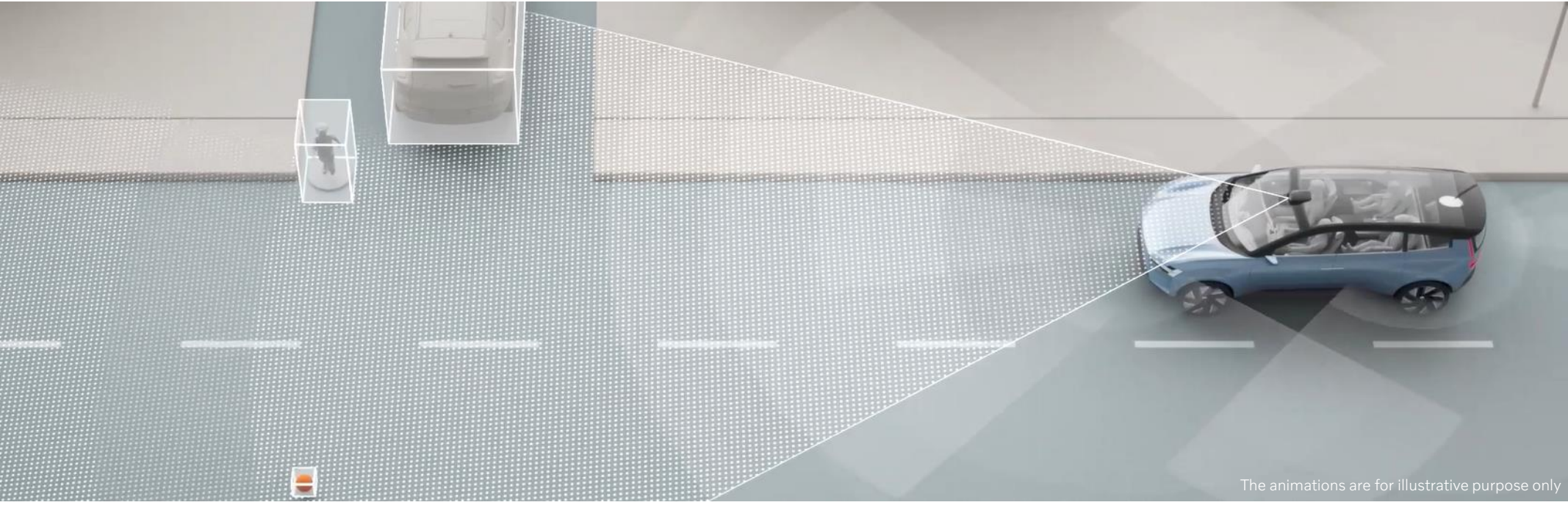
VOLVO

STPA for Autonomous Vehicles Functions



Anas Shahzad
Mona Noori
Ali Nouri

6/8/2022

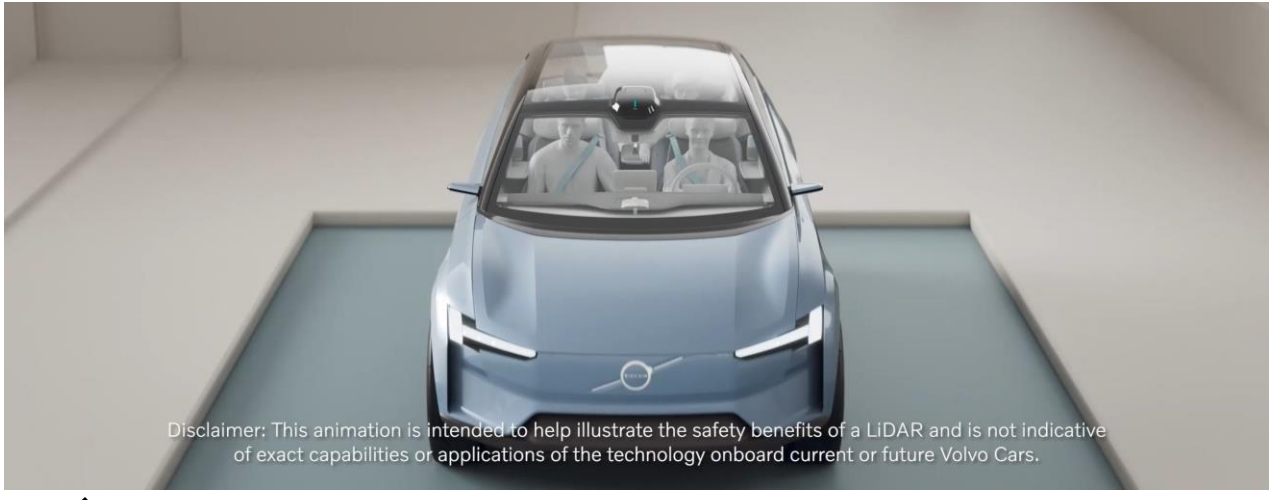
VOLVO

Disclaimer

The materials presented is the results of scientific work. All findings, results, and conclusions in