determine vehicle location and time values, then the TOSCo vehicle shall transition to ACC when a lead vehicle is present or Manual mode is no lead vehicle is present depending on the failure mode and provide a driver warning.	Prevent incorrect localization and path planning of vehicle due to unstable or loss of GPS	D	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	OBE (GPS Receiver) TOSCo Algorithm	Disable TOSCo Feature. Provide Driver Warning.	<ul style="list-style-type: none"> • [E356] • [E268] • [E270] 	ASIL D: If vehicle is in CSTOP with no vehicle in front, changing to CACC would run the red light

Table 20. Safety Requirements for Driver Take Over from TOSCo

<i>ID</i>	<i>Description</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Notes</i>
TOSCO_Veh_06.1	<p>If the TOSCo Vehicle is unable to allow driver to take complete control of vehicle from TOSCo mode when needed, the driver shall be provided with an independent means to disable TOSCo function that is outside the primary control path of TOSCo.</p> <p>NOTE: An external independent method (such as brake pedal input or a separate switch) can be used to deactivate TOSCo operation manually.</p>	Allow driver take over from TOSCo through independent means	D	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	TOSCo Controller External Vehicle System	External Shutdown of TOSCo by Driver	<ul style="list-style-type: none"> • [E281] • [E275] • [E273] 	
TOSCO_Veh_06.2	<p>If the vehicle hands over control to the driver without a warning or request from driver, the vehicle shall continue normal operation.</p> <p>NOTE: The driver is assumed to have hands on steering always, and hence can easily continue to take control of vehicle.</p>	Reaction to false takeover from TOSCo	QM		TOSCo Controller	NA	<ul style="list-style-type: none"> • [E274] 	

Table 21. Safety Requirements for Valid Trajectory Calculation for TOSCo Vehicles

<i>ID</i>	<i>Description</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Notes</i>
TOSCO_Veh_07.1	The TOSCo controller shall be incorporated with a Safety Monitor that shall be able to detect all internal single point faults due to random hardware faults or systematic software faults that could lead to invalid vehicle trajectory calculation.	Monitor random hardware faults and systematic software faults	D	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	TOSCo Controller	NA	<ul style="list-style-type: none"> • [E363] • [E320] • [E308] 	Systematic Software Faults include a) Failures in Planning of vehicle Trajectory b) Failure in Monitoring vehicle Trajectory c) Failure in Following Vehicle trajectory (Incorrect transition between vehicle modes) (Inability to follow restrictions within particular vehicle modes) (transition to incorrect operating mode without driver confirmation) d) Failure in determining TOSCo Approach based on MAP Matching

ID	Description	Rationale	ASIL	Safety Goals	Allocated To	Safe State	FTA_Event(s)	Notes
TOSCO_Veh_07.2	If the Safety Monitor of the TOSCo Feature detects hardware or software faults that could result in an invalid trajectory calculation, then the TOSCo feature shall be deactivated.	Mitigate incorrect trajectory planning by vehicle	D	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	TOSCo Controller	Disable TOSCo Feature. Transition to ACC when a lead vehicle is present or Manual mode is no lead vehicle is present.	• [E363]	
TOSCo_Veh_07.3	If the TOSCo Vehicle requests the "Creep" function and either of the following occur while in CREEP: A) an acceleration of more than CREEP_MAX_ACC m/s ² is requested or B) a creep speed greater than maximum creep speed (CREEP_MAX_SPD m/s) is requested, then the TOSCo vehicle transition to or remain in STOPPED, until the next valid CREEP function request is received.	Restrictions in TOSCo Trajectory during CREEP Mode	C	<ul style="list-style-type: none"> • [SG_001] 	TOSCo Controller	Transition to STOPPED. Remain in STOPPED, if already stopped.	• [E362]	

ID	Description	Rationale	ASIL	Safety Goals	Allocated To	Safe State	FTA_Event(s)	Notes
TOSCO_Veh_07.4	TOSCo shall not allow vehicle movement beyond the stop line when in Coordinated Stop or CREEP modes.	Restrictions in TOSCo Trajectory during STOPPED and CREEP modes	C	• [SG_001]	TOSCo Controller	Maintain current STOPPED state	• [E362]	
TOSCO_Veh_07.5	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).	Restrictions in maximum acceleration and deceleration requests	C	• [SG_001] • [SG_002] • [SG_003]	TOSCo Controller	NA	• [E362]	
TOSCO_Veh_07.6	TOSCo feature shall be disabled in case the vehicle speed goes above TOSCO_SPEED_LIMIT mph (e.g., 55 mph) inside the TOSCo range.	Restrictions on maximum speed	C	• [SG_001] • [SG_002] • [SG_003]	TOSCo Controller	Transition to FREE FLOW	• [E362]	ASIL C: Expect this mechanism to function further out of the intersection
TOSCO_Veh_07.7	If a forbidden state transition is attempted, then TOSCo shall warn the driver and transition to ACC when a lead vehicle is present or Manual mode is no lead vehicle is present mode depending on the current operating mode and driving scenario.	React to incorrect transition between vehicle modes	D	• [SG_001] • [SG_002] • [SG_003]	TOSCo Controller	Transition to ACC when a lead vehicle is present or Manual mode is no lead vehicle is present depending on the failure	• [E361]	

<i>ID</i>	<i>Description</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Notes</i>
						mode and warn the driver.		
TOSCO_Veh_07.8	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	Restrictions during CREEP Mode	C	• [SG_001]	TOSCo Controller	Transition to STOPPED	• [E303]	

Table 22. Safety Requirements for Propulsion Commands from TOSCo Vehicle(s)

<i>ID</i>	<i>Description</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Notes</i>
TOSCO_Veh_08.1	A central arbitration control system shall process valid acceleration or deceleration values to be sent out from both the TOSCo and the CACC Controller by determining the most conservative propulsion command from each of the two longitudinal controllers.	Process valid acceleration/deceleration commands from longitudinal motion controllers	D	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	TOSCo Controller CACC Controller Vehicle Central arbitration System	NA	<ul style="list-style-type: none"> • [E369] 	
TOSCO_Veh_08.2	<p>In the case the central arbitration controller determines an invalid propulsion command from either of the two longitudinal controllers, TOSCo Feature shall be disabled and if required disable CACC operation depending on the operating scenario.</p> <p>NOTE: Invalid propulsion command includes: a) TOSCo calculates incorrect propulsion command b) CACC or TOSCo incorrectly converts optimized speed setpoint c) Incorrect selection (CACC instead of TOSCO or vice versa)</p>	Prevent unintended acceleration or deceleration command to the vehicle system	D	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	TOSCo, CACC, Central arbitration system	Disable TOSCo and if required CACC operation	<ul style="list-style-type: none"> • [E369] • [E310] • [E301] • [E300] 	

Table 23. Safety Requirements for Providing Driver Take-over Requests or Warning

<i>ID</i>	<i>Description</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated to</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Notes</i>
TOSCO_Veh_09.1	<p>The TOSCo controller shall provide independent means to warn the driver to take over in the event the TOSCo controller is unable to provide driver take over request during safety critical operating scenarios.</p> <p>NOTE: Warning notifications to the driver could include audio, vibrating seat, or vibrating steering wheel (or any other means).</p>	React to loss of take over request to driver	D	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	TOSCo Controller	Provide driver warning	<ul style="list-style-type: none"> • [E343] • [E262] 	
TOSCO_Veh_09.2	TOSCo feature shall ensure the driver is warned whenever there is a transition to Safe State due to a detected fault.	Provide Driver Warning on fault detection	B	<ul style="list-style-type: none"> • [SG_001] • [SG_002] • [SG_003] 	TOSCO Controller	Transition to Safe State (Disable TOSCo, go to ACC when a lead vehicle is present or Manual mode if no lead vehicle is present depending on the failure mode) and Provide Driver Warning.		This is a dual point fault

Requirements below are dedicated to the TOSCo Infrastructure Portion. A “safety parameter” is considered where applicable to define the criteria for design and specify necessary thresholds and values. Safety Requirements for queue length detection and determination for Infrastructure and Requirements for RTCM data and Security are not considered here as they are not safety related based on Phase 2 study.

Table 24. Safety Requirements for GPS Time Synchronization for Infrastructure

<i>ID</i>	<i>Description</i>	<i>Safety Parameter</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>Notes</i>
TOSCo_Inf_10.1	A common time source shall be utilized for all TOSCo infrastructure components within a safe threshold or margin to ensure time synchronization.		Ensure time synchronization between infrastructure components	D	[SG_001] [SG_002] [SG_003]	TIP RSU	N/A	NOTE: The infrastructure does not know the vehicle clock. The Global Navigation Satellite System (GNSS) reference time is utilized by the Infrastructure.
TOSCo_Inf_10.2	The TOSCo infrastructure system shall detect when the clock is not synchronized among the infrastructure components which can lead to inaccurate time values.	Specify detection measure	Detect incorrect time values due to Clock Failure to vehicle and incorrect synchronization between vehicle and infrastructure system	D	[SG_001] [SG_002] [SG_003]	TIP	N/A	
TOSCo_Inf_10.3	Upon detection of clock synchronization failure, the TOSCo Infrastructure System shall define the TOSCo	“Undefined” data elements	Mitigate incorrect trajectory planning by	D	[SG_001] [SG_002]	TIP RSU	Send an "undefined" value over the	

<i>ID</i>	<i>Description</i>	<i>Safety Parameter</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>Notes</i>
	Enhanced SPAT data elements as “undefined.”		vehicle due to Clock Failure		[SG_003]		Enhanced SPaT. TOSCo vehicle cannot maintain TOSCo operation and driver is notified.	

