Open Call: Proposal for conceptual architectures for an SAE L4 Highway Pilot

Contents

Version history

Version	Date	Responsible	Comment
1.0	25 March 2022	Christoph Schulze / The Autonomous	

Introduction

“The Autonomous” aims to accelerate the market readiness and series development of safe self-driving cars. For that reason, The Autonomous establishes Working Groups (WG) to solve specific open challenges.

As part of the Innovation Stream, The Autonomous kicked off in June 2021 the first Working Group on “Safety & Architecture,” thus bringing together diverse companies and academia to define the state-of-the-art system architecture for safe self-driving cars, and more precisely, for an SAE Level 4 Highway Pilot.

Safety is the number one priority for all The Autonomous community members and contributors. We all strongly believe it is not an area to compete on but collaborate on so that ultimately people gain trust in this revolutionizing and life-critical autonomous technology.

For this reason, the members of our Working Group Safety & Architecture have recently decided to actively engage with even more industry stakeholders on this crucial topic.

This open call invites companies and research institutions to submit innovative proposals for a state-of-the-art fault-tolerant architecture for safe self-driving cars.

Following this open call, the different conceptual architecture candidates will be evaluated and compared using appropriate KPIs. Safety argumentation and HW and SW mapping considerations shall support the choice for a best-fit architecture candidate for the given reference AD use case and problem statement. The public report will be released at the end of 2022.

1. Format of the conceptual architecture

Scope and system boundary

The scope of the "Safety and Architecture" WG is to consider different architectural options for the AD Intelligence, i.e., the system processing sensor information to compute actuator commands. The boundary of the system under consideration, i.e., the AD Intelligence, is shown in Figure 1.

