Introduction

This document consists of a hazard catalog for L4 ADS vehicle operations as MaaS.
It is based on the Hazard Identification Framework presented in Figure 1.
I. System Modeling: functional breakdown and operational phase definition.
Agents: ADS vehicle, Fleet Operations Center (FOC), Maintenance Operations Center (MOC)
Operation Phases: On-route without passengers, On-route with passengers, On-route to MOC, Passenger pick-up, Passenger drop-off, Post-incident management
II. Scenario Modeling
Tools used: ESD, COTA, STPA, FTA
III. Hazard Identification. Details in Figure 2.
Identify (a) hazard scenarios, (b) risk contributors (agents), (c) failure modes/mechanisms and (e) consequences of hazard scenarios. Root cause and contributing factor analysis (d) is not included explicitly in this document.
Supporting documents: Risk Scale categorizing each consequence by severity, controllability and relative frequency. Scale from 1 (lowest risk) to 5 (highest risk).
Results: Identified 43 hazards, 19 of them are high risk (level 5).

How to read:

Page 1: Hazards List
Shows the total list of hazards identified mapped to each operational phase. Some hazards may appear in more than one operational phase and lead to different consequences.
Column A: ID number of each hazard.
Columns B-D: Hazard Scenario (format: "agent responsible" fails to "perform a task")
Columns E-L: Hazards occurring in each operational phase are marked with an 'x' on the respective column.
Column M: Highest risk level consequence associated with the hazard.

H#.#.# Hazard sheets
Each hazard is described in a separate sheet.
The sheet will provide information on the hazard scenario ("What happened?"), its failure modes ("How did it happen?") and consequences ("What does it lead to?").
It also provides insight to the agent responsible and what actions/procedures are intended to avoid the hazard ("Who failed?") .

C1:I3 **Hazard reference information: "What happened?"** (See light blue box in Figure 3).
C1:D1 Operational phases where hazard may occur.
C2:D2 ID number of the hazard.
C3:F3 Hazard Scenario (format: "agent responsible" fails to "perform a task").
F1:I3 ID numbers of ESD events, COTA tasks, STPA control loops and FTA events associated with hazard. The nomenclature used is the same as used in the supporting documents for each method.

C4:D26 **Hazard characterization: "How did it happen?"**
Column C-D:
C4:D17 a) Failure modes. Read as "[C] fails to/fails to provide [D]". Each failure mode may lead to the hazard scenario ("OR" relationship). See red box in Figure 3.

C19:D26 b) Prior failures. Read as "[C] fails to/fails to provide [D]". Each prior failure leads to a failure mode. Included to provide traceability of failure sequences. See green box in Figure 3.
E.g.: For H1.1.1 the failure mode C9:D9 "ADS [Fails to provide] Detected context (perception data) for DDT planning" may be caused by a prior failure mode C22:D22 "ADS [Fails to provide] Raw sensor data for DDT planning".

E5:E26 Column E:
Provides connection to other hazards in which the failure mode is also involved (following the sequence of events provided in the ESD). See yellow box in Figure 3.
E.g.: For H1.1.1 'ADS vehicle fails to perform the entire DDT' many failure modes trace back to H3.3.3 'MOC fails to perform inspection process correctly' or H3.3.9 'MOC fails to correctly update the vehicle'.

F4:I26 **Column F: Risk Contributors "Who failed?"**
F4:F26 Each agent is divided into functions to identify the element which contributes to the hazard (referred as sub-agents). See orange box in Figure 3.

G4:I26 Column G-I: Agent Responsible/Agent Responsibility
[G] Sub-agent responsible for avoiding the hazard.
[H] Sub-agent task
[I] Risk contributor element/function affected
The task the sub-agent is responsible of performing to avoid the hazard (format "[G] is responsible for [H] of/from [I]". See purple box in Figure 3.
The 'Agent Responsibility' is further explored in the risk mitigation measure analysis.

A28:H45 **Consequences: "What does it lead to?"**
Potential ESD end-states resulting from hazard divided per operational phase. See dark blue box in Figure 3.
For details on Controllability, Severity, Relative Frequency, Risk Level refer to Risk Scale document.

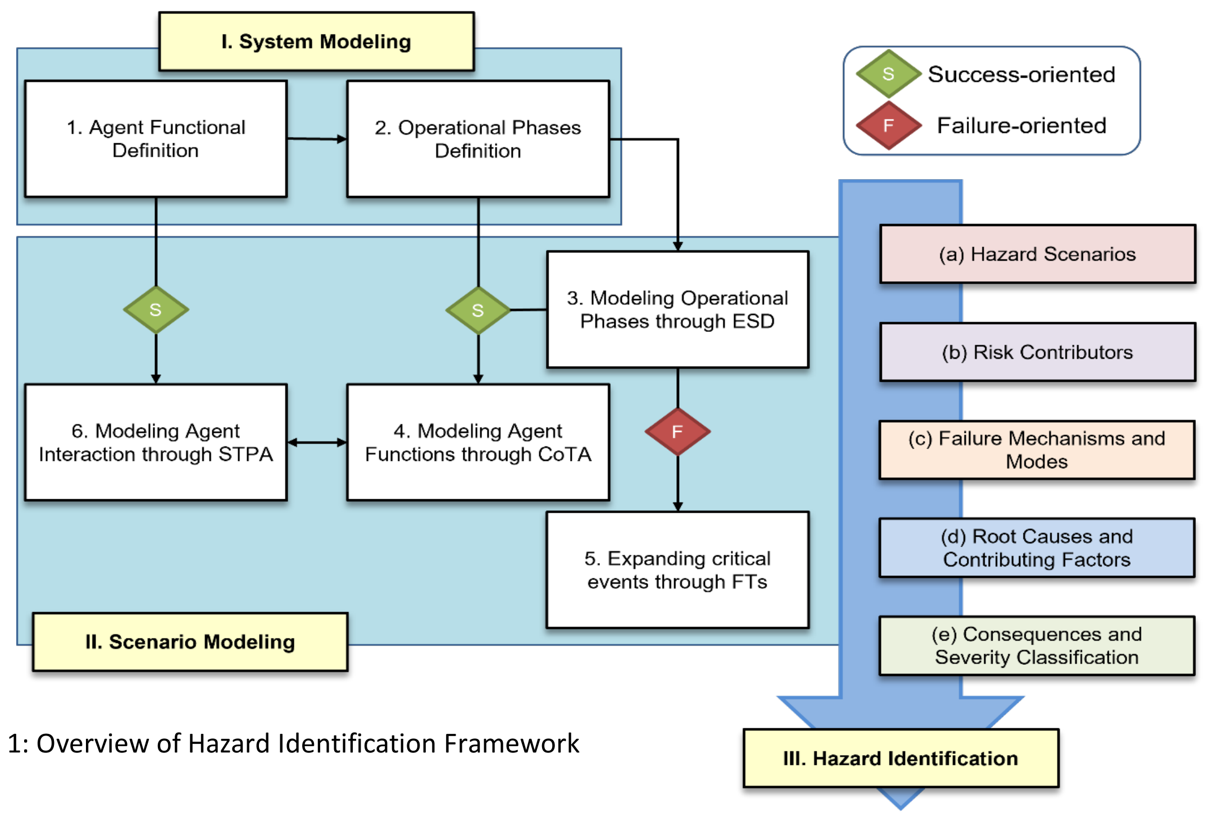

I. System Modeling
1. Agent Functional Definition
2. Operational Phases Definition
3. Modeling Operational Phases through ESD
S
S
F
6. Modeling Agent Interaction through STPA
4. Modeling Agent Functions through CoTA
5. Expanding critical events through FTs
II. Scenario Modeling
Success-oriented
Failure-oriented
(a) Hazard Scenarios
(b) Risk Contributors
(c) Failure Mechanisms and Modes
(d) Root Causes and Contributing Factors
(e) Consequences and Severity Classification
III. Hazard Identification

Figure 1: Overview of Hazard Identification Framework

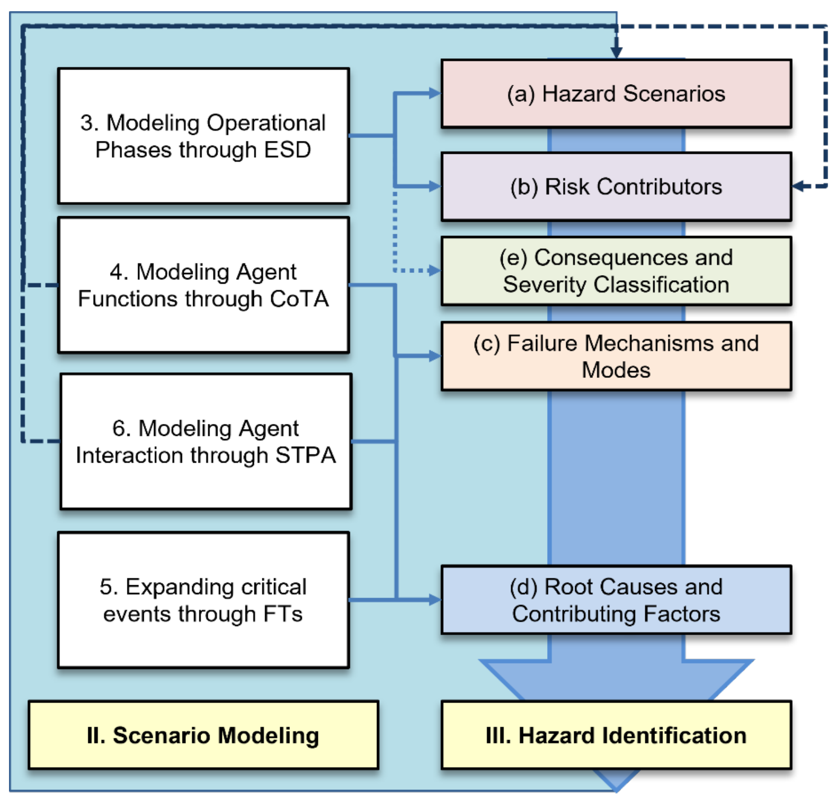
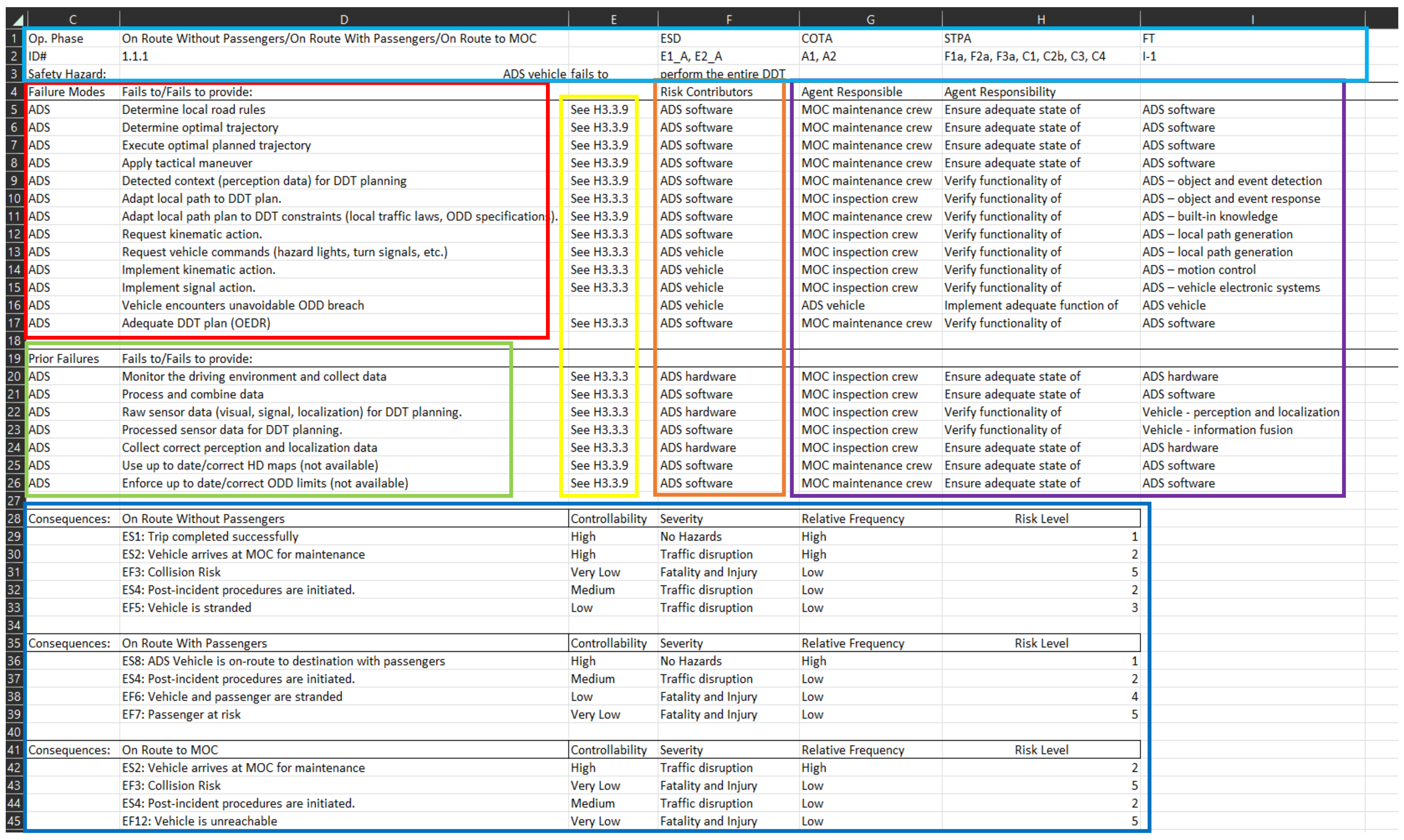