Table 25. Safety Requirements for RTCM Data and Security for Infrastructure

<i>ID</i>	<i>Description</i>	<i>Safety Parameter</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Notes</i>
TOSCo_Inf_12.1	The Infrastructure System shall determine the position correction information (RTCM) transmission validity by applying it to the infrastructure receiver before sending it to the vehicle. NOTE: Invalid Correction Data can	RTCM version Correction Position data	Detect RTCM transmission issues at vehicle level	D		RTCM generator TIP	NA	<ul style="list-style-type: none"> • [E159] • [E160] • [E161] • [E190] • [E191] • [E192] • [E212] • [E213] 	Currently the RTCM can only determine if it is receiving the data from the correction station. ASIL D possible only when

<i>ID</i>	<i>Description</i>	<i>Safety Parameter</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Notes</i>
	be considered as Loss of Data, Corrupted Data or Intermittent Transmission of data.								approaching intersection and no vehicle in front.
TOSCo_Inf_12.2	Upon detection of invalid correction information from the RTCM generator, the Infrastructure System shall not broadcast the correction data to the TOSCo Vehicle.		Prevent vehicle collision due to invalid RTCM	D		RTCM generator	Broadcast correction data as not available	<ul style="list-style-type: none"> • [E432] • [E161] • [E160] 	
TOSCo_Veh_12.3	When the TOSCo vehicle does not receive RTCM data, vehicle positioning system shall revert to WAAS corrections and evaluate positioning quality. Note: Actions to be dependent on drop range.		Prevent vehicle collision due to not broadcast of RTCM	D		OBE. TOSCo algorithm	TOSCo_Veh_0.51. and TOSCo_Veh_05.2 specify further safety mechanisms for RTCM	<ul style="list-style-type: none"> • [E433] • [E212] • [E213] 	

Table 26. Safety Requirements for Receiving SPaT Information to Infrastructure

<i>ID</i>	<i>Description</i>	<i>Safety Parameter</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated to</i>	<i>Safe State</i>	<i>FTA_Event(s)</i>	<i>Notes</i>
TOSCo_Inf_13.1	The Traffic Infrastructure Processor (TIP) of the Connected Infrastructure shall monitor loss of SPaT information provided by the Traffic Signal Controller (TSC) to detect communication issues.	Periodicity of valid SPaT within logical bounds	Detect loss of SPaT message to Infrastructure System	D	<ul style="list-style-type: none"> •[SG_001] •[SG_002] •[SG_003] 	TIP, TSC	N/A	<ul style="list-style-type: none"> • [E217] • [E162] 	
TOSCo_Inf_13.2	The TIP of the Connected Infrastructure shall verify the content of the SPaT data elements provided by the TSC to ensure the data is within reasonable and safe limits.	Reasonability of the content of the data elements (example, a range check can be performed to verify if data is reasonable).	Detect incorrect SPaT message to Infrastructure System	D	<ul style="list-style-type: none"> •[SG_001] •[SG_002] •[SG_003] 	TIP, TSC	N/A	<ul style="list-style-type: none"> • [E217] • [E163] • [E164] 	

ID	Description	Safety Parameter	Rationale	ASIL	Safety Goals	Allocated to	Safe State	FTA_Event(s)	Notes
TOSCo_Inf_13.3	If the Spat information is lost or not within reasonable and safe limits from the TSC of the Connected Infrastructure, then the SPaT information shall be sent as not available to the TOSCo vehicles.		Report Invalid SPaT into to vehicle	D	<ul style="list-style-type: none"> •[SG_001] •[SG_002] •[SG_003] 	TIP, TSC	Prevent broadcast of further Enhanced SPaT Information to the TOSCO Vehicle(s)	<ul style="list-style-type: none"> •[E164] •[E162] •[E163] •[E217] •[E331] 	
TOSCo_Inf_13.4	If the TIP from the Infrastructure system detects faults in the queue message data (wrong queue objects), then the Connected Infrastructure shall indicate that the queue and green window portions of the Enhanced SPaT message is invalid to the TOSCo vehicles.		Report Invalid queue and GW to the vehicle	D	<ul style="list-style-type: none"> •[SG_001] •[SG_002] •[SG_003] 	TIP, TSC	Prevent broadcast of further Enhanced SPaT Information to the TOSCO Vehicle(s)	<ul style="list-style-type: none"> •[E164] •[E162] •[E163] •[E217] •[E331] 	

Table 27. Safety Requirements for MAP Configuration for Infrastructure and MAP Messages Sent Between TOSCo Infrastructure and TOSCo Vehicle(s)

<i>ID</i>	<i>Description</i>	<i>Safety Parameter</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated to</i>	<i>Safe State</i>	<i>FTA Event(s)</i>	<i>Notes</i>
TOSCo_Inf_14.1	The TSC shall indicate to the RSU which MAP to broadcast to the vehicle for use.		Determine correct map to be used	D	•[SG_001] •[SG_002] •[SG_003]	MAP Configuration file TSC	N/A	• [E220] • [E156]	
TOSCo_Inf_14.2	The infrastructure operator shall verify the proper MAP creation and configuration using systematic processes.	Determine verification of MAP data	Systematic process for MAP creation	NONE		MAP Configuration file	N/A	• [E220] • [E166]	SCMS process to "certify" that the MAP data is accurate
TOSCo_Inf_14.3	The infrastructure operator shall verify the proper implementation of the created map on infrastructure using systematic processes.	Determine proper MAP implementation of the infrastructure	Systematic process for Installation of MAP on Infrastructure	NONE		MAP Configuration installation	N/A	• [E220] • [E166]	SCMS process to "certify" that the MAP data is installed correctly
TOSCo_Inf_14.4	The infrastructure operator shall routinely verify the Configured MAP data to ensure consistency with desired operation of the traffic signal and the		Systematic Maintenance and Monitoring of MAP	NONE		MAP Configuration file	N/A	• [E220] • [E166]	SCMS process to "certify" that the MAP data is accurate

<i>ID</i>	<i>Description</i>	<i>Safety Parameter</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated to</i>	<i>Safe State</i>	<i>FTA Event(s)</i>	<i>Notes</i>
	traffic signal timing plans.								
TOSCo_Inf_14.5	If the TSC doesn't indicate to the RSU which map to use at the appropriate periodic rate, then the RSU should not send any MAP data to the vehicle(s).		React and Mitigate incorrect MAP (Infrastructure Portion)	D	<ul style="list-style-type: none"> •[SG_001] •[SG_002] •[SG_003] 	RSU, MAP configuration	MAP is no longer sent to the TOSCo vehicle(s).	<ul style="list-style-type: none"> • [E166] • [E220] • [E330] • [E188] • [E189] 	The MAP Data does not cover for dynamic changes in the geography and vehicle movement (such as lane change etc.).
TOSCo_Inf_Veh_14.6	If the TOSCo Vehicle OBE stopped receiving MAP message (or never received a MAP message) from RSU when vehicle is in TOSCo Range, then TOSCo feature shall be disabled and vehicle transitions to ACC or Manual mode depending on the failure mode and operating scenario.		React and Mitigate incorrect MAP (Vehicle Portion)	D		OBE, RSU, TOSCo Algorithm	Transition to ACC when a lead vehicle is present or Manual mode if no lead vehicle is present depending on the failure mode and warn driver.	<ul style="list-style-type: none"> • [E166] • [E220] • [E330] • [E188] • [E189] 	

Table 28. Safety Requirements for Enhanced SPaT Message Generation

<i>ID</i>	<i>Description</i>	<i>Safety Parameter</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>FTA Event(s)</i>	<i>Notes</i>
TOSCo_Inf_15.1	The TIP of the Connected Infrastructure shall verify the data elements in the processing of the Enhanced SPaT generation that could lead to inability to determine Green Window.	Verify if data elements are populated Frequency of GW Accuracy of GW	Detect Failure in population of Enhanced SPaT message from Infrastructure	D	•[SG_001] •[SG_002] •[SG_003]	TIP	N/A	• [E333] • [E222]	
TOSCo_Inf_Veh_15.2	The OBE of TOSCo vehicle(s) shall verify if Enhanced SPaT message from the infrastructure is updated at defined regular intervals to ensure if the information about queue objects and green window is up to date.	Enhanced SPaT Update Interval (Age of Data)	Detect Failure in population of Enhanced SPaT message to Vehicle	D	•[SG_001] •[SG_002] •[SG_003]	OBE	N/A	• [E332] • [E222]	

Table 29. Safety Requirements for Green Window Determination at TOSCo Infrastructure and Safety Requirements for Communicating Enhanced SPaT Message to TOSCo Vehicle(s)

<i>ID</i>	<i>Description</i>	<i>Safety Parameter</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>FTA Event(s)</i>	<i>Notes</i>
TOSCo_Inf_16.1	<p>The TIP of the connected Infrastructure System shall detect incorrect or intermittently generated Green window information by performing periodic post-processing checks of the predicted and actual GW outputs.</p> <p>NOTE: Verification of the GW to satisfy the expected tolerance and threshold.</p>	Periodic Interval for post processing checks	Detect incorrect and intermittent determination of green window	D	<ul style="list-style-type: none"> •[SG_001] •[SG_002] •[SG_003] 	TIP	N/A	<ul style="list-style-type: none"> • [E204] • [E201] • [E327] 	

ID	Description	Safety Parameter	Rationale	ASIL	Safety Goals	Allocated To	Safe State	FTA Event(s)	Notes
TOSCo_Inf_16.2	If TIP of the Infrastructure system identifies an incorrect or intermittent Green Window value between the actual and predicted outputs for green window calculation, then the resultant Green Window shall be designated as invalid by TIP.		Prevent sending invalid Green window to TOSCo vehicles	D	[SG_001] •[SG_002] •[SG_003]	TIP	TIP shall populate GW Information on the Enhanced SPaT message as invalid	• [E201] • [E204] • [E327]	
TOSCo_Inf_16.3	The TIP of Infrastructure system shall detect aged or slow green window generation outside of expected periodic transmission rate design parameters.	Determine means of identifying aged data	Detect Green Window being determined less frequently (aged data)	D	[SG_001] •[SG_002] •[SG_003]	TIP	N/A	• [E229] • [E200]	
TOSCo_Inf_16.4	If the green window is determined less frequently (aged or slow), i.e., the time interval between successive green window updates is beyond an acceptable threshold, then the TIP	Acceptable threshold for successful GW updates	React to Green Window being determined less frequently (aged data)	D	•[SG_001] •[SG_002] •[SG_003]	TIP	Stop broadcasting Enhanced SPaT Messages to the TOSCo Vehicles	• [E200] • [E229]	

