

Holistic perspectives on safety of ADSs

2024-11-20 – SCSSS, Göteborg

Magnus Gyllenhammar

Co-authors: G. R. de Campos (Zenseact) and M. Törngren (KTH)





ADS safety – Lives at stake



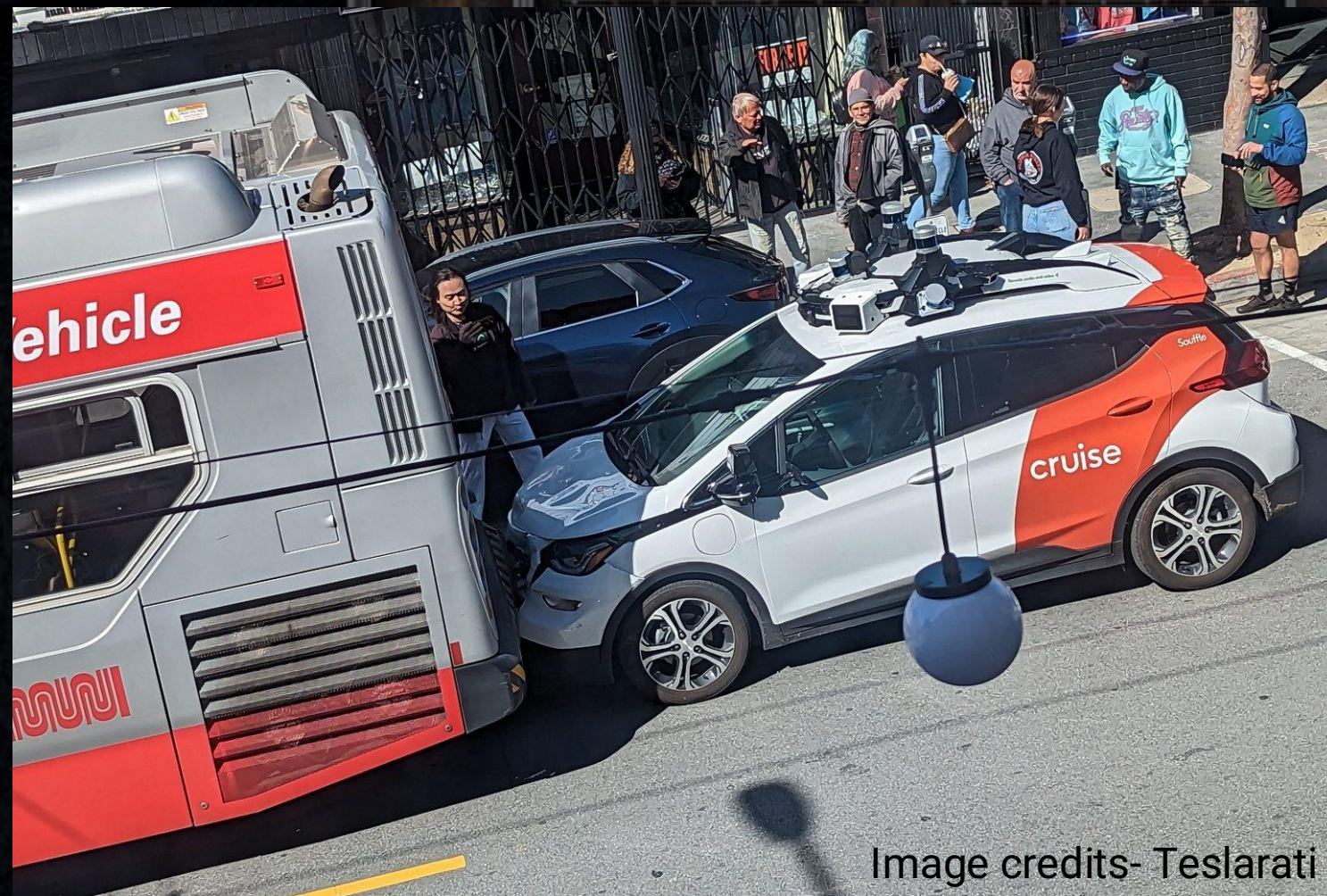


Image credits- Teslarati



[<https://wonderfuleengineering.com/waymo-recalls-robotaxis-to-give-telephone-poles-a-higher-damage-score/>]



Outline

- Setting the stage – eight challenges
- Overview of categories of methods and techniques
 - Deep dive – Scenario-based V&V
- Research gaps



[M. Gyllenhammar, G. R. de Campos, and M. Törngren. *“The Road to Safe Automated Driving Systems: A Review of Methods Providing Safety Evidence”*. TBA]



Challenges for safety

Safety = Absence of unreasonable risk

$$R = E \cdot S$$

No standard yet → up to each OEM/company to decide

Society would not accept vastly different from human driving accidents.