3. Modeling Operational Phases through ESD
4. Modeling Agent Functions through CoTA
6. Modeling Agent Interaction through STPA
5. Expanding critical events through FTs
(a) Hazard Scenarios
(b) Risk Contributors
(e) Consequences and Severity Classification
(c) Failure Mechanisms and Modes
(d) Root Causes and Contributing Factors
II. Scenario Modeling
III. Hazard Identification

Figure 2: Details on stage II-III of hazard identification process

Figure 3: Example of Hazard Sheet



	C	D	E	F	G	H	I
1	Op. Phase	On Route Without Passengers/On Route With Passengers/On Route to MOC		ESD	COTA	STPA	FT
2	ID#	1.1.1		E1_A, E2_A	A1, A2	F1a, F2a, F3a, C1, C2b, C3, C4	I-1
3	Safety Hazard:	ADS vehicle	fails to	perform the entire DDT			
4	Failure Modes	Fails to/Fails to provide:		Risk Contributors	Agent Responsible	Agent Responsibility	
5	ADS	Determine local road rules	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software
6	ADS	Determine optimal trajectory	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software
7	ADS	Execute optimal planned trajectory	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software
8	ADS	Apply tactical maneuver	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software
9	ADS	Detected context (perception data) for DDT planning	See H3.3.9	ADS software	MOC maintenance crew	Verify functionality of	ADS – object and event detection
10	ADS	Adapt local path to DDT plan.	See H3.3.3	ADS software	MOC inspection crew	Verify functionality of	ADS – object and event response
11	ADS	Adapt local path plan to DDT constraints (local traffic laws, ODD specifications).	See H3.3.9	ADS software	MOC maintenance crew	Verify functionality of	ADS – built-in knowledge
12	ADS	Request kinematic action.	See H3.3.3	ADS software	MOC inspection crew	Verify functionality of	ADS – local path generation
13	ADS	Request vehicle commands (hazard lights, turn signals, etc.)	See H3.3.3	ADS vehicle	MOC inspection crew	Verify functionality of	ADS – local path generation
14	ADS	Implement kinematic action.	See H3.3.3	ADS vehicle	MOC inspection crew	Verify functionality of	ADS – motion control
15	ADS	Implement signal action.	See H3.3.3	ADS vehicle	MOC inspection crew	Verify functionality of	ADS – vehicle electronic systems
16	ADS	Vehicle encounters unavoidable ODD breach		ADS vehicle	ADS vehicle	Implement adequate function of	ADS vehicle
17	ADS	Adequate DDT plan (OEDR)	See H3.3.3	ADS software	MOC maintenance crew	Verify functionality of	ADS software
18							
19	Prior Failures	Fails to/Fails to provide:					
20	ADS	Monitor the driving environment and collect data	See H3.3.3	ADS hardware	MOC inspection crew	Ensure adequate state of	ADS hardware
21	ADS	Process and combine data	See H3.3.3	ADS software	MOC inspection crew	Ensure adequate state of	ADS software
22	ADS	Raw sensor data (visual, signal, localization) for DDT planning.	See H3.3.3	ADS hardware	MOC inspection crew	Verify functionality of	Vehicle - perception and localization
23	ADS	Processed sensor data for DDT planning.	See H3.3.3	ADS software	MOC inspection crew	Verify functionality of	Vehicle - information fusion
24	ADS	Collect correct perception and localization data	See H3.3.3	ADS hardware	MOC inspection crew	Ensure adequate state of	ADS hardware
25	ADS	Use up to date/correct HD maps (not available)	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software
26	ADS	Enforce up to date/correct ODD limits (not available)	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software
27							
28	Consequences:	On Route Without Passengers	Controllability	Severity	Relative Frequency	Risk Level	
29		ES1: Trip completed successfully	High	No Hazards	High	1	
30		ES2: Vehicle arrives at MOC for maintenance	High	Traffic disruption	High	2	
31		EF3: Collision Risk	Very Low	Fatality and Injury	Low	5	
32		ES4: Post-incident procedures are initiated.	Medium	Traffic disruption	Low	2	
33		EF5: Vehicle is stranded	Low	Traffic disruption	Low	3	
34							
35	Consequences:	On Route With Passengers	Controllability	Severity	Relative Frequency	Risk Level	
36		ES8: ADS Vehicle is on-route to destination with passengers	High	No Hazards	High	1	
37		ES4: Post-incident procedures are initiated.	Medium	Traffic disruption	Low	2	
38		EF6: Vehicle and passenger are stranded	Low	Fatality and Injury	Low	4	
39		EF7: Passenger at risk	Very Low	Fatality and Injury	Low	5	
40							
41	Consequences:	On Route to MOC	Controllability	Severity	Relative Frequency	Risk Level	
42		ES2: Vehicle arrives at MOC for maintenance	High	Traffic disruption	High	2	
43		EF3: Collision Risk	Very Low	Fatality and Injury	Low	5	
44		ES4: Post-incident procedures are initiated.	Medium	Traffic disruption	Low	2	
45		EF12: Vehicle is unreachable	Very Low	Fatality and Injury	Low	5	

FOC Contributors:	**MOC Contributors:**	**ADS Contributors:**
FOC safety operator	MOC maintenance crew	ADS vehicle
FOC service operator	MOC inspection crew	ADS hardware
FOC communication	MOC coordinators	ADS software
	MOC communication	ADS communication

	C	D	E	F	G	H	I
1	Op. Phase	OPERATIONAL PHASES IN WHICH THE SAFETY HAZARD APPEARS		ESD	COTA	STPA	FT
2	ID#	ID NUMBER OF THE SAFETY HAZARD		EVENTS OF THE ESD	TASKS OF THE COTA	UCAS OF STPA	EVENTS OF THE FT
3	Safety Hazard:	NAME OF THE SAFETY HAZARD					
4							
5	Failure Modes	Fails to/Fails to provide:		Risk Contributors	Agent Responsible	Agent Responsibility	
6		LIST OF FAILURE MODES ASSOCIATED WITH THE SAFETY HAZARD	PREVIOUS HAZARD IN WHICH THIS FAILURE MODE APPEARS	RISK CONTRIBUTOR ASSOCIATED WITH THE FAILURE MODE	AGENT RESPONSIBLE FOR AVOIDING OR MITIGATING FAILURE MODE	RESPONSIBILITY OF THE AGENT FOR AVOIDING OR MITIGATIN FAILURE MODE	
7							
8							
9							
10	Prior Failures	Fails to/Fails to provide:					
11		trigger/interface tasks, control steps directly before, and "or" events in the fault trees					
12							
13	Consequences:	On Route Without Passengers	Controllability	Severity	Relative Frequency	Risk Level	
14		CONSEQUENCES FOR EACH OPERATIONAL PHASE IN WHICH THIS SAFETY HAZARD CAN OCCUR					
15							
16	Consequences:	On Route With Passengers	Controllability	Severity	Relative Frequency	Risk Level	
17							
18	Consequences:	On Route to MOC	Controllability	Severity	Relative Frequency	Risk Level	

				Operational Phase								
ID #			Hazard Scenario	On-route without passengers	On-route with passengers	On-route to MOC	Pre-shift inspection and corrective maintenance	Preventive maintenance and system updates	Passenger pick-up	Passenger drop-off	Post-incident management	Highest Risk Level
1.1.1	ADS	fails to	perform the entire DDT	x	x	x						5
1.1.2	ADS	fails to	detect DDT-fallback is required	x								5
1.1.3	ADS	fails to	perform DDT-fallback correctly	x								5
1.1.4	ADS	fails to	dispatch vehicle to MOC	x								5
1.1.5	ADS	fails to	successfully travel to MOC	x		x					x	5
1.1.6	ADS	fails to	request post-incident management procedures	x		x						3
1.2.1	FOC	fails to	detect DDT fallback is required	x								5
1.2.2	FOC	fails to	send correct DDT fallback command	x		x						5
1.2.3	FOC	fails to	dispatch vehicle to MOC	x		x					x	5
1.2.4	FOC	fails to	initiate post-incident procedures	x		x						3
2.1.1	ADS	fails to	detect DDT-fallback is required		x							5
2.1.2	ADS	fails to	perform DDT-fallback correctly		x				x	x		5
2.1.3	ADS	fails to	request post-incident management procedures		x				x	x		5
2.2.1	FOC	fails to	detect DDT fallback is required		x				x	x		5
2.2.2	FOC	fails to	send correct DDT fallback command		x				x	x		5
2.2.3	FOC	fails to	initiate post-incident procedures		x				x	x		4
2.2.4	FOC	fails to	communicate with passenger		x				x	x		5
3.2.1	FOC	fails to	schedule vehicle for inspection or corrective maintenance			x						2
3.2.2	FOC	fails to	schedule vehicle for preventive maintenance			x						2
3.2.3	FOC	fails to	locate missing vehicle			x						5
3.3.1	MOC	fails to	report missing vehicle to FOC			x						5
3.2.4	FOC	fails to	follow procedure on vehicle status				x	x				2
3.3.2	MOC	fails to	inspect vehicle				x					2
3.3.3	MOC	fails to	perform inspection correctly				x					2
3.3.4	MOC	fails to	perform maintenance at MOC				x					2
3.3.5	MOC	fails to	schedule external maintenance				x					2
3.3.6	MOC	fails to	follow procedure on vehicle status				x	x				2
3.3.7	MOC	fails to	schedule external maintenance					x				2
3.3.8	MOC	fails to	perform system updates at MOC					x				2
3.3.9	MOC	fails to	correctly perform system updates					x				2
3.3.10	MOC	fails to	inspect vehicle					x				2
3.3.11	MOC	fails to	perform service inspection correctly					x				2
3.3.12	MOC	fails to	perform preventive maintenance at MOC					x				2
4.1.1	ADS	fails to	achieve SSC for pickup/dropoff						x	x		5
4.1.2	ADS	fails to	start the trip						x			5
4.1.3	ADS	fails to	end the trip							x		5
5.2.1	FOC	fails to	confirm other road users are involved								x	4
5.2.2	FOC	fails to	contact first responders								x	4
5.2.3	FOC	fails to	report incident to MOC								x	4
5.2.4	FOC	fails to	communicate with passenger								x	4
5.2.5	FOC	fails to	dispatch secondary vehicle for passengers								x	4
5.2.6	FOC	fails to	send correct DDT fallback command								x	4
5.3.1	MOC	fails to	dispatch recovery team								x	4
											Hazards	43
											High Risk (5)	**19**

Op. Phase	On Route Without Passengers/On Route With Passengers/On Route to MOC		ESD	COTA	STPA	FT
ID#	1.1.1		E1_A, E2_A	A1, A2	F1a, F2a, F3a, C1, C2b, C3, C4	I-1
Safety Hazard:	ADS vehicle	fails to	perform the entire DDT			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
ADS	Determine local road rules	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Determine optimal trajectory	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: local path planning)
ADS	Execute optimal planned trajectory	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Apply tactical maneuver	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Detected context (perception data) for DDT planning	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Adapt local path to DDT plan	See H3.3.3	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Adapt local path plan to DDT constraints (local traffic laws, ODD specifications).	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Request kinematic action	See H3.3.3	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Request vehicle commands (hazard lights, turn signals, etc.)	See H3.3.3	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Implement kinematic action	See H3.3.3	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: motion control)
ADS	Implement signal action	See H3.3.3	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: electronic systems)
ADS	Avoid ODD breach due to external events		ADS vehicle	ADS vehicle	Implement adequate function of	ADS software (DDT: object and event detection)
ADS	Adequate DDT plan (OEDR)	See H3.3.3	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Monitor the driving environment and collect data	See H3.3.3	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Process and combine data	See H3.3.3	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Raw sensor data (visual, signal, localization) for DDT planning.	See H3.3.3	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Processed sensor data for DDT planning.	See H3.3.3	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Collect correct perception and localization data	See H3.3.3	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Use up to date/correct HD maps (not available)	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H3.3.9	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
Consequences:	On Route Without Passengers	Controllability	Severity	Relative Frequency	Risk Level	
	ES1: Trip completed successfully	High	No Hazards	High	1	
	ES2: Vehicle arrives at MOC for maintenance	High	Traffic disruption	High	2	
	EF3: Collision Risk	Very Low	Fatality and Injury	Low	5	
	ES4: Post-incident procedures are initiated.	Medium	Traffic disruption	Low	2	
	EF5: Vehicle is stranded	Low	Traffic disruption	Low	3	
Consequences:	On Route With Passengers	Controllability	Severity	Relative Frequency	Risk Level	
	ES8: ADS Vehicle is on-route to destination with passengers	High	No Hazards	High	1	
	ES4: Post-incident procedures are initiated.	Medium	Traffic disruption	Low	2	
	EF6: Vehicle and passenger are stranded	Low	Fatality and Injury	Low	4	
	EF7: Passenger at risk	Very Low	Fatality and Injury	Low	5	
Consequences:	On Route to MOC	Controllability	Severity	Relative Frequency	Risk Level	
	ES2: Vehicle arrives at MOC for maintenance	High	Traffic disruption	High	2	
	EF3: Collision Risk	Very Low	Fatality and Injury	Low	5	
	ES4: Post-incident procedures are initiated.	Medium	Traffic disruption	Low	2	
	EF12: Vehicle is unreachable	Very Low	Fatality and Injury	Low	5	

