

Hazard Analysis & Risk Assessment

Updated:

Situational Analysis						
Hazard ID	Operational Mode	Operational Scenario	Environmental Details	Situation Details	Other Details (optional)	Item Usage (function)
HA-001	OM03 - Normal Driving	OS04 - Highway	EN06 - Rain (slippery road)	SD02 - High speed	N/A	IU01 - Correctly used
HA-002	OM03 - Normal Driving	OS03 - Country Road	EN01 - Normal conditions	SD02 - High speed	N/A	IU02 - Incorrectly used
HA-003	OM03 - Normal Driving	OS03 - Country Road	EN01 - Normal conditions	SD02 - High speed	N/A	IU01 - Correctly used
HA-004	OM04 - Backward Driving	OS02 - City Road	EN01 - Normal conditions	SD01 - Low speed	N/A	IU03 - N/A

Hazard Identification						
Hazard ID	Function	Deviation	Deviation Details	Hazardous Event (resulting effect)	Event Details	Hazardous Event Description
HA-001	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver with haptic feedback.	DV04 - Actor effect is too much	The LDW function applies an oscillating torque with very high torque (above limit)	EV00 - Collision with other vehicle	High haptic feedback can affect driver's ability to steer as intended. The driver could lose control of the vehicle and collide with another vehicle or road infrastructure.	The LDW function applies too high an oscillating torque to the steering wheel (above limit).
HA-002	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane.	DV03 - Function always activated	The driver is misusing the system by exploiting the LKA function as a fully autonomous function.	EV00 - Collision with other vehicle	The driver takes both hands off the wheel indefinitely and cannot react to other vehicles on the road that are merging or turning into the current lane, causing a collision.	The LKA function has no time limit so the driver misinterprets and misuses the function to be fully autonomous.
HA-003	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane.	DV03 - Function always activated	The LKA function does not deactivate when the driver regains control of the steering wheel.	EV00 - Collision with other vehicle	Changing lanes may cause the vehicle to unexpectedly jerk in an attempt to perform the LKA function and collide with another vehicle or road infrastructure.	The LKA function never deactivates when the driver regains control of the steering wheel and therefore continues to operate in an improper state.
HA-004	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane.	DV19 - Sensor detection is wrong	The LKA function detects the sidewalk as the current lane when backing out of a parking space that backs up to a city road.	EV02 - Collision with pedestrian	The LKA function takes over control of the vehicle unexpectedly from the driver's perspective and corrects the vehicle to the sidewalk (the current lane), bumping into a pedestrian at low speed.	The LKA function actuates as expected but identifies and corrects to the wrong lane due to inaccurate sensor data.

Hazard Analysis & Risk Assessment

Updated:

Hazard ID	Hazardous Event Classification					
ID	Exposure (of situation)	Rationale (for exposure)	Severity (of potential harm)	Rationale (for severity)	Controllability (of hazardous event)	Rationale (for controllability)
HA-001	E2 - Low probability	Driver tends to maintain higher attention to driving task while travelling in rainy weather conditions.	S3 - Life-threatening or fatal injuries	Driver is travelling at high speed.	C3 - Difficult to control or uncontrollable	Driver cannot control vehicle while LKA function is operating.
HA-002	E2 - Low probability	Driver does not live near country roads. Limited country road driving. The driver slows down naturally on unfamiliar roads.	S3 - Life-threatening or fatal injuries	Driver is travelling at high speed.	C3 - Difficult to control or uncontrollable	Driver cannot control vehicle while LKA function is operating.
HA-003	E2 - Low probability	Driver does not live near country roads. Limited country road driving. The driver slows down naturally on unfamiliar roads.	S3 - Life-threatening or fatal injuries	Driver is travelling at high speed.	C3 - Difficult to control or uncontrollable	Driver cannot control vehicle while LKA function is operating.
HA-004	E2 - Low probability	Situation dependent on uncommon parking lot design.	S1 - Light and moderate injuries	Dependent on pedestrian response.	C3 - Difficult to control or uncontrollable	Driver cannot control vehicle while LKA function is operating.

Hazard ID	Determination of ASIL and Safety Goals	
ID	ASIL Determination	Safety Goal
HA-001	ASIL B	The LKA function shall end after a given time interval to prevent over applying torque.
HA-002	ASIL B	The LKA function shall be time limited so that the driver cannot misuse the system for autonomous driving.
HA-003	ASIL B	The LKA function shall be time limited and the additional steering torque shall end after a given time interval so that the system cannot maintain an improper state.
HA-004	QM	Sensors shall maintain a high quality of readings. If this does not happen, the LKA function shall be deactivated and a warning light shall be displayed.

8/27/17

Situation Description
Normal driving on a highway during rain (slippery road) with high speed.
Normal driving on country roads during normal conditions with high speed.
Normal driving on country roads during normal conditions with high speed.
Backwards driving on city roads during normal driving conditions with low speed.

8/27/17