ADAPTIVE OPERATIONAL DESIGN DOMAIN

Institute for AI Safety and Security

13-14 of November 2024, Safetronic

Ryan Mut, Gerald Sauter, Yannick Kees, Frank Köster and Sven Hallerbach

safetronic®

DLR

Presenter


safetronic®
13.-14. November 2024, Stuttgart
My presentation topic at Safetronic 2024 is "Adaptive operational design Domain".
Ryan Mut
Research fellow AI Engineering,
German Aerospace Center (DLR)
safetronic.fraunhofer.de

Agenda

DLR

- **Introduction**
- Terms and Definitions
- Adaptive Operational Design Domain (AODD) and Resilience
- Subsystem
- Demonstration
- Summary

safetronic®

Institute for AI Safety & Security

AI Engineering: Convince the Engineer.

AI Engineering

Providing AI engineers with **robust process models, procedures and tools** to **accelerate the development** of safe and secure AI-based systems for a wide range of application domains.

Assessment & Test

Supporting engineers to **find vulnerabilities in AI eco-systems** before others will do. This includes all components that influences AI decision making.

Human-in-the-Loop

Focusing on **AI scenarios within different domains** where human interaction and judgement is required and **identifying potential for improvements** in the context of safety and security.

Motivation

- Strategy for system and AI safety e.g., automotive domain
- Address violations of safety conditions
- Provide solutions for handling exceptional system behavior
- Not considered here Minimum Risk Manoeuvre (ISO 23793-1:2024)
- Increase system availability and reducing interruptions

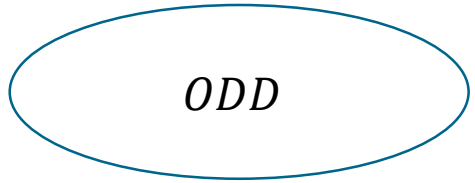
→ Increase the availability and safety of the AI-based system

Agenda

- Introduction
- **Terms and Definitions**
- AODD and Resilience
- Subsystem
- Demonstration
- Summary

Operational Design Domain

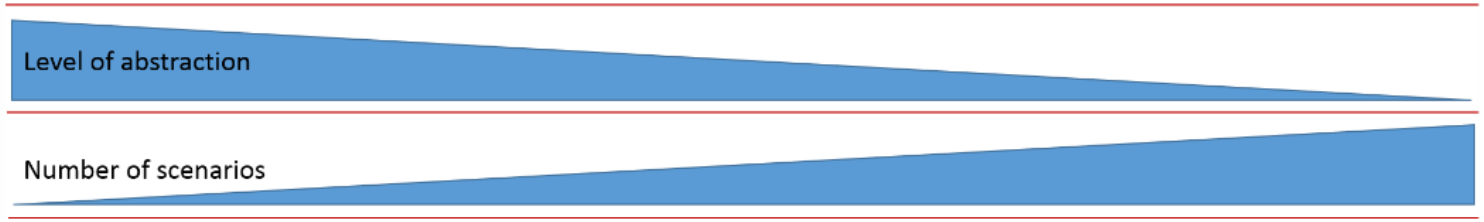
- Different standards have proposed definitions for an Operational Design Domain (ODD) over the years:
  - ISO 21448:2022 - Safety of the intended functionality
  - SAE J3016 Taxonomy and definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
  - or the UL4600 Evaluation of Autonomous Products
- In SAE J3016 the ODD is defined:



"Operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics"

Scenario Descriptions

Functional scenarios	Logical scenarios	Concrete scenarios
Base road network:	**Base road network:**	**Base road network:**
three-lane motorway in a curve, 100 km/h speed limit indicated by traffic signs	Lane width [2.3..3.5] m Curve radius [0.6..0.9] km Position traffic sign [0..200] m	Lane width [3.2] m Curve radius [0.7] km Position traffic sign [150] m
Stationary objects:	**Stationary objects:**	**Stationary objects:**
-	-	-
Moveable objects:	**Moveable objects:**	**Moveable objects:**
Ego vehicle, traffic jam; Interaction: Ego in maneuver „approaching“ on the middle lane, traffic jam moves slowly	End of traffic jam [10..200] m Traffic jam speed [0..30] km/h Ego distance [50..300] m Ego speed [80..130] km/h	End of traffic jam 40 m Traffic jam speed 30 km/h Ego distance 200 m Ego speed 100 km/h
Environment:	**Environment:**	**Environment:**
Summer, rain	Temperature [10..40] °C Droplet size [20..100] µm	Temperature 20 °C Droplet size 30 µm

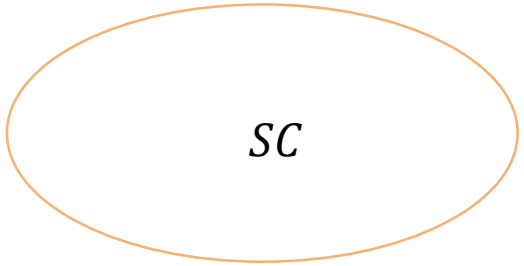


PEGASUS, "Scenario Description", 2018. [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/PDF-Symposium/04_Scenario-Description.pdf. Accessed on: March 03, 2020.

System Capability

- The system capability (SC) is derived from the capabilities of hardware and software e.g., Advanced Driving Systems (ADS).
- Builds on DoDAF and ISO 9000:2015
- **System Capability**:

“The ability to achieve specified performance metrics within a specific operating environment or condition”



Set of Scenarios determine SC and ODD

Logical scenarios		
Base road network:		
	Lane width	[2.3..3.5] m
	Curve radius	[0.6..0.9] km
	Position traffic sign	[0..200] m
Stationary objects:		
	-	
Moveable objects:		
	End of traffic jam	[10..200] m
	Traffic jam speed	[0..30] km/h
	Ego distance	[50..300] m
	Ego speed	[80..130] km/h
Environment:		
	Temperature	[10..40] °C
	Droplet size	[20..100] µm

SC

Braking force [0 kN .. 3 kN]

PEGASUS, "Scenario Description", 2018. [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/PDF-Symposium/04_Scenario-Description.pdf. Accessed on: March 03, 2020.

