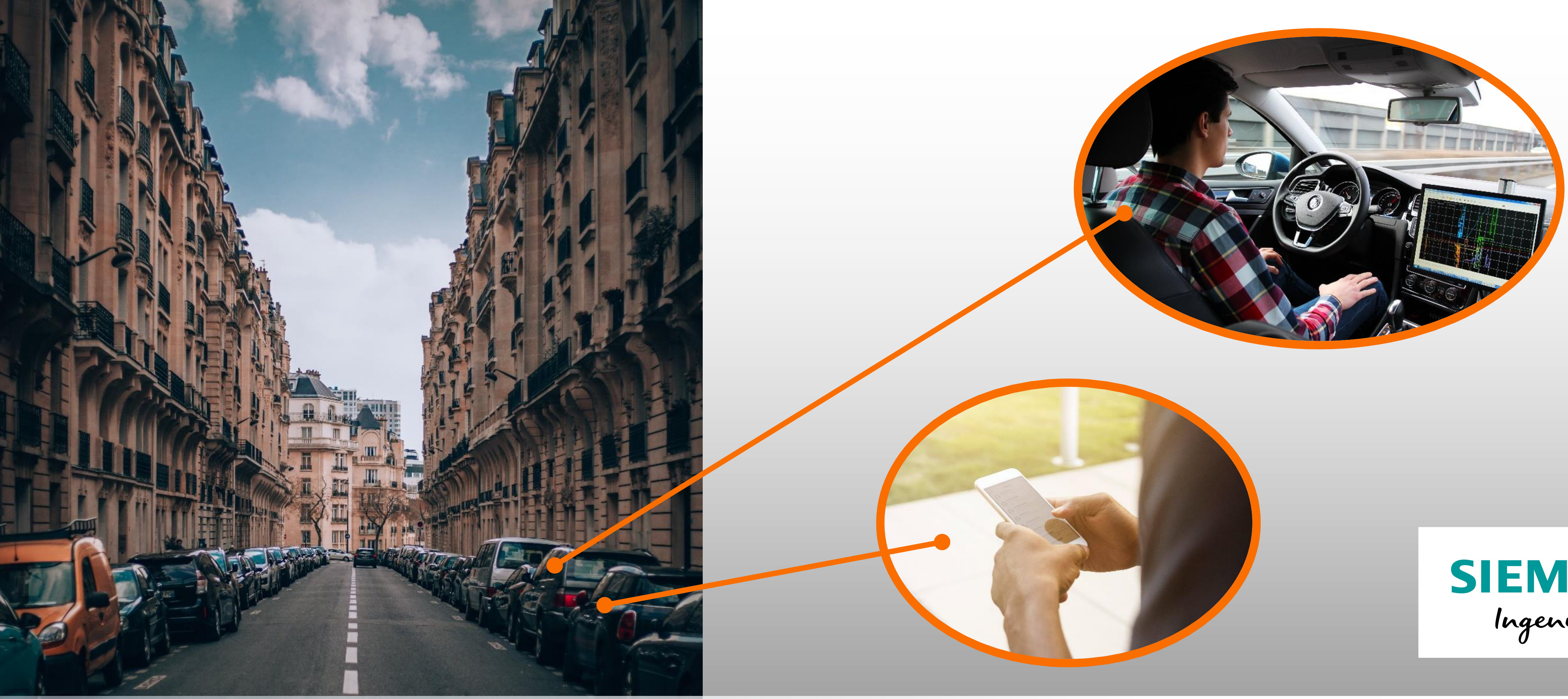


SIEMENS
Ingenuity for life

Verification and Validation of Automated Valet Parking System - Safety Challenges and Solutions

Dr. Alexandru Forrai, USP Event, 16-Dec-2020

USP
UrbanSmartPark

eit Urban Mobility

EIT Urban Mobility is supported by the EIT, a body of the European Union

Presentation Outline

Automated driving systems - main challenges

Verification and validation of automated valet parking system

ISO 26262 perspective

Verification and validation of automated valet parking system

SOTIF perspective

Remarks, conclusions and discussions

Autonomous Vehicles: What are the Main Challenges?

SIEMENS
Ingenuity for life

Technology challenge: build a safe car

- it can perceive the road environment better than a human driver
- it makes “reasonable” decisions like a human driver

Regulatory challenge: build a functional car, accepted by society

- it makes a proper trade-off between safety and functionality – “I am safe if I do not drive but then I am not functional, not accepted“
- it fits into the defined regulatory bounds – ongoing process

Business challenge: build a cost-effective car

- it means consumers are willing to switch to driverless car
- it means new business models, and/or redefinition of “mobility”

EIT Urban Mobility is supported by the EIT, a body of the European Union
eit Urban Mobility

Safety in Different Industry Sectors

SIEMENS
Ingenuity for life

Pick and place robot	Chemical plant	Elevators	Airplane
			
System complexity			
Mid-complexity	High-complexity	Mid-complexity	High-complexity
Safe state (in case of malfunction)			
Sudden stop	Safe stop within ΔT	Stop nearest floor	Land nearest airport
Operational environment			
Known & Defined	Known & Controlled	Known & Defined	Unknown-Predicted