this presentation are those of authors and do not necessarily reflect the views of Volvo Cars.

VOLVO

Towards Safe **Un-Supervised** Autonomous Driving



Functional Safety (ISO 26262)

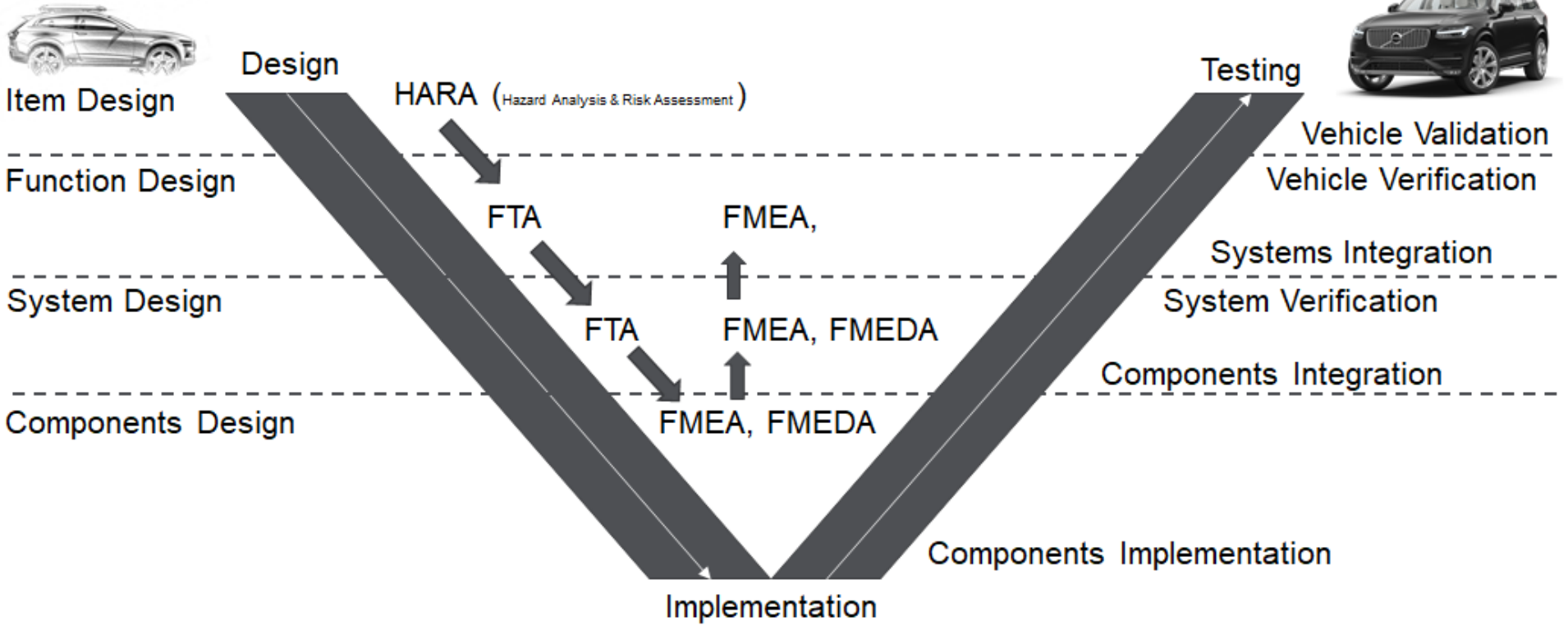
- Systematic SW failure
- Systematic HW failure
- Random HW failure