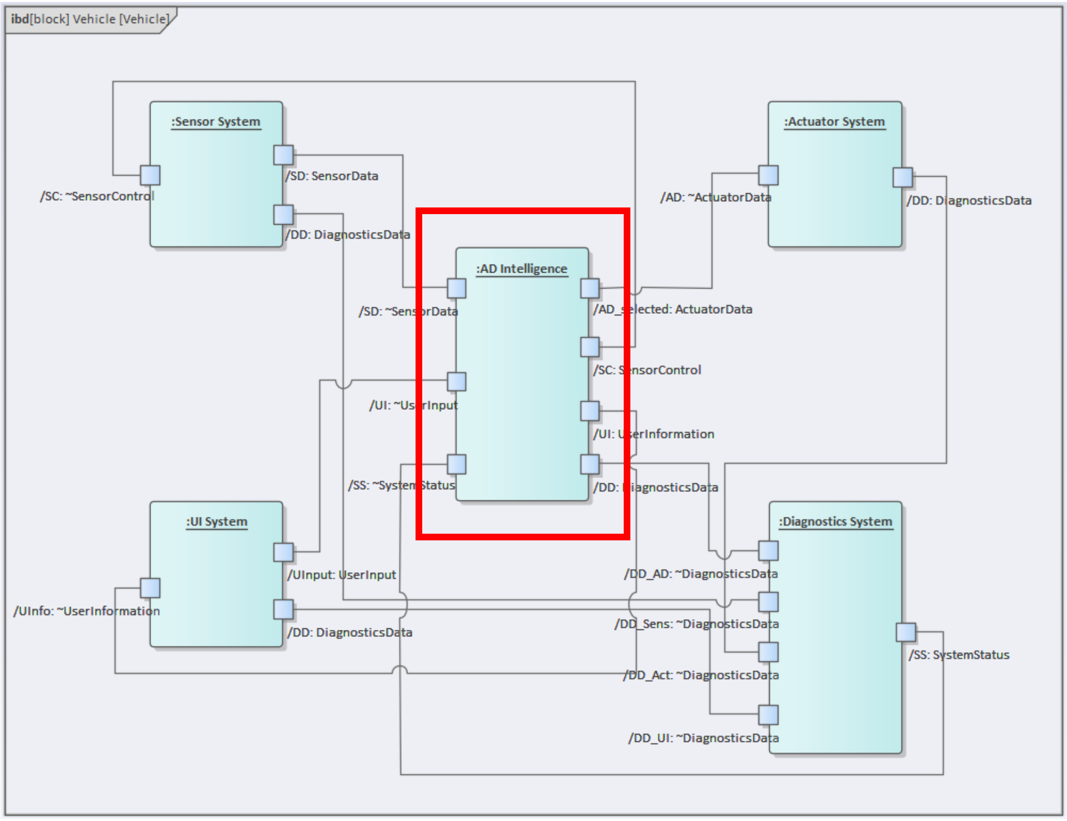

Figure 1: AD Intelligence and its interfaces to surrounding systems. Ports on the left side of a block indicate inputs, ports on the right outputs.

The AD Intelligence shall be able to cover a reference AD use case. For the "Safety and Architecture" WG, this is given by an "SAE Level 4 Highway Pilot" feature, outlined in Section 0.

Such an AD use case already implies several system-level requirements, particularly fail-operational behavior.

ID	Statement	Notes
SR1	The AD Intelligence shall provide outputs to the Actuator System (receivers) in a timely manner (with real-time characteristics and in every cycle).	Real-time refers to fast enough (for the dynamics at hand) and predictably (e.g., with sufficiently low jitter)
SR2	The AD Intelligence shall provide outputs to the Actuator System (receivers) in a fail-operational way on the base of two independent communication channels to each receiver.	"In a fail-operational way" means that the AD Intelligence continues to perform its nominal function or a safe degraded function in the presence of a single point or residual fault.

SR3	The AD Intelligence shall not provide unsafe outputs to the Actuator System (receivers).	Allowing an "unsafe" output to reach the actuators would lead to potential harm to the passengers or other traffic participants, e.g., due to a collision.
SR4	The AD Intelligence shall enable the Actuator System (receivers) to ensure the consistency of executed actuator setpoints.	This applies to consistency between the two independent communication channels and between different receivers.
SR5	The AD Intelligence shall implement strategies to detect and react to perception malfunctions and performance limitations due to environmental conditions or other causes related to the Sensor System.	This is not expected to be a differentiating factor between different conceptual architecture candidates.
SR6	The AD Intelligence shall implement strategies to monitor driver availability and ensure safe transitions through appropriate and timely status information and warning signals via the UI System.	As described in the AD use case outline, an MRM (leading to an MRC) should be performed if the driver doesn't respond. This is not expected to be a differentiating factor between different conceptual architecture candidates.
SR7	The AD Intelligence shall report its status to the Diagnostics System.	This is not expected to be a differentiating factor between different conceptual architecture candidates.

Considered level of detail

The "Safety and Architecture" WG considers architectures on a *conceptual* level only:

- The AD Intelligence should be broken down into subsystems far enough to describe how the system-level requirements (in particular regarding functional safety and fail-operational behavior) are achieved.
- The subsystems of the AD Intelligence should not be broken down to the level of particular HW or SW mappings.

Description of structure

A submission must describe the structure of the conceptual architecture proposed for the AD Intelligence. This includes at least the following:

- Which subsystems is the system (AD Intelligence) composed of?
- What interfaces exist between the different subsystems?
- To what extent can faults arising within a subsystem be prevented from spreading to other subsystems, i.e., to what extent are the subsystems Fault Containment Units (FCUs)?

Preferably, this information should be provided as a block diagram (e.g., SysML) or similar. However, a comprehensive textual description is also possible.

Description of behavior

A submission must describe the behavior and interactions of the different subsystems making up the conceptual architecture. This includes at least the following:

- What is the role and functionality of each subsystem?
- What is the data and control flow through the system, i.e., the temporal sequence of interactions between different subsystems?
- What different branches can be taken depending on the inputs received from other subsystems, i.e., how does each subsystem act?