Logical scenarios		
Base road network:		
	Lane width	[2.3..3.5] m
	Curve radius	[0.6..0.9] km
	Position traffic sign	[0..200] m
Stationary objects:		
	-	
Moveable objects:		
	End of traffic jam	[10..200] m
	Traffic jam speed	[0..30] km/h
	Ego distance	[50..300] m
	Ego speed	[80..130] km/h
Environment:		
	Temperature	[10..40] °C
	Droplet size	[20..100] µm

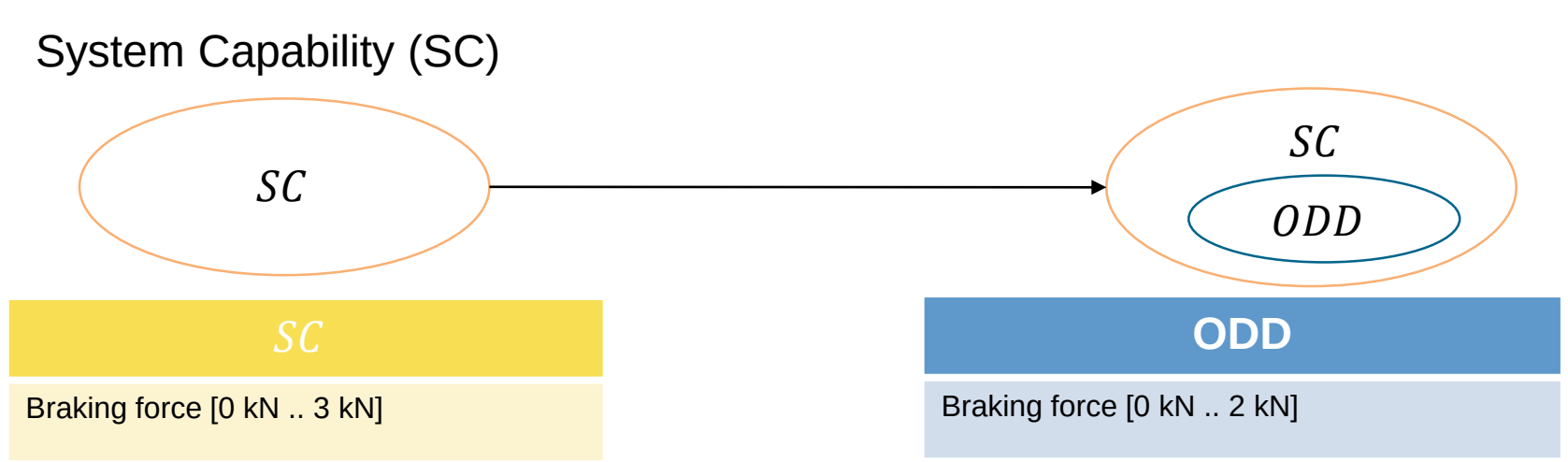
ODD

Braking force [0 kN .. 2 kN]

SC and ODD

- The SC is a set of safe scenarios for which the ADS is functioning safely.
- The safe functionality is determined by the developer of ADS.
- The ODD defines a set of safe scenarios and is controlled by a third party.

Logical scenarios	
Base road network:	
Lane width	[2.3..3.5] m
Curve radius	[0.6..0.9] km
Position traffic sign	[0..200] m
Stationary objects:	
-	
Moveable objects:	
End of traffic jam	[10..200] m
Traffic jam speed	[0..30] km/h
Ego distance	[50..300] m
Ego speed	[80..130] km/h
Environment:	
Temperature	[10..40] °C
Droplet size	[20..100] µm

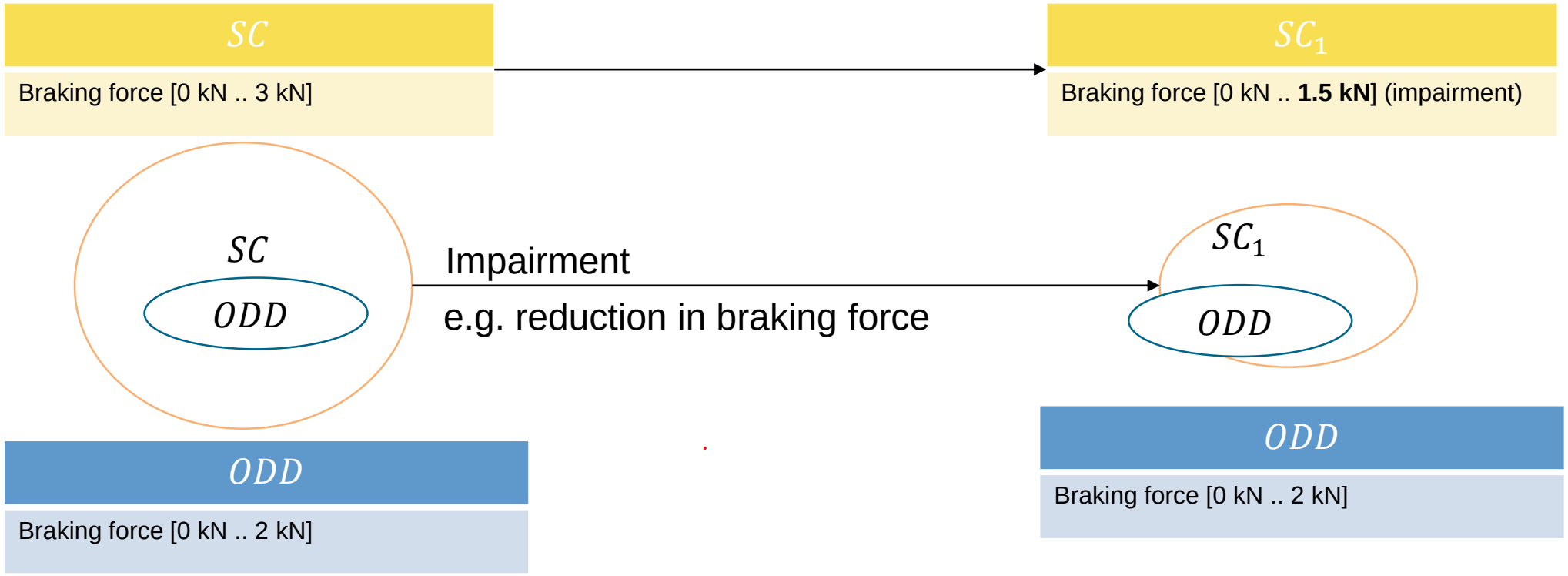


Logical scenarios	
Base road network:	
Lane width	[2.3..3.5] m
Curve radius	[0.6..0.9] km
Position traffic sign	[0..200] m
Stationary objects:	
-	
Moveable objects:	
End of traffic jam	[10..200] m
Traffic jam speed	[0..30] km/h
Ego distance	[50..300] m
Ego speed	[80..130] km/h
Environment:	
Temperature	[10..40] °C
Droplet size	[20..100] µm