Safety of the Intended Functionality (ISO 21448)

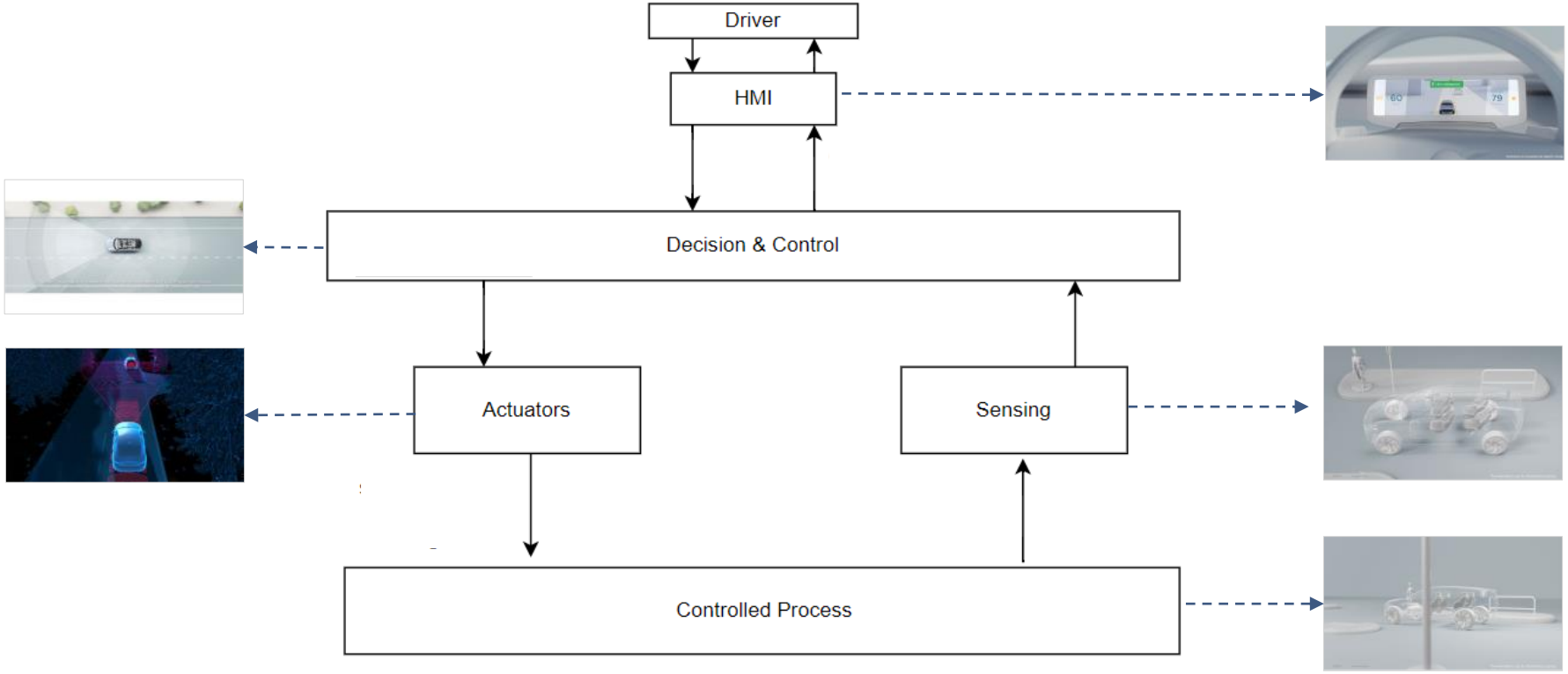
- Performance limitations
- Insufficiencies of specification
- etc.