ID	Description	Safety Parameter	Rationale	ASIL	Safety Goals	Allocated To	Safe State	FTA Event(s)	Notes
	system shall send GW as invalid in the Enhanced SPaT messages to the TOSCo Vehicle.								
TOSCo_Inf_16.5	The TIP of the connected Infrastructure System shall utilize a Safety Monitor to detect and verify Green Window being provided more often than necessary.	Determine Safety Monitor mechanism used for detection	Detect Green Window message being generated too frequently	D	<ul style="list-style-type: none"> •[SG_001] •[SG_002] •[SG_003] 	TIP		<ul style="list-style-type: none"> • [E199] • [E184] • [E329] • [E185] • [E186] 	
TOSCo_Inf_16.6	The TIP of the connected Infrastructure System shall utilize a Safety Monitor to detect and verify for invalid Enhanced SPaT Messages. NOTE: Invalid Enhanced SPaT Message includes Incorrect / intermittent (loss) / Excessively generated.	Determine Safety Monitor mechanism used for detection	Detect Invalid Enhanced SPaT Message to the TOSCo Vehicle(s)	D	<ul style="list-style-type: none"> •[SG_001] •[SG_002] •[SG_003] 	TIP		<ul style="list-style-type: none"> • [E199] • [E184] • [E329] • [E185] • [E186] 	Another method to verify intermittent GW or Enhanced SPaT would be to frequently verify the time stamp of the Enhanced SPaT received to ensure constant updates.

ID	Description	Safety Parameter	Rationale	ASIL	Safety Goals	Allocated To	Safe State	FTA Event(s)	Notes
TOSCo_Inf_16.7	<p>If the TIP has detected Green Window being calculated too frequently or Enhanced SPaT is invalid, then the TIP shall indicate the GW info as invalid in Enhanced SPaT Message to the RSU.</p> <p>NOTE: Resource usage too high leading to communication issues.</p>	<p>Determine “too frequently” for GW</p> <p>Determine maximum Enhanced SpaT broadcast rate</p>	Prevent too many Enhanced SPaT messages or determining Green Window more often than necessary to TOSCo Vehicles	D	<ul style="list-style-type: none"> •[SG_001] •[SG_002] •[SG_003] 	TIP, RSU	Enhanced SPaT Messages shall not be sent out to TOSCo Vehicle(s)	<ul style="list-style-type: none"> • [E199] • [E184] • [E329] • [E185] • [E186] 	
TOSCo_Inf_16.8	<p>If the Green window is determined too late or is missing from the TIP of Infrastructure system, then the TIP shall indicate the GW info as invalid in Enhanced SPaT Message to the RSU.</p>	<p>Determine what constitutes “too late” for GW</p> <p>Determine periodic message strategy for “lost” messages</p>	Prevent Loss of Green Window Information from Infrastructure	D	<ul style="list-style-type: none"> •[SG_001] •[SG_002] •[SG_003] 	TIP, RSU	Stop broadcasting Enhanced SPaT Messages to the TOSCo Vehicles	<ul style="list-style-type: none"> • [E203] • [E197] • [E227] • [E182] 	
TOSCo_Inf_Veh_16.9	<p>If the TOSCo Vehicle receives an Enhanced SPaT message without green window information (does not receive Enhanced</p>		Prevent from collisions that occur due to loss of green window	D	<ul style="list-style-type: none"> •[SG_001] •[SG_002] •[SG_003] 	RSU, OBE, TOSCo Algorithm, Longitudin	Transition to ACC when a lead vehicle is present or Manual	<ul style="list-style-type: none"> • [E227] • [E203] • [E197] 	

<i>ID</i>	<i>Description</i>	<i>Safety Parameter</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated To</i>	<i>Safe State</i>	<i>FTA Event(s)</i>	<i>Notes</i>
	<p>SPaT message), then the vehicle shall transition to ACC or Manual depending on the failure mode by deactivating TOSCo.</p> <p>Note: The vehicle shall verify unknown queue and green window to determine loss of Enhanced SPaT.</p>		information from Vehicle			al control system	mode if no lead vehicle is present depending on the failure mode		

Table 30. Assumptions for External Safety Measures

<i>ID</i>	<i>Description</i>	<i>Rationale</i>	<i>ASIL</i>	<i>Safety Goals</i>	<i>Allocated to</i>	<i>Safe State</i>	<i>Notes</i>
TOSCo_Inf_Veh_17.1	The TOSCo Vehicle shall be equipped with a forward collision avoidance system (e.g., AEB system).	Availability of a Collision Avoidance System	D	[SG_001] [SG_002] [SG_003]	External Vehicle System	N/A	This is a design criterion. Not a functional requirement.

Chapter 7. Functional Safety Analysis

The objective of safety analyses is to ensure that the risk of a safety goal violation due to systematic faults or random hardware faults is sufficiently low. Safety analyses are performed at the appropriate level of abstraction during the concept and product development phases. Quantitative analysis methods predict the frequency of failures while qualitative analysis methods identify failures but do not predict the frequency of failures. Both types of analysis methods depend upon a knowledge of the relevant fault types and fault models.

To define functional safety requirements, a qualitative Fault Tree Analysis (FTA) was performed. 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.


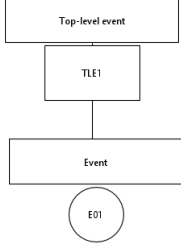
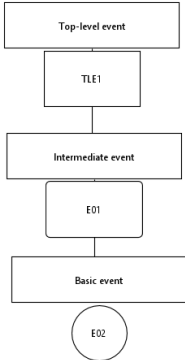



Scope of Fault Tree Analysis for TOSCo

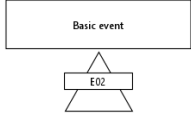
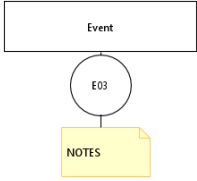
Separate fault trees are developed for each of the safety goals. Fault Tree Analysis was conducted for SG 01 *“Prevent Incorrect Excessive Acceleration due to malfunctions in TOSCo”* and then two more FTAs were performed for SG02 *“Prevent Incorrect Insufficient Deceleration due to malfunctions in TOSCo”* and SG03 *“Prevent Incorrect Excessive Deceleration due to malfunctions in TOSCo”* based on the results from SG01. The malfunctions from the Hazard Analysis were used as the primary inputs to identify failure events for the Fault Tree for both the Vehicle System and the Infrastructure System. Safety Measures for mitigating each of the failure events were also documented throughout the fault tree development process.

The fault tree analysis was performed using Medini Analyze software. Excerpts from the Fault Tree Analysis and relevant event pages from Medini Analyze for SG01 along with the chain of failure events from the top events (vehicle hazard), to the basic events (individual failure mode) are provided in the report.

The notations used for FTA are note in Table 25 and Table 26.

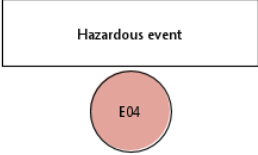
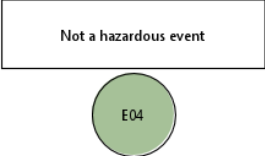

Table 31. Notations Used for Fault Tree Analysis

Notation type	Notation	Description
Basic Event		<p>A circle (at the bottom of description of event) represents a basic event.</p> <p>It occurs at the lowest level of the FTA. This basic event cannot be (or is not) divided further. This is typically a fault of a given mode.</p> <p>The number in the circle represents the event number.</p>
Top-level Event		<p>The top-most event in a fault tree, indicating a failure of a sub-system or system. It can be caused by a combination of basic events and/or intermediate events.</p>
Intermediate Event		<p>A rectangle (below the description) represents in intermediate event. It can occur if a certain combination of underlying events occurs.</p>
AND gate		<p>This shape represents an AND gate. When all events below the AND gate occur, then the event above the AND gate occurs.</p>
OR gate		<p>This shape represents an OR gate. When any one of the events below the OR gate occur, then the event above the OR gate occurs.</p>
NOT gate		<p>This shape represents a NOT gate. When the event given as input to NOT gate does not occur, then the event above the NOT gate occurs.</p>

Notation type	Notation	Description
Transfer gate		The triangle (at the bottom of description) represents a transfer gate. An event represented with transfer gate implies there is a presence of a sub-tree and a transfer to that sub-tree.
Notes		Notes provide explanation or comments made for an event

The color notations used for events are as follows:

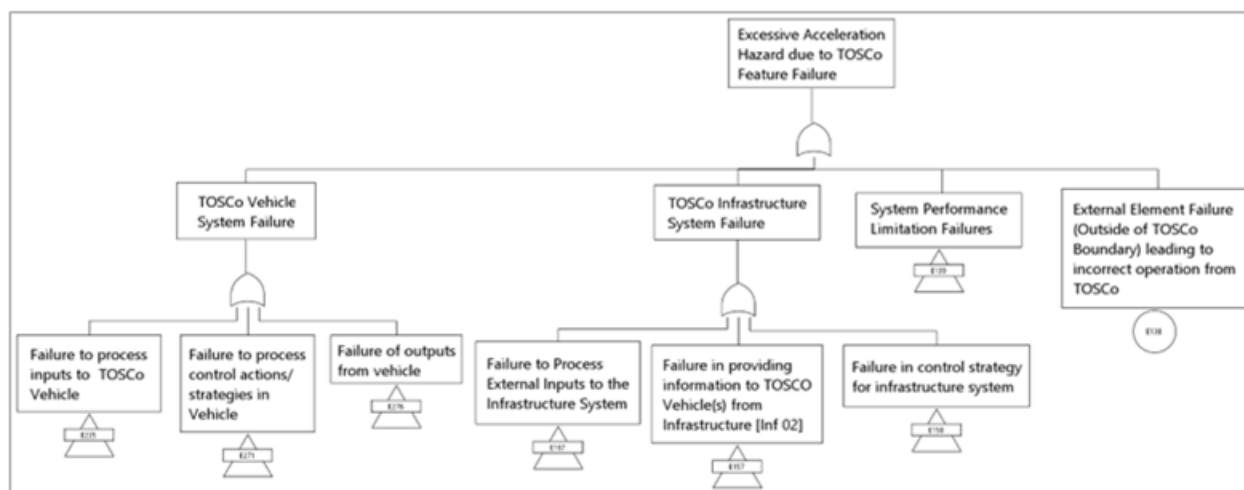
Table 32. Colored Notations used in Fault Trees

Color Notation	Description
	The red color code is used to denote an event that can result in a hazard and can compromise the safety.
	The green color code is used to denote an event that does not result in a hazard. However, it can represent a reliability concern.
	The blue color code is used to denote a safety mechanism, which is used to mitigate or reduce the risk.