EIT Urban Mobility is supported by the EIT, a body of the European Union
eit Urban Mobility

System and Operational Environment

SIEMENS
Ingenuity for life

		System	
		Simple	**Complex**
Operational environment	**Known**	✓	✓
	Unknown	? maybe not safe	

Remarks:

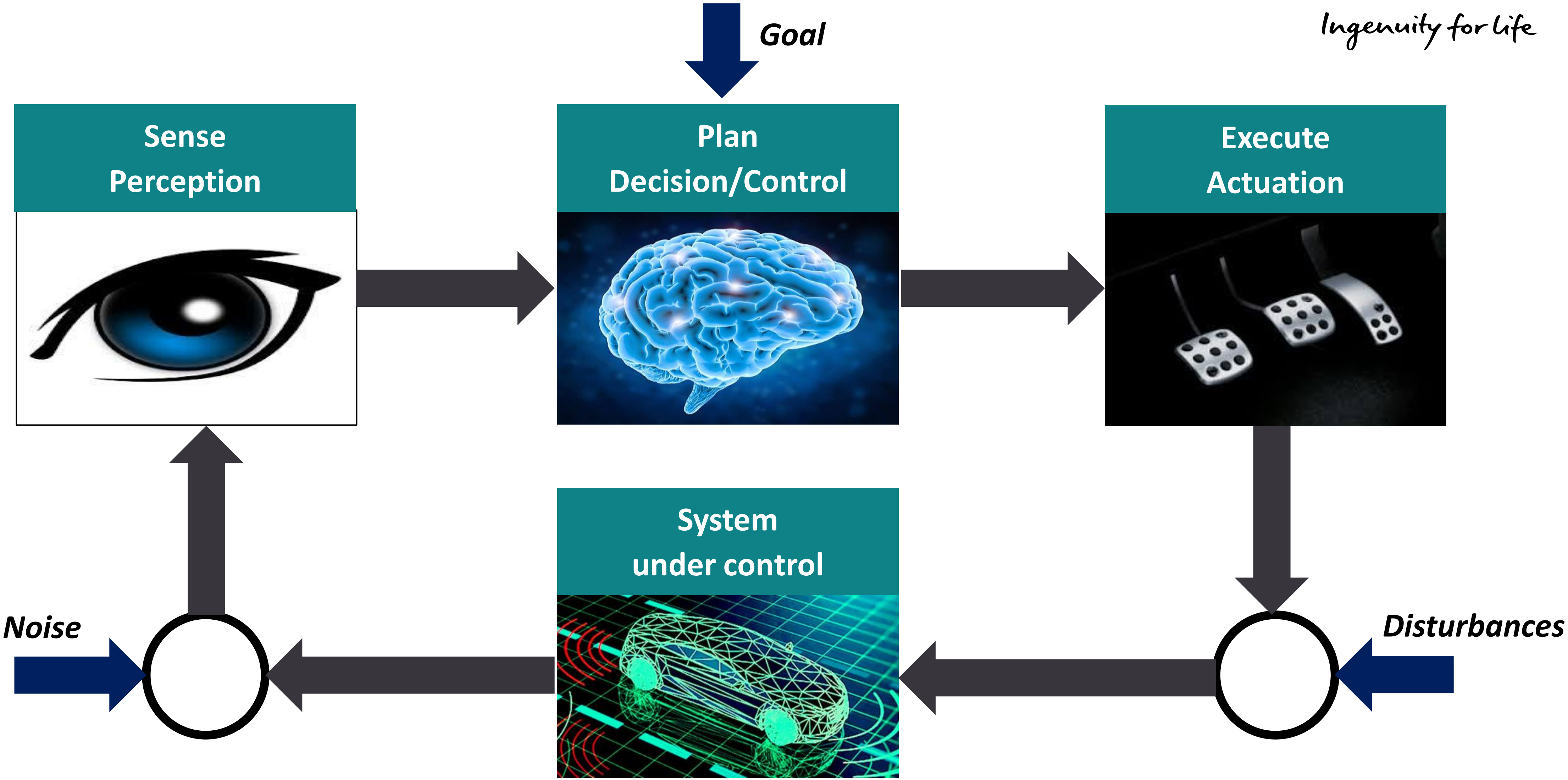
The system is designed for the known operational environment, where should operate safely.

Operational env. shall be known/monitored/predicted – otherwise operational safety cannot be assured.