PEGASUS, "Scenario Description", 2018. [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/PDF-Symposium/04_Scenario-Description.pdf. Accessed on: March 03, 2020.

Impairment: Operational Design Domain

- System impairments reduce the range of safe Logical Scenarios for the ADS

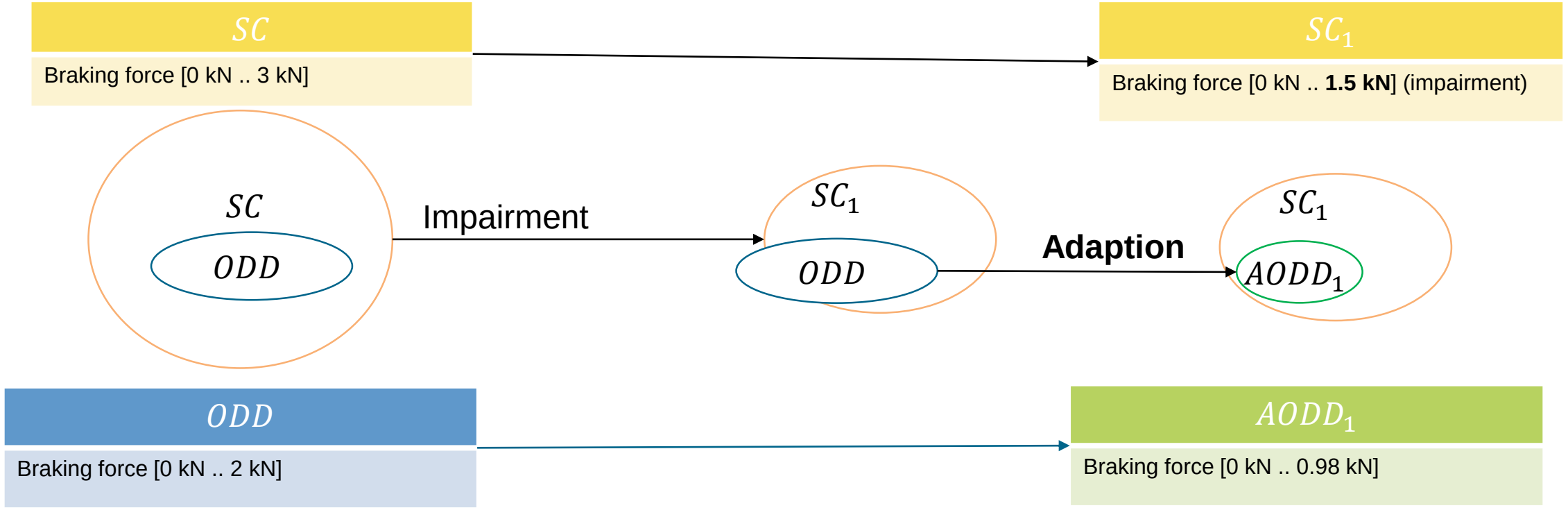


Agenda

- Introduction
- Terms and Definitions
- **AODD and Resilience**
- Subsystem
- Demonstration
- Summary

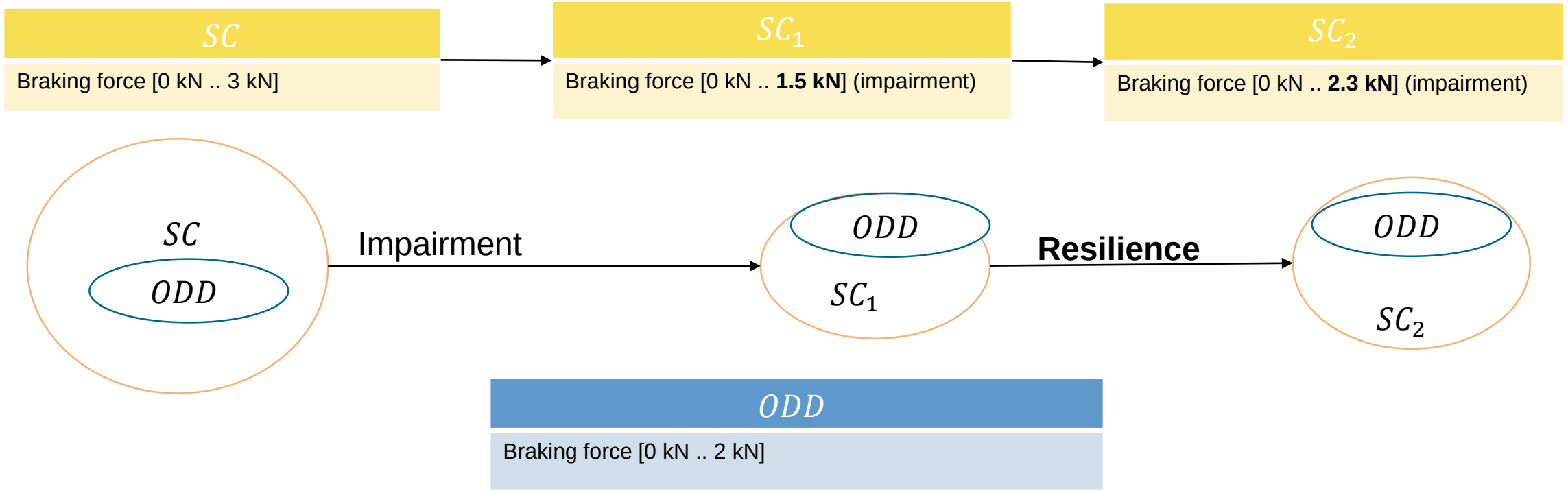
Impairment:
Adaptive Operational Design Domain (AODD)

- The Adaptive Operational Design is a reduced set of safe Logical Scenarios of the Operational Design Domain, due to the reduction of System Capability.