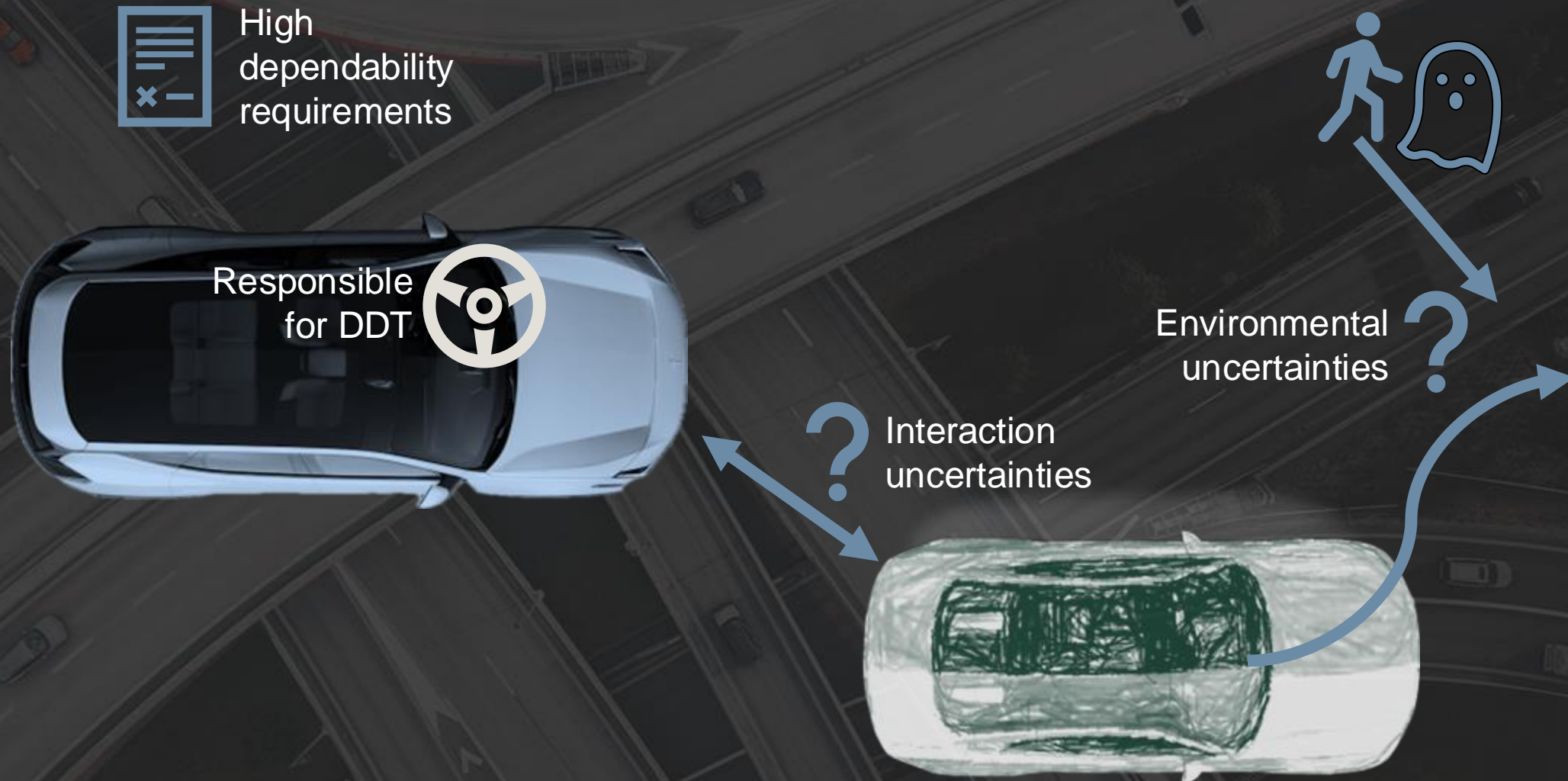
– $\sim 10^{-8}$ fatalities per hour

[P. Junietz, et al. (2019). Macroscopic safety requirements for highly automated driving. Transportation research record.]

TABLE 1 Accidents on German controlled-access highways






















Severity	ISO 26262 Severity level	Average distance between two accidents of this level	Accident rate per driven distance
Fatal	S3	$660 \cdot 10^6$ km	$1.52 \cdot 10^{-9}/\text{km}$
Severe Injuries	S2	$53.2 \cdot 10^6$ km	$1.88 \cdot 10^{-8}/\text{km}$
Injuries	S1	$12.5 \cdot 10^6$ km	$8.00 \cdot 10^{-8}/\text{km}$
w/o Injuries	S0	$7.5 \cdot 10^6$ km	$1.33 \cdot 10^{-7}/\text{km}$