Development of FTA

For TOSCo system to construct an FTA, the followings steps were performed:

1. Define top-level events for FTA. In the case of TOSCo system, the top-level events are the vehicle-level hazards that are identified from the Hazard Analysis and Risk Assessment. Because insufficient acceleration is a hazard of ASIL level QM, an FTA was not constructed for it.
2. For each top-level event (one for each safety goal), the sources of failure modes from the TOSCo Infrastructure system and TOSCo vehicle(s) were identified. Additional sources of failures regarding Safety of the Intended Functionality (SOTIF) and external elements outside TOSCo system have been considered (such as vehicle powertrain control system, braking control system) that may impact TOSCo behavior but not evaluated in detail. The FTA only focused on the EE malfunctions and failure modes of the TOSCo Feature that violated functional safety as per ISO 26262. Figure 10 shows the fault tree with higher-level events.



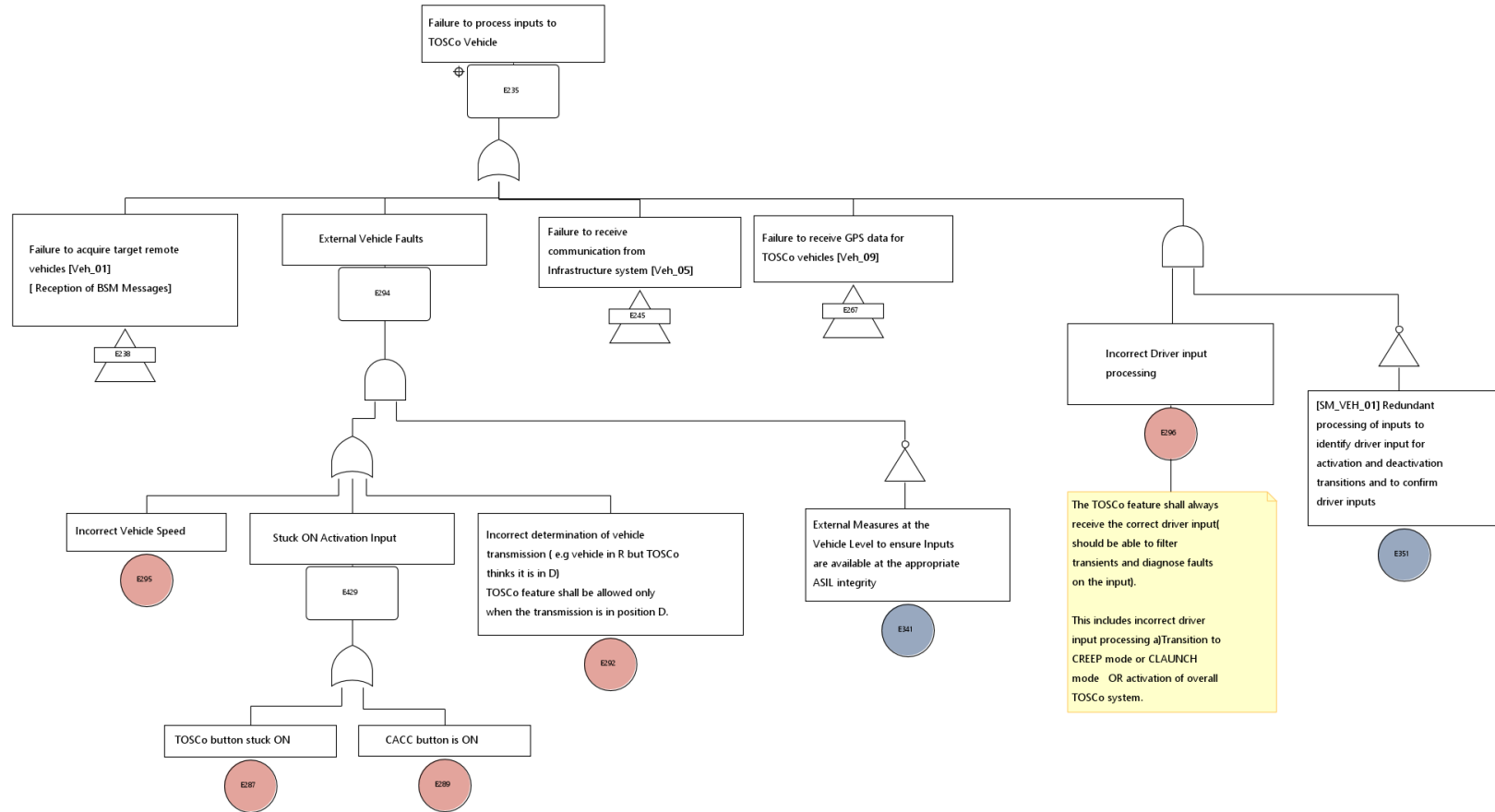
Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle to Infrastructure (V2I) Consortium, 2022

Figure 10. Top-level FTA Events for the Excessive Acceleration Hazard of the TOSCo System

3. For TOSCo Vehicle and TOSCo Infrastructure system, failure events with respect to input processing, control logic and output behavior were considered for the intermediate level events of the fault tree.
4. The intermediate events were further broken down to the malfunctions and repeated the process until the events cannot be broken down further.
5. After this process, by discussion with stakeholders, safety mechanism was proposed for each failure event and merged into existing fault trees.
6. A concise Fault Tree Analysis was performed for SG02 and SG03 based on the results of the Fault Tree Analysis for SG01.

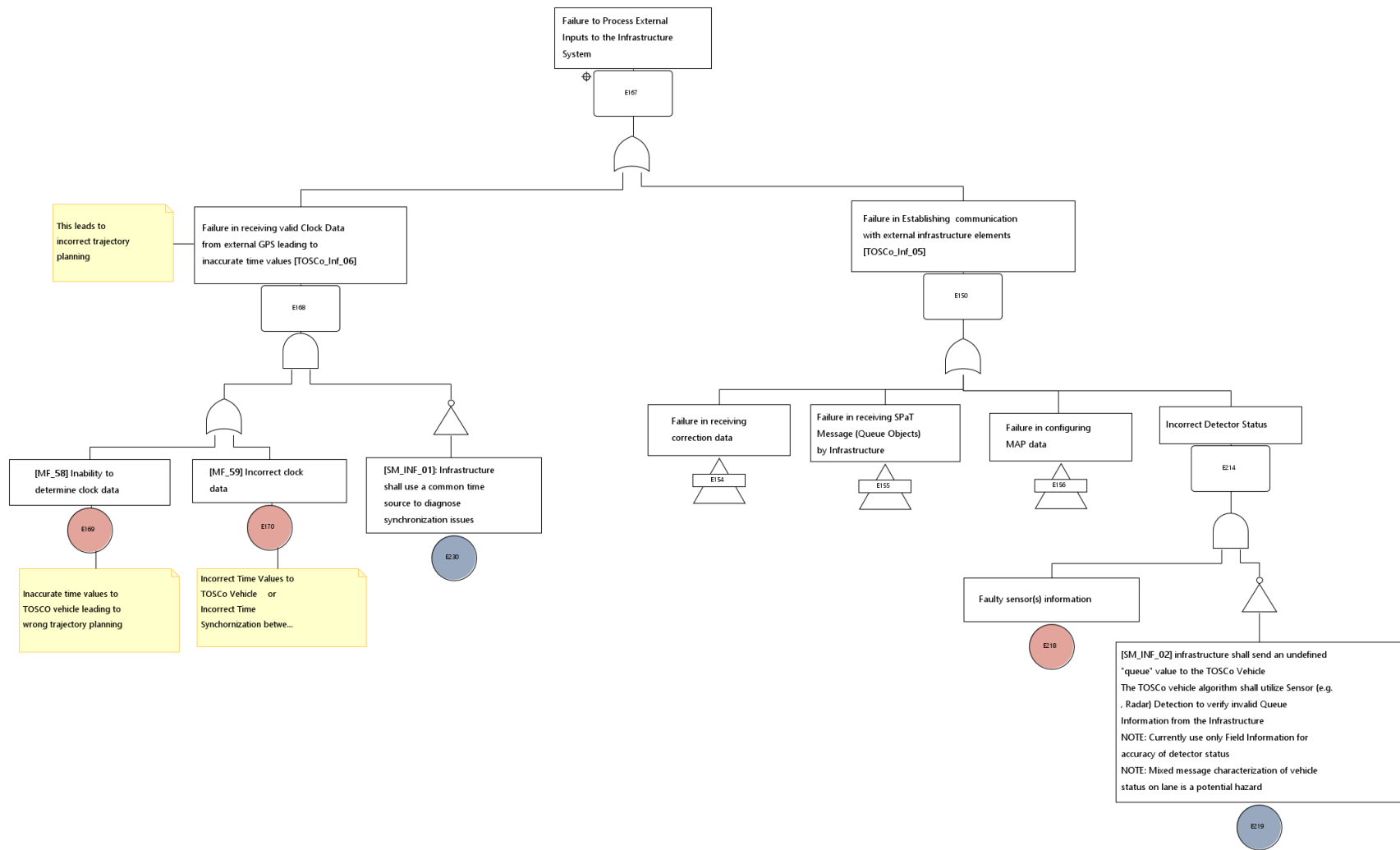
NOTE: The FTA figures below constitute the fault tree structure for SG01 “Prevent Excessive Acceleration” and represent some of the high-level events of the analysis.

