Collection of research gaps – identified from discussion sections IV through VII

Magnus Gyllenhammar[1,2], Gabriel Rodrigues de Campos[1], Martin Törngren[2]
[1]Zenseact AB, Sweden. [2]KTH – Royal Institute of Technology, Sweden.

The tables presented below provide the basis for conducting the research gap analysis for our survey paper titled: "The Road to Safe Automated Driving Systems: A Review of Methods Providing Safety Evidence". For each discussed method, the challenges (C1-C8 of Sec. III) classified as either a C (fundamental challenge), O (obstacle) or U (unclear) (as per TABLE I in the survey paper) result in a separate row in the table below. Further, for each such row a gap is identified by consulting the discussions of sections IV through VII. Subsequently, the raw identified gaps are collected and eventual connections to similar considerations between different rows, both of the same method as well as other methods are given. The table below presents this intermediate step of identified gaps before they are collected into categories and formulated as proper research questions, as presented in Sec. VIII.C of the survey paper.

Notably, for operational data collection no challenge (C1-C8) has been identified as posing significant obstacles or unclarities. However, there are other short-comings of this method highlighted in Sec. VI.A that warrant considerations for using this method to provide safety evidence for the ADS.

	Method	Challenge	Classification	Identified gap
Design techniques	Operational design domain	C1	C	Completeness and appropriate spec.
		C2	C	
	Hazard and risk assessment	C1	C	Completeness of hazards
		C2	C	
		C3	C	
		C4	C	
		C5	O	
		C6	O	How to automate usage of data to bridge high integrity requirements and support agile release cadence?
		C8	U	
	Process arguments	C1	C	Quantitative contributions with safety evidence
		C2	C	
		C3	O	
		C4	O	
		C5	O	
		C6	O	
		C7	U	Processes for AI/ML
		C8	O	How to integrate processes with an agile release cycle, alt. Produce adequate safety evidence from within an agile cycle?
	Contract-based design	C1	C	Unable to formalise completely (joint with formal;rt_certy)
		C2	C	
		C3	C	
		C4	O	Scalability of method (jointly with CBD;arch.;formal;run-time cert.;degradation;PCS)
		C7	O	Contracts for AI
	Supervisor architectures	C4	O	Scalability of method (jointly with CBD;arch.;formal;run-time cert;degradation;PCS)

	Method	Challenge	Classification	Identified gap
Verification and validation methods	Field operational tests	C2	O	Scalability/how to leverage (jointly with EVT)
		C3	O	
		C6	C	
		C8	C	How to use FOTs within an agile framework of release?
	Extreme value theory	C2	O	How to collect closed loop data? (jointly with FOT)
		C3	O	
	Scenario-based V&V	C1	C	Completeness of scenario space
		C2	C	
		C3	C	Testing of relevant scenarios considering tactical decisions
		C6	O	How to ensure coverage of rare scenarios?
		C7	C	Non-interpolatable results from testing
	Formal methods	C1	C	Unable to formalise completely (joint with formal;run-time cert)
		C2	C	
		C3	C	
		C4	O	Scalability of method (jointly with CBD;arch.;formal;run-time cert;degradation;PCS)
		C6	O	How to mitigate the specification gap?
		C7	O	Soundness and completeness for AI/ML components?

	Method	Challenge	Classification	Identified gap
Run-time risk assessment	Operational data collection	N/A		Other limitations listed in the section
	Threat assessment	C1	O	How to capture uncertainties of C1 and C2?
		C2	O	
	Out-of-distribution detection	C6	O	How to ensure integrity of run-time methods? (jointly with DRA;DSM)
	Dynamic risk assessment	C3	U	Impact from tactical decisions? (jointly with PCS;DSM)
		C5	U	How well does DRA accommodate degradations?
		C6	U	How to ensure integrity of run-time methods? (jointly with DRA;DSM)
		C7	U	How to derive quantitative risk metrics for AI/ML-components? (Jointly with DSM)

Run-time (self-)adaptation	Degradation strategies	C4	O	Scalability of method (jointly with CBD;arch.;formal;run-time cert;degradation;PCS)
		C8	O	How to facilitate frequent releases when considering proper analysis of degradations strategies
	Runtime certification	C1	O	Unable to formalise completely (joint with formal;run-time cert)
		C2	O	
		C3	O	
		C4	O	Scalability of method (jointly with CBD;arch.;formal;run-time cert;degradation;PCS)
	Dynamic safety management	C3	O	Impact from tactical decisions? (jointly with PCS;DSM)
		C6	O	How to ensure integrity of run-time methods? (jointly with DRA;DSM)
		C7	O	How to derive quantitative risk metrics for AI/ML-components? (Jointly with DSM)
	Precautionary safety	C3	U	Impact from tactical decisions? (jointly with PCS;DSM)
		C4	U	Scalability of method (jointly with CBD;arch.;formal;run-time cert;degradation;PCS)
		C8	U	How can PCS help support frequent releases?