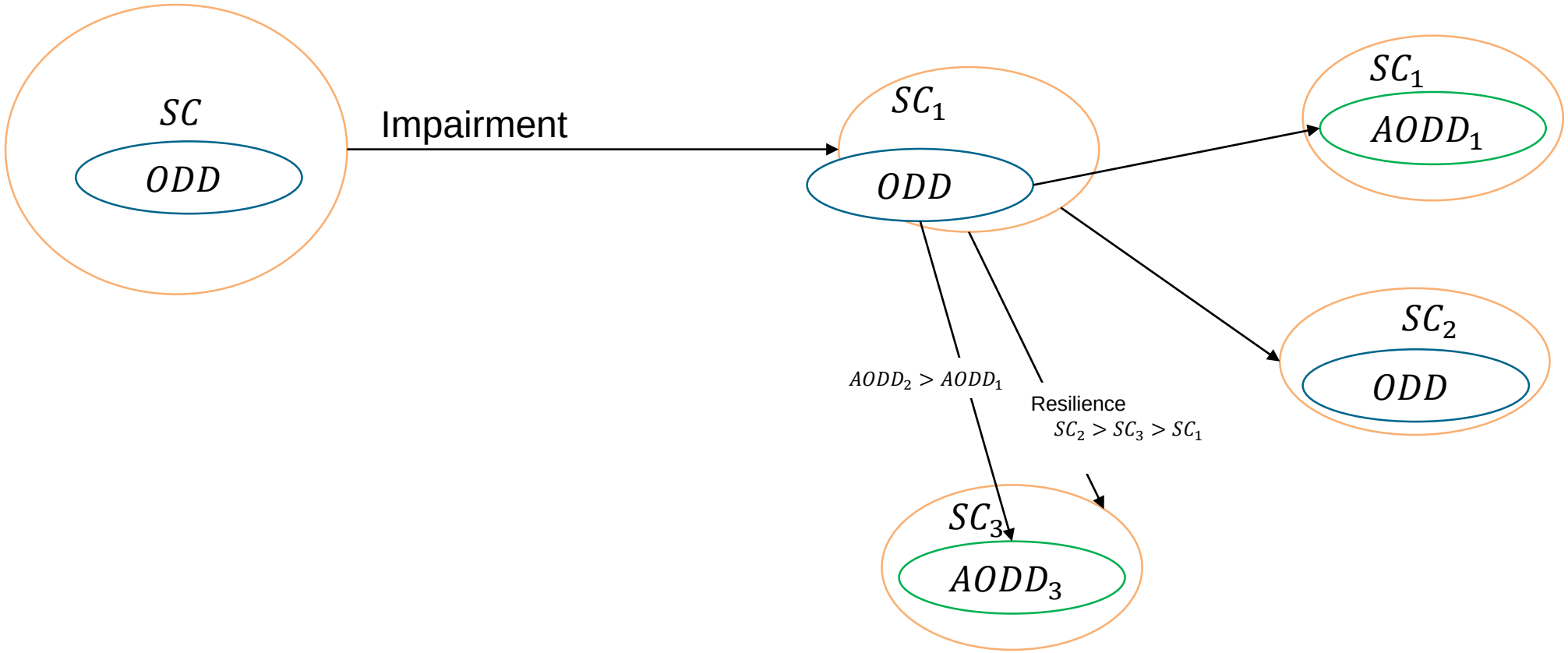


Impairment: Deriving Resilience

- Resilience: System impairment does not reduce the range of safe Logical Scenarios for ADS