Product Cybersecurity (e.g., ISO 21434)

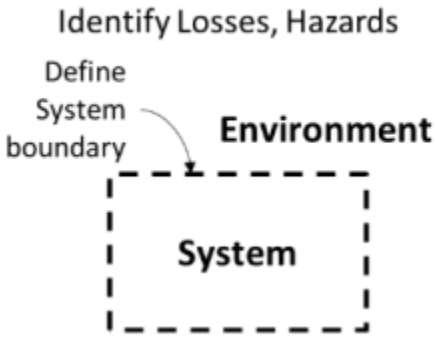
Automotive abstraction levels & traditional safety analysis methods



Functional Architecture



Step 1: Define the purpose & scope of the analysis



Losses
L -1: Injury or loss of life
L-2: Damage to the vehicle
L-3: Loss of mission
L-4: Loss of customer satisfaction
L-5: Loss of finances

Hazards
H-1: AV does not maintain a safe distance from vulnerable road users (VRUs) or other stationary or moving objects in the surroundings [L-1, L-2, L-4, L-5]
H-2: AV leaves designated path [L-3, L-4]
H-3: AV violates allowed operating conditions [L-4]
H-5: AV behavior is uncomfortable for the passengers [L-3, L-4]
H-6: AV loses control [L-1, L-2, L-3, L-4, L-5]

Step 1: Define the purpose & scope of the analysis

Hazards
H-1: AV does not maintain a safe distance from vulnerable road users (VRUs) or other stationary or moving objects in the surroundings [L-1, L-2, L-4, L-5]
H-2: AV leaves designated path [L-3, L-4]
H-3: AV violates allowed operating conditions [L-4]
H-5: AV behavior is uncomfortable for the passengers [L-3, L-4]
H-6: AV loses control [L-1, L-2, L-3, L-4, L-5]

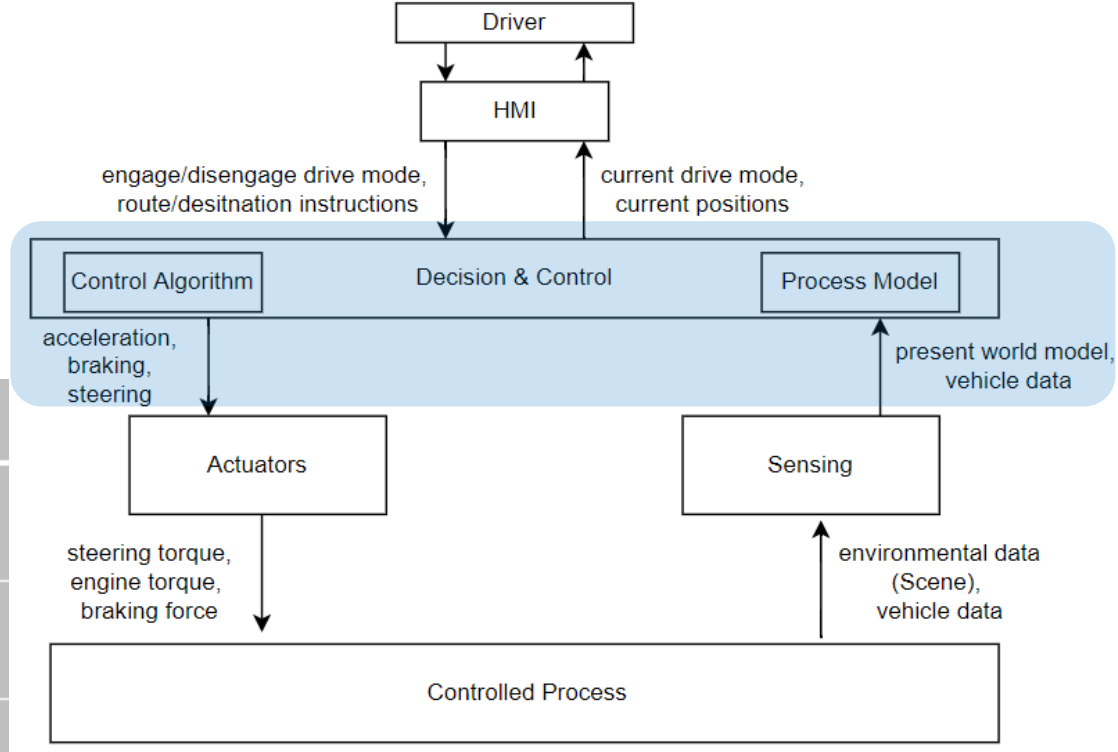
System level constraints
SC-1: AV must maintain a safe distance from VRUs and other stationary and moving objects in the surroundings [H-1]
SC-2: AV must adhere to the designated path [H-2]
SC-3: AV must adhere to the allowed operating limits advised by the traffic rules and ODD limitations [H-3]
SC-5 AV must provide a comfortable experience to the passengers when driving or stationary [H-5]
SC-6: AV must never lose control [H-6]