EIT Urban Mobility is supported by the EIT, a body of the European Union

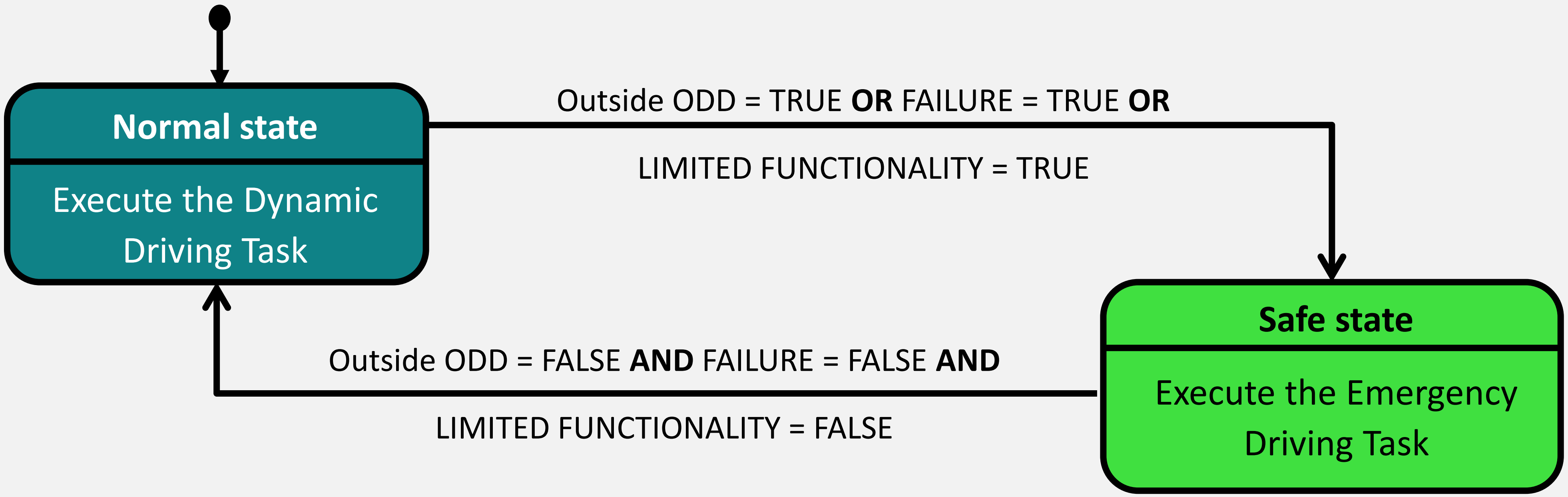
eit Urban Mobility

Automated Driving System



EIT Urban Mobility is supported by the EIT, a body of the European Union

Autonomous Vehicle – a State Machine Representation



Rules for autonomous vehicles (in hierarchical order)

1. Shall prevent harm and avoid accidents
2. Shall maintain free movement of the traffic
3. Shall respect traffic rules and safety distances

Remarks: Emergency Driving Task- move to emergency lane and stop OR stop safely (e.g. no emergency lane)
Operational Design Domain (ODD)

Summary: Main Challenges

Operational environment (operational design domain):

- shall be known, shall be monitored/controlled or shall be well-predicted, otherwise operational safety becomes a very difficult task.

For complex systems – in case of malfunction or limited functionality:

- fault-tolerance or operation under degraded performance shall be guaranteed, so the system can make a smooth transition into the safe state.

Presentation Outline

Automated driving systems - main challenges

Verification and validation of automated valet parking system

ISO 26262 perspective

Verification and validation of automated valet parking system

SOTIF perspective

Remarks, conclusions and discussions

EIT Urban Mobility is supported by the EIT, a body of the European Union

What is Safety?

SIEMENS
Ingenuity for life

What is Safety? Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. (**MIL-STD-882E**).

How to assure safety?

Safety by design, which means: how we **Define →Design →Develop → Deploy.**

Some of the relevant automotive safety standards in use or expected to come:

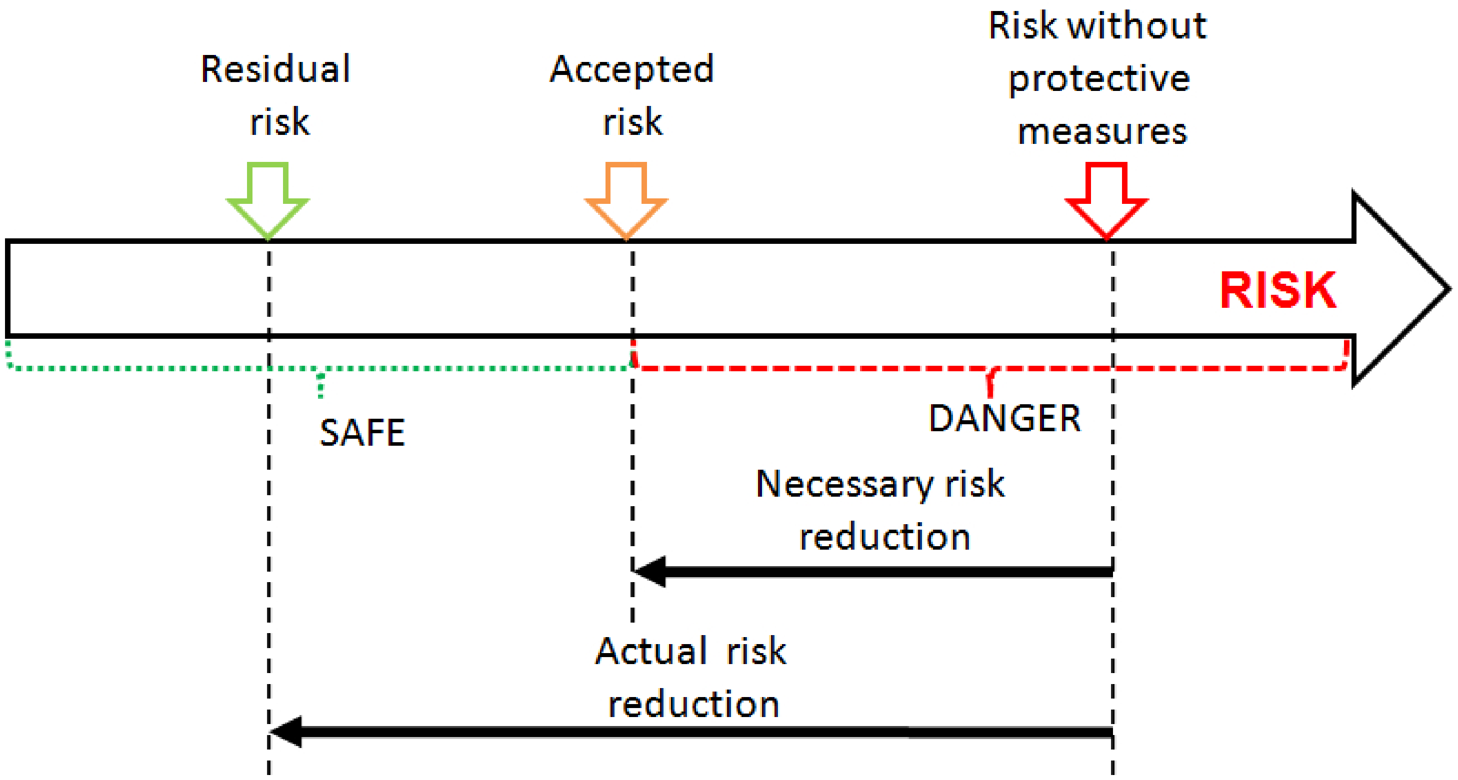
2nd edition ISO26262 (IEC61508)