Eight Challenges for Safety of ADSs



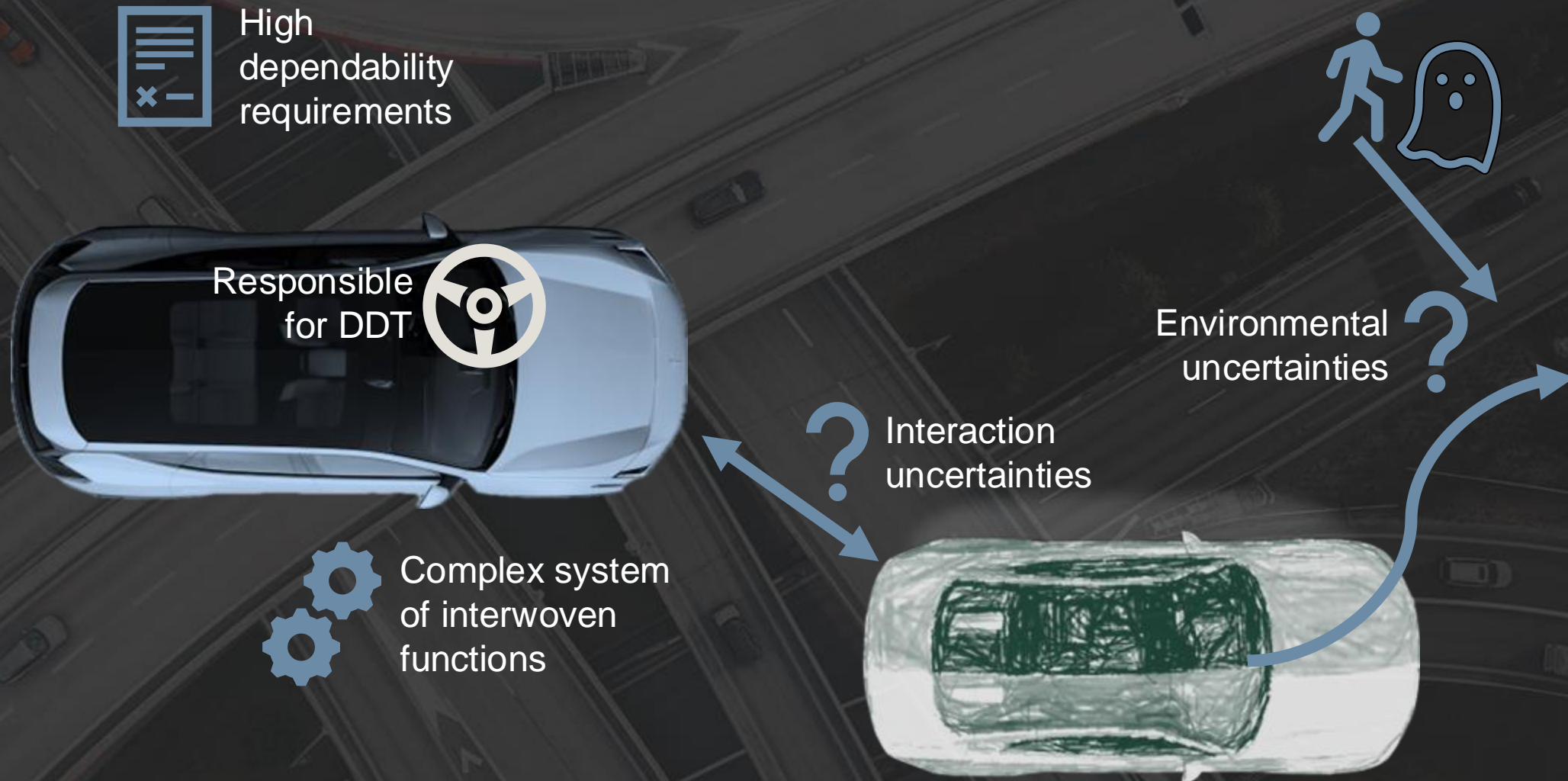
ADS responsible for the entire driving task

For on-road vehicles

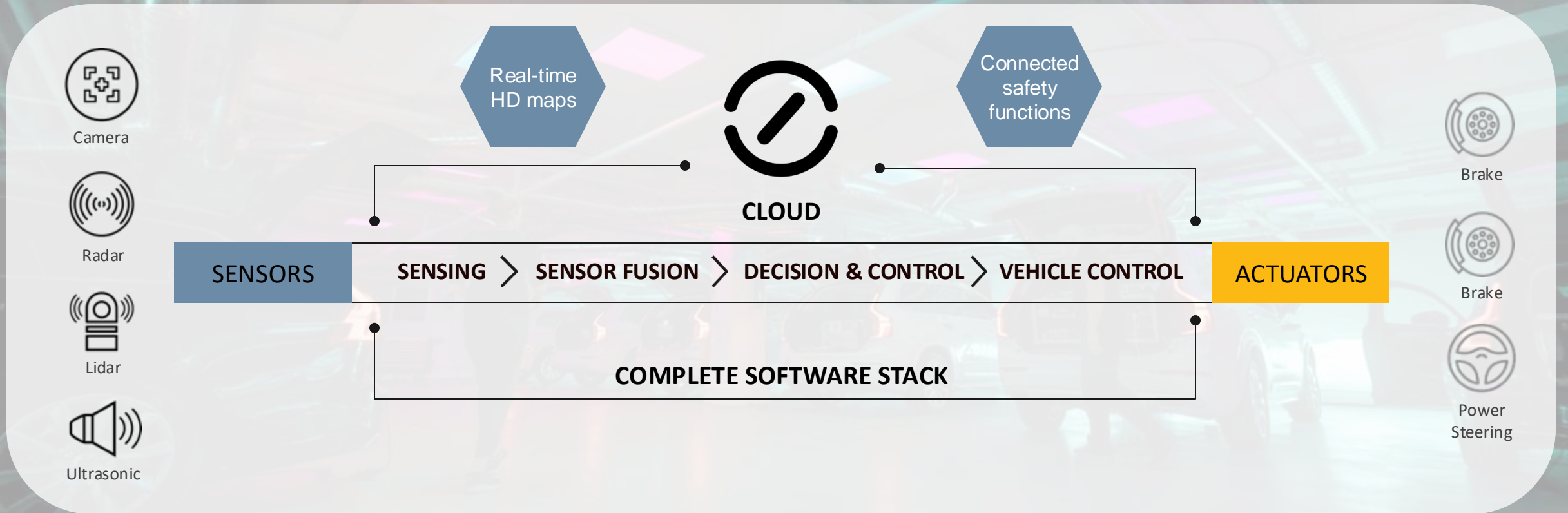
		 Human driver	 Automated system		
		Steering and acceleration/ deceleration	Monitoring of driving environment	Fallback when automation fails	Automated system is in control
Human driver monitors the road	0 NO AUTOMATION				N/A
	1 DRIVER ASSISTANCE				SOME DRIVING MODES
	2 PARTIAL AUTOMATION				SOME DRIVING MODES
Automated driving system monitors the road	3 CONDITIONAL AUTOMATION				SOME DRIVING MODES
	4 HIGH AUTOMATION				SOME DRIVING MODES
	5 FULL AUTOMATION				