Impairment:
Adaptive Operational Design Domain and Resilience



Ryan Mut, Institute for AI Safety and Security

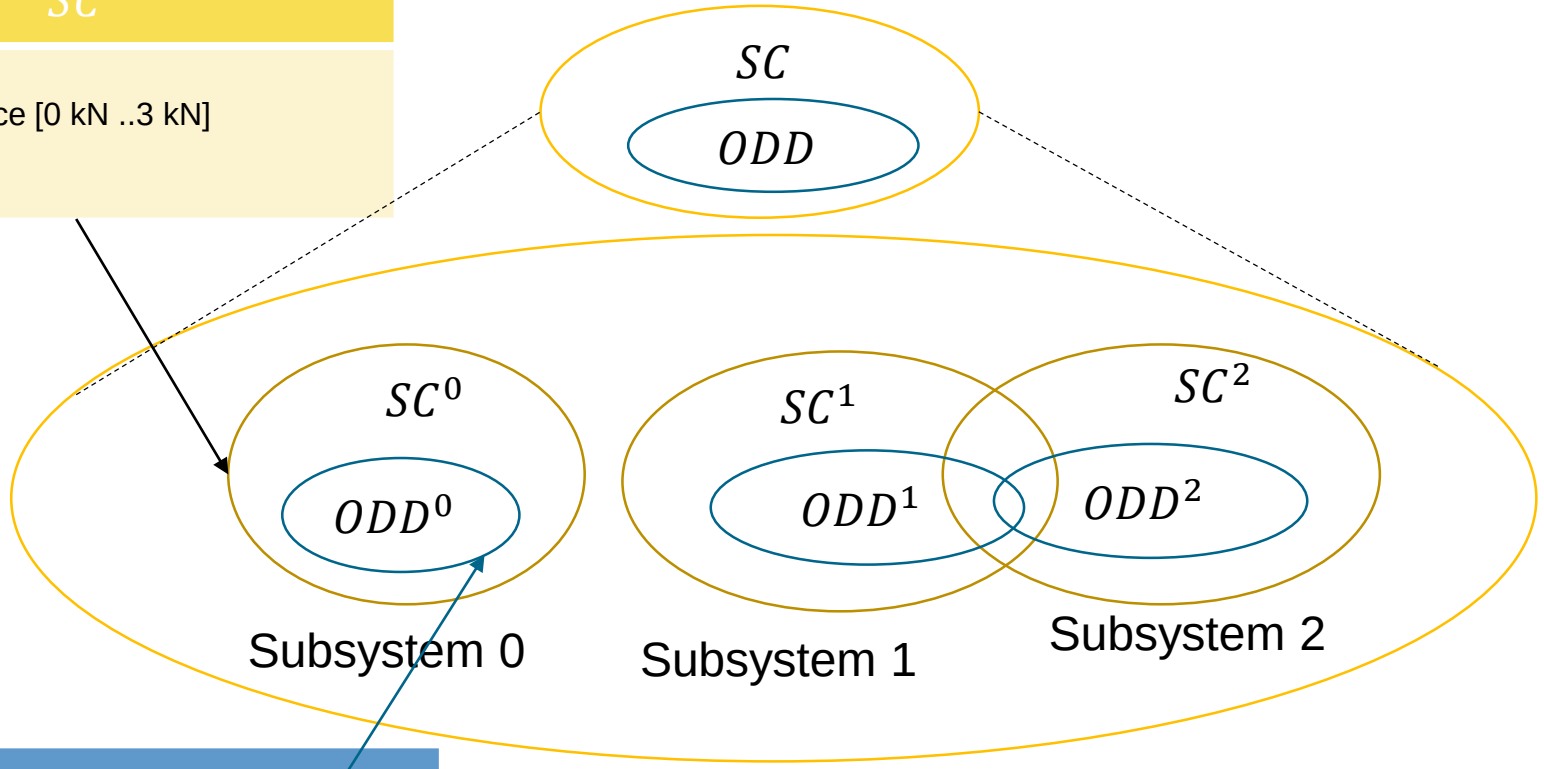
Agenda

- Introduction
- Terms and Definitions
- AODD and Resilience
- **Subsystem**
- Demonstration
- Summary

System Capability, ODD and Subsystem

SC

Subsystem:
SC^1 Braking force [0 kN ..3 kN]
Subsystem:
….



ODD

Subsystem:
ODD^1 Braking force [0 kN .. 2 kN]
Subsystem:
….

Logical scenarios	
Base road network:	
Lane width	[2.3..3.5] m
Curve radius	[0.6..0.9] km
Position traffic sign	[0..200] m
Stationary objects:	
-	
Moveable objects:	
End of traffic jam	[10..200] m
Traffic jam speed	[0..30] km/h
Ego distance	[50..300] m
Ego speed	[80..130] km/h
Environment:	
Temperature	[10..40] °C
Droplet size	[20..100] µm

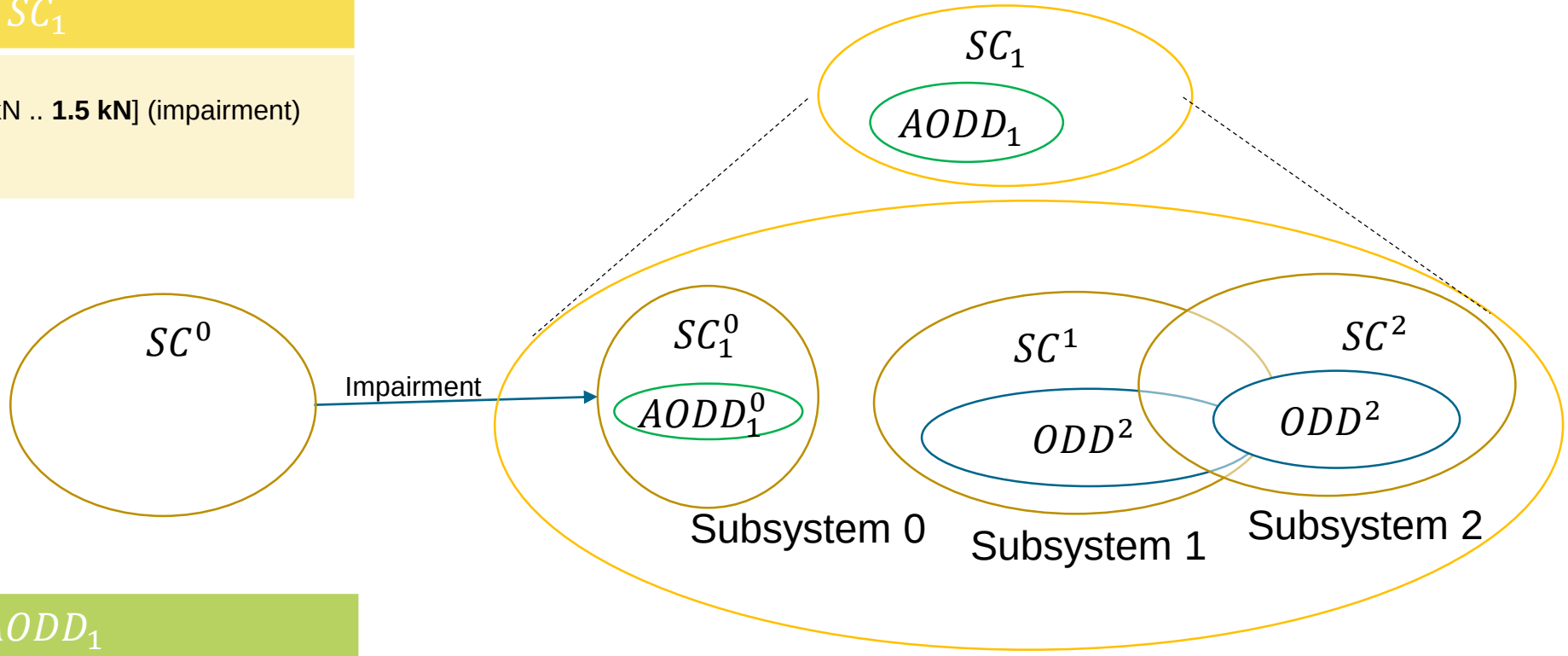
Logical scenarios	
Base road network:	
Lane width	[2.3..3.5] m
Curve radius	[0.6..0.9] km
Position traffic sign	[0..200] m
Stationary objects:	
-	
Moveable objects:	
End of traffic jam	[10..200] m
Traffic jam speed	[0..30] km/h
Ego distance	[50..300] m
Ego speed	[80..130] km/h
Environment:	
Temperature	[10..40] °C
Droplet size	[20..100] µm

PEGASUS, "Scenario Description", 2018. [Online]. Available: https://www.pegasusprojekt.de/files/tmpl/PDF-Symposium/04_Scenario-Description.pdf. Accessed on: March 03, 2020.