ISO PAS 21448 (SOTIF) – complementing ISO26162
Road vehicles -- Safety of the intended functionality

SAE J3101 Hardware-Protected Security for Ground Vehicle Applications

SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

What is Risk?



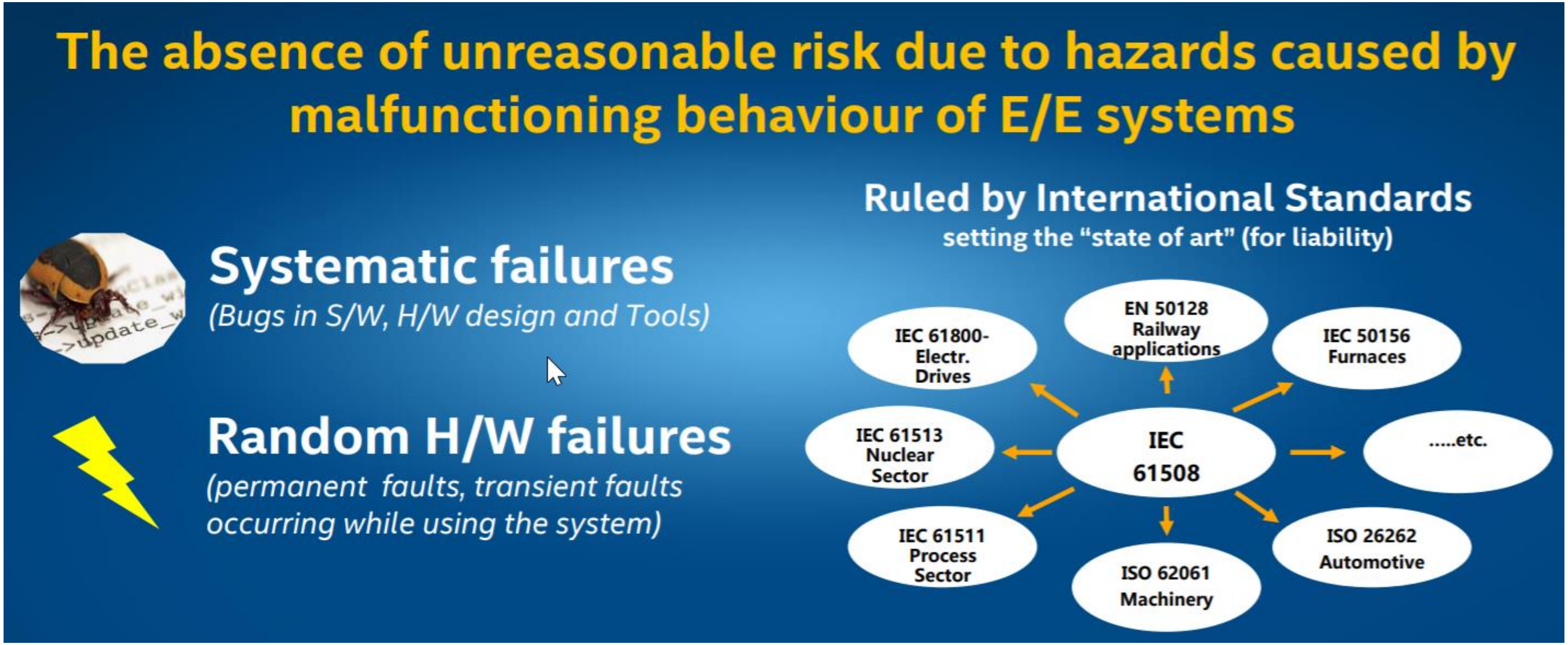
Risk = **S**everity * Probability of **E**xposure = **S * E**

Residual risk = **S**everity * Probability of **E**xposure * (1-**C**ontrollability) = **S * E * (1- C)**

Remark: it is required to minimize the risk at least to the **accepted (tolerable)** risk.