Preferably, this information should be provided as an activity diagram (e.g., SysML) or similar. However, pseudo-code or a comprehensive textual description are also possible.

2. Reference AD use case

Functionality provided to user

In the following, we define an assumed version of an SAE Level 4 Highway Pilot (HWP) feature, similar to proposals from different OEMs. These allow the driver of a passenger car (sedan, SUV, crossover, or similar vehicle with relatively low center of gravity and simple vehicle dynamics) to take their eyes off the road and perform other tasks while on a highway, with the AD system performing the entire DDT (lateral and longitudinal vehicle motion control and complete Object and Event Detection and Reaction (OEDR)) and assuming full responsibility.

The Operational Design Domain (ODD) of the reference AD use case is outlined in Appendix: ODD outline, following the scheme proposed in [2].

Item	Statement
1.1.1	The HWP feature supports lane keeping (with or without a lead vehicle).
1.1.2	The HWP feature supports lane changes.
1.1.3	The HWP feature supports traffic jams (stop & go traffic).
1.1.4	The HWP feature can be set to continue driving on the current highway.
1.1.5	The HWP feature can be set to go to a target highway exit.
1.1.6	The HWP feature supports speeds of up to 130 km/h.
1.1.7	The HWP feature visually presents its world model, motion plan, and status to the passengers.

Feature activation, deactivation, and requests to intervene

Item	Statement
1.2.1	We assume that “regular activation” of the HWP feature could proceed as follows: • The driver presses the "activate HWP" button. The system checks that all conditions for its activation are fulfilled (see • Appendix: ODD outline) and indicates the result to the driver. • The system gradually offers more resistance to steering wheel and pedals.
1.2.2	We assume that “regular system-initiated deactivation” of the HWP feature could proceed as follows: • The system visually represents the automated driving system’s world model, motion plan and diagnostics to the user to simplify the (requested) control take over for the user. • The system indicates that it is approaching a point where the conditions for activation will no longer be fulfilled (end of the mission, change of external circumstances, detected failure, etc.). • The driver presses the "deactivate HWP" button. • The system checks that the driver is capable of driving (attentive, hands on steering wheel) and indicates the result to the driver. • The system gradually offers less resistance to steering wheel and pedals. • If the driver fails to resume control, the system executes an MRM when the conditions for activation are no longer fulfilled.

1.2.3	We assume that "regular driver-initiated deactivation" of the HWP feature could proceed similar to "regular system-initiated deactivation", but without the first two steps.
1.2.4	We assume that "fast driver-initiated deactivation" of the HWP feature could proceed as follows: • The driver puts their hands on the steering wheel and/or feet on the pedals. • The driver overrides the resistance offered by the system. • The system indicates to the driver that it has relinquished control.
1.2.5	We assume that "driver-initiated emergency deactivation" of the HWP could proceed as follows: • The driver presses the "pull over" button. • The system indicates to the driver that it will come to a controlled stop. • The system executes an MRM.

Degraded functionality

Item	Statement
1.3.1	The HWP feature has a nominal mode (routine/normal operation), during which it is capable of executing the mission.
1.3.2	The HWP feature has a degraded mode, during which it is incapable of continuing the mission. Instead, it will execute an MRM (pulling over, controlled stop, or emergency stop).
1.3.3	The HWP feature will enter degraded mode if any part of the AD system encounters a fault or a performance limitation or if the ODD is violated.
1.3.4	After entering degraded mode (unable to continue mission), the HWP feature will not activate again without a full reboot.
1.3.5	In degraded mode, the HWP feature will try to come to a safe, controlled stop in a safe location (i.e., emergency lane or right-most lane).
1.3.6	If this is not possible, the HWP feature will try to come to a safe, controlled stop in the current lane of travel.
1.3.7	If this is not possible, the HWP feature will try to come to an emergency stop.
1.3.8	The HWP feature **does not** have a limp-home mode, during which it is capable of continuing the mission with reduced functionality (e.g., reduced speed) and/or try to restore full functionality (e.g., partial reboot while continuing to drive).

