Hazard Analysis & Risk Assessment

Hazard ID	Situational Analysis						
	Operational Mode	**Operational Scenario**	**Environmental Details**	**Situation Details**	**Other Details (optional)**	**Item Usage (function)**	**Situation Description**
HA-001	OM03 - Normal driving	OS04 - Highway	EN06 - Rain (slippery road)	SD02 - High speed	SD07 - N/A	IU01 - Correctly used	Normal driving on a highway during rain (slippery road) with high speed and correctly used system.
HA-002	OM03 - Normal driving	OS03 - Country Road	EN01 - Normal conditions	SD02 - High speed	SD07 - N/A	IU02 - Incorrectly used	Normal driving on a country road during normal conditions with high speed and incorrectly used system.
HA-003	OM03 - Normal driving	OS02 - City Road	EN01 - Normal conditions	SD01 - Low speed	SD07 - N/A	IU01 - Correctly used	Normal driving on a city road during normal conditions with high speed and correctly used system.
HA-004	OM03 - Normal driving	OS02 - City Road	EN01 - Normal conditions	SD01 - Low speed	SD07 - N/A	IU01 - Correctly used	Normal driving on a city road during normal conditions with any speed and correctly used system.

Hazard ID	Hazard Identification					
	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 loose control and could collide with another nearby vehicle or the side of the road.	The amount of oscillating torque applied to the steering wheel by the Lane Departure Warning item is too significant and above the 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 and keeps it always active.	EV00 - Collision with other vehicle	The driver takes both hands off the wheel indefinitely and looses attentiveness. As a result, the driver can not react to events happening on the road such as cars merging into the ego lane.	The LKA does not disengage and the function exits its operational domain.
HA-003	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	DV13 - Sensor sensitivity is too low	The lane on the road is not correctly marked and the Camera Sensor unit does not detect it.	EV02 - Collision with pedestrian	The car leaves it ego lane after not detecting a lane and run over a pedestrian walking nearby.	The LKA does not detect a lane because of software sensibility threshold.
HA-004	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	DV06 - Actor action too early	The system starts following the wrong set of line right after activation.	EV-02 - Side collision with other traffic	The LKA functionality is activated and takes immediate effect. It tries to keep the car in-between a set of lanes on the road which the driver didn’t want to follow.	The LKA functionality triggers an abrupt and unexpected lane change which results in a potential collision with obstacles or vehicles.

Hazard ID	Hazardous Event Classification					
	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	The probability to maintain a high speed on the highway over a slippery road is less than 3% of the operating time of the vehicle.	S3 - Life-threatening or fatal injuries	Collisions at high speed would most probably cause fatal injuries.	C3 - Difficult to control or uncontrollable	It would become challenging to keep the hands on the wheel. The steering wheel oscillations could be impacting the trajectory of the car.
HA-002	E3 - Medium probability	Destined to the US Market, country road are frequent, driving is likely to have low or inexistent understanding of the Lane Keeping Assistance function.	S3 - Life-threatening or fatal injuries	Collisions at high speed would most probably cause fatal injuries.	C3 - Difficult to control or uncontrollable	Understanding of the immediate situation after taking the eyes off the road could take up to 5 seconds before being able to control of the vehicle in a safe manner. At high speed 5 seconds translates to an extremely long driven distance.
HA-003	E4 - High probability	Almost every drive happens near a pedestrian area at some point along the way.	S2 - Severe and life-threatening injuries	Collisions at low to medium speed could result in life-threatening injuries.	C3 - Difficult to control or uncontrollable	The difficulty to control the car in that situation results form the fact that the driver must react instantaneously in order to avoid the collision once he/she has noticed the missed lane detection.
HA-004	E4 - High probability	Every day we choose to steer away from the main lane marking in order to leave the main road form a smaller one for example.	S2 - Severe and life-threatening injuries	Abrupt lane change can result in a collision with other vehicles.	C3 - Difficult to control or uncontrollable	Abrupt lane change can surprise the driver who might react erratically and panic.

Hazard ID	Determination of ASIL and Safety Goals	
	ASIL Determination	**Safety Goal**
HA-001	C	The amplitude of the oscillating steering torque from the Lane Departure Warning function shall be limited and could never exceed a defined safety threshold.
HA-002	C	The LKA function shall be time limited to keep the driver focused on the driving task.
HA-003	C	Function disengagements shall be notified to the driver by significant and simultaneous warnings in the form of visual, acoustic and haptic feedbacks.
HA-004	C	The LKA function shall only be available to the driver on the highway where the lines of the ego lanes are clearly defined. The LKA function shall only start applying torque on the steering wheel after it has been activated for some time and its output was matching the driver effective behavior.