A) Input Processing Failures (E01)



Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle to Infrastructure (V2I) Consortium, 2022

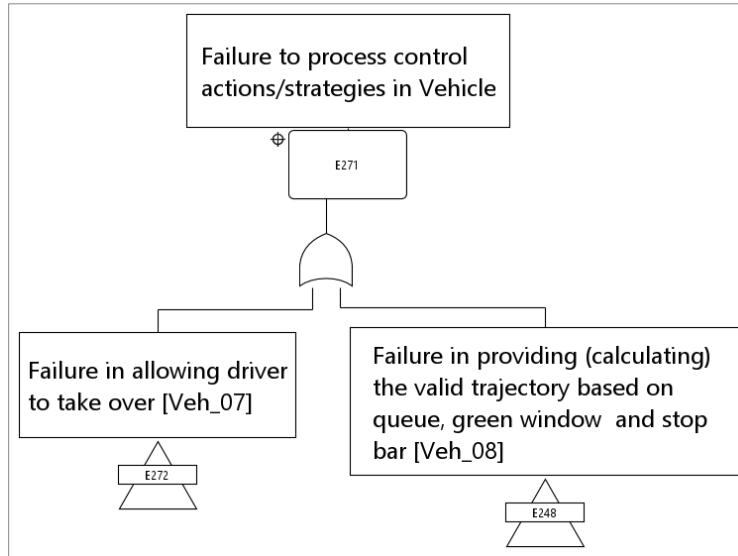
Figure 11. Input Processing Failures for TOSCo Vehicle



Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle to Infrastructure (V2I) Consortium, 2022

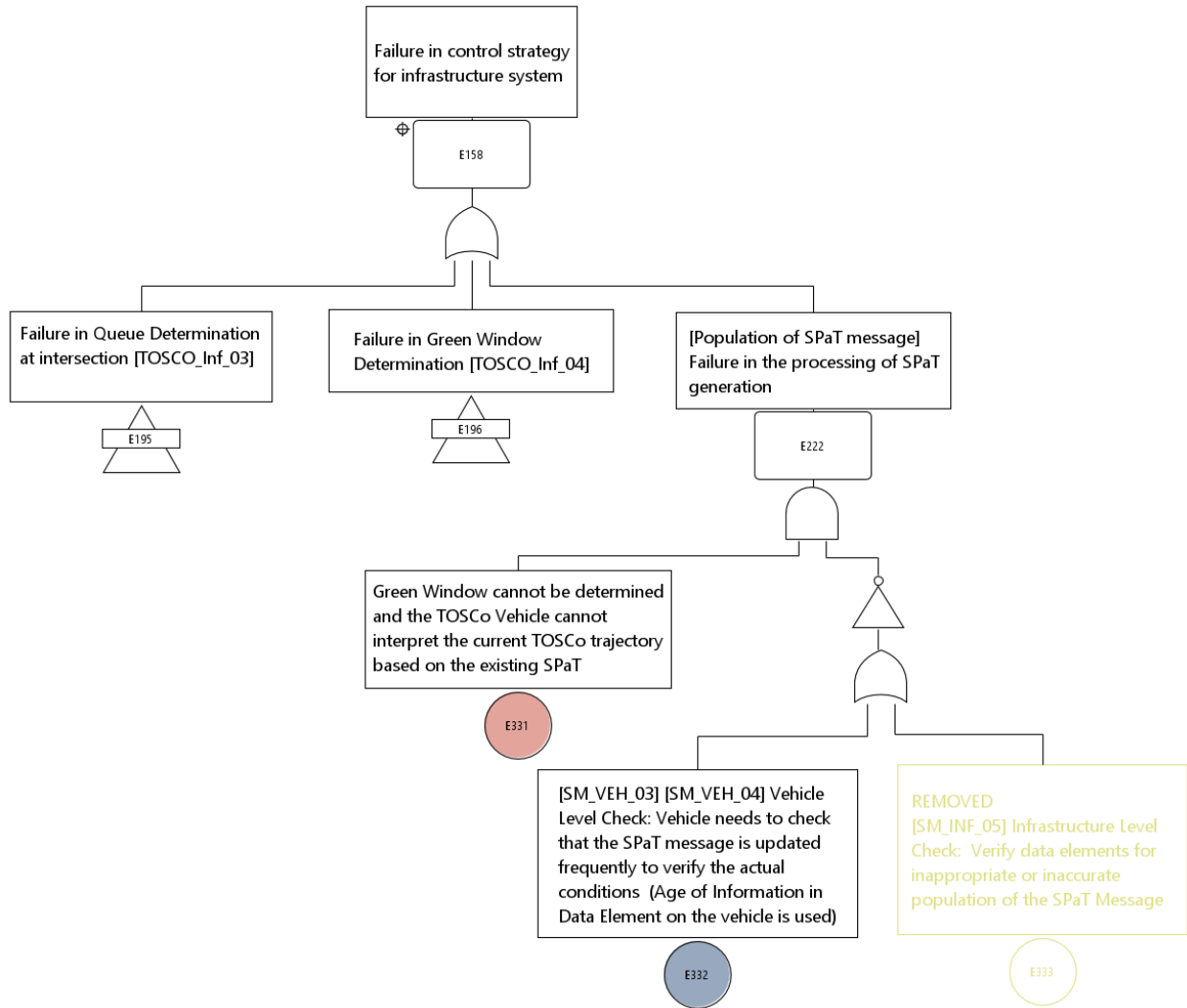
Figure 12. Input Processing Failures for TOSCo Infrastructure

B) Control Strategy Failures



Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle to Infrastructure (V2I) Consortium, 2022

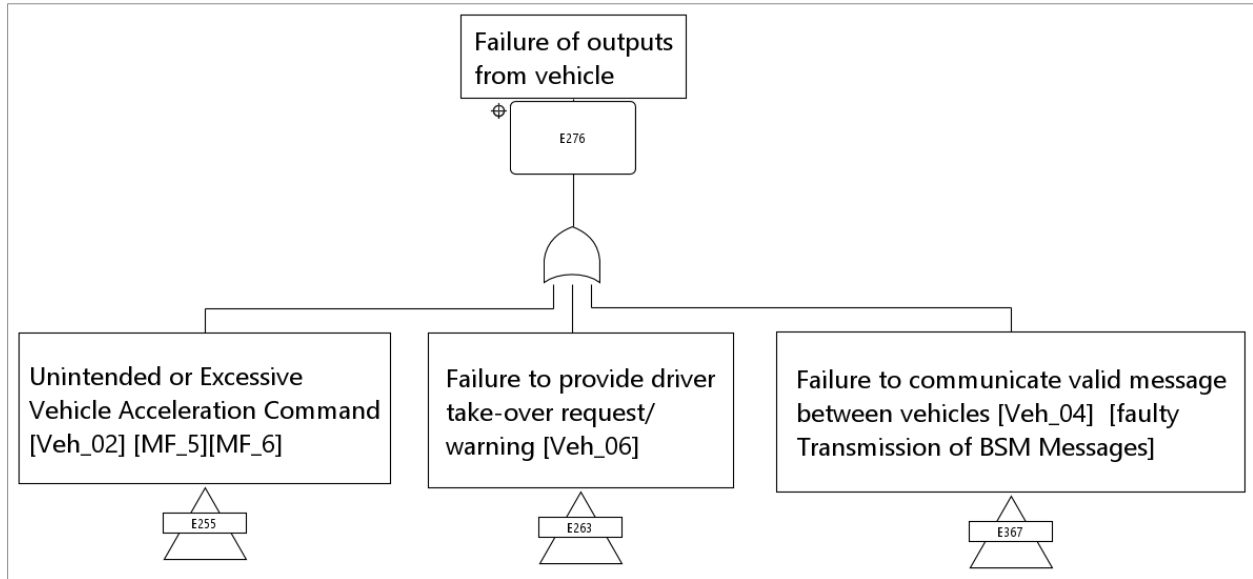
Figure 13. Control Strategy Failures in TOSCo Vehicle



Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle to Infrastructure (V2I) Consortium, 2022