List of abbreviations

Abbreviation	Meaning
ACM	Association for Computing Machinery
AD	Automated / Autonomous Driving
ADS	Automated Driving System
DDT	Dynamic Driving Task
DFI	Dependent Failure Initiator
ECU	Electronic Control Unit
EOTI	Emergency Operation Time Interval
FCU	Fault-Containment Unit
FFI	Freedom from Interference
FTTI	Fault-Tolerant Time Interval
HW	Hardware
HWP	Highway Pilot
IEC	International Electrotechnical Commission
IEEE	Institute for Electrical and Electronics Engineers
ISO	International Organization for Standardization
KPI	Key Performance Indicator
MRC	Minimal Risk Condition
MRM	Minimal Risk Maneuver
NHTSA	National Highway Traffic Safety Administration
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response
OEM	Original Equipment Manufacturer
SAE	Society of Automotive Engineers
SEooC	Safety Element out of Context
SOTIF	Safety of the Intended Functionality
SUV	Sports Utility Vehicle
SW	Software
VRU	Vulnerable Road User
V2X	Vehicle-to-anything (vehicle, infrastructure)
WG	Working Group

References

[1] ISO, "ISO 26262:2018 Road vehicles - Functional safety," 2018.

[2] BSI, "BSI PAS 1883:2020 Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) - Specification," 2020.

Appendix: ODD outline

Scenery

Zones

Attribute	Sub-attribute (1)	Sub-attribute (2)	Capability
Zones	Geo-fenced areas		Yes, as designated by OEM
	Traffic management zones		No
	School zones		No
	Regions or states		Yes, as designated by OEM
	Interference zones	Dense foliage	Yes
		Tall buildings	Yes

Drivable area

Attribute	Sub-attribute (1)	Sub-attribute (2)	Sub-attribute (3)	Capability
Drivable area	Drivable area type	Motorways (highways)		Yes, maximum 130 km/h
		Radial roads		No
		Distributor roads		No
		Minor roads		No
		Slip roads		No
		Parking		No
		Shared space		No
	Drivable area geometry	Horizontal plane	Straight roads	Yes
			Curves	Yes, maximum 1/100 m
		Transverse plane (cross-section)	Divided / undivided	Divided
			Pavement	No
			Barrier on the edge	
			Types of lanes together	
		Longitudinal plane (vertical)	Up-slope	Yes, maximum +4%
			Down-slope	Yes, maximum -4%
			Level plane	Yes
	Lane specification	Lane dimensions		Minimum 3.5 m
		Lane marking		Yes, in good condition
		Lane type	Bus lane	No
			Traffic lane	Yes
			Cycle lane	No
			Tram lane	No
			Emergency lane	No
			Other special purpose lane	Yes, carpool lanes
		Number of lanes		Yes, minimum 2 lanes
		Direction of travel	Right-hand traffic	Yes
			Left-hand traffic	No
	Drivable area signs	Information	Variable	Yes, full-time and temporary

Attribute	Sub-attribute (1)	Sub-attribute (2)	Sub-attribute (3)	Capability
			Uniform	Yes, full-time and temporary
		Regulatory	Variable	Yes, full-time and temporary
			Uniform	Yes, full-time and temporary
		Warning	Variable	Yes, full-time and temporary
			Uniform	Yes, full-time and temporary
	Drivable area edge	Line markers		Yes
		Shoulder (paved or gravel)		Yes
		Shoulder (grass)		Yes
		Solid barriers		Yes, obligatory on left side
		Temporary line markers		No
		None		No
	Drivable area surface	Surface type	Asphalt	Yes
			Concrete	Yes
			Cobblestone	No
			Gravel	No
			Granite setts	No
		Surface features	Cracks	Yes, minor only
			Potholes	No
			Ruts or swells	Yes, minor only
			Damage caused by weather	Yes, minor only
			Damage caused by traffic	Yes, minor only
		Induced conditions	Icy	No
			Flooded	No
			Mirage	Yes
			Snow	No
			Standing water	No
			Wet	Yes
			Contaminated	Yes, minor only

Additional assumptions:

- Changed road markings or reduced lane width are not supported.
- Static obstacles on the road are uncommon. These include debris, boulders, or fallen trees.
- The speed limit is appropriate for the curve radius and slope such that the entire stopping distance is visible without occlusions (in the absence of other vehicles).