Op. Phase	On Route Without Passengers		ESD	COTA	STPA	FT
ID#	1.1.2		E1_D	A3, A5	F3a, F3b, C5a	I-1
Safety Hazard:	ADS vehicle	fails to	detect DDT-fallback is required			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
ADS	Evaluate if the ODD is breached		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if there is an ADS vehicle failure		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Determine if a collision has occured		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if external party requested a stop		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Establish and maintain communication with FOC		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Command DDT fallback		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Monitor the driving environment and collect data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Process collected raw information		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Assess surrounding objects and events		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine local road rules	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Perform ADS software and hardware self-diagnosis tests		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Evaluate outcome of ADS software and hardware self-diagnosis tests		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Transmit outcome of self diagnosis tests		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Raw sensor data (visual, signal, localization) for system diagnostics.		ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Processed sensor data for DDT planning.	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Processed sensor data for system diagnostics.		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Detected context (perception data) for DDT planning	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Detected context (perception data) for diagnostics.		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event detection)
ADS	Processed sensor data (vehicle data) for system diagnostics.		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Detect a system failure (diagnostic module failure)		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
Consequences:	On Route Without Passengers	Controllability	Severity	Relative Frequency	Risk Level	
	ES1: Trip completed successfully	High	No Hazards	High	1	
	ES2: Vehicle arrives at MOC for maintenance	High	Traffic disruption	High	2	
	EF3: Collision Risk	Very Low	Fatality and Injury	Low	5	
	ES4: Post-incident procedures are initiated.	Medium	Traffic disruption	Low	2	
	EF5: Vehicle is stranded	Low	Traffic disruption	Low	3	

Op. Phase	On Route Without Passengers		ESD	COTA	STPA	FT
ID#	1.1.3		E1_E	A4.1, A4.2, A4.3	C1, C2, C3, C4	I-2
Safety Hazard:	ADS vehicle	fails to	perform DDT-fallback correctly			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
ADS	Determine if DDT can continue		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if MR-DDT is achievable		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if vehicle should go into MRC		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Request plan for DDT fallback strategy from FOC	See H1.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Receive DDT fallback strategy from FOC	See H1.2.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Determine if SSC is achievable		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Perform DDT vehicle motion and maneuver execution to return to ODD		ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: maneuver execution)
ADS	Achieve SSC		ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: maneuver execution)
ADS	Achieve MRC		ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: maneuver execution)
ADS	Drive to MOC in MR-DDT		ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: maneuver execution)
ADS	Evaluate outcome of implementation of DDT fallback plan		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Request kinematic action	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Request vehicle commands (hazard lights, turn signals, etc.)	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Implement kinematic action	See H1.1.1	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: motion control)
ADS	Implement signal action	See H1.1.1	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: electronic systems)
ADS	Correct vehicle control command		ADS vehicle	MOC maintenance crew	Ensure adequate state of	ADS vehicle (Control: motion control)
ADS	Implement correct DDT-fallback strategies		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Implement remote commands		ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: maneuver execution)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Evaluate if the ODD is breached	See H1.1.2	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if there is an ADS vehicle failure	See H1.1.2	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Determine if a collision has occured	See H1.1.2	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if external party requested a stop	See H1.1.2	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Establish and maintain communication with FOC	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Receive remote commands	See H1.2.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Transmit ADS fallback plan	See H1.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
ADS	Detected context (perception data) for DDT planning	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Adapt local path to DDT plan	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Adapt local path plan to provided waypoints.	See H1.2.2	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Adapt local path plan to DDT constraints (local traffic laws, ODD specifications).	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Request to adapt local path plan to waypoints provided by FOC.	See H1.2.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).	See H1.2.4	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Detect a system failure (diagnostic module failure)	See H1.1.2	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Adequate DDT plan (OEDR)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
Consequences:	On Route Without Passengers	Controllability	Severity	Relative Frequency	Risk Level	
	EF3: Collision Risk	Very Low	Fatality and Injury	Low	5	
	ES4: Post-incident procedures are initiated.	Medium	Traffic disruption	Low	2	
	EF5: Vehicle is stranded	Low	Traffic disruption	Low	3	

Op. Phase	On Route Without Passengers		ESD	COTA	STPA	FT
ID#	1.1.4		E1_G	A4.1.2, A2.2	F3a, C1, F6b, C2a, C2b	I-3
Safety Hazard:	ADS vehicle	fails to	dispatch vehicle to MOC			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
ADS	Determine optimal trajectory	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: local path planning)
ADS	Determine if MR-DDT is achievable	See H1.1.3	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Adapt local path to DDT plan	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Adapt local path plan to provided waypoints.	See H1.1.3	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Adapt local path plan to DDT constraints (local traffic laws, ODD specifications).	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Receive remote dispatch command		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Receive internal dispatch command		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Monitor the driving environment and collect data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Determine local road rules	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Evaluate if the ODD is breached	See H1.1.2	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if there is an ADS vehicle failure	See H1.1.2	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Establish and maintain communication with FOC	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Receive remote commands	See H1.2.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Processed sensor data for DDT planning.	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Detected context (perception data) for DDT planning	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Request new global path.		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: local path planning)
ADS	Implement correct DDT-fallback strategies	See H1.1.3	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
Consequences:	On Route Without Passengers	Controllability	Severity	Relative Frequency	Risk Level	
	EF3: Collision Risk	Very Low	Fatality and Injury	Low	5	

Op. Phase	On Route Without Passengers/On Route to MOC/Post-incident Management		ESD	COTA	STPA	FT
ID#	1.1.5		E1_H	A1, A2, A4.2.4	C3, C4	I-3
Safety Hazard:	ADS vehicle	fails to	successfully travel to MOC			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
ADS	Execute optimal planned trajectory	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Apply tactical maneuver	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Drive to MOC in MR-DDT	See H1.1.3	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: maneuver execution)
ADS	Request kinematic action	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Request vehicle commands (hazard lights, turn signals, etc.)	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Implement kinematic action	See H1.1.1	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: motion control)
ADS	Implement signal action	See H1.1.1	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: electronic systems)
ADS	Early warning of safety-critical failures		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Alert battery charging is required		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Monitor the driving environment and collect data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Process and combine data	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Determine local road rules	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Determine optimal trajectory	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: local path planning)
ADS	Determine if MR-DDT is achievable	See H1.1.3	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Detected context (perception data) for DDT planning	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Adapt local path to DDT plan	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Adapt local path plan to provided waypoints.	See H1.1.3	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Adapt local path plan to DDT constraints (local traffic laws, ODD specifications).	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Receive remote dispatch command	See H1.1.4	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Receive internal dispatch command	See H1.1.4	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
FOC	Remote vehicle dispatch command	See H1.2.3	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Dispatching)
Consequences:	On Route Without Passengers/On Route to MOC		Controllability	Severity	Relative Frequency	Risk Level
	EF3: Collision Risk		Very Low	Fatality and Injury	Low	5
Consequences:	Post-incident Management		Controllability	Severity	Relative Frequency	Risk Level
	EF3: Collision Risk		Very Low	Fatality and Injury	Low	5
	EF37: Vehicle and others road users at risk		Very Low	Fatality and Injury	Very Low	4

	C	D	E	F	G	H	I
1	Op. Phase	On Route Without Passengers/On Route to MOC		ESD	COTA	STPA	FT
2	ID#	1.1.6		E1_J1	A4.2.3.4	F5b, F8b	N/A
3	Safety Hazard:	ADS vehicle	fails to	request post-incident management procedures			
4	Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
5	ADS	Alert FOC	See H1.1.3	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
6							
7	Agent	Prior Failures: Fails to/Fails to provide					
8	ADS	Determine if vehicle should go into MRC	See H1.1.3	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
9	ADS	Receive DDT fallback strategy from FOC	See H1.2.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
10	ADS	Establish and maintain communication with FOC	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
11	FOC	Acknowledge that ADS vehicle entered MRC or requested post-incident procedures	See H1.2.4	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
12	FOC	Evaluate state of vehicle	See H1.2.1, H1.2.4	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
13	FOC	Determine if vehicle should go into MRC	See H1.2.2, H1.2.4	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
14	FOC	Evaluate the need and Initiate post-incident procedures	See H1.2.4	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
15	ADS	Recorded diagnostic logs for FOC operator supervision.	See H1.2.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
16	ADS	Transmit communication from vehicle to FOC (control center).		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
17							
18	Consequences:	On Route Without Passengers/On Route to MOC		Controllability	Severity	Relative Frequency	Risk Level
19		EF5: Vehicle is stranded		Low	Traffic disruption	Low	3

Op. Phase	On Route Without Passengers		ESD	COTA	STPA	FT
ID#	1.2.1		E1_D2	F3.1	F2b, F5b, C5b, F8b	II-1
Safety Hazard:	FOC	fails to	detect DDT fallback is required			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Evaluate if the ODD is breached		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if there is an ADS vehicle failure		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if a collision has occurred		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if external party asked for a stop		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Receive request from ADS		FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Receive outcome of DDT fallback implementation		FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Evaluate state of vehicle		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Request plan for DDT fallback strategy from FOC	See H1.1.3	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Transmit to FOC prescribed information	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Establish and maintain communication with FOC	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Respond to request for information	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event detection)
ADS	Make general request	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Transmit outcome of self diagnosis tests	See H1.1.2	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
FOC	Monitor ADS vehicle operations		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Evaluate ADS vehicle safety		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Determine if more information is needed		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Transmit request to ADS for specific information		FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Evaluate information from ADS		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Respond to ADS request		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
ADS	Processed sensor data (perception) for FOC operator supervision.		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Recorded diagnostic logs for FOC operator supervision.		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Alert DDT fallback is required		ADS communication	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Transmit communication from vehicle to FOC (control center).	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Informative vehicle status		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: information fusion)
ADS	Transmit information due to vehicle communication channel failure	See H1.1.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to external connectivity failure	See H1.1.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
Consequences:	On Route Without Passengers		Controllability	Severity	Relative Frequency	Risk Level
	EF3: Collision Risk		Very Low	Fatality and Injury	Low	5

C	D	E	F	G	H	I
Op. Phase	On Route Without Passengers/On Route to MOC		ESD	COTA	STPA	FT
ID#	1.2.2		E1_D3	F3.2	C8b, C6c	II-2
Safety Hazard:	FOC	fails to	send correct DDT fallback command			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Determine if DDT can continue		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if MR-DDT is achievable		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if vehicle should go into MRC		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if SSC is achievable		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Transmit ADS fallback plan		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).	See H1.2.4	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Request to adapt local path plan to waypoints provided by FOC.		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Follow DDT-fallback requirements		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Follow DDT-fallback procedure		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
ADS	Transmit information due to vehicle communication channel failure	See H1.2.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to external connectivity failure	See H1.2.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Evaluate if the ODD is breached	See H1.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if there is an ADS vehicle failure	See H1.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if a collision has occurred	See H1.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if external party asked for a stop	See H1.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Receive request from ADS	See H1.2.1	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Evaluate state of vehicle	See H1.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
ADS	Processed sensor data (perception) for FOC operator supervision.	See H1.2.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Recorded diagnostic logs for FOC operator supervision.	See H1.2.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Transmit communication from vehicle to FOC (control center).	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Implement correct DDT-fallback strategies	See H1.1.3	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
Consequences:	On Route Without Passengers/On Route to MOC		Controllability	Severity	Relative Frequency	Risk Level
	EF3: Collision Risk		Very Low	Fatality and Injury	Low	5

Op. Phase	On Route Without Passengers/On Route to MOC/Post-incident Management		ESD	COTA	STPA	FT
ID#	1.2.3		E1_G1	F3.2.1.2, F3.2.1.3, F4.3, F2.1, F3.2.2	C8b, C6b, C11a, F11a	I-3
Safety Hazard:	FOC	fails to	dispatch vehicle to MOC			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Transmit dispatch commands		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Dispatching)
FOC	Transmit ADS fallback plan	See H1.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).	See H1.2.4	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Request to adapt global path plan to waypoints provided by FOC.		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: global path planning)
FOC	Schedule vehicle for maintenance		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Dispatching)
MOC	Confirm maintenance scheduling		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
FOC	Remote vehicle dispatch command	See H1.1.5	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Dispatching)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Determine if MR-DDT is achievable	See H1.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if vehicle should go into MRC	See H1.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Assess if the ADS vehicle requires maintenance		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
ADS	Establish and maintain communication with FOC	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Receive remote commands	See H1.2.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Determine if more information is needed	See H1.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Transmit request to ADS for specific information	See H1.2.1	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Evaluate information from ADS	See H1.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Respond to ADS request	See H1.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Notify of scheduled maintenance or vehicle recall		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinator (Maintenance operations)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
FOC	Follow DDT-fallback requirements	See H1.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Follow DDT-fallback procedure	See H1.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
ADS	Transmit information due to vehicle communication channel failure	See H1.1.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to external connectivity failure	See H1.2.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
Consequences:	On Route Without Passengers/On Route to MOC		Controllability	Severity	Relative Frequency	Risk Level
	EF3: Collision Risk		Very Low	Fatality and Injury	Low	5
Consequences:	Post-incident Management		Controllability	Severity	Relative Frequency	Risk Level
	EF5: Vehicle is stranded		Low	Traffic disruption	Low	3
	EF38: Vehicle is stranded; others road users at risk		Very Low	Fatality and Injury	Very Low	4