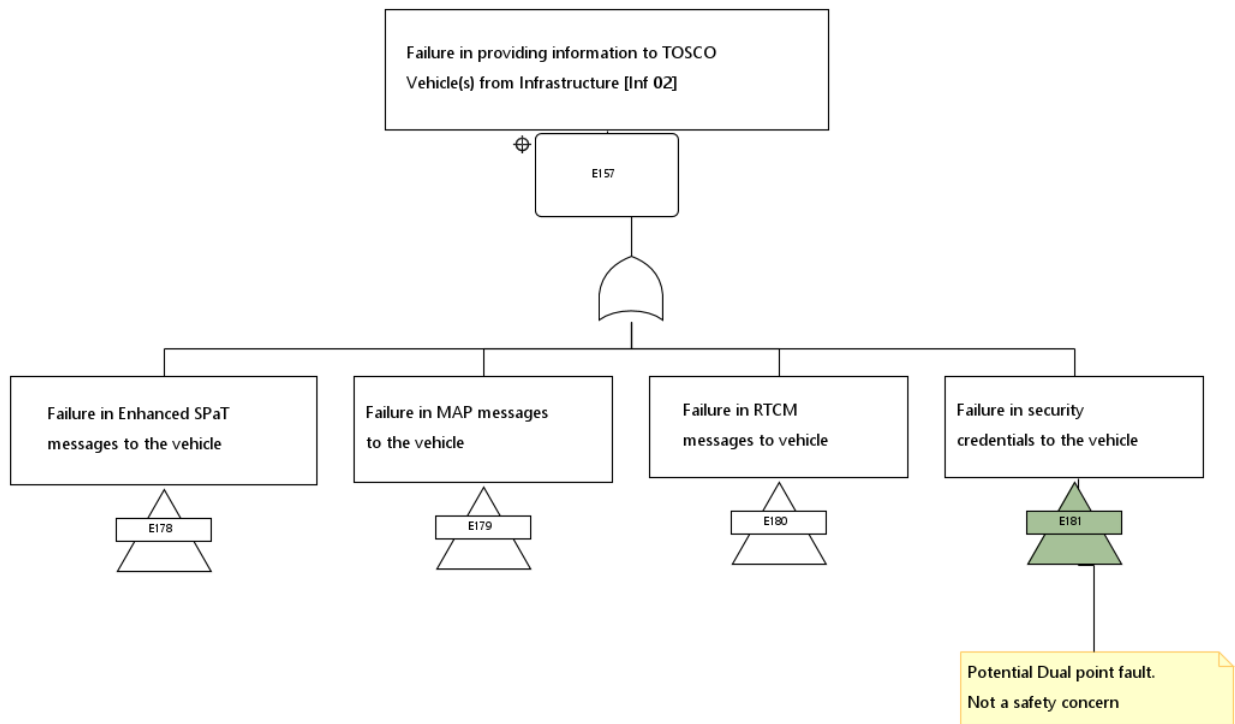
Figure 14. Control Strategy Failures in TOSCo Infrastructure

C) Output Strategy Failures



Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle to Infrastructure (V2I) Consortium, 2022

Figure 15. Output Strategy Failures in TOSCo Vehicle



Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle to Infrastructure (V2I) Consortium, 2022

Figure 16. Output Strategy Failures in TOSCo Vehicle

D) Complete FTA

The complete fault tree for the excessive acceleration hazard is obtained by expanding the fault tree segments illustrated in Figure 11 through Figure 16. Figure 10 is the top of the fault tree. To obtain a complete fault tree for the entire TOSCo feature, the same approach was utilized to obtain fault trees for each of the three remaining hazards.

The transfer gates from each of the figures below point to other sub trees where the events represent the failure modes for individual safety related functionalities of both the TOSCo Vehicle and the Infrastructure. Safety measures and diagnostic coverages that can be implemented in the system design to mitigate such failure modes are documented and can be found in the Fault Tree Report. Fault Tree Analysis for SG 02 and SG 03 hazards can also be found in the Fault Tree Report.

Findings from the FTA

The following are the findings from the Fault Tree Analysis:

- The safety measures identified to mitigate specific safety critical failure modes for both the vehicle and the infrastructure do not specify a physical architecture or solution on a component to achieve diagnostics, rather a methodology is proposed to identify the safety parameters for each failure modes and a design independent strategy is documented as a mitigation measure. The vehicle integrators would use these recommendations to determine their own architectures and safety solutions as per the relevant ASIL criteria.
- In case of driver confirmation, it was identified that separate sub fault trees need to be developed for the following:
 - Events towards faulty activation of CLaunch or CREEP
 - Events towards unintended activation of the TOSCo System.
- The Safe State allocated for various failure modes needs to be evaluated with respect to the underlying TOSCo vehicle scenario as well to understand whether the vehicle needs to transition to Free Flow (CACC), Manual Mode (Transition to Driver) or ACC (expect other collision avoidance systems to mitigate hazards). A study to evaluate these use cases by the vehicle integrator would support determining valid safe states.
- In certain cases, if the TOSCo vehicle is unable to transition to Safe State, it is expected that the driver is still informed or warned to ensure the system is taken to some relevant emergency operation that is within driver control.
- The Fault Tree Analysis identified certain safety critical vehicle functions that are documented in the revised Item Definition. These include the following:
 - Driver inputs to TOSCo Vehicle
 - Communicate with external inputs (vehicle speed, PRNDL) to TOSCo Vehicle
 - Receive Clock Data from External GPS
- External Safety critical inputs to the TOSCo vehicle were identified as follows:
 - Vehicle Speed
 - Vehicle Transmission (PRNDL) State
 - Vehicle Gear State

- d) Accelerator Pedal or Brake Pedal Input
 - e) TOSCo Activation by the driver
- The current design does not have provision for detecting and controlling incorrect GPS faults. Hence, a safety requirement has been allocated to the HDOP measurement for GPS position to ensure the system does not exceed its tolerable thresholds of accuracy.
- Certain special scenarios were identified while evaluating failure modes of acquiring BSM Data from Target Remote Vehicle(s). It is assumed that if BSM is not available from a particular vehicle, the other vehicles in the string would re-adjust trajectory depending on their current position in the queue.
- For Safety relevant communication from the Infrastructure (MAP), the vehicle does not have the capability to determine MAP accuracy. It is dependent on the Infrastructure to send out an “undefined” or “no” data for the vehicle to transition to Safe State.
- 12. Evaluation of Correction Data for safety criticality shall be considered during Vehicle Build and Test. It should be noted that RTCM generator cannot know if the correction data is valid or not. A safety mechanism is not currently identified.
- 13. The Connected Infrastructure shall verify the data elements in the processing of the Enhanced SPaT generation by monitoring the frequency and accuracy of the Green Window that is sent out to the TOSCo Vehicles(s). This can be done through periodic Interval post processing checks, verification of aged data or using a safety monitor at the Infrastructure depending on the failure mode.

Chapter 8. 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.

A functional safety concept was developed 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 through a Fault Tree Analysis (FTA) was also performed for the overall physical system along with its external interfaces to verify the completeness and correctness of the functional safety requirements and verify the effectiveness of the safety mechanisms based on identified causes of faults and the effects of failures. The FTA also provided a complete traceability to the malfunctions of the hazard analysis and primary functions from the Item Definition.

Summary of Updates for Phase 2

Below is a summary of updates specific to Phase 2 of the project and changes and modifications that were made for the functional safety work products.

- Traffic Infrastructure Sub-system is now within scope of the TOSCo Item Boundary (including external influences on the system and communication channel with TOSCo Vehicle).
- Updated Hazard Analysis identified highest ASIL criteria as ASIL D for “Excessive Acceleration” and “Insufficient Deceleration” hazard for a specific scenario where the TOSCo Vehicle is “too close to the intersection.”
- Assumptions on infrastructure functionality (such as queue object detection, Green Window determination and their limitations) has been documented in the Hazard Analysis and Functional Safety Concept.

Summary of Safety Relevant Functionality for the Infrastructure Sub-system

- Queue detection and determination of queue by the infrastructure processor are identified to be non - safety critical and only provide enhancements and optimization to the TOSCo trajectory calculations.
- Common Time Source for Clock Synchronization shall be used by all infrastructure elements to ensure data accuracy.
- In case of SPaT determination by the infrastructure certain safety parameters have been considered to mitigate failure modes as follows:
 - Verification of Periodicity of valid SPaT within logical bounds
 - Accuracy of the content of the data elements
 - Verify if data elements are populated
- Green Window determination that does not match the expected periodic rates within tolerances result in loss of enhanced SPaT to the TOSCo Vehicle(s).
- The MAP configuration is broadcasted periodically to the TOSCo vehicle.
- No enhanced SPaT values are sent out to the TOSCo vehicle to indicate that TOSCo functionality needs to be disabled in case of identification of relevant safety critical faults (MAP, Green Window Prediction, Time Synchronization) in the infrastructure. The TOSCo vehicle shall transition to safe state based on this “undefined” value from the infrastructure.

Chapter 9. Future Actions

The following is a list of future actions:

- Safety relevant functionality of correction data (RTCM) to be reviewed after Vehicle Build and Test.
- Hazard Analysis for certain scenarios to be reviewed in the next iteration to verify the appropriate ASIL criteria (i.e., CSTOP at very low speed).
- Safety “performance” parameters with appropriate safety threshold(s)/margin(s) need to be completely identified for all functional safety requirements for test, design, and validation purposes.
- Any new failure modes identified in the next iteration will be documented in the Functional Safety Concept. Diagnostic measures or solutions to applicable failure modes also need to be reviewed in the next iteration.
- Hazardous Behavior of TOSCo due to System Performance Limitations based on Safety of the Intended Functionality (SOTIF) may be considered in the next iteration of safety analysis.
- Safe state strategy needs to be reviewed for each of the safety goals at a TOSCo vehicle level based on the updated functional architecture of the system. A review of the Hazard Analysis and the functional safety requirements shall be performed after completion of Phase 2b which would lead to dedicated safe state strategy for individual features and functionalities of the TOSCo Feature.

Chapter 10. References and Input Documents

[1] ISO 26262:2018, "Road Vehicles - Functional Safety," International Organization for Standardization, Second edition.

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

[3] Guenther, Hendrik-Joern; Williams, Richard; Yoshida, Hiroyuki; Yumak, Tuncer; Hussain, Shah; Naes, Tyler; Vijaya Kumar, Vivek; Probert, Neal; Sommerwerk, Kay; Bondarenko, Dennis; Wu, Guoyuan; Deering, Richard K.; Goudy, R., "Traffic Optimization for Signalized Corridors (TOSCo) Phase 1 Project: Vehicle System Requirements and Architecture Specification," <https://rosap.ntl.bts.gov/view/dot/50738>, 2019.

[4] Balke, Kevin N.; Florence, David H.; Feng, Yiheng; LeBlanc, David J.; Wu, Guoyuan; Guenther, Hendrik-Joern; Probert, Neal; Vijaya Kumar, Vivek; Williams, Richard; Yoshida, Hiroyuki; Yumak, Tuncer; Deering, Richard K.; Goudy, R., "Traffic Optimization for Signalized Corridors (TOSCo) Infrastructure System Requirements and Architecture Specification," <https://rosap.ntl.bts.gov/view/dot/50739>, 2019.

APPENDIX A. 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.