System Capability, AODD and Subsystem

SC_1

Subsystem:
SC_1^0 Braking force [0 kN .. **1.5 kN**] (impairment)
Subsystem:
….



$AODD_1$

Subsystem:
$AODD_1^0$ Braking force [0 kN .. 0.98 kN]
Subsystem:
….

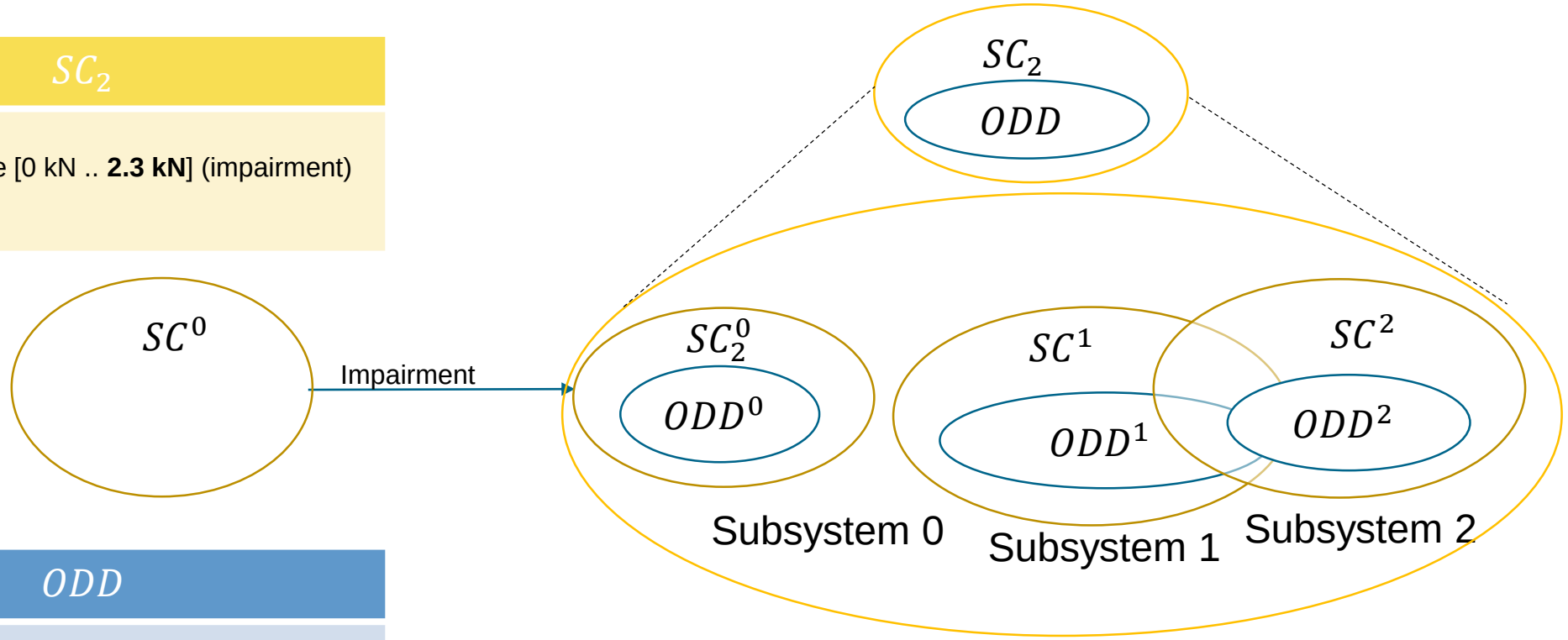
Resilience and Subsystem

SC_2

Subsystem:
SC_2^0 Braking force [0 kN .. **2.3 kN**] (impairment)
Subsystem:
….