C	D	E	F	G	H	I
Op. Phase	On Route Without Passengers/On Route to MOC		ESD	COTA	STPA	FT
ID#	1.2.4		E1_J	F3.3	C8b, C11b	II-3
			E1_J2	F2.4, F3.3	F8b, C11b	II-3
Safety Hazard:	FOC	fails to	initiate post-incident procedures			
	FOC	fails to	respond to ADS request and initiates post-incident procedures			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Acknowledge that ADS vehicle entered MRC or requested post-incident procedures		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Evaluate the need and Initiate post-incident procedures		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Initiate post-incident procedures		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).		FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Alert FOC	See H1.1.3	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Establish and maintain communication with FOC	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Respond to ADS request	See H1.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Evaluate state of vehicle	See H1.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Determine if vehicle should go into MRC	See H1.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
ADS	Transmit communication from vehicle to FOC (control center).	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
ADS	Transmit information due to vehicle communication channel failure	See H1.2.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to external connectivity failure	See H1.2.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Informative vehicle status	See H1.2.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: information fusion)
Consequences	On Route Without Passengers/On Route to MOC		Controllability	Severity	Relative Frequency	Risk Level
	ES4: Post-incident procedures are initiated.		Medium	Traffic disruption	Low	2
	EF5: Vehicle is stranded		Low	Traffic disruption	Low	3

Op. Phase	On Route With Passengers/Passenger Pick-up/Passenger Drop-off		ESD	COTA	STPA	FT
ID#	2.1.1		E2_D	A3, A5	F3a, F3b, C5a, C6d	I-1
Safety Hazard:	ADS vehicle	fails to	detect DDT-fallback is required			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
ADS	Evaluate if the ODD is breached		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if there is an ADS vehicle failure		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Determine if a collision has occured		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if a passenger has requested an emergency stop		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event detection)
ADS	Determine if external party requested a stop		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event detection)
ADS	Establish and maintain communication with FOC		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Command DDT fallback		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Command DDT fallback (emergency stop request)		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Activate emergency stop mechanism when requested		ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (Passenger interaction)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Monitor the driving environment and collect data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Process collected raw information		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Assess surrounding objects and events		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine local road rules	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Perform ADS software and hardware self-diagnosis tests		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Evaluate outcome of ADS software and hardware self-diagnosis tests		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Transmit outcome of self diagnosis tests		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Raw sensor data (visual, signal, localization) for system diagnostics.		ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Processed sensor data for DDT planning.	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Processed sensor data for system diagnostics.		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Detected context (perception data) for DDT planning	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Detected context (perception data) for diagnostics.		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event detection)
ADS	Processed sensor data (vehicle data) for system diagnostics.		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Detect a system failure (diagnostic module failure)		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
Consequences:	On Route With Passengers/Passenger Pick-up/Passenger Drop-off		Controllability	Severity	Relative Frequency	Risk Level
	ES4: Post-incident procedures are initiated.		Medium	Traffic disruption	Low	2
	EF6: Vehicle and passenger are stranded		Low	Fatality and Injury	Low	4
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5

Op. Phase	On Route With Passengers/Passenger Pick-up/Passenger Drop-off		ESD	COTA	STPA	FT
ID#	2.1.2		E2_E	A4.1, A4.2, A4.3	C1, C2, C3, C4	I-2
Safety Hazard:	ADS vehicle	fails to	perform DDT-fallback correctly			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
ADS	Determine if DDT can continue		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if MR-DDT is achievable		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if vehicle should go into MRC		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Request plan for DDT fallback strategy from FOC	See H2.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Receive DDT fallback strategy from FOC	See H2.2.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Determine if SSC is achievable		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Perform DDT vehicle motion and maneuver execution to return to ODD		ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: maneuver execution)
ADS	Achieve SSC		ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: maneuver execution)
ADS	Achieve MRC		ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: maneuver execution)
ADS	Evaluate outcome of implementation of DDT fallback plan		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Request kinematic action	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Request vehicle commands (hazard lights, turn signals, etc.)	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Implement kinematic action	See H1.1.1	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: motion control)
ADS	Implement signal action	See H1.1.1	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: electronic systems)
ADS	Correct vehicle control command		ADS vehicle	MOC maintenance crew	Ensure adequate state of	ADS vehicle (Control: motion control)
ADS	Implement correct DDT-fallback strategies		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Implement remote commands		ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: maneuver execution)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Evaluate if the ODD is breached	See H2.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if there is an ADS vehicle failure	See H2.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Determine if a collision has occured	See H2.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if a passenger has requested an emergency stop	See H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event detection)
ADS	Determine if external party requested a stop	See H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event detection)
ADS	Establish and maintain communication with FOC	See H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Receive remote commands	See H2.2.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Transmit ADS fallback plan	See H2.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
ADS	Detected context (perception data) for DDT planning	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Adapt local path to DDT plan	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Adapt local path plan to provided waypoints.	See H2.2.2	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Adapt local path plan to DDT constraints (local traffic laws, ODD specifications).	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Request to adapt local path plan to waypoints provided by FOC.	See H2.2.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).	See H2.2.3	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Command DDT fallback (emergency stop request)	See H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Detect a system failure (diagnostic module failure)	See H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Adequate DDT plan (OEDR)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
Consequences:	On Route With Passengers/Passenger Pick-up/Passenger Drop-off		Controllability	Severity	Relative Frequency	Risk Level
	ES4: Post-incident procedures are initiated.		Medium	Traffic disruption	Low	2
	EF6: Vehicle and passenger are stranded		Low	Fatality and Injury	Low	4
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5

C	D	E	F	G	H	I
Op. Phase	On Route With Passengers/Passenger Pick-up/Passenger Drop-off		ESD	COTA	STPA	FT
ID#	2.1.3		E1_J1	A4.2.3.4	F5b, F8b	N/A
Safety Hazard:	ADS vehicle	fails to	request post-incident management procedures			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
ADS	Alert FOC	See H2.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Determine if vehicle should go into MRC	See H2.1.2	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Receive DDT fallback strategy from FOC	See H2.2.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Establish and maintain communication with FOC	See H2.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Acknowledge that ADS vehicle entered MRC or requested post-incident procedures	See H2.2.3	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Evaluate state of passengers and vehicle	See H2.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Determine if vehicle should go into MRC	See H2.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Evaluate the need and Initiate post-incident procedures	See H2.2.3	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
ADS	Recorded diagnostic logs for FOC operator supervision.	See H2.2.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Transmit communication from vehicle to FOC (control center).		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
Consequences:	On Route With Passengers/Passenger Pick-up/Passenger Drop-off		Controllability	Severity	Relative Frequency	Risk Level
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5

Op. Phase	On Route With Passengers/Passenger Pick-up/Passenger Drop-off		ESD	COTA	STPA	FT
ID#	2.2.1		E2_D2	F3.1	F2b, F5b, C5b, F8b, C9a	II-1
Safety Hazard:	FOC	fails to	detect DDT fallback is required			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Evaluate if the ODD is breached		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if there is an ADS vehicle failure		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if a collision has occurred		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if a passenger has requested an emergency stop		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if external party asked for a stop		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Receive request from ADS		FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Receive outcome of DDT fallback implementation		FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Evaluate state of passengers and vehicle		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Request plan for DDT fallback strategy from FOC	See H2.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Transmit to FOC prescribed information	See H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Determine if a passenger has requested an emergency stop	See H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event detection)
ADS	Determine if external party requested a stop	See H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event detection)
ADS	Establish and maintain communication with FOC	See H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Respond to request for information	See H2.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event detection)
ADS	Make general request	See H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Transmit outcome of self diagnosis tests	See H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
FOC	Monitor ADS vehicle operations		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Evaluate ADS vehicle safety		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Determine if more information is needed		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Transmit request to ADS for specific information		FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Evaluate information from ADS		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Respond to ADS request		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Receive requests from passengers		FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
FOC	Passenger emergency stop request		FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Incident management)
FOC	Communicate with passengers		FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
ADS	Transmit communication from passenger to vehicle.		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Transmit passenger contact request to FOC		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Transmit communication from vehicle to FOC (service operator).		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
FOC	Alert DDT fallback is required		FOC service operator	FOC safety operator	Follow established procedure of	FOC service operator (Incident management)
ADS	Processed sensor data (perception) for FOC operator supervision.		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Recorded diagnostic logs for FOC operator supervision.		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Alert DDT fallback is required		ADS communication	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Transmit communication from vehicle to FOC (control center).	See H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Command DDT fallback (emergency stop request)	See H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Informative vehicle status		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: information fusion)
ADS	Transmit information due to vehicle communication channel failure	See H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to external connectivity failure	See H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Notify of scheduled maintenance or vehicle recall		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinator (Maintenance operations)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
Consequences:	On Route With Passengers		Controllability	Severity	Relative Frequency	Risk Level
	ES4: Post-incident procedures are initiated.		Medium	Traffic disruption	Low	2
	EF6: Vehicle and passenger are stranded		Low	Fatality and Injury	Low	4
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5
Consequences:	Passenger Pick-up		Controllability	Severity	Relative Frequency	Risk Level
	ES4: Post-incident procedures are initiated.		Medium	Traffic disruption	Low	2
	EF6: Vehicle and passenger are stranded		Low	Fatality and Injury	Low	4
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5
	ES8: ADS Vehicle is on-route to destination with passengers		High	No Hazards	High	1
	EF19: Passenger is stranded, and vehicle is at risk of collision		Very Low	Fatality and Injury	Low	5
Consequences:	Passenger Drop-off		Controllability	Severity	Relative Frequency	Risk Level
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5

Op. Phase	On Route With Passengers/Passenger Pick-up/Passenger Drop-off		ESD	COTA	STPA	FT
ID#	2.2.2		E2_D3	F3.2	C8b, C6c, C9a, F9a	II-2
Safety Hazard:	FOC	fails to	send correct DDT fallback command			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Determine if DDT can continue		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if MR-DDT is achievable		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if vehicle should go into MRC		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if SSC is achievable		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Transmit ADS fallback plan		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).	See H2.2.3	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Request to adapt local path plan to waypoints provided by FOC.		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Follow DDT-fallback requirements		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Follow DDT-fallback procedure		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
ADS	Transmit information due to vehicle communication channel failure	See H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to external connectivity failure	See H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Evaluate if the ODD is breached	See H2.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if there is an ADS vehicle failure	See H2.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if a collision has occurred	See H2.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if a passenger has requested an emergency stop	See H2.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if external party asked for a stop	See H2.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Receive request from ADS	See H2.2.1	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Evaluate state of passengers and vehicle	See H2.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Receive requests from passengers	See H2.2.1	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
FOC	Passenger emergency stop request	See H2.2.1	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Incident management)
FOC	Respond to passenger contact request		FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
FOC	Communicate with passengers	See H2.2.1	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
ADS	Processed sensor data (perception) for FOC operator supervision.	See H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Alert DDT fallback is required	See H2.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Recorded diagnostic logs for FOC operator supervision.	See H2.2.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Transmit communication from vehicle to FOC (control center).	See H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Alert DDT fallback is required	See H2.2.1	FOC service operator	FOC safety operator	Follow established procedure of	FOC service operator (Incident management)
FOC	Inform passenger status.	See H2.2.1	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Incident management)
ADS	Transmit communication from passenger to vehicle.	See H2.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Transmit passenger contact request to FOC	See H2.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Transmit communication from vehicle to FOC (service operator).	See H2.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Implement correct DDT-fallback strategies	See H2.1.2	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
Consequences:	On Route With Passengers		Controllability	Severity	Relative Frequency	Risk Level
	ES4: Post-incident procedures are initiated.		Medium	Traffic disruption	Low	2
	EF6: Vehicle and passenger are stranded		Low	Fatality and Injury	Low	4
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5
Consequences:	Passenger Pick-up		Controllability	Severity	Relative Frequency	Risk Level
	ES4: Post-incident procedures are initiated.		Medium	Traffic disruption	Low	2
	EF6: Vehicle and passenger are stranded		Low	Fatality and Injury	Low	4
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5
	EF19: Passenger is stranded, and vehicle is at risk of collision		Very Low	Fatality and Injury	Low	5
Consequences:	Passenger Drop-off		Controllability	Severity	Relative Frequency	Risk Level
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5

C	D	E	F	G	H	I
Op. Phase	On Route With Passengers/Passenger Pick-up/Passenger Drop-off		ESD	COTA	STPA	FT
ID#	2.2.3		E2_J	F3.3	C8b, C11b	II-3
			E2_J2	F2.4, F3.3	F8b, C11b	II-3
Safety Hazard:	FOC	fails to	initiate post-incident procedures			
	FOC	fails to	respond to ADS request and initiates post-incident procedures			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Acknowledge that ADS vehicle entered MRC or requested post-incident procedures		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Evaluate the need and Initiate post-incident procedures		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Initiate post-incident procedures		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).		FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Alert FOC	See H2.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Establish and maintain communication with FOC	See H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Respond to ADS request	See H2.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Evaluate state of passengers and vehicle	See H2.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Determine if vehicle should go into MRC	See H2.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Receive requests from passengers	See H2.2.4	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
FOC	Respond to passenger contact request	See H2.2.2	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
FOC	Communicate with passengers	See H2.2.2	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
ADS	Transmit communication from vehicle to FOC (control center).	See H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Transmit communication from passenger to vehicle.		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Transmit passenger contact request to FOC		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Transmit communication from vehicle to FOC (service operator).		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
ADS	Transmit information due to vehicle communication channel failure	See H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to external connectivity failure	See H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Informative vehicle status	See H2.2.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: information fusion)
Consequences:	On Route With Passengers/Passenger Pick-up/Passenger Drop-off		Controllability	Severity	Relative Frequency	Risk Level
	ES4: Post-incident procedures are initiated.		Medium	Traffic disruption	Low	2
	EF6: Vehicle and passenger are stranded		Low	Fatality and Injury	Low	4