Exposure

Exposure to a vehicle operational situation is based on one of the five levels as shown in Table 27 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 33. 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

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 28 below.

Table 34. 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

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 to avoid harm is made. The controllability of a hazardous event is assigned to one of four levels as shown in Table 29 below.

Table 35. 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 C

APPENDIX B. Risk Mitigation for On-road Testing

A Risk Mitigation Strategy was implemented during TOSCo Phase 2 system testing to mitigate potential TOSCo failures in the situation where the vehicle is approaching an intersection during a red signal phase with no queue present and the vehicle is 'too close' to the stop bar for the driver to intervene and bring the vehicle to a stop before entering the intersection. This condition was identified as an ASIL D risk during the TOSCo functional safety analysis. This mitigation strategy implemented is not intended as a recommendation for production vehicles. It relies on trained driver(s)^[1] assessing the state of health of the TOSCo system during red light approaches when prompted by an electronically independent warning system at a speed / distance from the stop bar where the kinematics of the situation are still controllable as described below.

Risk Mitigation Approach

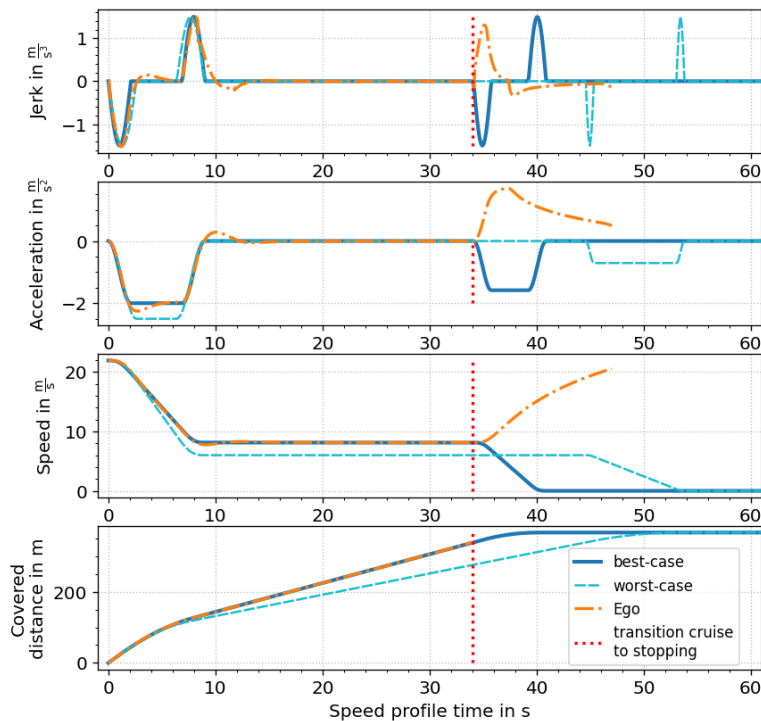
There are two key requirements needed for a trained driver to mitigate the risk of a TOSCo system failure while approaching a red light with no queue present:

- The approach trajectory must be consistent from intersection to intersection, so the driver can recognize deviations, and controllable, so driver intervention does not disturb surrounding traffic.
- An independent warning system separate from TOSCo must provide an indication to the driver at the point during the approach when evaluation of TOSCo behavior is needed to assess the system state of health.

To achieve the first element, a 'virtual stop bar' is introduced into the approach speed profile calculation upstream of the physical stop bar (which is painted on the road and defined in the MAP message). The TOSCo vehicle calculates a CSC approach profile to arrive at the virtual stop bar at the point in time when the signal head is expected to turn green. This position is dynamically adjusted depending on the CSC approach cruise speed so that a CSTOP profile from this virtual stop bar position would bring the vehicle to a stop in front of the physical stop bar in case the transition to green does not happen as expected. If the signal does transition to green as expected, then the CSTOP profile is discarded, and a new CSC-UP profile is implemented to accelerate the vehicle through the intersection.

Figure 17 illustrates the intended CSC approach profile from vehicle level simulation. As the vehicle approaches the red light it executes a CSC-DOWN profile to lower its approach speed at the virtual stop bar and extends this to plan a CSTOP at the stop bar in case the light doesn't change as expected. In this simulation the signal changes to green at the 34 second mark, as indicated by the vertical dashed red line, and the vehicle recalculates a CSC-UP solution which it then follows, discarding the CSTOP.

^[1] For the purposes of TOSCo testing a 'trained' driver is defined as an individual who has completed the equivalent of SAE level 2 driver training (DL2 as defined in SAE J3300_202005) for the purpose of operating non-production automated vehicles in a controlled manner under non-limit handling conditions.



Source: Crash Avoidance Metrics Partners LLC (CAMP) Vehicle to Infrastructure (V2I) Consortium, 2022

Figure 17 – Risk Mitigation Speed Profile Approaching a Red Light

The second element is attained using an independent electronic device dubbed a ‘virtual cone’ located inside the vehicle which issues an audible tone to alert the trained driver when the vehicle is 90 m away from the stop bar, having slowed to a speed of 35 mph (56.3 km/h). The parameters of 90 m and 35 mph (maximum speed) are derived from a traffic engineering perspective to ensure that the driver can bring the vehicle to a full stop without having to introduce an emergency braking maneuver. The virtual cone utilizes real time GNSS location information about the vehicle and compares this to a set of fixed alert points established for each of the intersections along the corridor to know when to issue the driver alert.

When hearing this notification, the trained driver checks to see if:

- The signal head is now green and the TOSCo vehicle is speeding up under CSC-UP control
- The signal head remains red and the TOSCo vehicle is slowing down under CSC-DOWN control or stopping under CSTOP control

If neither of these two conditions are true, a system fault is likely and the trained driver takes over longitudinal control of the vehicle overriding (accelerator pedal) or disengaging (brake pedal) TOSCo as appropriate.

Impact on Functional Safety

The acoustic notification and reduction of TOSCo operating domain during safety critical malfunctions act as an external safety measure to reduce risk from TOSCo vehicle malfunctions when entering an intersection. The overall functional safety risk for TOSCo is still rated at ASIL D as the same hazardous behavior exists during TOSCo malfunctions. However introduction and implementation of this additional safety measure

ensures that the overall risk can be controlled and avoided for all operating conditions during on-road testing using trained drivers.

APPENDIX C. Traceability of TOSCo Functions, Hazards and Scenarios

Table 30 below provides a traceability of all item functions for the TOSCo Feature with respect to the major driving scenarios from the HARA and the associated hazard and ASIL. This is a concise version of the hazard analysis and provides the ability to link safety functions and their applicable safety requirements to the applicable driving scenarios. The highest ASIL identified for each function from the table below would be allocated the same Safety Goal and ASIL to all its applicable functional safety requirements. For example, All FSRs under “Requirements for driver confirmation to TOSCo Vehicle” would be allocated ASIL C with safety Goal “Prevent Excessive Acceleration.”

This prevents over design of certain functionality with respect to functional safety, and restricts the development strategy only to the applicable level of safety for that function (a failure of a certain function maybe less severe or more controllable compared to a different safety critical function). Applying ASIL D safety criteria universally to all components of the TOSCo Feature could lead to unnecessary complexity of the system.

NOTE: The highest ASIL applicable for each Item Function is indicated in bold underline text in Table 31.

Table 36: Traceability with Item Function, Hazard and ASIL

FSR Table (Section ID)	Item Function (based on Item Definition)	TOSCo Driving Scenarios	Hazard	ASIL
1. Requirements for Driver Confirmation to TOSCo Vehicle:	Driver Confirmation to TOSCo Vehicle	Vehicle decelerating to stop or already stopped (no queue)	Excessive Accel	C
2. Requirements for Communication with External Vehicle Inputs:	Communication with External Vehicle Inputs	Vehicle decelerating to stop or already stopped (No queue)		B
		Vehicles decelerating to stop (static queue or growing queue)		C
		Vehicles accelerating to leave queue (dissipating queue)		C
		No vehicle in the front (No queue) (Too close to the intersection)		D
2. Requirements for Communication with External Vehicle Inputs:	Communication with external Vehicle Inputs	No vehicle in the front (No queue)	All Hazards	B

FSR Table (Section ID)	Item Function (based on Item Definition)	TOSCo Driving Scenarios	Hazard	ASIL
3. Safety Requirements for Communication with Remote Vehicles:	Acquire Target Remote Vehicle(s)	No vehicle in the front (No queue) (Too close to the intersection)		QM
		Vehicles accelerating to leave queue (dissipating queue)		B
		Vehicles decelerating to stop (static queue or growing queue)		C
		Vehicle decelerating to stop or already stopped (no queue)		C
3. Safety Requirements for Communication with Remote Vehicles:	Acquire Target Remote Vehicle(s)	No vehicle in the front (No queue)	All Hazards	QM
8. Safety Requirements for Propulsion Commands from TOSCo Vehicle(s):	Provide Acceleration Commands	Vehicle decelerating to stop or already stopped (no queue)		B
		Vehicles decelerating to stop (static queue or growing queue)		C
		Vehicles accelerating to leave queue (dissipating queue)		C
		No vehicle in the front (No queue) (Too close to the intersection)		D
8. Safety Requirements for Propulsion Commands from TOSCo Vehicle(s):	Provide Acceleration Command	No vehicle in the front (No queue)	Excessive Accel	B
8. Safety Requirements for Propulsion Commands from TOSCo Vehicle(s):	Provide Acceleration Commands	No vehicle in the front (No queue) (Too close to the intersection)		QM
		Vehicles decelerating to stop (static queue or growing queue)		QM
		Vehicles accelerating to leave queue (dissipating queue)		QM
		Vehicle decelerating to stop or already stopped (No queue)		QM