SAE J3016

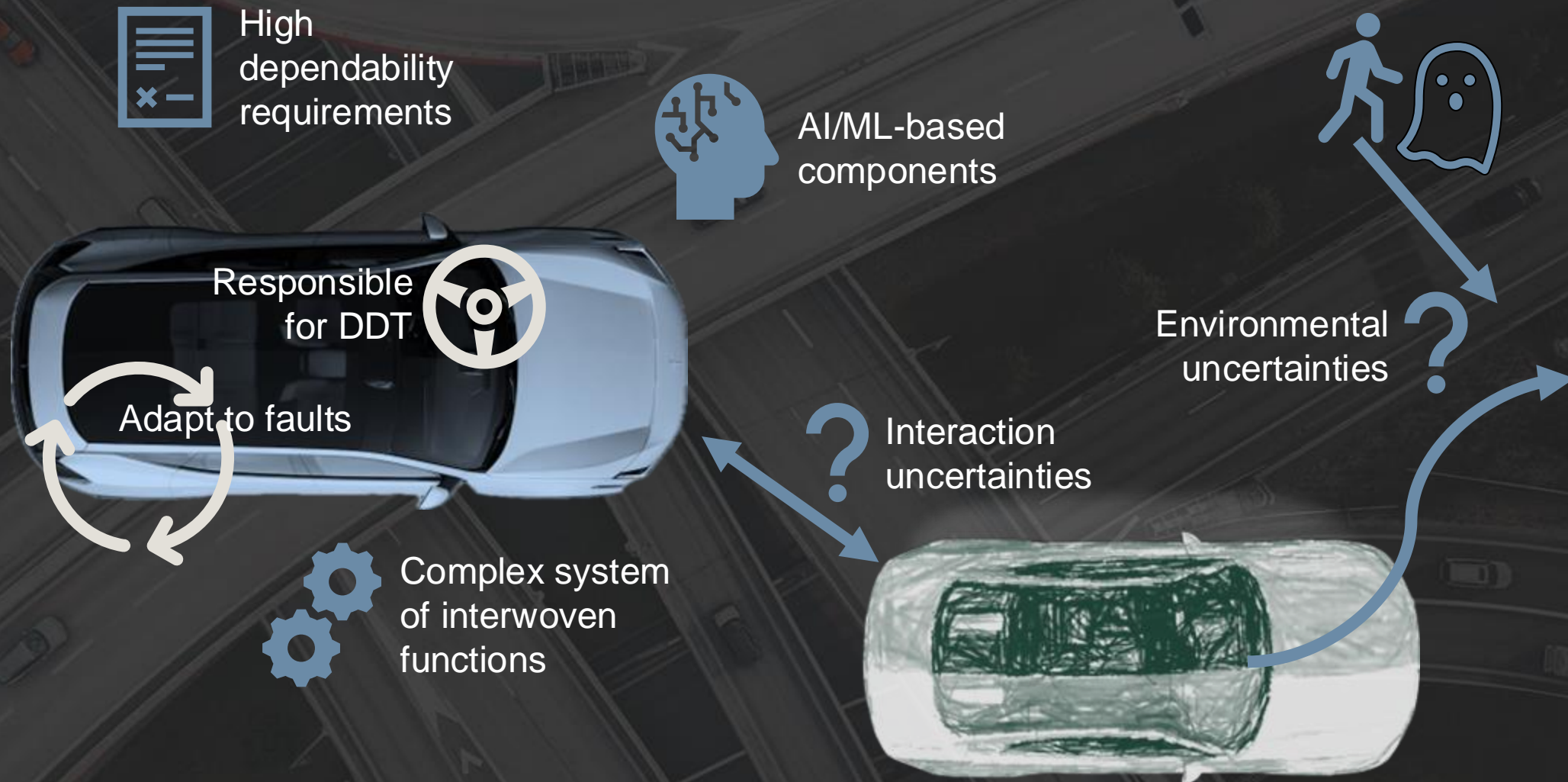
Eight Challenges for Safety of ADSs



Complex system with interwoven functions



Eight Challenges for Safety of ADSs



AI-based components – issues

Interpretability – black box

Interpolatability – lack of generalisability

Robustness – adversarial attacks

[Goodfellow et al. (2015)]