C	D	E	F	G	H	I
Op. Phase	On Route With Passengers/Passenger Pick-up/Passenger Drop-off		ESD	COTA	STPA	FT
ID#	2.2.4	Note:	E2_N	F3.3	C8b, C11b	II-3
			E2_N1	F4.1, F4.3	C7a, F7a, F8a, C7b	II-1
			E2_O	N/A	F7a, F8a, F9a	II-1
			E4_G	A5.1	E2, C7a, F8b	II-1
Safety Hazard:	FOC	fails to	communicate with passenger			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Evaluate the need and Initiate post-incident procedures	See H2.2.3	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Receive requests from passengers		FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
FOC	Communicate with passengers		FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
ADS	Establish and maintain communication with FOC	See H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Alert DDT fallback is required		FOC service operator	FOC safety operator	Follow established procedure of	FOC service operator (Incident management)
FOC	Inform passenger status.		FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Incident management)
FOC	Transmit FOC (service operator) contact request to passengers		FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Acknowledge that ADS vehicle entered MRC or requested post-incident procedures	See H2.2.3	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Evaluate state of passengers and vehicle	See H2.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Passenger emergency stop request	See H2.1.1	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Incident management)
FOC	Respond to passenger contact request	See H2.2.2	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
ADS	Transmit passenger contact request to FOC	See H2.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Transmit communication from FOC (service operator) to vehicle.		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Transmit communication from vehicle to FOC (service operator).	See H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Transmit communication from vehicle to FOC (control center).	See H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Inform DDT fallback is required.		FOC safety operator	FOC safety operator	Follow established procedure of	FOC service operator (Passenger requests)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).	See H2.2.3	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit communication from passenger to vehicle.	See H2.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Connect FOC (service operator) to passenger		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Detect a system failure (diagnostic module failure)	See H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Transmit information due to vehicle communication channel failure	See H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to external connectivity failure	See H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
Consequences:	On Route With Passengers/Passenger Pick-up		Controllability	Severity	Relative Frequency	Risk Level
	ES4: Post-incident procedures are initiated.		Medium	Traffic disruption	Low	2
	EF6: Vehicle and passenger are stranded		Low	Fatality and Injury	Low	4
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5
	ES8: ADS Vehicle is on-route to destination with passengers		High	No Hazards	High	1
Consequences:	Passenger Drop-off		Controllability	Severity	Relative Frequency	Risk Level
	ES4: Post-incident procedures are initiated.		Medium	Traffic disruption	Low	2
	EF6: Vehicle and passenger are stranded		Low	Fatality and Injury	Low	4
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5
	ES20: ADS Vehicle is on-route to destination without passengers		High	No Hazards	High	1

Op. Phase	On Route to MOC		ESD	COTA	STPA	FT
ID#	3.2.1		E3_B	F1	C11a, F11a, C12a, F12a	III-1
Safety Hazard:	FOC	fails to	schedule vehicle for inspection or corrective maintenance			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Transmit prescribed information to MOC		FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
FOC	Receive request for information		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
FOC	Provide requested information		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
MOC	Confirm maintenance scheduling		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
FOC	Schedule vehicle for maintenance		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Dispatching)
FOC	Confirm maintenance scheduling request		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
MOC	Communicate schedule correctly		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
FOC	Request maintenance activities schedule verification		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
MOC	Monitor FOC communications		MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
FOC	Monitor MOC communications		FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Assess if the ADS vehicle requires maintenance	See H1.2.3, H2.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
ADS	Establish and maintain communication with FOC	See H1.1.2, H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Receive remote commands	See H1.2.2, H2.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).	See H1.2.4, H2.2.3	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Request to adapt global path plan to waypoints provided by FOC.	See H1.2.3, H2.2.2	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: global path planning)
ADS	Detect a system failure (diagnostic module failure)	See H1.1.2, H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Transmit information due to vehicle communication channel failure	See H1.1.2, H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to external connectivity failure	See H1.1.2, H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Notify of scheduled maintenance or vehicle recall		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinator (Maintenance operations)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
Consequences:	On Route to MOC		Controllability	Severity	Relative Frequency	Risk Level
	ES10: Vehicle scheduled for preventive maintenance or system updates		High	No Hazards	Medium	1
	ES11: Vehicle is stationed at MOC		Medium	No Hazards	Medium	2

C	D	E	F	G	H	I
Op. Phase	On Route to MOC		ESD	COTA	STPA	FT
ID#	3.2.2	Note:	E3_C	F1	C11a, F11a, C12a, F12a	III-1
Safety Hazard:	FOC	fails to	schedule vehicle for preventive maintenance			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Transmit prescribed information to MOC		FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
FOC	Receive request for information		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
FOC	Provide requested information		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
FOC	Confirm maintenance scheduling request		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
MOC	Communicate schedule correctly		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
FOC	Request maintenance activities schedule verification		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
MOC	Monitor FOC communications		MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
FOC	Monitor MOC communications		FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Assess if the ADS vehicle requires maintenance	See H1.2.3, H2.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
ADS	Establish and maintain communication with FOC	See H1.1.2, H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Receive remote commands	See H1.2.2, H2.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).	See H1.2.4, H2.2.3	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Request to adapt global path plan to waypoints provided by FOC.	See H1.2.3, H2.2.2	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: global path planning)
ADS	Detect a system failure (diagnostic module failure)	See H1.1.2, H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Transmit information due to vehicle communication channel failure	See H1.1.2, H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to external connectivity failure	See H1.1.2, H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Collect correct perception and localization data	See H2.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Use up to date/correct HD maps (not available)	See H2.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Notify of scheduled maintenance or vehicle recall		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinator (Maintenance operations)
Consequences:	On Route to MOC		Controllability	Severity	Relative Frequency	Risk Level
	ES11: Vehicle is stationed at MOC		Medium	No Hazards	Medium	2

	C	D	E	F	G	H	I
1	Op. Phase	On Route to MOC		ESD	COTA	STPA	FT
2	ID#	3.2.3		E3_E	F3.2, F3.3	F8b, C8b	I-3
3	Safety Hazard:	FOC	fails to	locate missing vehicle			
4	Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
5	FOC	Attempt to communicate with missing vehicle		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
6	FOC	Evaluate condition of missing vehicle		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
7	ADS	Transmit communication from vehicle to FOC (control center).	See H1.2.4, H2.2.3	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
8	FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).	See H1.2.4, H2.2.3	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
9	FOC	Detect vehicle is stranded		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
10	FOC	Implement vehicle recovery procedure		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
11	FOC	Deliver requested information		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Connectivity: MOC)
12							
13	Agent	Prior Failures: Fails to/Fails to provide					
14	FOC	Transmit prescribed information to MOC		FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
15	FOC	Receive request for information		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
16	FOC	Provide requested information		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
17	FOC	Receive that ADS vehicle is missing	See H3.3.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Connectivity: MOC)
18	MOC	Collect data from the FOC	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
19	MOC	Request specific information from FOC	See H3.3.1	MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
20	MOC	Evaluate and process information collected	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
21	MOC	Determine if vehicle is missing	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
22	FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
23	MOC	Request vehicle information	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
24	MOC	Confirm maintenance scheduling		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
25	MOC	Report missing vehicle	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
26							
27	Consequences:	On Route to MOC		Controllability	Severity	Relative Frequency	Risk Level
28		EF12: Vehicle is unreachable		Very Low	Fatality and Injury	Low	5

Op. Phase	Pre-shift Inspection and Corrective Maintenance		ESD	COTA	STPA	FT
ID#	3.2.4		E3_K	F2.2	C8b, C2a	III-4
Safety Hazard:	FOC	fails to	follow procedure on vehicle status			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Receive from the MOC if the vehicle is cleared		FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
FOC	Dispatch the ADS vehicle for operation		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Dispatching)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).		FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Adapt local path plan to provided waypoints.		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
FOC	Comply to "not cleared" status and incorrectly transmits a dispatch command		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Dispatching)
Agent	Prior Failures: Fails to/Fails to provide					
MOC	Communicate vehicle status	See H3.3.6	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Inform abnormal vehicle conditions and status (cleared/not cleared).	See H3.3.3	MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Vehicle clearance)
MOC	Inform abnormal vehicle conditions.	See H3.3.6	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
ADS	Correctly execute a dispatch command	See H3.3.4	ADS software	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
Consequences:	Pre-shift Inspection and Corrective Maintenance		Controllability	Severity	Relative Frequency	Risk Level
	ES11: Vehicle is stationed at MOC		Medium	No Hazards	Medium	2
	EF17: Vehicle is not scheduled for external maintenance		Medium	No Hazards	Medium	2

Op. Phase	On Route to MOC		ESD	COTA	STPA	FT
ID#	3.3.1		E3_D	M1.4	C11b, C12b, F12b	I-3
Safety Hazard:	MOC	fails to	report missing vehicle to FOC			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
MOC	Collect data from the FOC		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Request specific information from FOC		MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
MOC	Evaluate and process information collected		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Determine if vehicle is missing	See H3.2.3	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Report missing vehicle	See H3.2.3	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Transmit prescribed information to MOC	See H3.2.1	FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
FOC	Receive request for information	See H3.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
FOC	Provide requested information	See H3.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
MOC	Confirm maintenance scheduling	See H1.2.3	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Request vehicle information		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Schedule vehicle for maintenance		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Dispatching)
MOC	Communicate schedule correctly	See H3.2.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
FOC	Request maintenance activities schedule verification	See H3.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
MOC	Monitor FOC communications	See H3.2.1	MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
FOC	Monitor MOC communications	See H3.2.1	FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
ADS	Transmit information due to external connectivity failure	See H1.1.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
Consequences:	On Route to MOC		Controllability	Severity	Relative Frequency	Risk Level
	EF12: Vehicle is unreachable		Very Low	Fatality and Injury	Low	5

	C	D	E	F	G	H	I
1	Op. Phase	Pre-shift Inspection and Corrective Maintenance		ESD	COTA	STPA	FT
2	ID#	3.3.2	Note:	E3_G	M2.1	C13b	III-1
3	Safety Hazard:	MOC	fails to	inspect vehicle			
4	Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
5	MOC	Evaluate and process information collected	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
6	MOC	Determine type of inspection		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
7	MOC	Instructs inspection procedure		MOC coordinators	MOC coordinators	Follow established procedure of	MOC maintenance operations (Procedural)
8	MOC	Schedule vehicle inspection crew		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
9	MOC	Perform pre-shift inspection procedure		MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Pre-shift Inspection)
10							
11	Agent	Prior Failures: Fails to/Fails to provide					
12	MOC	Collect data from the FOC	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
13	MOC	Request specific information from FOC	See H3.3.1	MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
14	FOC	Transmit prescribed information to MOC	See H3.2.1	FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
15	FOC	Receive request for information	See H3.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
16	FOC	Provide requested information	See H3.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
17	MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external reque	MOC maintenance operations (Procedural)
18	MOC	Confirm maintenance scheduling	See H1.2.3	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
19	FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
20	FOC	Schedule vehicle for maintenance	See H1.2.3	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Dispatching)
21	MOC	Communicate schedule correctly	See H3.2.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
22	FOC	Request maintenance activities schedule verification	See H3.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
23	MOC	Monitor FOC communications	See H3.2.1	MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
24	FOC	Monitor MOC communications	See H3.2.1	FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
25	ADS	Transmit information due to external connectivity failure	See H1.1.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
26							
27	Consequences:	Pre-shift Inspection and Corrective Maintenance		Controllability	Severity	Relative Frequency	Risk Level
28		ES11: Vehicle is stationed at MOC		Medium	No Hazards	Medium	2
29		EF14: Vehicle incorrectly dispatched for operation		Medium	No Hazards	Medium	2
30		EF16: Vehicle incorrectly cleared for operation		Medium	No Hazards	Medium	2