ODD

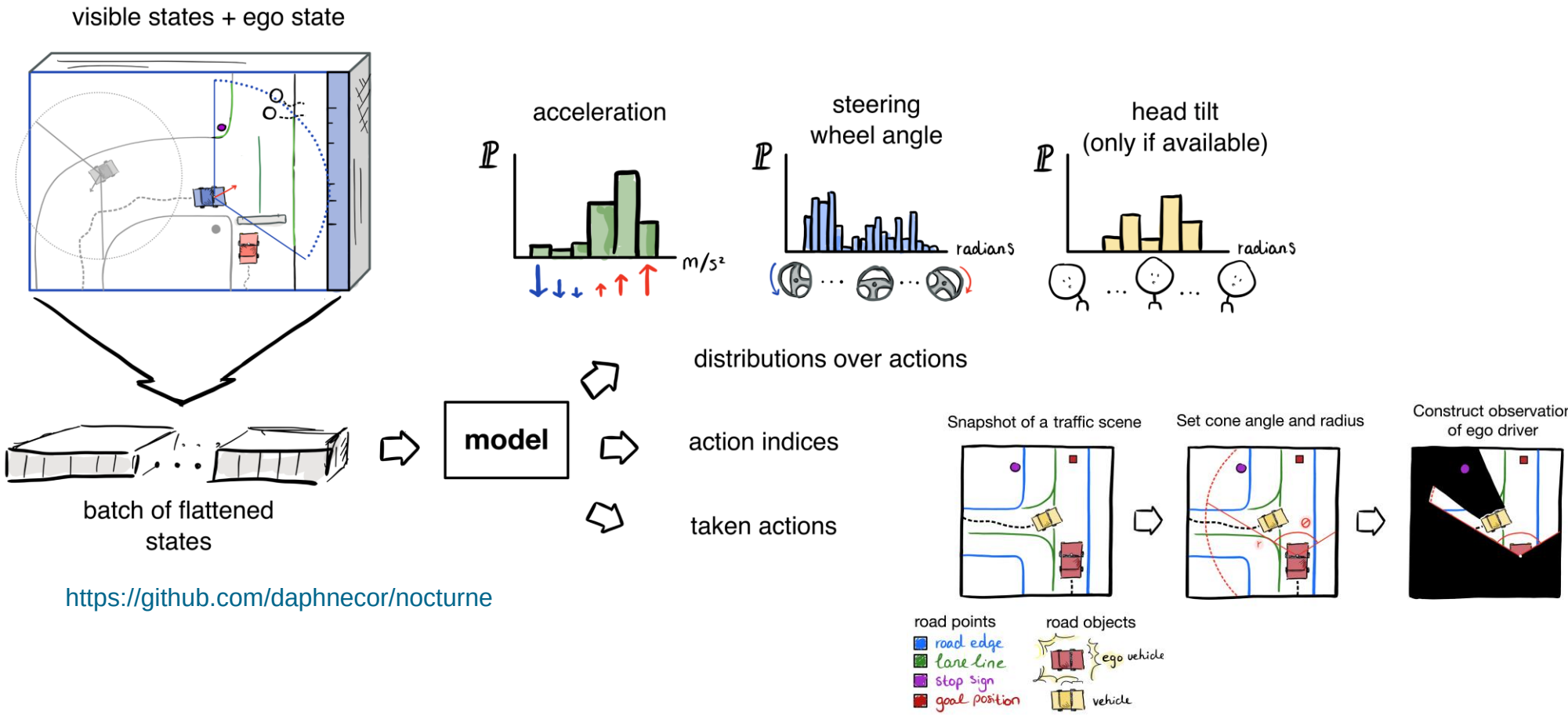
Subsystem:
ODD^0 Braking force [0 kN .. 2 kN]
Subsystem:
….



Agenda

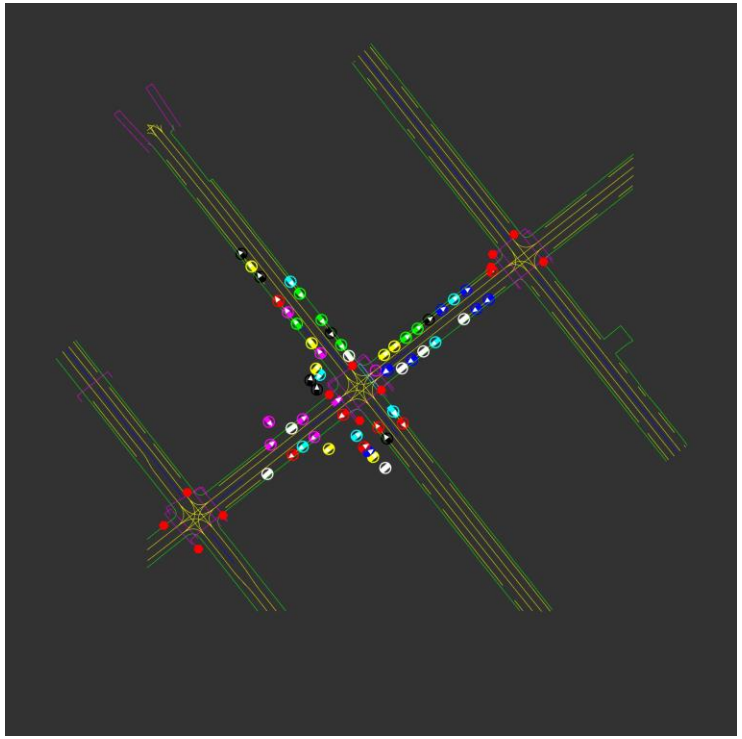
- Introduction
- Terms and Definitions
- AODD and Resilience
- Subsystem
- **Demonstration**
- Summary