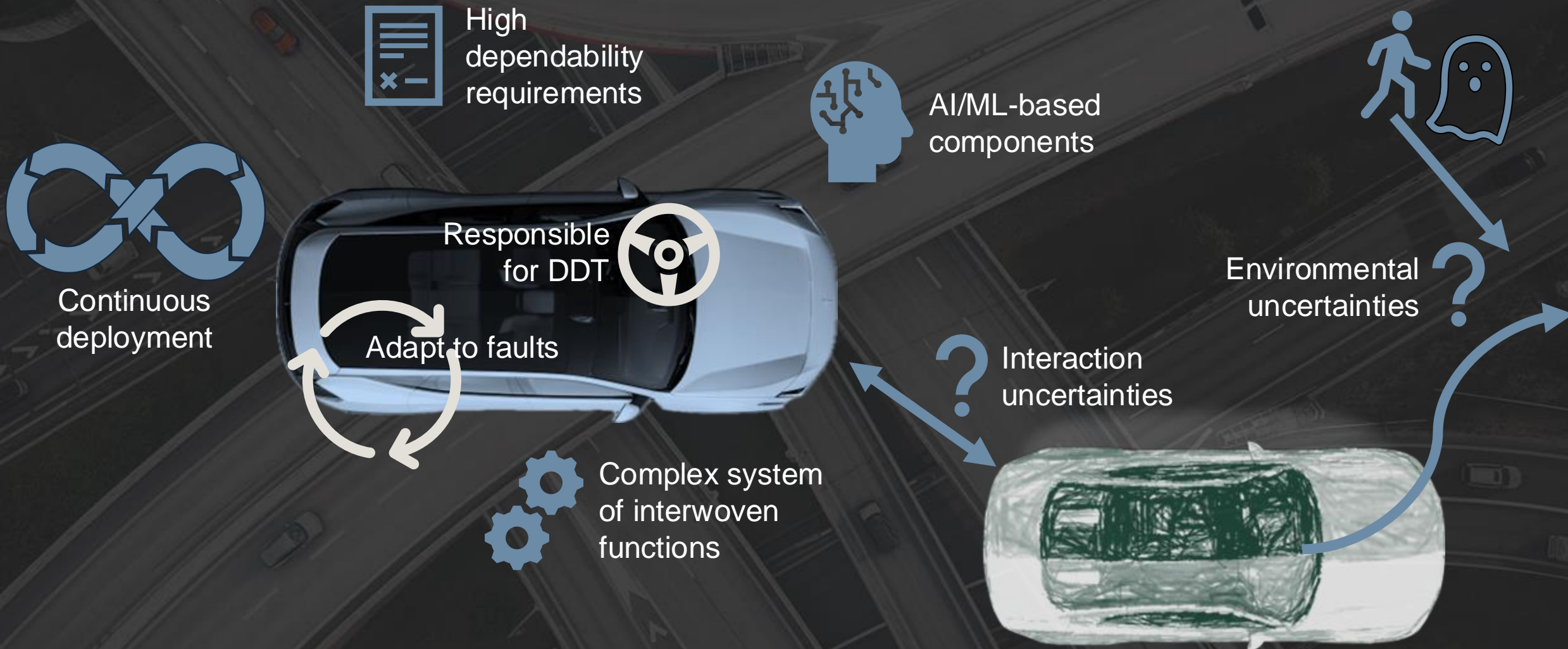


“Panda”

Noise

“Gibbon”