C	D	E	F	G	H	I
Op. Phase	Pre-shift Inspection and Corrective Maintenance		ESD	COTA	STPA	FT
ID#	3.3.3	Note:	E3_H	M2.2, M2.3	C13a, F13a, F13b	III-2
Safety Hazard:	MOC	fails to	perform inspection correctly			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
MOC	Follow inspection procedure		MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Pre-shift inspection)
MOC	Determine if vehicle passed inspection		MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Pre-shift inspection)
MOC	Inform abnormal vehicle conditions and status (cleared/not cleared).		MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Vehicle clearance)
MOC	Inform vehicle detected issues.		MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Pre-shift inspection)
Agent	Prior Failures: Fails to/Fails to provide					
MOC	Collect data from the FOC	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Request specific information from FOC	See H3.3.1	MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
MOC	Evaluate and process information collected	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Determine type of inspection	See H3.3.2	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
FOC	Transmit prescribed information to MOC	See H3.2.1	FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
FOC	Receive request for information	See H3.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
FOC	Provide requested information	See H3.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
ADS	Transmit outcome of self diagnosis tests	See H1.1.2, H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Recorded diagnostic logs for MOC crew inspection.	See H1.1.2, H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Recorded diagnostic logs for FOC operator supervision.	See H1.1.2, H2.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Transmit communication from vehicle to FOC (control center).	See H1.1.2, H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
MOC	Instructs inspection procedure		MOC coordinators	MOC coordinators	Follow established procedure of	MOC maintenance operations (Procedural)
MOC	Adequate inspection procedure		MOC inspection crew	MOC coordinators	Follow established procedure of	MOC external operations (ADS Developer)
ADS	Record informative vehicle logs		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Detect a system failure (diagnostic module failure)	See H1.1.2, H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
Consequences:	Pre-shift Inspection and Corrective Maintenance		Controllability	Severity	Relative Frequency	Risk Level
	ES11: Vehicle is stationed at MOC		Medium	No Hazards	Medium	2
	ES13: Vehicle cleared for operation		High	No Hazards	High	1
	EF14: Vehicle incorrectly dispatched for operation		Medium	No Hazards	Medium	2
	ES15: Vehicle is scheduled for external maintenance		High	No Hazards	Medium	1
	EF16: Vehicle incorrectly cleared for operation		Medium	No Hazards	Medium	2
	EF17: Vehicle is not scheduled for external maintenance		Medium	No Hazards	Medium	2
	EF18: Vehicle passes a faulty inspection		Medium	No Hazards	Medium	2

Op. Phase	Pre-shift Inspection and Corrective Maintenance		ESD	COTA	STPA	FT
ID#	3.3.4	Note:	E3_I2	M4.2.1, M4.3.1	F13b, C14a, C14b	III-3
Safety Hazard:	MOC	fails to	perform maintenance at MOC			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
MOC	Perform low-complexity corrective maintenance		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Follow corrective maintenance procedures		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Perform post-maintenance test		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Inform abnormal vehicle conditions.		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Follow correct maintenance procedure		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Instructs maintenance procedure		MOC coordinators	MOC coordinators	Follow established procedure of	MOC maintenance operations (Procedural)
MOC	Schedule vehicle maintenance crew		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Request vehicle information		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
Agent	Prior Failures: Fails to/Fails to provide					
MOC	Determine type of inspection	See H3.3.2	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Follow inspection procedure	See H3.3.3	MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Pre-shift inspection)
MOC	Determine if vehicle passed inspection	See H3.3.3	MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Pre-shift inspection)
MOC	Follow full inspection procedure	See H3.3.10	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Service inspection)
MOC	Determine ADS vehicle failures	See H3.3.3, 3.3.10	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Service inspection)
MOC	Inform vehicle detected issues.	See H3.3.3, 3.3.10	MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Pre-shift inspection)
MOC	Instructs inspection procedure	See H3.3.2	MOC coordinators	MOC coordinators	Follow established procedure of	MOC maintenance operations (Procedural)
MOC	Schedule vehicle inspection crew	See H3.3.2	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Inform abnormal vehicle conditions and status (cleared/not cleared).	See H3.3.3	MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Vehicle clearance)
MOC	Adequate maintenance procedures		MOC maintenance crew	MOC coordinators	Follow established procedure of	MOC external operations (ADS Developer)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
Consequences:	Pre-shift Inspection and Corrective Maintenance		Controllability	Severity	Relative Frequency	Risk Level
	EF14: Vehicle incorrectly dispatched for operation		Medium	No Hazards	Medium	2
	ES15: Vehicle is scheduled for external maintenance		High	No Hazards	Medium	1
	EF16: Vehicle incorrectly cleared for operation		Medium	No Hazards	Medium	2
	EF17: Vehicle is not scheduled for external maintenance		Medium	No Hazards	Medium	2
	EF18: Vehicle passes a faulty inspection		Medium	No Hazards	Medium	2

	C	D	E	F	G	H	I
1	Op. Phase	Pre-shift Inspection and Corrective Maintenance		ESD	COTA	STPA	FT
2	ID#	3.3.5	Note:	E3_I3	M4.2.2, M4.3.3	F13, C15b, F15a	N/A
3	Safety Hazard:	MOC	fails to	schedule external maintenance			
4	Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
5	MOC	Schedule maintenance with ADS developer		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
6	MOC	Request external maintenance to ADS vehicle manufacturer.		MOC coordinators	MOC coordinators	Follow established procedure of	MOC external operations (ADS Developer)
7	MOC	Confirm external maintenance request.		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
8	MOC	Follow correct maintenance procedure	See H3.3.4	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
9							
10	Agent	Prior Failures: Fails to/Fails to provide					
11	MOC	Determine ADS vehicle failures	See H3.3.3, 3.3.10	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Service inspection)
12	MOC	Perform low-complexity corrective maintenance	See H3.3.4	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
13	MOC	Follow corrective maintenance procedures	See H3.3.4	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
14	MOC	Perform post-maintenance test	See H3.3.4	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
15	MOC	Inform abnormal vehicle conditions.	See H3.3.4	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
16	MOC	Inform vehicle detected issues.	See H3.3.3, 3.3.10	MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Pre-shift inspection)
17	MOC	Instructs maintenance procedure	See H3.3.4	MOC coordinators	MOC coordinators	Follow established procedure of	MOC maintenance operations (Procedural)
18	MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
19	MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
20							
21	Consequences:	Pre-shift Inspection and Corrective Maintenance		Controllability	Severity	Relative Frequency	Risk Level
22		EF14: Vehicle incorrectly dispatched for operation		Medium	No Hazards	Medium	2
23		EF16: Vehicle incorrectly cleared for operation		Medium	No Hazards	Medium	2
24		EF17: Vehicle is not scheduled for external maintenance		Medium	No Hazards	Medium	2

	C	D	E	F	G	H	I
1	Op. Phase	Pre-shift Inspection and Corrective Maintenance		ESD	COTA	STPA	FT
2	ID#	3.3.6	Note:	E3_J	M3	F13a, F14a	III-4
3				E3_M	M3	F13a, F13b	III-4
4	Safety Hazard:	MOC	fails to	follow procedure on vehicle status			
5	Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
6	MOC	Communicate vehicle status		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
7	MOC	Verify if the vehicle is correctly cleared		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
8	MOC	Label the vehicle status correctly		MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Pre-shift inspection)
9							
10	Agent	Prior Failures: Fails to/Fails to provide					
11	MOC	Determine if vehicle passed inspection	See H3.3.3	MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Pre-shift inspection)
12	MOC	Perform post-maintenance test	See H3.3.4	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
13	MOC	Inform abnormal vehicle conditions.	See H3.3.4	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
14	MOC	Instructs inspection procedure	See H3.3.2	MOC coordinators	MOC coordinators	Follow established procedure of	MOC maintenance operations (Procedural)
15	MOC	Schedule vehicle inspection crew	See H3.3.2	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
16	MOC	Inform abnormal vehicle conditions and status (cleared/not cleared).	See H3.3.3	MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Vehicle clearance)
17	MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
18	MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
19							
20	Consequences:	Pre-shift Inspection and Corrective Maintenance		Controllability	Severity	Relative Frequency	Risk Level
21		ES11: Vehicle is stationed at MOC		Medium	No Hazards	Medium	2
22		EF14: Vehicle incorrectly dispatched for operation		Medium	No Hazards	Medium	2
23		EF17: Vehicle is not scheduled for external maintenance		Medium	No Hazards	Medium	2

Op. Phase	Preventive Maintenance and System Updates		ESD	COTA	STPA	FT
ID#	3.3.7	Note:	E3_I3	M2.4, M4.3	F14a, F14b, C16a, F16a	N/A
Safety Hazard:	MOC	fails to	schedule external maintenance			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
MOC	Request external maintenance to ADS vehicle manufacturer.		MOC coordinators	MOC coordinators	Follow established procedure of	MOC external operations (ADS Developer)
MOC	Confirm external maintenance request.		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Follow correct maintenance procedure	See H3.3.4	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
Agent	Prior Failures: Fails to/Fails to provide					
MOC	Follow service inspection procedure	See H3.3.11	MOC inspection crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Service inspection)
MOC	Determine if vehicle passed service inspection	See H3.3.11	MOC inspection crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Service inspection)
MOC	Determine if preventive maintenance was successful	See H3.3.12	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Update ADS software	See H3.3.9	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: System updates)
MOC	Replace perception components	See H3.3.9	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: System updates)
MOC	Calibrate equipment	See H3.3.9	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: System updates)
MOC	Perform post-preventive maintenance or system updates test	See H3.3.9	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Instructs maintenance procedure	See H3.3.4	MOC coordinators	MOC coordinators	Follow established procedure of	MOC maintenance operations (Procedural)
MOC	Inform detected issues during tests	See H3.3.9	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: System updates)
MOC	Inform abnormal vehicle conditions.	See H3.3.12	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
Consequences:	Preventive Maintenance and System Updates		Controllability	Severity	Relative Frequency	Risk Level
	EF14: Vehicle incorrectly dispatched for operation		Medium	No Hazards	Medium	2
	EF16: Vehicle incorrectly cleared for operation		Medium	No Hazards	Medium	2
	EF17: Vehicle is not scheduled for external maintenance		Medium	No Hazards	Medium	2

Op. Phase	Preventive Maintenance and System Updates		ESD	COTA	STPA	FT
ID#	3.3.8	Note:	E3_O	M1.3	C14a, C14b, C15a	III-5
Safety Hazard:	MOC	fails to	perform system updates at MOC			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
MOC	Evaluate and process information collected	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Instructs maintenance procedure		MOC coordinators	MOC coordinators	Follow established procedure of	MOC maintenance operations (Procedural)
MOC	Schedule vehicle maintenance crew		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Follow software update or instrument calibration procedure		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: System updates)
Agent	Prior Failures: Fails to/Fails to provide					
MOC	Collect data from the FOC	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Request specific information from FOC	See H3.3.1	MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
FOC	Transmit prescribed information to MOC	See H3.2.1	FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
FOC	Receive request for information	See H3.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
FOC	Provide requested information	See H3.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Follow correct maintenance procedure	See H3.3.4	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
Consequences:	Preventive Maintenance and System Updates		Controllability	Severity	Relative Frequency	Risk Level
	EF14: Vehicle incorrectly dispatched for operation		Medium	No Hazards	Medium	2
	ES15: Vehicle is scheduled for external maintenance		High	No Hazards	Medium	1
	EF16: Vehicle incorrectly cleared for operation		Medium	No Hazards	Medium	2
	EF17: Vehicle is not scheduled for external maintenance		Medium	No Hazards	Medium	2

	C	D	E	F	G	H	I
1	Op. Phase	Preventive Maintenance and System Updates		ESD	COTA	STPA	FT
2	ID#	3.3.9	Note:	E3_P	M3.1, M3.2, M3.3	C15a, F14b	III-5
3				E3_Q	M4.1	C13, F13	III-5
4	Safety Hazard:	MOC	fails to	correctly perform system updates			
5	Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
6	MOC	Update ADS software		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: System updates)
7	MOC	Replace perception components		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: System updates)
8	MOC	Calibrate equipment		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: System updates)
9	MOC	Perform post-preventive maintenance or system updates test		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
10	MOC	Update ADS built-in knowledge.		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: System updates)
11	MOC	Inform abnormal vehicle conditions.	See H3.3.6	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
12	MOC	Inform detected issues during tests	See H3.3.9	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: System updates)
13	MOC	Adequate system update or calibration test design		MOC maintenance crew	MOC coordinators	Follow established procedure of	MOC external operations (ADS Developer)
14							
15	Agent	Prior Failures: Fails to/Fails to provide					
16	MOC	Evaluate and process information collected	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
17	MOC	Instructs maintenance procedure	See H3.3.4	MOC coordinators	MOC coordinators	Follow established procedure of	MOC maintenance operations (Procedural)
18	MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
19	MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
20	ADS	Detect a system failure (diagnostic module failure)		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
21	MOC	Follow software update or instrument calibration procedure	See H3.3.8	MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: System updates)
22							
23	Consequences:	Preventive Maintenance and System Updates		Controllability	Severity	Relative Frequency	Risk Level
24		EF14: Vehicle incorrectly dispatched for operation		Medium	No Hazards	Medium	2
25		ES15: Vehicle is scheduled for external maintenance		High	No Hazards	Medium	1
26		EF16: Vehicle incorrectly cleared for operation		Medium	No Hazards	Medium	2
27		EF17: Vehicle is not scheduled for external maintenance		Medium	No Hazards	Medium	2

	C	D	E	F	G	H	I
1	Op. Phase	Preventive Maintenance and System Updates		ESD	COTA	STPA	FT
2	ID#	3.3.10		E3_R	M1.3	C13b	III-1
3	Safety Hazard:	MOC	fails to	inspect vehicle			
4	Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
5	MOC	Evaluate and process information collected	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
6	MOC	Instructs inspection procedure		MOC coordinators	MOC coordinators	Follow established procedure of	MOC maintenance operations (Procedural)
7	MOC	Follow service inspection procedure		MOC inspection crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Service inspection)
8							
9	Agent	Prior Failures: Fails to/Fails to provide					
10	MOC	Collect data from the FOC	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
11	MOC	Request specific information from FOC	See H3.3.1	MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
12	FOC	Transmit prescribed information to MOC	See H3.2.1.	FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
13	FOC	Receive request for information	See H3.2.1.	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
14	FOC	Provide requested information	See H3.2.1.	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
15	FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
16	MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
17	MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
18	MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
19	MOC	Communicate schedule correctly	See H3.2.1.	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
20	FOC	Request maintenance activities schedule verification	See H3.2.1.	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
21	MOC	Monitor FOC communications	See H3.2.1.	MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
22	FOC	Monitor MOC communications	See H3.2.1.	FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
23	ADS	Transmit information due to external connectivity failure	See H1.1.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
24							
25	Consequences:	Preventive Maintenance and System Updates		Controllability	Severity	Relative Frequency	Risk Level
26		ES11: Vehicle is stationed at MOC		Medium	No Hazards	Medium	2
27		EF14: Vehicle incorrectly dispatched for operation		Medium	No Hazards	Medium	2
28		EF16: Vehicle incorrectly cleared for operation		Medium	No Hazards	Medium	2