Demonstration of an Impairment
Nocturne

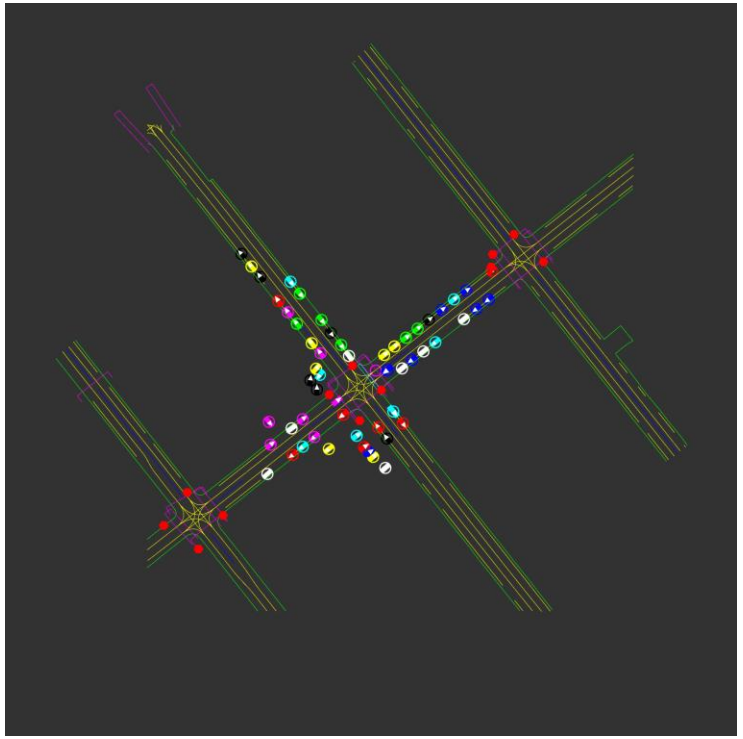


https://github.com/daphnecor/nocturne

Demonstration: Traffic scenario within Nocturne



Real Driven Scenario



AI driven Scenario

https://github.com/daphnecor/nocturne

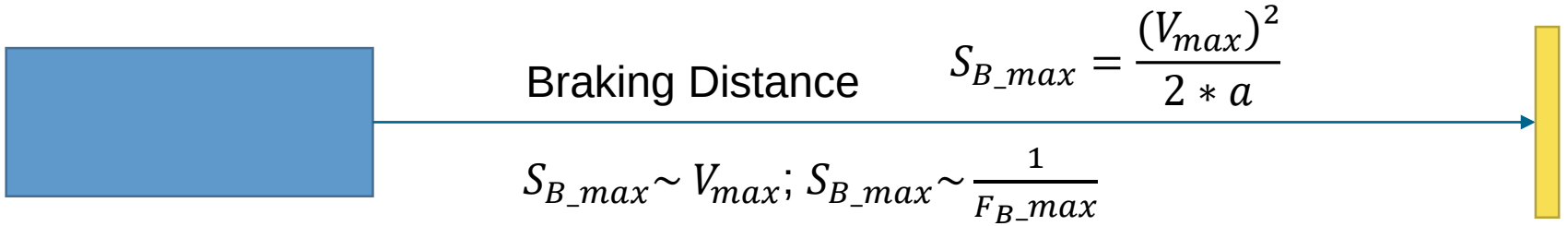
Evaluation:

'goal_achieved': True,
'collided': False
'veh_veh_collision': False,
'veh_edge_collision': False

'goal_achieved': True,
'collided': False,
'veh_veh_collision': False,
'veh_edge_collision': False

Safety Justification:
Exceptional Behavior for Impaired system

- Impaired Braking system → Reduced maximum Speed



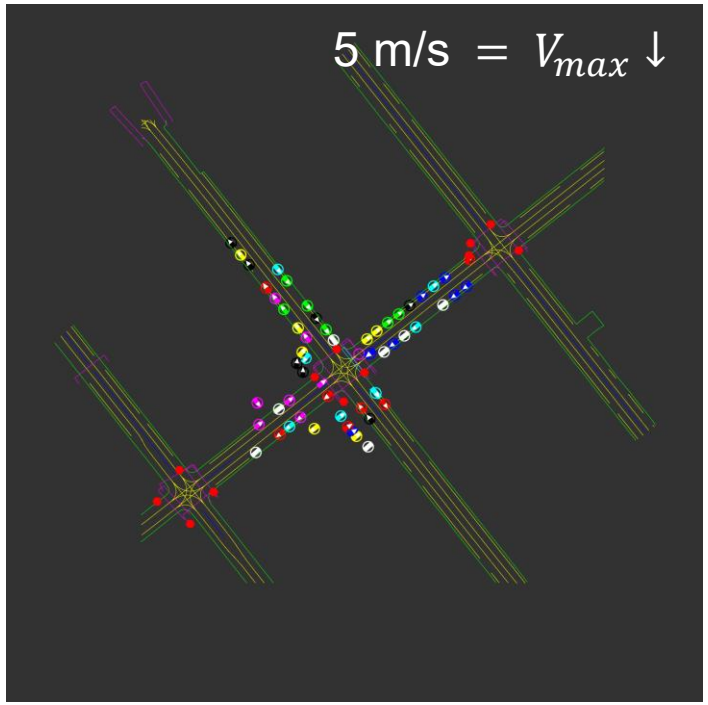
$S_{B\_max} \rightarrow Cost.$

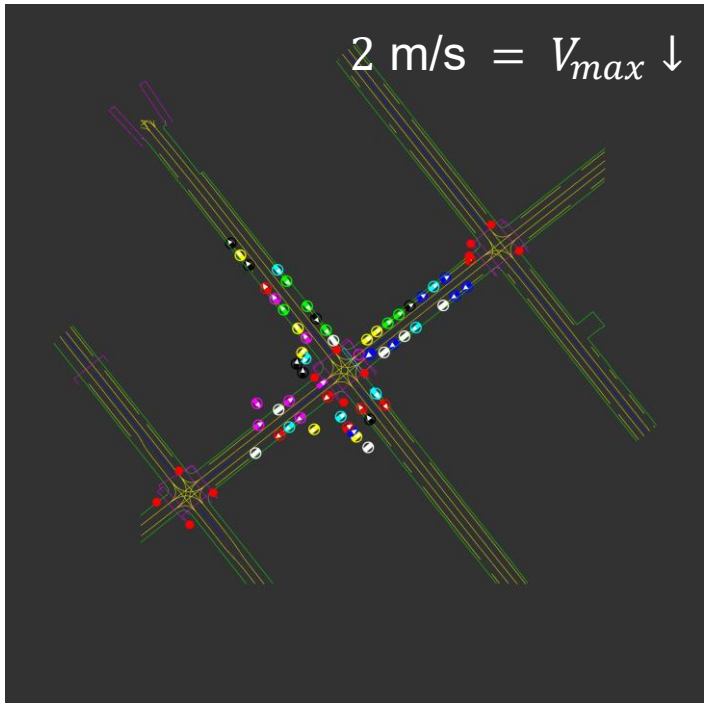
- The reduction of maximum Speed is proportional to the los of braking force. The reduced maximum Speed $V_{max} \downarrow$.

Ryan Mut, Institute for AI Safety and Security

Demonstration: Impaired system with an applied AODD

- Impaired Braking system → Reduced maximum Speed





Evaluation:

'goal_achieved': True,
'collided': False,
'veh_veh_collision': False,
'veh_edge_collision': False

'goal_achieved': False,
'collided': False,
'veh_veh_collision': False,
'veh_edge_collision': False

Agenda

- Introduction
- Terms and Definitions
- AODD and Resilience
- Subsystem
- Demonstration
- **Summary**

Summary

- Strategy for impaired systems to handle exceptional conditions
- SC and ODD for Automated Driving Systems (ADS)
- Impaired system and AODD
- Impaired system and Resilience
- Dependencies between SC, ODD, Resilience and AODD

→AODD and Resilience increase the availability of the system

Contact

Ryan Mut, Institute for AI Safety and Security
German Aerospace Center (DLR)
Institute for AI-Safety and Security
Postal Address: Rathausallee 12
53757 Sankt Augustin
Germany

ryan.mut@dlr.de