Eight Challenges for Safety of ADSs

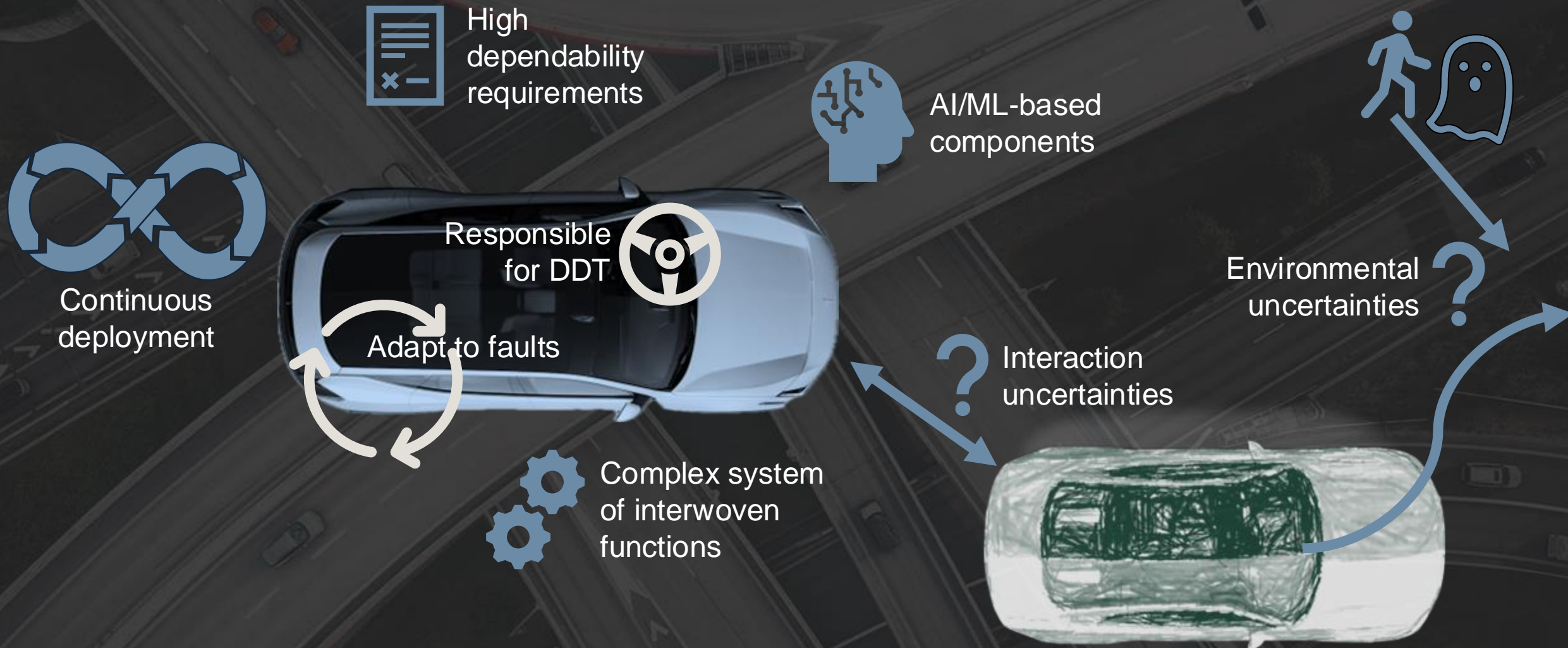


Crowdstrike incident – issue with release processes and QA



Credit: CLTMotorSpdwy, X