C	D	E	F	G	H	I
Op. Phase	Preventive Maintenance and System Updates		ESD	COTA	STPA	FT
ID#	3.3.11	Note:	E3_S	M2.1	C13a, F13a, F13b	III-2
Safety Hazard:	MOC	fails to	perform service inspection correctly			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
MOC	Follow service inspection procedure		MOC inspection crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Service inspection)
MOC	Determine if vehicle passed service inspection		MOC inspection crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Service inspection)
MOC	Inform abnormal vehicle conditions and status (cleared/not cleared).		MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Vehicle clearance)
MOC	Inform vehicle detected issues.		MOC inspection crew	MOC inspection crew	Follow established procedure of	MOC Crew (Procedures: Pre-shift inspection)
Agent	Prior Failures: Fails to/Fails to provide					
MOC	Collect data from the FOC	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Request specific information from FOC	See H3.3.1	MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
MOC	Evaluate and process information collected	See H3.3.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
FOC	Transmit prescribed information to MOC	See H3.2.1	FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
FOC	Receive request for information	See H3.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
FOC	Provide requested information	See H3.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Maintenance operations)
ADS	Transmit outcome of self diagnosis tests	See H1.1.2, H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Recorded diagnostic logs for MOC crew inspection.	See H1.1.2, H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Recorded diagnostic logs for FOC operator supervision.	See H1.2.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Transmit communication from vehicle to FOC (control center).	See H1.1.2, H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
MOC	Instructs inspection procedure		MOC coordinators	MOC coordinators	Follow established procedure of	MOC maintenance operations (Procedural)
MOC	Adequate inspection procedure		MOC inspection crew	MOC coordinators	Follow established procedure of	MOC external operations (ADS Developer)
ADS	Record informative vehicle logs		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Detect a system failure (diagnostic module failure)	See H1.1.2, H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
Consequences:	Preventive Maintenance and System Updates		Controllability	Severity	Relative Frequency	Risk Level
	ES11: Vehicle is stationed at MOC		Medium	No Hazards	Medium	2
	ES13: Vehicle cleared for operation		High	No Hazards	High	1
	EF14: Vehicle incorrectly dispatched for operation		Medium	No Hazards	Medium	2
	ES15: Vehicle is scheduled for external maintenance		High	No Hazards	Medium	1
	EF16: Vehicle incorrectly cleared for operation		Medium	No Hazards	Medium	2
	EF17: Vehicle is not scheduled for external maintenance		Medium	No Hazards	Medium	2
	EF18: Vehicle passes a faulty inspection		Medium	No Hazards	Medium	2

Op. Phase	Preventive Maintenance and System Updates		ESD	COTA	STPA	FT
ID#	3.3.12		E3_U	M2.2	F13b, C14a, C14b	III-3
Safety Hazard:	MOC	fails to	perform preventive maintenance at MOC			
Agent	Failure Mode: Fails to/Fails to provide			Risk Contributors	Agent Responsible	Agent Responsibility
MOC	Follow preventive maintenance procedures		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Determine if preventive maintenance was successful		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Perform low complexity preventive maintenance		MOC coordinators	MOC coordinators	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Inform abnormal vehicle conditions.		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Follow correct maintenance procedure		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
MOC	Instructs maintenance procedure		MOC coordinators	MOC coordinators	Follow established procedure of	MOC maintenance operations (Procedural)
MOC	Schedule vehicle maintenance crew		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Request vehicle information		MOC maintenance crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Maintenance)
Agent	Prior Failures: Fails to/Fails to provide					
MOC	Follow service inspection procedure	See H3.3.11	MOC inspection crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Service inspection)
MOC	Determine if vehicle passed service inspection	See H3.3.11	MOC inspection crew	MOC maintenance crew	Follow established procedure of	MOC Crew (Procedures: Service inspection)
MOC	Adequate maintenance procedures		MOC maintenance crew	MOC coordinators	Follow established procedure of	MOC external operations (ADS Developer)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
Consequences:	Preventive Maintenance and System Updates		Controllability	Severity	Relative Frequency	Risk Level
	EF14: Vehicle incorrectly dispatched for operation		Medium	No Hazards	Medium	2
	ES15: Vehicle is scheduled for external maintenance		High	No Hazards	Medium	1
	EF16: Vehicle incorrectly cleared for operation		Medium	No Hazards	Medium	2
	EF17: Vehicle is not scheduled for external maintenance		Medium	No Hazards	Medium	2

Op. Phase	Passenger Pick-Up/Passenger Drop-Off		ESD	COTA	STPA	FT
ID#	4.1.4		E4_A	A2	F2a, F3a, C1, C3, C4	I-2
Safety Hazard:	ADS	fails to	achieve SSC for pick-up/drop-off			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
ADS	Determine local road rules	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Determine optimal trajectory	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: local path planning)
ADS	Execute optimal planned trajectory	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Apply tactical maneuver	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Determine optimal trajectory	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: local path planning)
ADS	Adapt local path to DDT plan	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Adapt local path plan to DDT constraints (local traffic laws, ODD specifications).	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Request kinematic action	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Request vehicle commands (hazard lights, turn signals, etc.)	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Implement kinematic action	See H1.1.1	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: motion control)
ADS	Implement signal action	See H1.1.1	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: electronic systems)
ADS	Correct vehicle control command	See H1.1.3, H2.1.2	ADS vehicle	MOC maintenance crew	Ensure adequate state of	ADS vehicle (Control: motion control)
ADS	Implement remote commands	See H1.1.3, H2.1.2	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: maneuver execution)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Monitor the driving environment and collect data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Process collected raw information	See H1.1.2, H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Assess surrounding objects and events	See H1.1.2, H2.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine if SSC is achievable	See H1.1.3, H2.1.2	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Processed sensor data for DDT planning.	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Detected context (perception data) for DDT planning	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Transmit information due to vehicle communication channel failure	See H1.1.2, H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to external connectivity failure	See H1.1.2, H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
Consequences:	Passenger Pick-Up		Controllability	Severity	Relative Frequency	Risk Level
ES4: Post-incident procedures are initiated.			Medium	Traffic disruption	Low	2
EF6: Vehicle and passenger are stranded			Low	Fatality and Injury	Low	4
EF7: Passenger at risk			Very Low	Fatality and Injury	Low	5
ES8: ADS Vehicle is on-route to destination with passengers			High	No Hazards	High	1
Consequences:	Passenger Drop-Off		Controllability	Severity	Relative Frequency	Risk Level
ES4: Post-incident procedures are initiated.			Medium	Traffic disruption	Low	2
EF6: Vehicle and passenger are stranded			Low	Fatality and Injury	Low	4
EF7: Passenger at risk			Very Low	Fatality and Injury	Low	5
ES20: ADS Vehicle is on-route to destination without passengers			High	No Hazards	High	1

Op. Phase	Passenger Pick-Up		ESD	COTA	STPA	FT
ID#	4.1.2		E4_C	A5.4	F6a, C2a	I-1
			E4_D	A5.4	C2a	I-1
Safety Hazard:	ADS vehicle	fails to	start the trip			
	ADS vehicle	fails to	wait for trip confirmation			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
ADS	Receive confirmation that pick-up has been completed		ADS communication	MOC inspection crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Execute optimal planned trajectory	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Apply tactical maneuver	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Trip confirmation		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: global path planning)
ADS	Request kinematic action	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Request vehicle commands (hazard lights, turn signals, etc.)	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Implement kinematic action	See H1.1.1	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: motion control)
ADS	Implement signal action	See H1.1.1	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: electronic systems)
ADS	Adequate DDT plan (OEDR)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Monitor the driving environment and collect data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Process collected raw information	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Assess surrounding objects and events	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Determine local road rules	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Determine optimal trajectory	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: local path planning)
ADS	Establish and maintain communication with FOC	See H1.1.2, H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Processed sensor data for DDT planning.	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Detected context (perception data) for DDT planning	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Adapt local path to DDT plan	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: object and event response)
ADS	Adapt local path plan to provided waypoints.	See H1.2.2, H2.2.2	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Adapt local path plan to DDT constraints (local traffic laws, ODD specifications).	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Request to adapt global path to selected destination.		ADS software	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Request new global path.		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: local path planning)
Consequences:	Passenger Pick-Up		Controllability	Severity	Relative Frequency	Risk Level
	ES4: Post-incident procedures are initiated.		Medium	Traffic disruption	Low	2
	EF6: Vehicle and passenger are stranded		Low	Fatality and Injury	Low	4
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5
	ES8: ADS Vehicle is on-route to destination with passengers		High	No Hazards	High	1

Op. Phase	Passenger Drop-Off		ESD	COTA	STPA	FT
ID#	4.1.3		E4_H	A5.4	F6a	I-1
Safety Hazard:	ADS vehicle	fails to	end the trip			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
ADS	Receive confirmation that drop-off has completed		ADS communication	MOC inspection crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Trip confirmation		ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: global path planning)
ADS	Request vehicle commands (hazard lights, turn signals, etc.)	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: local path planning)
ADS	Implement signal action	See H1.1.1	ADS vehicle	MOC inspection crew	Verify functionality of	ADS vehicle (Control: electronic systems)
ADS	Adequate DDT plan (OEDR)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Request new global path.		ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: local path planning)
Agent	Prior Failures: Fails to/Fails to provide					
ADS	Monitor the driving environment and collect data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Process collected raw information	See H1.1.2, H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Assess surrounding objects and events	See H1.1.2, H2.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Processed sensor data for DDT planning.	See H1.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Detected context (perception data) for DDT planning	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event detection)
ADS	Establish and maintain communication with FOC	See H1.1.2, H2.1.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
Consequences:	Passenger Drop-Off		Controllability	Severity	Relative Frequency	Risk Level
	ES4: Post-incident procedures are initiated.		Medium	Traffic disruption	Low	2
	EF6: Vehicle and passenger are stranded		Low	Fatality and Injury	Low	4
	EF7: Passenger at risk		Very Low	Fatality and Injury	Low	5
	ES20: ADS Vehicle is on-route to destination without passengers		High	No Hazards	High	1

C	D	E	F	G	H	I
Op. Phase	Post-Incident Management		ESD	COTA	STPA	FT
ID#	5.2.1		E5_C	F1.1	F2b, F8b	II-4
Safety Hazard:	FOC	fails to	confirm other road users are involved			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Determine if there are passengers or other road users were involved		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Communicate with vehicle		FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Determine if first responders should be alerted		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
ADS	Transmit information due to external connectivity failure	See H1.1.2, H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Follow emergency procedures		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Evaluate state of vehicle	See H1.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Evaluate state of passengers and vehicle	See H2.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
FOC	Receive requests from passengers	See H2.2.1	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
ADS	Processed sensor data (perception) for FOC operator supervision.	See H1.2.1, H2.2.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Transmit communication from vehicle to FOC (control center).		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Transmit communication from passenger to vehicle.	See H2.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Transmit communication from vehicle to FOC (service operator).	See H2.2.1	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Connect FOC (service operator) to passenger	See H2.2.4	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Transmit communication from FOC (service operator) to vehicle.	See H2.2.4	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Informative vehicle status	See H1.2.1, H2.2.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: information fusion)
ADS	Detect a system failure (diagnostic module failure)	See H1.1.2, H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
Consequences:	Post-Incident Management		Controllability	Severity	Relative Frequency	Risk Level
	F24: Passengers and/or other road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF25: Passengers, and/or others at risk; vehicle not recovered		Very Low	Fatality and Injury	Very Low	4
	EF26: Passengers and/or others, at risk; incident is not reported		Very Low	Fatality and Injury	Very Low	4
	EF30: Other road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF31: Other road users at risk; vehicle not recovered		Very Low	Fatality and Injury	Very Low	4
	EF32: Other road users at risk; incident is not reported		Very Low	Fatality and Injury	Very Low	4
	EF33: Passenger is stranded; other road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF34: Passenger is stranded; vehicle is not recovered; other road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF35: Passenger is stranded; incident is not reported; other road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF36: Vehicle arrives at MOC for maintenance; other road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF37: Vehicle and others road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF38: Vehicle is stranded; others road users at risk		Very Low	Fatality and Injury	Very Low	4