EXAMPLE DISCUSSED IN THE PROJECT INSTRUCTIONS - Headlamp System

Hazard ID	Situational Analysis						
	Operational Mode	Operational Scenario	Environmental Details	Situation Details (optional)	Other Details (optional)	Item Usage (function)	Situation Description
HA-001	Normal Driving	City Road	Normal Conditions	Low Speed	Night time + Obstacle on the	Correctly Used	Normal Driving on a City Road in Normal

Hazard ID	Hazard Identification					
	Function	Deviation	Deviation Details	Hazardous Event (resulting effect)	Event Details	Hazardous Event Description
HA-001	Low beam illuminates the	Function not activated	Both headlights stop working	Front collision with obstacle	Vehicle crashes into the	Total loss of low beam

Hazard ID	Hazardous Event Classification						Determination of ASIL and Safety Goals	
	Exposure (of situation)	Rationale (for exposure)	Severity (of potential harm)	Rationale (for severity)	Controllability (of hazardous event)	Rationale (for controllability)	ASIL Determination	Safety Goal
HA-001	E4 - High probability	night driving in the city is a regular	S1 - Light and moderate injuries	In city traffiic, speed of vehicle is expected to be low	C0 - Controllable in general	At city speed, most drivers will be able to	QM	Total Loss of Beam Shall

MORE EXAMPLES - Headlamp System

Hazard ID	Situation Analysis						
	Operational Mode	Operational Scenario	Environmental Details	Situation Details (optional)	Other Details (optional)	Item Usage (function)	Situation Description
HA-001	OM03 - Normal Driving	OS01 - City Road	EN01 - Normal conditions	SD03 - Low speed	Night time + Obstacle on the	IU01 - Correctly used	Normal Driving on City Road during Normal
HA-002	OM03 - Normal Driving	OS01 - City Road	EN04 - Snowfall (degraded view)	SD03 - Low speed	Night time + Obstacle on the	IU01 - Correctly used	Normal Driving on City Road during Snowfall
HA-003	OM03 - Normal Driving	OS03 - Highway	EN04 - Snowfall (degraded view)	SD03 - High speed	Night time + Obstacle on the	IU01 - Correctly used	Normal Driving on Highway during Snowfall
HA-004	OM03 - Normal Driving	OS02 - Country Road	EN01 - Normal conditions	SD02 - High speed	Night time + Oncoming	IU01 - Correctly used	Normal Driving on Country Road during Normal
HA-005	OM03 - Normal Driving	OS02 - Country Road	EN04 - Snowfall (degraded view)	SD04 - High speed	Night time + Obstacle on the	IU01 - Correctly used	Normal Driving on Country Road during Snowfall

Hazard ID	Hazard Identification					
	Function	Deviation	Deviation Details	Hazardous Event (resulting effect)	Event Details	Hazardous Event Description
HA-001	Low beam illuminates the	DV01 - Function not activated	Both headlights stop working	EV04 - Front collision with obstacle	Vehicle crashes into the	Total loss of low beam
HA-002	Low beam illuminates the	DV01 - Function not activated	Both headlights stop working	EV04 - Front collision with obstacle	Vehicle crashes into the	Total loss of low beam
HA-003	Low beam illuminates the	DV01 - Function not activated	Both headlights stop working	EV04 - Front collision with obstacle	Vehicle crashes into the	Total loss of low beam
HA-004	Low beam illuminates the	DV01 - Function not activated	Both headlights stop working	EV08 - Collision with other vehicle	Vehicle crashes into the	Total loss of low beam
HA-005	Low beam illuminates the	DV01 - Function not activated	Both headlights stop working	EV04 - Front collision with obstacle	Vehicle crashes into the	Total loss of low beam