Step 2: Modelling the control Structure

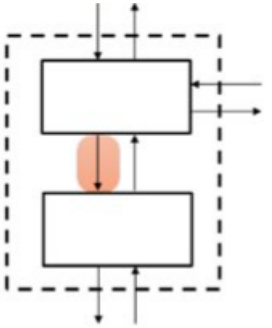
State responsibility of each sub-system to identify and refine control actions and feedback required by the system

	Responsibilities
Decision controller	**R-1** Issues acceleration command to speed up the AV
	R-2 Issues braking command to slow down the AV
	R-3 Issue steering commands to maneuver the AV

System	**Responsibility**	**Control Action**	**Feedback**
Decision Controller	R- 1	Acceleration	Vehicle data and present world model
	R-2	Braking	Vehicle data and present world model
	R-3	Steering	Vehicle data and present world model



Step 3: Identify unsafe control actions



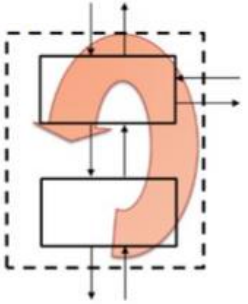
Control Action	Providing causes hazard	Not-providing causes hazard	Started early/late/ out of order	Stopped soon/applied longer
Accelerate	[UCA-1] Controller keeps provides accelerate cmd when vehicle is trying to slow down in a busy slow-moving lane [H-1, H-2, H-8] [UCA-1.1] Controller provides high rate of acceleration command when road is bumpy [H-8] [UCA-1.1.1] Controller provides high rate of acceleration command when while changing lateral movement [H-8]	[UCA-5] Controller doesn't provide accelerate cmd when the user requests in user mode [H-7] [UCA-5.1] Controller stops providing acceleration command if user disengages X seconds while AV is [H-7] [UCA-5.2] Controller stops providing acceleration cmd when user changes destination on the interface [H-7]	[UCA-6] Controller started providing accelerate cmd with a delay after user requested [H-6]	[UCA-7] Controller keeps on providing accelerate command after user stopped/still requesting [H-1, H-7]

	Providing causes hazard
Acceleration	[UCA-5.7] Decision & Control subsystem keeps speeding the AV by providing acceleration command when there is an object in the path while the visibility is low[H-1]
	[UCA-5.15] Decision & Control subsystem provides excessive acceleration command which makes the vehicle go beyond allowed speed limits [H-3]

	Controller Constraints
Acceleration	[SC-5.7] Decision & Control subsystem must not speed the AV by providing acceleration command when there is an object in the path [UCA-5.7]
	[SC-5.15] Decision & Control subsystem must not provide excessive acceleration command which makes the vehicle go beyond allowed speed limits [UCA-5.15]