Op. Phase	Post-Incident Management		ESD	COTA	STPA	FT
ID#	5.2.2		E5_D	F2.1	C9a, C9b, F9a, F9b	II-4
Safety Hazard:	FOC	fails to	contact first responders			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Alert first responders		FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Incident management)
ADS	Transmit information due to external connectivity failure	See H1.1.2, H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Follow emergency procedures	See H5.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Determine if first responders should be alerted	See H5.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Alert DDT fallback is required	See H2.2.1	FOC service operator	FOC safety operator	Follow established procedure of	FOC service operator (Incident management)
FOC	Inform passenger status.	See H2.2.2	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Incident management)
FOC	Inform vehicle status.		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Inform DDT fallback is required.	See H2.2.4	FOC safety operator	FOC safety operator	Follow established procedure of	FOC service operator (Passenger requests)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
Consequences:	Post-Incident Management		Controllability	Severity	Relative Frequency	Risk Level
	F24: Passengers and/or other road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF25: Passengers, and/or others at risk; vehicle not recovered		Very Low	Fatality and Injury	Very Low	4
	EF26: Passengers and/or others, at risk; incident is not reported		Very Low	Fatality and Injury	Very Low	4
	EF30: Other road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF31: Other road users at risk; vehicle not recovered		Very Low	Fatality and Injury	Very Low	4
	EF32: Other road users at risk; incident is not reported		Very Low	Fatality and Injury	Very Low	4

Op. Phase	Post-Incident Management		ESD	COTA	STPA	FT
ID#	5.2.3		E5_E	F3	C11b, C11d, F11b	III-6
Safety Hazard:	FOC	fails to	report incident to MOC			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Collect and transmit information on incident to MOC		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Initiate post-incident procedures	See H1.2.4, H2.2.3	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Deliver incident report		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
ADS	Transmit information due to external connectivity failure	See H1.1.2, H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Follow emergency procedures	See H5.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Determine if there are passengers or other road users were involved	See H5.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Communicate with vehicle	See H5.2.1	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Determine if first responders should be alerted	See H5.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Determine if vehicle can perform MR-DDT	See H5.2.6	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Determine if a recovery team should be dispatched	See H5.3.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Determine if a secondary vehicle should be dispatched	See H5.2.5	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Alert DDT fallback is required	See H5.2.4	FOC service operator	FOC safety operator	Follow established procedure of	FOC service operator (Incident management)
FOC	Inform passenger status.	See H5.2.4	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Incident management)
FOC	Inform vehicle status.	See H5.2.6	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Inform DDT fallback is required.	See H5.2.6	FOC safety operator	FOC safety operator	Follow established procedure of	FOC service operator (Passenger requests)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
Consequences:	Post-Incident Management		Controllability	Severity	Relative Frequency	Risk Level
	EF23: Vehicle not recovered; incident not reported to the MOC		Low	Fatality and Injury	Very Low	3
	EF26: Passengers and/or others, at risk; incident is not reported		Very Low	Fatality and Injury	Very Low	4
	EF29: Passenger is stranded; vehicle is not recovered; incident not reported		Low	Property-damage only	Very Low	3
	EF32: Other road users at risk; incident is not reported		Very Low	Fatality and Injury	Very Low	4
	EF35: Passenger is stranded; incident is not reported; other road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF41: Incident not reported to the MOC. No other parties are involved.		Low	Property-damage only	Very Low	3

	C	D	E	F	G	H	I
1	Op. Phase	Post-Incident Management		ESD	COTA	STPA	FT
2	ID#	5.2.4		E5_G	F1.2	C7b, F7a, F8a, F9a	II-4
3	Safety Hazard:	FOC	fails to	communicate with passenger			
4	Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
5	FOC	Communicate with vehicle	See H5.2.1	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
6	FOC	Determine if first responders should be alerted	See H5.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
7	FOC	Determine if a secondary vehicle should be dispatched	See H5.2.5	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
8	ADS	Transmit communication from passenger to vehicle.		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
9	ADS	Transmit communication from vehicle to FOC (service operator).		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
10	ADS	Connect FOC (service operator) to passenger		ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
11	FOC	Transmit FOC (service operator) contact request to passengers		FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
12	FOC	Inform passenger status.		FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Incident management)
13	ADS	Transmit information due to vehicle communication channel failure	See H1.1.2, H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
14	ADS	Transmit information due to external connectivity failure	See H1.1.2, H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
15	FOC	Follow emergency procedures	See H5.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
16							
17	Agent	Prior Failures: Fails to/Fails to provide					
18	FOC	Determine if there are passengers or other road users were involved	See H5.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
19	ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
20	ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
21	ADS	Detect a system failure (diagnostic module failure)	See H1.1.2, H2.1.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
22	MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
23	MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
24	MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
25	FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
26							
27	Consequences:	Post-Incident Management		Controllability	Severity	Relative Frequency	Risk Level
28		ES21: Post-incident procedures are completed		High	Fatality and Injury	Low	2
29		EF22: Vehicle is not recovered		Low	Fatality and Injury	Very Low	3
30		EF23: Vehicle not recovered; incident not reported to the MOC		Low	Fatality and Injury	Very Low	3
31		F24: Passengers and/or other road users at risk		Very Low	Fatality and Injury	Very Low	4
32		EF25: Passengers, and/or others at risk; vehicle not recovered		Very Low	Fatality and Injury	Very Low	4
33		EF26: Passengers and/or others, at risk; incident is not reported		Very Low	Fatality and Injury	Very Low	4
34		EF30: Other road users at risk		Very Low	Fatality and Injury	Very Low	4
35		EF31: Other road users at risk; vehicle not recovered		Very Low	Fatality and Injury	Very Low	4
36		EF32: Other road users at risk; incident is not reported		Very Low	Fatality and Injury	Very Low	4

C	D	E	F	G	H	I
Op. Phase	Post-Incident Management		ESD	COTA	STPA	FT
ID#	5.2.5		E5_H	F2.4	C9a, C6b, F9b, C9c	II-4
Safety Hazard:	FOC	fails to	dispatch secondary vehicle for passengers			
Agent	Failure Mode: Fails to/Fails to provide			Risk Contributors	Agent Responsible	Agent Responsibility
FOC	Dispatch a secondary vehicle to complete trip		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Dispatching)
FOC	Transmit dispatch commands	See H1.2.3	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Dispatching)
ADS	Establish and maintain communication with FOC	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Receive remote commands	See H1.2.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Request secondary passenger vehicle	See H5.2.4	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).	See H1.2.4	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Request to adapt global path plan to waypoints provided by FOC.	See H1.2.3	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: global path planning)
FOC	Inform vehicle status.		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
ADS	Transmit information due to external connectivity failure	See H1.1.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to vehicle communication channel failure	See H1.1.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
FOC	Follow emergency procedures	See H5.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
MOC	Provide a secondary vehicle		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Incident management)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Determine if there are passengers or other road users were involved	See H5.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Determine if a secondary vehicle should be dispatched		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
ADS	Transmit communication from passenger to vehicle.	See H5.2.4	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Transmit communication from vehicle to FOC (service operator).	See H5.2.4	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
ADS	Connect FOC (service operator) to passenger	See H5.2.4	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: Passenger)
FOC	Transmit FOC (service operator) contact request to passengers	See H5.2.4	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Passenger requests)
FOC	Inform passenger status.	See H5.2.4	FOC service operator	FOC service operator	Follow established procedure of	FOC service operator (Incident management)
ADS	Use up to date/correct HD maps (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Detect a system failure (diagnostic module failure)	See H1.1.2	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
Consequences:	Post-Incident Management		Controllability	Severity	Relative Frequency	Risk Level
	EF27: Passengers are stranded		Medium	Property-damage only	Very Low	2
	EF28: Passengers are stranded; vehicle is not recovered		Low	Property-damage only	Very Low	3
	EF29: Passenger is stranded; vehicle is not recovered; incident not reported		Low	Property-damage only	Very Low	3
	EF33: Passenger is stranded; other road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF34: Passenger is stranded; vehicle is not recovered; other road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF36: Vehicle arrives at MOC for maintenance; other road users at risk		Very Low	Fatality and Injury	Very Low	4

Op. Phase	Post-Incident Management		ESD	COTA	STPA	FT
ID#	5.2.6	Note:	E5_I	F1.3.2	F2b, F5b, C8b	II-4
Safety Hazard:	FOC	fails to	send correct DDT fallback command			
Agent	Failure Mode: Fails to/Fails to provide		Risk Contributors	Agent Responsible	Agent Responsibility	
FOC	Determine if vehicle can perform MR-DDT	See H1.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Dispatch vehicle to MOC in MR-DDT	See H1.2.3	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Connect FOC (safety operator) to vehicle (DDT fallback plans and waypoints).	See H1.2.4	FOC communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Request to adapt local path plan to waypoints provided by FOC.	See H1.2.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
FOC	Follow DDT-fallback requirements	See H2.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
FOC	Follow DDT-fallback procedure	See H2.2.2	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (DDT-fallback)
ADS	Transmit information due to vehicle communication channel failure	See H1.1.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
ADS	Transmit information due to external connectivity failure	See H1.1.2	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Evaluate state of vehicle	See H1.2.1	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Monitoring)
ADS	Establish and maintain communication with FOC	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Transmit outcome of self diagnosis tests	See H1.1.2	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: diagnostics)
ADS	Processed sensor data (perception) for FOC operator supervision.	See H1.2.1	ADS software	MOC inspection crew	Verify functionality of	ADS software (DDT: information fusion)
ADS	Recorded diagnostic logs for FOC operator supervision.	See H1.2.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: diagnostics)
ADS	Transmit communication from vehicle to FOC (control center).	See H1.1.2	ADS communication	MOC inspection crew	Verify functionality of	ADS vehicle (Connectivity: FOC)
ADS	Implement correct DDT-fallback strategies	See H1.1.3	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: object and event response)
ADS	Collect correct perception and localization data	See H1.1.1	ADS hardware	MOC inspection crew	Verify functionality of	ADS hardware (DDT: perception and localization)
ADS	Use up to date/correct HD maps (not available)	See H2.1.2	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
ADS	Enforce up to date/correct ODD limits (not available)	See H1.1.1	ADS software	MOC maintenance crew	Ensure adequate state of	ADS software (DDT: built-in knowledge)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
Consequences:	Post-Incident Management		Controllability	Severity	Relative Frequency	Risk Level
	EF30: Other road users at risk		Very Low	Fatality and Injury	Very Low	4
	EF31: Other road users at risk; vehicle not recovered		Very Low	Fatality and Injury	Very Low	4
	EF32: Other road users at risk; incident is not reported		Very Low	Fatality and Injury	Very Low	4
	ES39: Post-incident procedures are completed. No other parties are involved.		High	Property-damage only	Low	2
	EF40: Vehicle is not recovered. No other parties are involved.		Low	Property-damage only	Very Low	3
	EF41: Incident not reported to the MOC. No other parties are involved.		Low	Property-damage only	Very Low	3

Op. Phase	Post-Incident Management		ESD	COTA	STPA	FT
ID#	5.3.1		E5_F	M3.1	C10, C11c, F10a, F10b, F11c	III-6
Safety Hazard:	MOC	fails to	dispatch recovery team			
Agent	Failure Mode: Fails to/Fails to provide			Risk Contributors	Agent Responsible	Agent Responsibility
MOC	Follow incident procedures	See H5.2.1	MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Incident Management)
MOC	Confirm FOC vehicle recovery request		MOC communication	MOC coordinators	Follow established procedure of	MOC coordinators (Incident Management)
MOC	Dispatch recovery team to retrieve vehicle.		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Incident Management)
MOC	Confirm vehicle recovery request		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Recovery team)
MOC	Inform vehicle has been recovered		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Recovery team)
MOC	Schedule maintenance		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
Agent	Prior Failures: Fails to/Fails to provide					
FOC	Collect and transmit information on incident to MOC	See H5.2.3	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Receive request for information		FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
FOC	Provide requested information		FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
MOC	Request specific information from FOC		MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
MOC	Evaluate and process information collected		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Maintenance operations)
MOC	Receive command to dispatch vehicle		MOC communication	MOC coordinators	Follow established procedure of	MOC coordinators (Incident Management)
FOC	Initiate post-incident procedures	See H1.2.4, H2.2.3	FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
FOC	Request vehicle recovery		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Incident management)
MOC	Implement operational procedure update		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
FOC	Confirm operational procedure update		FOC safety operator	FOC safety operator	Follow established procedure of	FOC safety operator (Procedural)
MOC	Update operational procedures		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC external operations (ADS Developer)
MOC	Confirm procedure update has been implemented		MOC coordinators	MOC coordinators	Implement updates or external requests from	MOC maintenance operations (Procedural)
MOC	Monitor FOC communications		MOC communication	MOC coordinators	Report anomalies of	MOC coordinators (Connectivity: FOC)
FOC	Monitor MOC communications		FOC communication	FOC safety operator	Report anomalies of	FOC safety operator (Connectivity: MOC)
ADS	Transmit information due to external connectivity failure	See H1.1.2, H2.1.1	ADS communication	FOC safety operator	Report anomalies of	ADS vehicle (Connectivity: FOC)
MOC	Confirm post-incident procedures have been initiated		MOC coordinators	MOC coordinators	Follow established procedure of	MOC coordinators (Incident Management)
Consequences:	Post-Incident Management		Controllability	Severity	Relative Frequency	Risk Level
	EF22: Vehicle is not recovered		Low	Fatality and Injury	Very Low	3
	EF25: Passengers, and/or others at risk; vehicle not recovered		Very Low	Fatality and Injury	Very Low	4
	EF28: Passengers are stranded; vehicle is not recovered		Low	Property-damage only	Very Low	3
	EF31: Other road users at risk; vehicle not recovered		Very Low	Fatality and Injury	Very Low	4
	EF40: Vehicle is not recovered. No other parties are involved.		Low	Property-damage only	Very Low	3