Functional Safety Standards

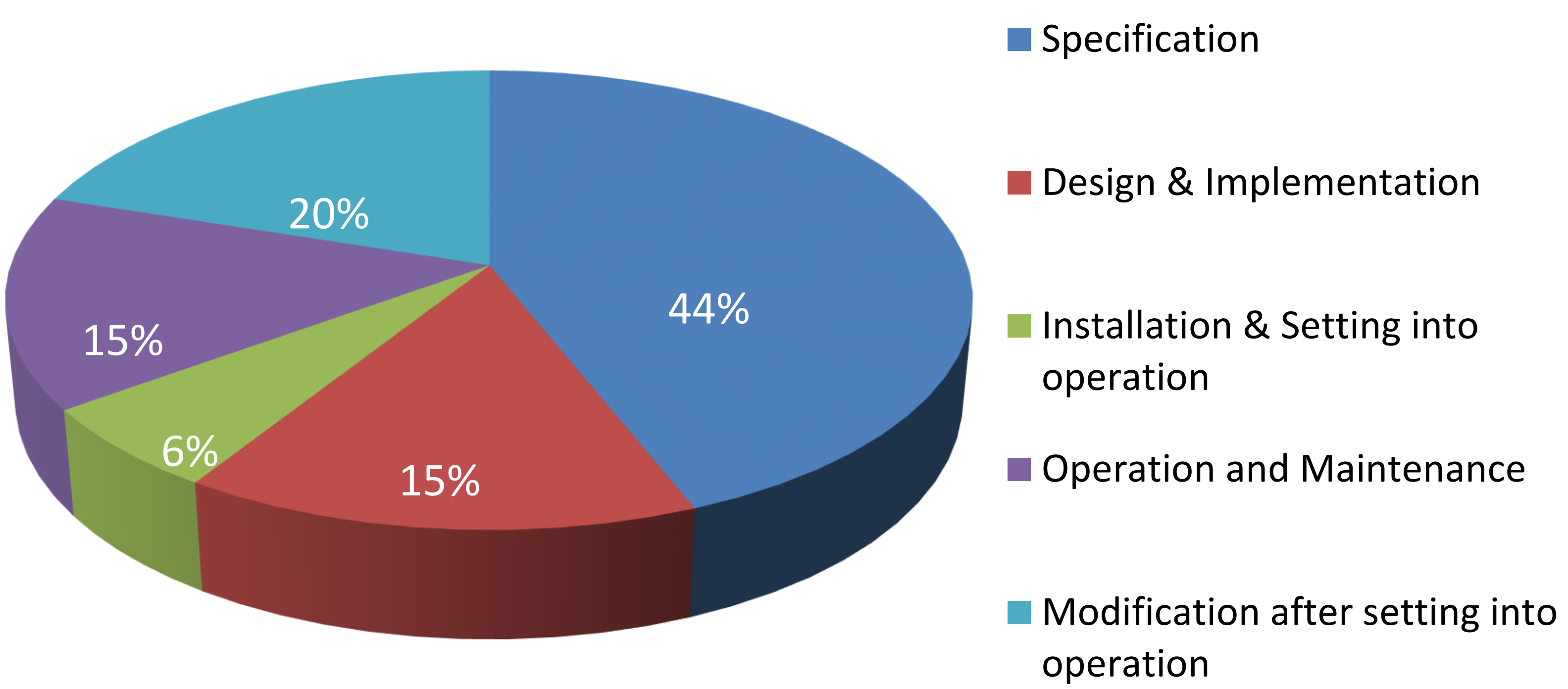
SIEMENS
Ingenuity for life



Functional Safety Standards used in different industry sectors

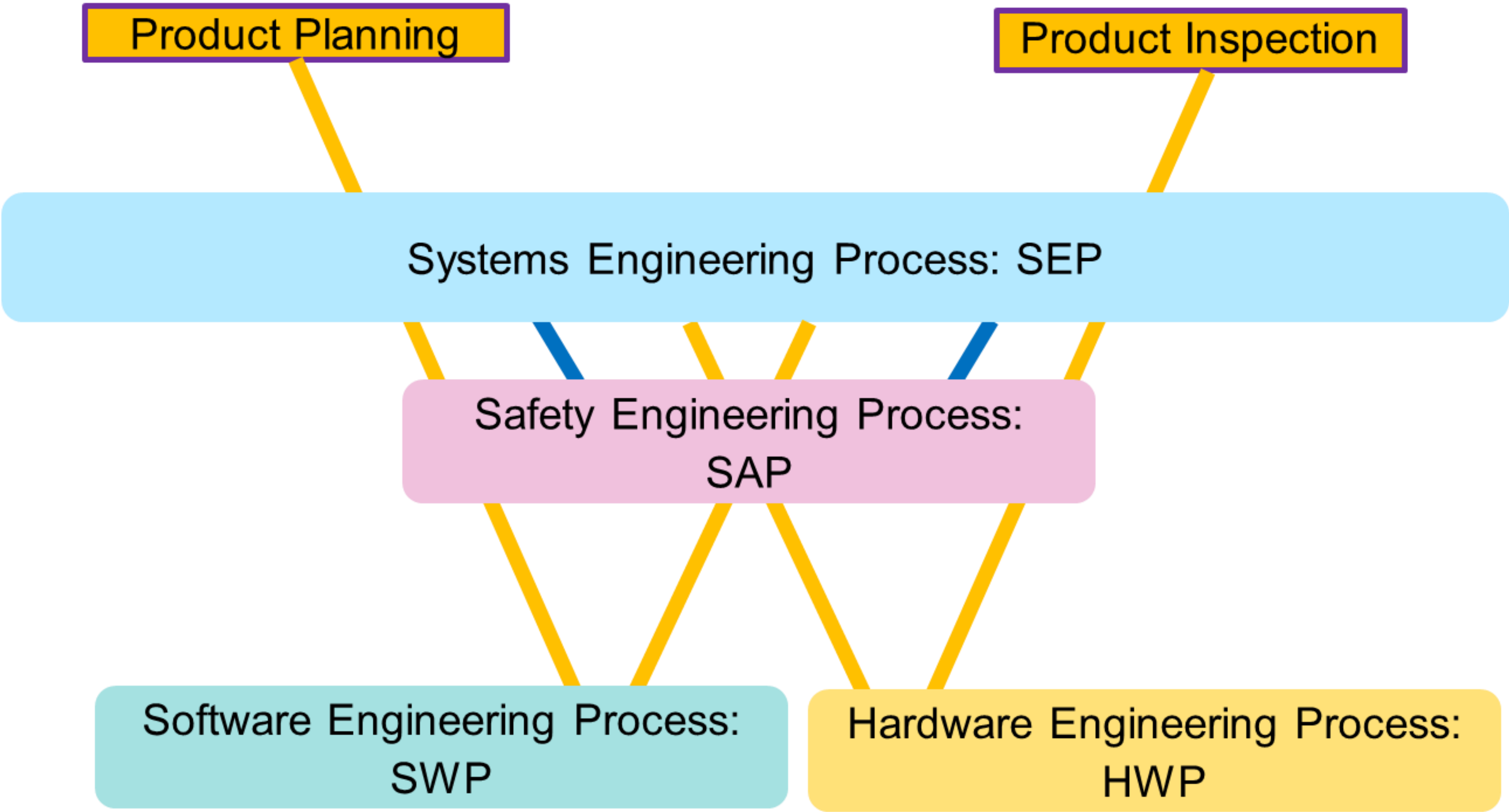
Systematic Failures (SW, Process, Tools)

Failures distribution during development & deployment



Source: UK Health and Safety Executive (HSE)