VOLVO

Step 4: Identify loss scenarios



	Loss Scenarios
UCA-5.7	**[Scenario-1]** The AV does not detect vulnerable road users, stationary or moving objects in the passage due to processing delays in the decision & control algorithm and keeps speeding the vehicle by providing acceleration command which can result in a collision [H-1]
	[Scenario-2] Decision & Control subsystem keeps speeding the vehicle by providing acceleration command because it believes the passage is clear due to insufficient information in the environmental perception data received from the sensing subsystem due to lack of adequate sensor to detect objects in low visibility condition which can result in a collision [H-1]
	[Scenario-3] Decision & Control subsystem believes the passage is clear due to incorrect environmental perception data being received from the sensing subsystem and keeps speeding the vehicle by providing acceleration command which can result in a collision [H-1]
UCA-5.15	**[Scenario-1]** Decision & Control algorithm provides excessive acceleration which makes the AV exceed the speed limit because it doesn't follow the localized traffic rules, which can result in the vehicle exceeding allowed operating conditions [H-3]
	[Scenario-2] Decision & Control subsystem provides excessive acceleration which makes the AV exceed the speed limit because the sensing subsystem fails to correctly localize the ego vehicle which can result in the vehicle exceeding safe operating conditions [H-3]
	[Scenario-3] Decision & Control subsystem provides excessive acceleration which makes the AV exceed the speed limit because it believes the vehicle speed is within limits due to incorrect vehicle speed information being received from the sensing subsystem which can result in the vehicle exceeding safe operating conditions [H-3]

VOLVO

Step 4: Identify loss scenarios

	Solutions
UCA-5.7	If the Decision & Control subsystem is stuck in processing it should engage a suitable minimum risk maneuver **[Scenario-1]**
	Sensing subsystem must include adequate sensor to be able to detect vulnerable road users, stationary or moving objects in low visibility conditions **[Scenario-2]**
	Sensing subsystem must implement redundant sensors and to be able to verify the environmental perception data being received by the controller **[Scenario-3]**
UCA-5.15	Decision & Control algorithm must consider local traffic rules for speed limits before providing acceleration command **[Scenario-1]**
	A suitable minimum risk maneuver must be engaged (by a backup controller) if the vehicle speeds beyond the speed limit and is not slowing down **[Scenario-1]**
	Sensing subsystem must provide reliable information regarding location of the ego vehicle by having redundant methods **[Scenario-3]**

VOLVO

Losses

L -1: Injury or loss of life

L-2: Damage to the vehicle

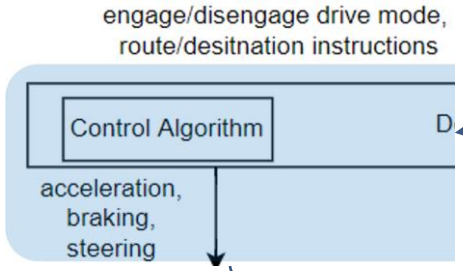
Hazards

H-1: AV does not maintain a safe distance from vulnerable road users (VRUs) or other stationary or moving objects in the surroundings [L-1, L-2, L-4, L-5]

System level constraints

SC-1: AV must maintain a safe distance from VRUs and other stationary and moving objects in the surroundings [H-1]

Control structure



UCA

[UCA-5.7] Decision & Control subsystem keeps speeding the AV by providing acceleration command when there is an object in the path while the visibility is low[H-1]

Loss scenarios

[Scenario-3] Decision & Control subsystem believes the passage is clear due to incorrect environmental perception data being received from the sensing subsystem and keeps speeding the vehicle by providing acceleration command which can result in a collision [H-1]

Solutions

Sensing subsystem must implement redundant sensors and to be able to verify the environmental perception data being received by the controller **[Scenario-3]**

VOLVO

Thank You

VOLVO