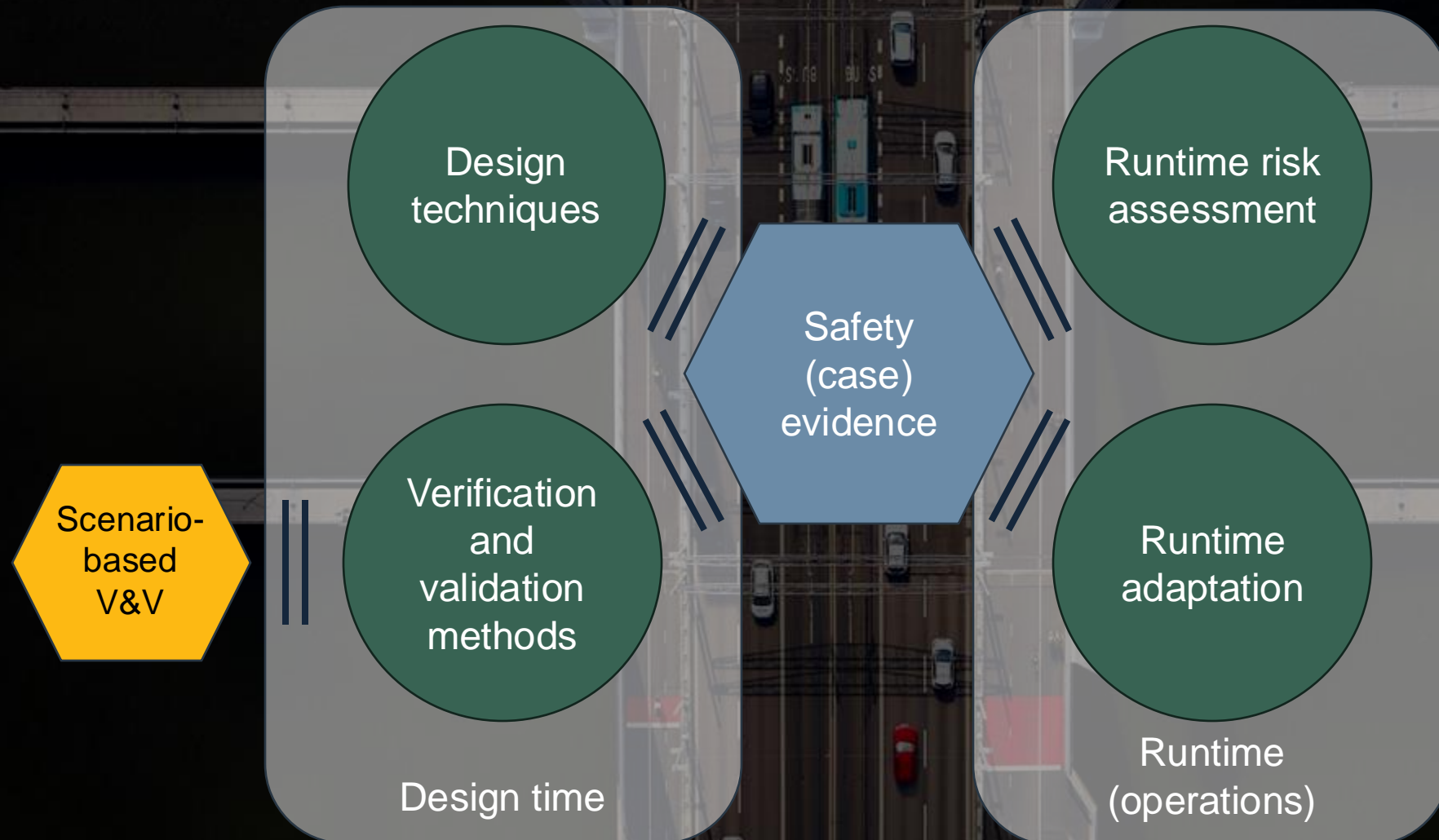
Eight Challenges for Safety of ADSs





Overview of methods

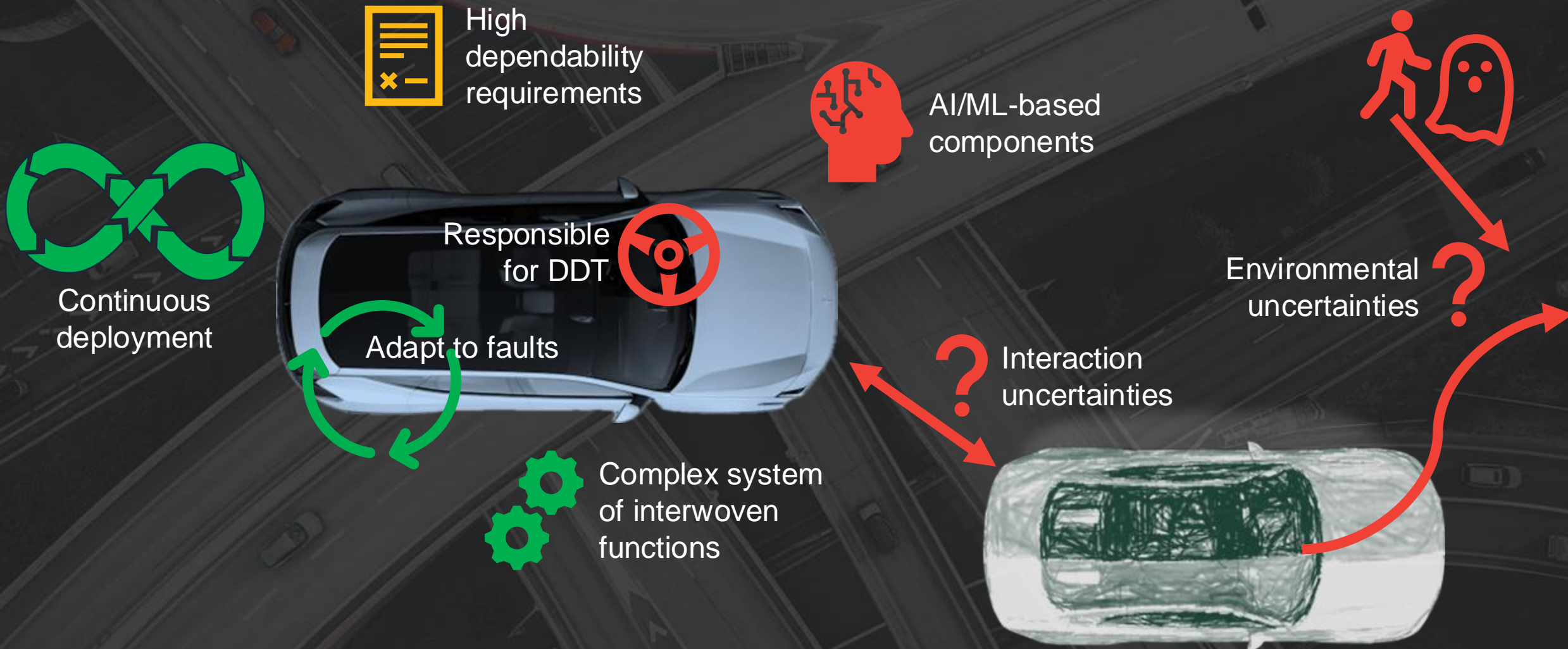
Methods span design, development and operations