Hazard ID	Hazardous Event Classification						Determination of ASIL and Safety Goals	
	Exposure (of situation)	Rationale (for exposure)	Severity (of potential harm)	Rationale (for severity)	Controllability (of hazardous event)	Rationale (for controllability)	ASIL Determination	Safety Goal
HA-001	E4 - High probability	night driving in the city is a regular	S1 - Light and moderate injuries	In city traffiic, speed of vehicle is expected to be low	C0 - Controllable in general	At city speed, most drivers will be able to	QM	Total loss of low beam
HA-002	E1 - Very low probability	night driving in the city on	S1 - Light and moderate injuries	In city traffiic, speed of vehicle is expected to be low	C1 - Simply controllable	On completely unilluminated city roads,	QM	Total loss of low beam
HA-003	E2 - Low probability	High driving is part of regular	S3 - Life-threatening or fatal injuries	On highway speed of vehicle is expected to be high	C2 - Normally controllable	When driving on highway with low beam, it	A	Total loss of low beam
HA-004	E4 - High probability	country driving is part of regular	S3 - Life-threatening or fatal injuries	On country roads speed of vehicle is expected to be high	C1 - Simply controllable	Since there is usually no other form of	B	Total loss of low beam
HA-005	E2 - Low probability	country driving is part of regular	S3 - Life-threatening or fatal injuries	On country roads speed of vehicle is expected to be high	C3 - Difficult to control or uncontrollable	Since there is usually no other form of	B	Total loss of low beam

Hazard & Risk Analysis Definitions

Operational Mode

ID	Mode	Remarks	Reference
OM01	Parked	Car is parked, ignition is off	OM01 - Parked
OM02	Ignition on	Car is parked, ignition is on	OM02 - Ignition on
OM03	Normal driving	Car is driving	OM03 - Normal driving
OM04	Backward driving	Car is driving	OM04 - Backward driving
OM05	Degraded driving	Limp home mode	OM05 - Degraded driving
OM06	Towing (active)	Towing another car	OM06 - Towing (active)
OM07	Towing (passive)	Beeing towed by another car	OM07 - Towing (passive)
OM08	Service	Vehicle is in repair garage	OM08 - Service
OM09	N/A	not applicable or not relevant	OM09 - N/A

Operational Scenario

ID	Scenario	Remarks	Reference
OS01	Any Road	road type	OS01 - Any Road
OS02	City Road	road type	OS02 - City Road
OS03	Country Road	road type	OS03 - Country Road
OS04	Highway	road type	OS04 - Highway
OS05	Mountain Pass	road type	OS05 - Mountain Pass
OS06	Off Road	road type	OS06 - Off Road
OS07	Road with gradient	road attribute	OS07 - Road with gradient
OS08	Road with bump	road attribute	OS08 - Road with bump
OS09	Road tunnel	road attribute	OS09 - Road tunnel
OS10	Road with construction site	road attribute	OS10 - Road with construction site
OS11	N/A	not applicable or not relevant	OS11 - N/A

Situation Details

ID	Scenario	Remarks	Reference
SD01	Low speed	driving attribute	SD01 - Low speed
SD02	High speed	driving attribute	SD02 - High speed
SD03	Normal acceleration	driving attribute	SD03 - Normal acceleration
SD04	High acceleration	driving attribute	SD04 - High acceleration
SD05	Normal braking	driving attribute	SD05 - Normal braking
SD06	High braking	driving attribute	SD06 - High braking
SD07	N/A	not applicable or not relevant	SD07 - N/A

Item Usage

ID	Mode	Remarks	Reference
IU01	Correctly used	Intended usage	IU01 - Correctly used
IU02	Incorrectly used	Unintended usage (foreseeable)	IU02 - Incorrectly used
IU03	N/A	not applicable or not relevant	IU03 - N/A

Environmental Details

ID	Scenario	Remarks	Reference
EN01	Normal conditions	weather attribute	EN01 - Normal conditions
EN02	Sun blares (degraded view)	weather attribute	EN02 - Sun blares (degraded view)
EN03	Fog (degraded view)	weather attribute	EN03 - Fog (degraded view)
EN04	Snowfall (degraded view)	weather attribute	EN04 - Snowfall (degraded view)
EN05	Cross-wind (lateral force)	weather attribute	EN05 - Cross-wind (lateral force)
EN06	Rain (slippery road)	road attribute	EN06 - Rain (slippery road)
EN07	Snow (slippery road)	road attribute	EN07 - Snow (slippery road)
EN08	Glace (slippery road)	road attribute	EN08 - Glace (slippery road)
EN09	N/A	not applicable or not relevant	EN09 - N/A