Development Process: Systems Engineering Approach

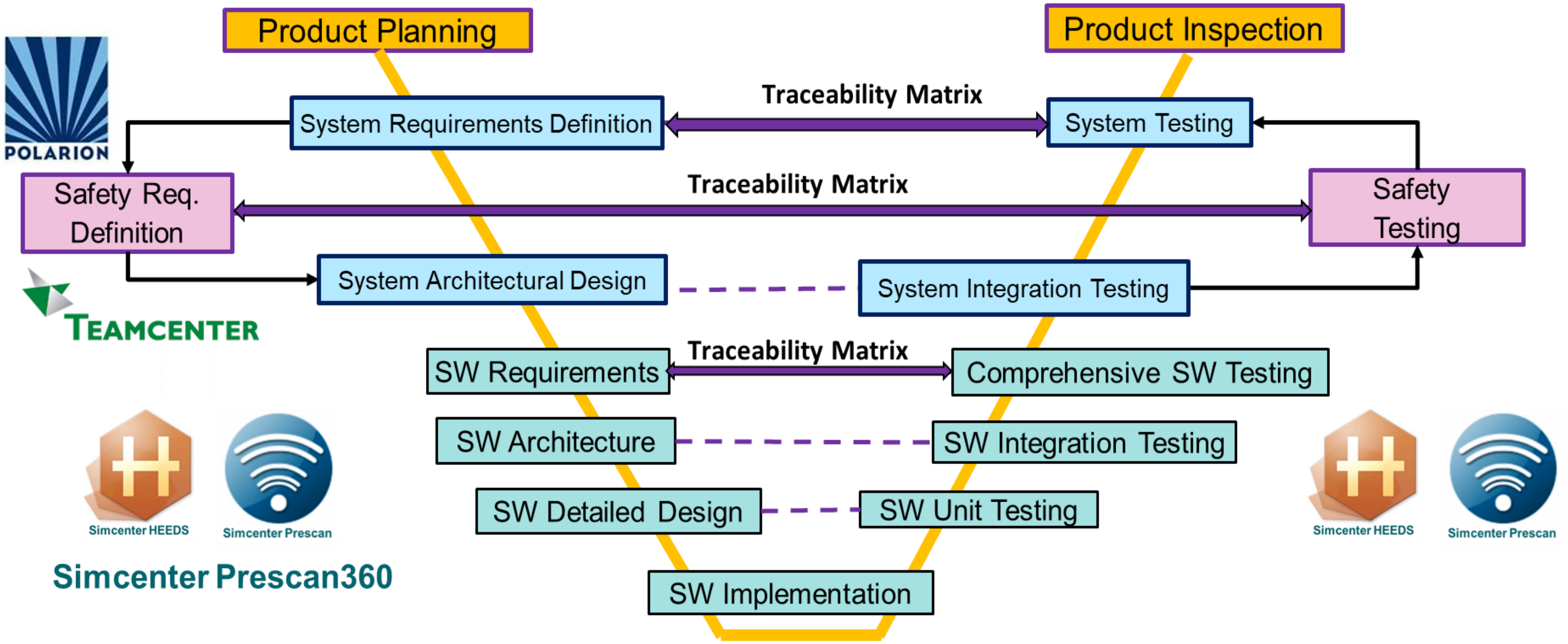


How to assure safety? Safety by design, which means: how we **Define →Design →Develop → Deploy.**

EIT Urban Mobility is supported by the EIT, a body of the European Union

Software Development: Systems Engineering Approach

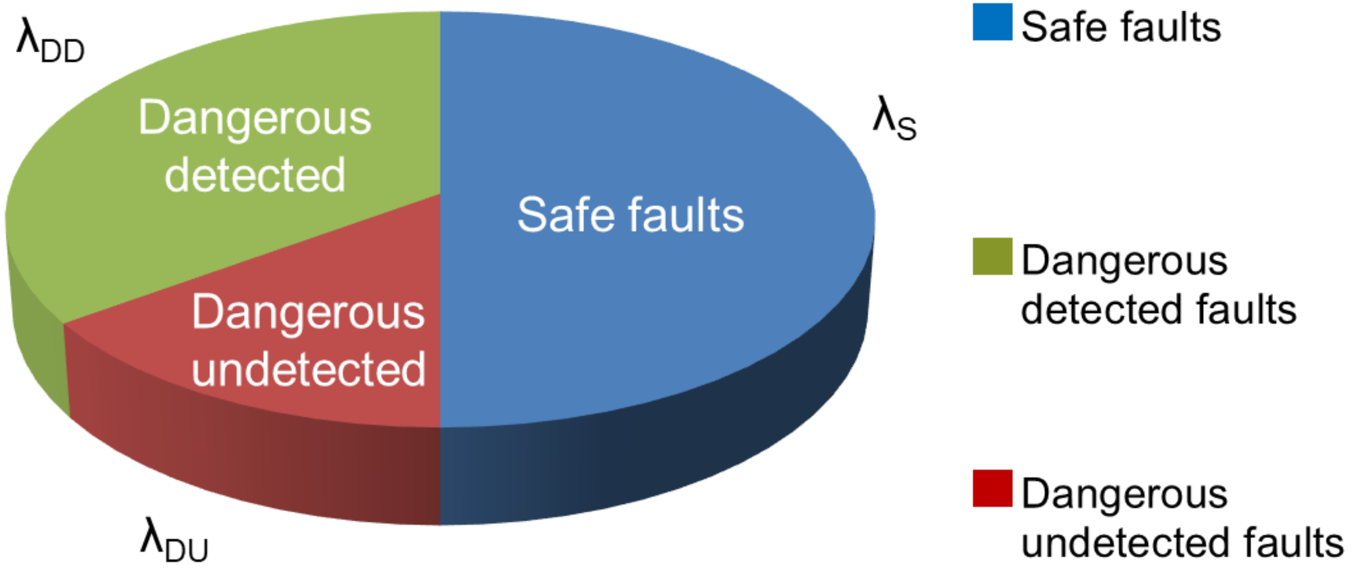
SIEMENS
Ingenuity for life



How to assure safety? Safety by design, which means how we **Define →Design →Develop → Deploy.**

Random (Hardware) Failures

SIEMENS
Ingenuity for life



To be minimized via diagnostics, redundancy, diversity and better quality components.

According to: IEC61508

Remark: undetected fault means that the fault is known but with the current risk reduction methods cannot be detected.

Hazard Analysis and Risk Assessment (HARA)