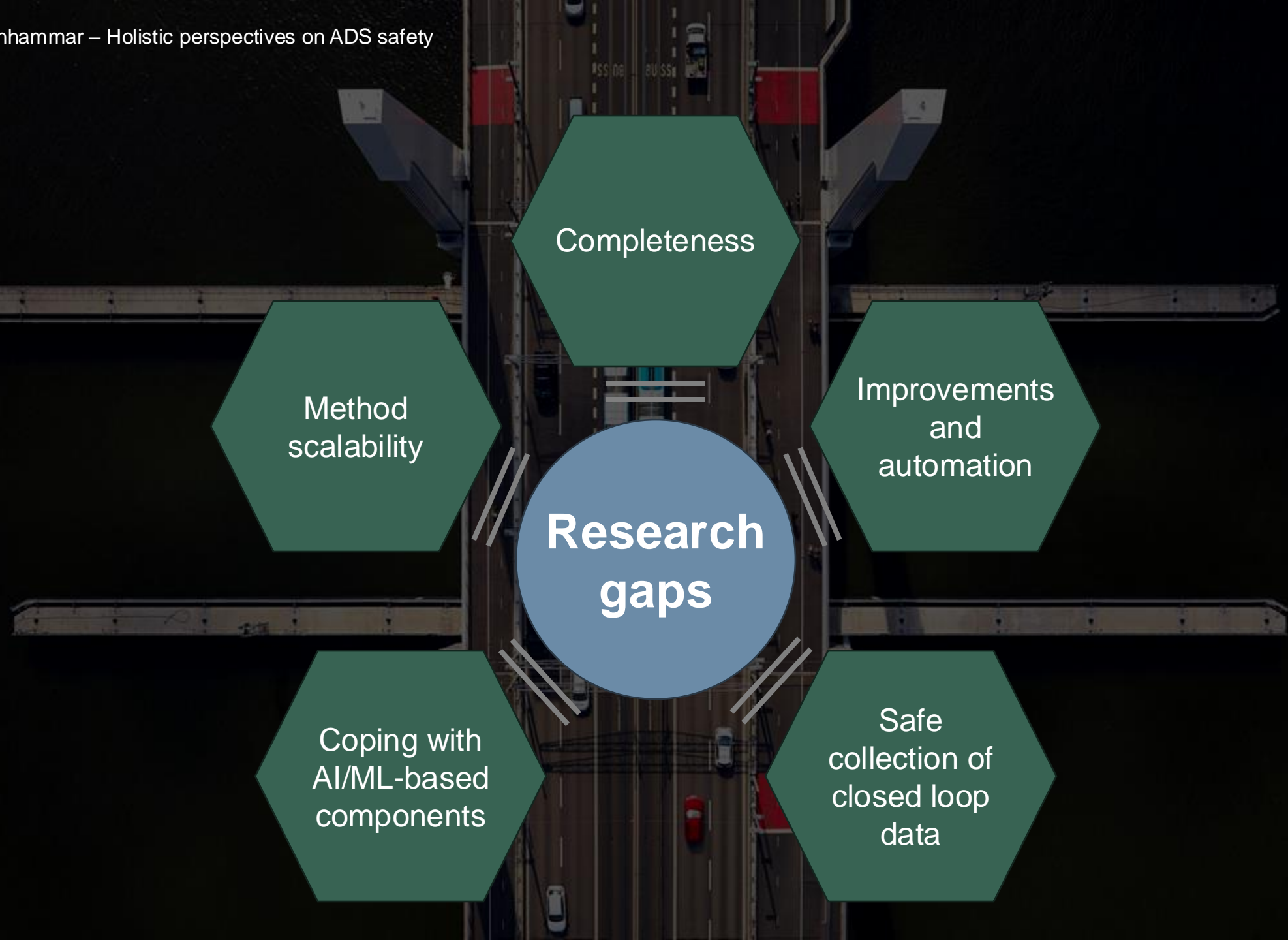


Missed or superfluous scenarios

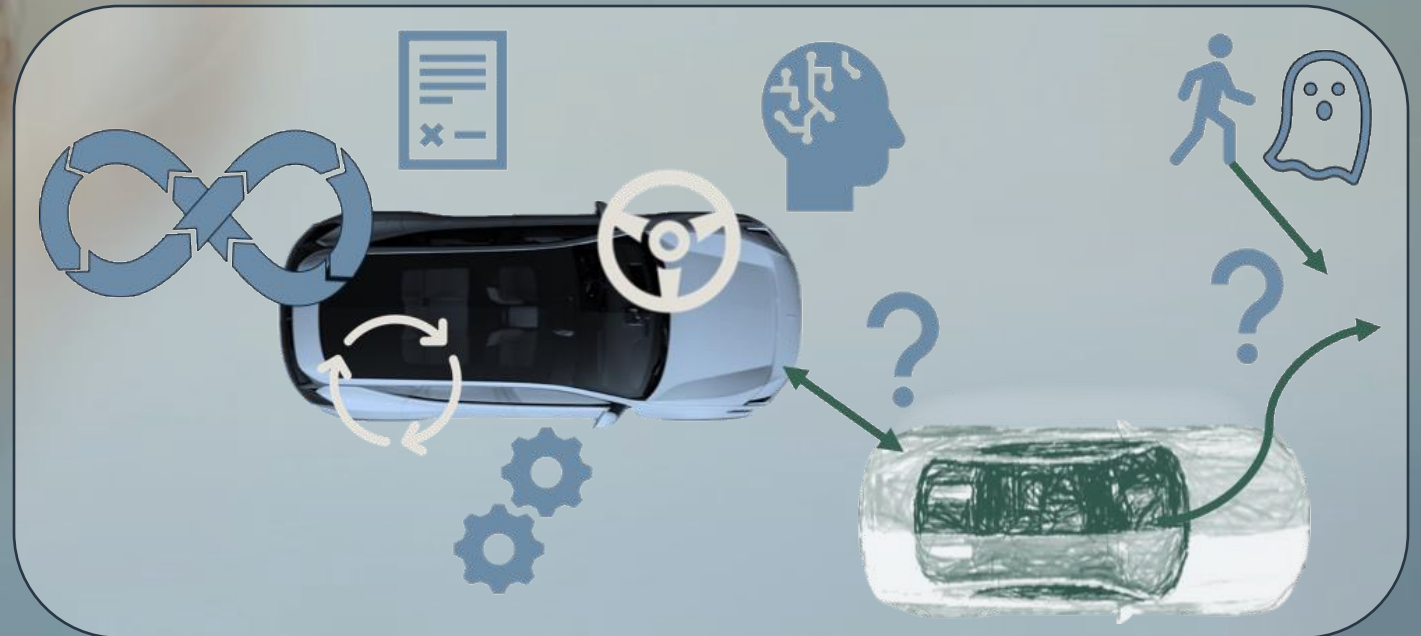


Assessment for scenario-based V&V





Holistic perspectives and collaboration towards safety



[M. Gyllenhammar, G. R. de Campos, and M. Törngren. *“The Road to Safe Automated Driving Systems: A Review of Methods Providing Safety Evidence”*. TBA]

Thanks for listening

Magnus Gyllenhammar



Methods span design, development and operations