Junctions

Attribute	Sub-attribute (1)	Sub-attribute (2)	Sub-attribute (3)	Capability
Junctions	Roundabout			No
	Intersection	T-junction		No
		Staggered		No

Attribute	Sub-attribute (1)	Sub-attribute (2)	Sub-attribute (3)	Capability
		Y-junction	On-ramp and off-ramp	No (except driving by)
			Other	No
		Crossroads		No
		Grade-separated	Interchange	No
			Other	No

Road structures

Attribute	Sub-attribute (1)	Capability
Special structures	Automatic access control	No
	Bridges	Yes
	Pedestrian crossings	No
	Rail crossings	No
	Tunnels	Yes, with separate driving directions
	Toll plaza	No
Fixed road structures	Buildings	No
	Street lights	Yes
	Street furniture	No
	Vegetation	No
Temporary road structures	Construction site detours	No
	Refuse collection	No
	Road works	No
	Road signage	No

Environmental conditions

Attribute	Sub-attribute (1)	Sub-attribute (2)	Capability
Weather	Wind	Calm - fresh breeze (<10.7 m/s)	Yes
		Strong breeze (>10.7 m/s) - hurricane force	No
	Rainfall	Light rain (<2.5 mm/h)	Yes
		Moderate rain (>2.5 mm/h) - cloudburst	No
	Snowfall	Light snow (>1 km visibility)	Yes
		Moderate snow (<1 km visibility) - heavy snow	No
Particulates	Marine		No
	Mist and fog		No
	Sand and dust		No
	Smoke and pollution		No
	Volcanic ash		No
Illumination	Day		Yes
	Night or low-ambient		No
	Cloudiness	Clear - overcast	Yes
	Artificial illumination		Yes
Connectivity	Communication	V2V, V2I	Yes
		Cellular	Yes
		Satellite	No
		DSRC and ITS-G5	No
	Positioning	Galileo	Yes

Attribute	Sub-attribute (1)	Sub-attribute (2)	Capability
		GLONASS	Yes
		GPS	Yes

Additional assumptions:

- Not being warned of major road or traffic conditions is uncommon. We assume that the road layout is known ahead of time and that unexpectedly encountering challenging road or traffic conditions is uncommon as authorities are in charge of keeping the road in an acceptable state of repair and/or informing traffic participants (via signs, map data, and/or V2X) if this is not the case.
- HD Maps are available for all supported highway segments.

Dynamic elements

Attribute	Sub-attribute (1)	Sub-attribute (2)	Capability
Traffic	Density of agents	Dense traffic (including stop & go)	Yes
		Free-flow traffic (including no lead vehicle)	Yes
	Volume of traffic		
	Flow rate		
	Agent type	Cars	Yes
		Buses and trucks	Yes
		Motorbikes	Yes
		VRUs (pedestrians, bicyclists)	Yes, but uncommon
		Animals	Yes, but uncommon
	Special vehicles		Yes
Subject vehicle (ego vehicle)	Behavior capabilities	Ego vehicle speed	0-130 km/h
		Lane change	Yes
		Lane merge	Yes
	Vehicle	All sensors and actuators fully operational	Yes
		Sensor or actuator non-operational	No
		Superficial body damage	Yes
		Moderate - major body damage	No
		Door or window open	No
		Low fuel or charge level	No
	Passengers	Driver not in driver seat	No
		Unbelted passenger	No
		Driver asleep or incapacitated	No

Additional assumptions:

- All human traffic participants are aware that the highway is a restricted environment and act accordingly (responsibly).