FSR Table (Section ID)	Item Function (based on Item Definition)	TOSCo Driving Scenarios	Hazard	ASIL
8. Safety Requirements for Propulsion Commands from TOSCo Vehicle(s):	Provide Acceleration Commands	No vehicle in the front (No Queue)	Insufficient Acceleration	QM
8. Safety Requirements for Propulsion Commands from TOSCo Vehicle(s):	Provide Deceleration Commands	Vehicles accelerating to leave queue (dissipating queue) Vehicles decelerating to stop (static queue or growing queue) Vehicle decelerating to stop or already stopped (no queue) No vehicle in the front (No queue) (Too close to the intersection)		B C C D
8. Safety Requirements for Propulsion commands from TOSCo Vehicle(s):	Provide Deceleration Commands	No vehicle in the front (No queue)	Insufficient Deceleration	B
8. Safety Requirements for Propulsion Commands from TOSCo Vehicle(s):	Provide Deceleration Commands	No vehicle in the front (No queue) (Too close to the intersection) Vehicles decelerating to stop (static queue or growing queue) Vehicles accelerating to leave queue (dissipating queue) Vehicle decelerating to stop or already stopped (no queue)		B None None None
8. Safety Requirements for Propulsion Commands from TOSCo Vehicle(s):	Provide Deceleration Commands	No vehicle in the front (No queue)	Excessive Deceleration	B
3. Safety Requirements for Communication with Remote Vehicles:	Communicate with other Remote Vehicles	No vehicle in the front (No queue) (Too close to the intersection) Vehicles accelerating to leave queue (dissipating queue) Vehicles decelerating to stop (static queue or growing queue)		QM B C

FSR Table (Section ID)	Item Function (based on Item Definition)	TOSCo Driving Scenarios	Hazard	ASIL
		Vehicle decelerating to stop or already stopped (no queue)		C
3. Safety Requirements for Communication with Remote Vehicles:	Communicate with other Remote Vehicles	No vehicle in the front (No queue)	All Hazards	QM
4. Safety Requirements for Receiving Communication from Infrastructure (Enhanced SPaT and MAP):	Communicate with Infrastructure	Vehicles accelerating to leave queue (dissipating queue) Vehicles decelerating to stop (static queue or growing queue) Vehicle decelerating to stop or already stopped (no queue) No vehicle in the front (No queue) (Too close to the intersection)		B C C D
4. Safety Requirements for Receiving Communication from Infrastructure (Enhanced SPaT and MAP):	Communicate with Infrastructure	No vehicle in the front (No queue)	All Hazards	B
9. Safety Requirements for Providing Driver Take-over Requests or Warning:	Provide Driver Take-over Request/ Warning	Vehicles accelerating to leave queue (dissipating queue) Vehicle decelerating to stop or already stopped (no queue) Vehicles decelerating to stop (static queue or growing queue) No vehicle in the front (No queue) (Too close to the intersection)		B C C D
9. Safety Requirements for Providing Driver Take-over Requests or Warning:	Provide Driver Take-over Request/ Warning	No vehicle in the front (No queue)	All Hazards	B
6. Safety Requirements for	Allow Driver Take-over	Vehicles accelerating to leave queue (dissipating queue)		B

FSR Table (Section ID)	Item Function (based on Item Definition)	TOSCo Driving Scenarios	Hazard	ASIL
Driver Take over from TOSCo:		Vehicle decelerating to stop or already stopped (no queue) Vehicles decelerating to stop (static queue or growing queue) No vehicle in the front (No queue) (Too close to the intersection)		C C D
6. Safety Requirements for Driver Take-over from TOSCo:	Allow Driver Take-over	No vehicle in the front (No queue)	All Hazards	B
7. Safety Requirements for Valid Trajectory Calculation for TOSCo Vehicles:	Provide the Trajectory based on Queue, Green Window, and Stop Bar	No vehicle in the front (No queue) Vehicles accelerating to leave queue (dissipating queue) Vehicle decelerating to stop or already stopped (no queue) No vehicle in the front (No queue) (Too close to the intersection)		B B C D
7. Safety Requirements for Valid Trajectory Calculation for TOSCo Vehicles:	Provide the Trajectory Based on Queue, Green Window, and Stop Bar	Vehicles decelerating to stop (static queue or growing queue)	All Hazards	C
5. Safety Requirements for GPS Reception for TOSCo Vehicles:	Receive GPS Data for TOSCo Vehicle (s)	No vehicle in the front (No queue) Vehicles accelerating to leave queue (dissipating queue) Vehicle decelerating to stop or already stopped (no queue)		B B C
5. Safety Requirements for GPS reception for TOSCo Vehicles:	Receive GPS Data for TOSCo Vehicle (s)	Vehicles decelerating to stop (static queue or growing queue)	Excessive Vehicle Deceleration	C
5. Safety Requirements for GPS reception for TOSCo Vehicles:	Receive GPS Data for TOSCo Vehicle (s)	No vehicle in the front (No queue) (Too close to the intersection)	Excessive Vehicle Acceleration	D
16. Safety Requirements for	Provide Information to	No vehicle in the front (No queue)		B

FSR Table (Section ID)	Item Function (based on Item Definition)	TOSCo Driving Scenarios	Hazard	ASIL
Communicating Enhanced SPaT Message to TOSCo Vehicle(s):	TOSCo Vehicle(s) (Enhanced SPaT)	Vehicles accelerating to leave queue (dissipating queue) Vehicle decelerating to stop or already stopped (no queue) No vehicle in the front (No queue) (Too close to the intersection)		B C D
16. Safety Requirements for Communicating Enhanced SPaT Message to TOSCo Vehicle(s):	Provide Information to TOSCo Vehicle(s) (Enhanced SPaT)	Vehicles decelerating to stop (static queue or growing queue)	All Hazards	C
14. Safety Requirements for MAP Messages Sent between TOSCo Infrastructure and TOSCo Vehicle(s):	Provide Information to TOSCo Vehicle(s) (MAP)	No vehicle in the front (No queue) Vehicles accelerating to leave queue (dissipating queue) Vehicle decelerating to stop or already stopped (no queue) No vehicle in the front (No queue) (Too close to the intersection)		B B C D
14. Safety Requirements for MAP Messages Sent between TOSCo Infrastructure and TOSCo Vehicle(s):	Provide Information to TOSCo Vehicle(s) (MAP)	Vehicles decelerating to stop (static queue or growing queue)	All Hazards	C
12. Safety Requirements for RTCM data and Security for Infrastructure:	Provide information to TOSCo Vehicle(s) (RTCM)	No vehicle in the front (No queue) Vehicles accelerating to leave queue (dissipating queue) Vehicles decelerating to stop (static queue or growing queue) Vehicle decelerating to stop or already stopped (no queue)		B B C C
12. Safety Requirements for RTCM data and Security for Infrastructure:	Provide Information to TOSCo Vehicle(s) (RTCM)	No vehicle in the front (No queue) (Too close to the intersection)	All Hazards	D

FSR Table (Section ID)	Item Function (based on Item Definition)	TOSCo Driving Scenarios	Hazard	ASIL
11. Safety Requirements for Queue Length Detection and Determination for Infrastructure:	Determine the Queue at the Intersection	No vehicle in the front (No queue)		QM
		No vehicle in the front (No queue) (Too close to the intersection)		QM
		Vehicles accelerating to leave queue (dissipating queue)		QM
		Vehicle decelerating to stop or already stopped (no queue)		QM
11. Safety Requirements for Queue Length Detection and Determination for Infrastructure:	Determine the Queue at the Intersection	Vehicles decelerating to stop (static queue or growing queue)	All hazards	QM
15. Safety Requirements for Enhanced SPaT Message Generation: 16. Safety Requirements for Green Window Determination at TOSCo Infrastructure:	Determine Green Window Prediction based on Queue Information	No vehicle in the front (No queue)		B
		Vehicles decelerating to stop (static queue or growing queue)		C
		Vehicle decelerating to stop or already stopped (no queue)		C
		No vehicle in the front (No queue) (Too close to the intersection)		D
15. Safety Requirements for Enhanced SPaT Message Generation: 16. Safety Requirements for Green Window Determination at TOSCo Infrastructure:	Determine Green Window Prediction Based on Queue Information	Vehicles accelerating to leave queue (dissipating queue)	All Hazards	B
13. Safety Requirements for Receiving SPaT Information to Infrastructure:	Establish Communication with External Infrastructure Elements -	No vehicle in the front (No queue)		B
		Vehicles accelerating to leave queue (dissipating queue)		B

FSR Table (Section ID)	Item Function (based on Item Definition)	TOSCo Driving Scenarios	Hazard	ASIL
	Receive Queue Objects	Vehicle decelerating to stop or already stopped (no queue) No vehicle in the front (No queue) (Too close to the intersection)		C D
13. Safety Requirements for Receiving SPaT Information to Infrastructure:	Establish Communication with External Infrastructure Elements - Receive Queue Objects	Vehicles decelerating to stop (static queue or growing queue)	All Hazards	C
14. Safety Requirements for MAP Configuration for Infrastructure:	Establish Communication with External Infrastructure Element- Configure MAP Data	No vehicle in the front (No queue) Vehicles accelerating to leave queue (dissipating queue) Vehicle decelerating to stop or already stopped (no queue) No vehicle in the front (No queue) (Too close to the intersection)		B B C D
14. Safety Requirements for MAP Configuration for Infrastructure:	Establish Communication with External Infrastructure Element- Configure MAP Data	Vehicles decelerating to stop (static queue or growing queue)	All Hazards	C
10. Safety Requirements for GPS Time Synchronization for Infrastructure:	Receive GPS Clock Data for TOSCo Infrastructure	Vehicles decelerating to stop (static queue or growing queue)	All Hazards	C
10. Safety Requirements for GPS Time Synchronization for Infrastructure:	Receive GPS Clock Data for TOSCo Infrastructure	No vehicle in the front (No queue) Vehicles accelerating to leave queue (dissipating queue) Vehicle decelerating to stop or already stopped (no queue) No vehicle in the front (No queue) (Too close to the intersection)		B B C D

U.S. Department of Transportation
ITS Joint Program Office – HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487

www.its.dot.gov

FHWA-JPO-22-961



U.S. Department of Transportation