Deviation

ID	Deviation (Guideword)	Remarks	Reference
DV01	Function not activated	Activation error	DV01 - Function not activated
DV02	Function unexpectedly activated	Activation error	DV02 - Function unexpectedly activated
DV03	Function always activated	Activation error	DV03 - Function always activated
DV04	Actor effect is too much	Quantitative error	DV04 - Actor effect is too much
DV05	Actor effect is too less	Quantitative error	DV05 - Actor effect is too less
DV06	Actor action too early	Timing error	DV06 - Actor action too early
DV07	Actor action too late	Timing error	DV07 - Actor action too late
DV08	Actor action before	Sequence error	DV08 - Actor action before
DV09	Actor action after	Sequence error	DV09 - Actor action after
DV10	Actor effect is reverse	Logical error	DV10 - Actor effect is reverse
DV11	Actor effect is wrong	Logical error	DV11 - Actor effect is wrong
DV12	Sensor sensitivity is too high	Quantitative error	DV12 - Sensor sensitivity is too high
DV13	Sensor sensitivity is too low	Quantitative error	DV13 - Sensor sensitivity is too low
DV14	Sensor detection too early	Timing error	DV14 - Sensor detection too early
DV15	Sensor detection too late	Timing error	DV15 - Sensor detection too late
DV16	Sensor detection before	Sequence error	DV16 - Sensor detection before
DV17	Sensor detection after	Sequence error	DV17 - Sensor detection after
DV18	Sensor detection is reverse	Logical error	DV18 - Sensor detection is reverse
DV19	Sensor detection is wrong	Logical error	DV19 - Sensor detection is wrong
DV20	N/A	not applicable or not relevant	DV20 - N/A

Hazardous Events (possibe effects)

ID	Hazardous Event	Remarks	Reference
EV-07	None		EV-07 - None
EV-06	Front collision with oncoming traffic		EV-06 - Front collision with oncoming traffic
EV-05	Front collision with ahead traffic		EV-05 - Front collision with ahead traffic
EV-04	Front collision with obstacle		EV-04 - Front collision with obstacle
EV-03	Rear collision with trailing traffic		EV-03 - Rear collision with trailing traffic
EV-02	Side collision with other traffic		EV-02 - Side collision with other traffic
EV-01	Side collision with obstacle		EV-01 - Side collision with obstacle
EV00	Collision with other vehicle		EV00 - Collision with other vehicle
EV01	Collision with train		EV01 - Collision with train
EV02	Collision with pedestrian		EV02 - Collision with pedestrian
EV03	Car spins out of control		EV03 - Car spins out of control
EV04	Car comes off the road		EV04 - Car comes off the road
EV05	Car catches file		EV05 - Car catches file
EV06	N/A		EV06 - N/A

Exposure

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

Severity

ID	Description	Remarks	Probability of Injuries	Reference
S0	No injuries	No injuries	AIS 0 and less than 10 % probability of AIS 1-6	S0 - No injuries
S1	Light and moderate injuries	Light and moderate injuries	More than 10 % probability of AIS 1-6 (and not S2 or S3)	S1 - Light and moderate injuries
S2	Severe and life-threatening injuries	Severe and life-threatening injuries (survival probable)	More than 10 % probability of AIS 3-6 (and not S3)	S2 - Severe and life-threatening injuries
S3	Life-threatening or fatal injuries	Life-threatening injuries (survival uncertain), fatal injuries	More than 10 % probability of AIS 5-6	S3 - Life-threatening or fatal injuries

Controllability

ID	Description	Remarks	Reference
C0	Controllable in general	Controllable in general	C0 - Controllable in general
C1	Simply controllable	99 % or more of all drivers or other traffic participants are usually able to avoid harm	C1 - Simply controllable
C2	Normally controllable	90 % or more of all drivers or other traffic participants are usually able to avoid harm	C2 - Normally controllable
C3	Difficult to control or uncontrollable	Less than 90 % of all drivers or other traffic participants are usually able, or barely able, to avoid harm	C3 - Difficult to control or uncontrollable

Controllability	Exposure	Severity			
		S0	S1	S2	S3
C1	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	A
	E4	QM	QM	A	B
C2	E1	QM	QM	QM	QM
	E2	QM	QM	QM	A
	E3	QM	QM	A	B
	E4	QM	A	B	C
C3	E1	QM	QM	QM	A
	E2	QM	QM	A	B
	E3	QM	A	B	C
	E4	QM	B	C	D