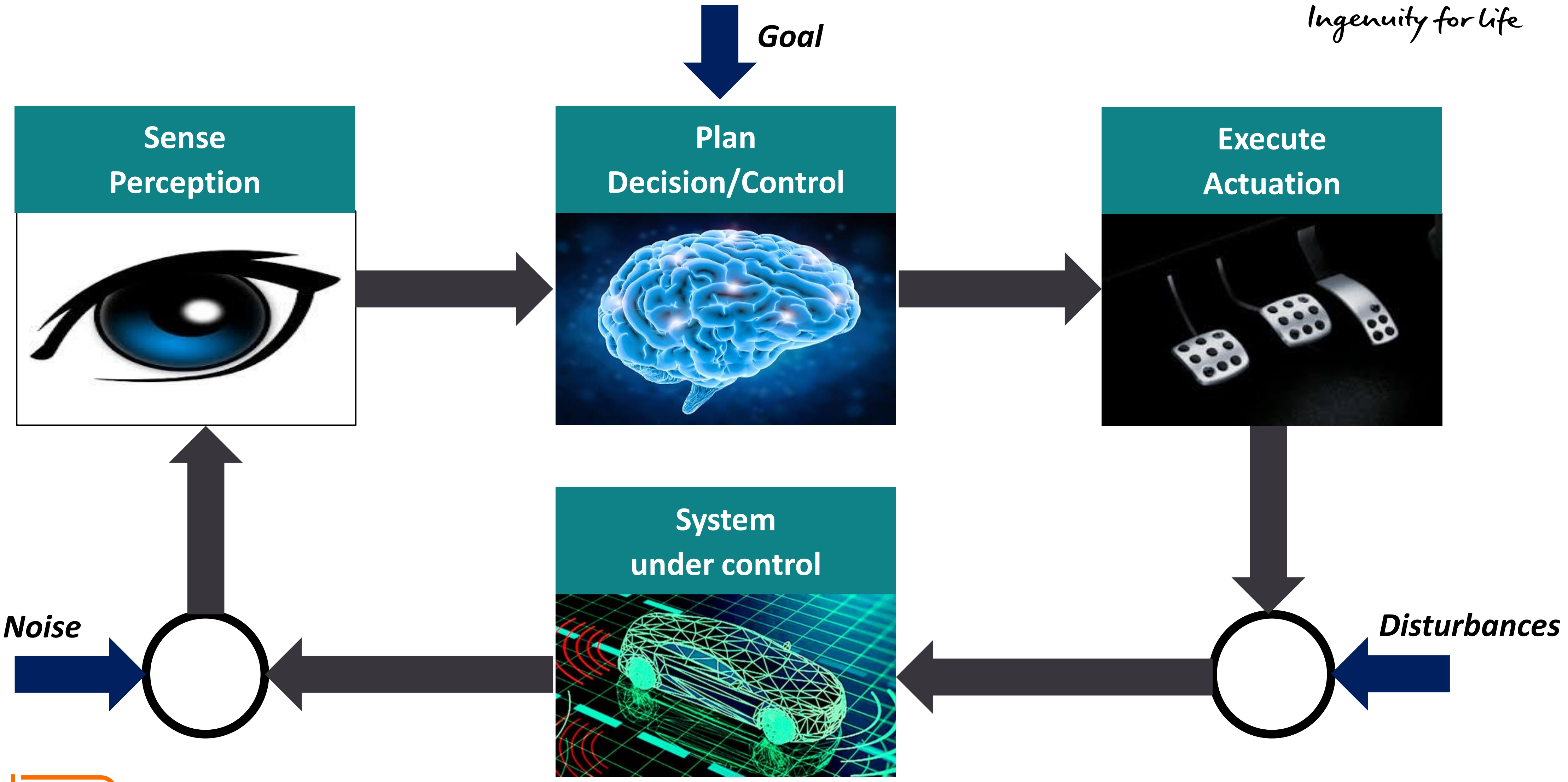
SIEMENS
Ingenuity for life

Malfunction	**ABS system failure**
Hazard Analysis (HA)	**What unintended situations (hazards) could happen?** Loss of stability on a split-friction surface
Risk Assessment (RA)	**Exposure:** How likely is the hazard to happen? → Oils spill, water potholes **Severity:** How harmful is the hazard? → Vehicle may spin out of control → crash **Controllability:** How controllable is the system if the hazard occurs? → driver
ASIL determination	**What is the required risk reduction level?** What is the admissible failure rate? What is the desired effectiveness of the failure detection?

ASIL A → **ASIL B** → **ASIL C** → **ASIL D**

Automotive Safety Integrity Level (ASIL)

Automated Driving System

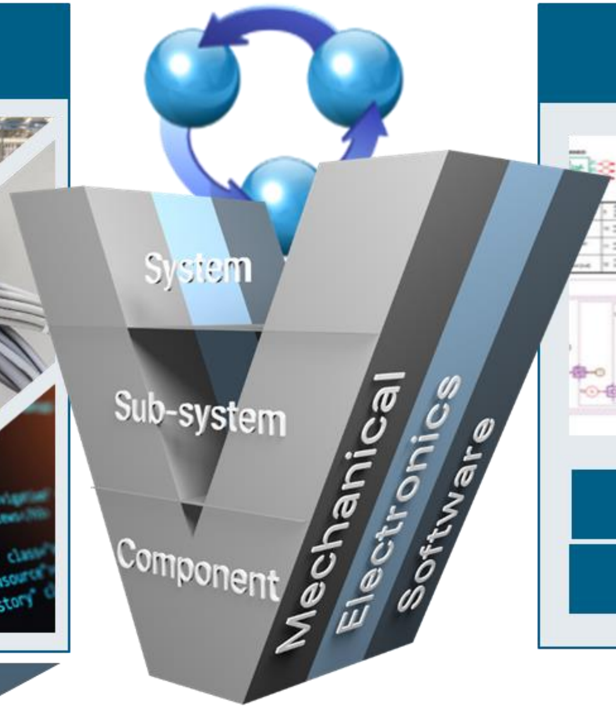


Verification and Validation Process

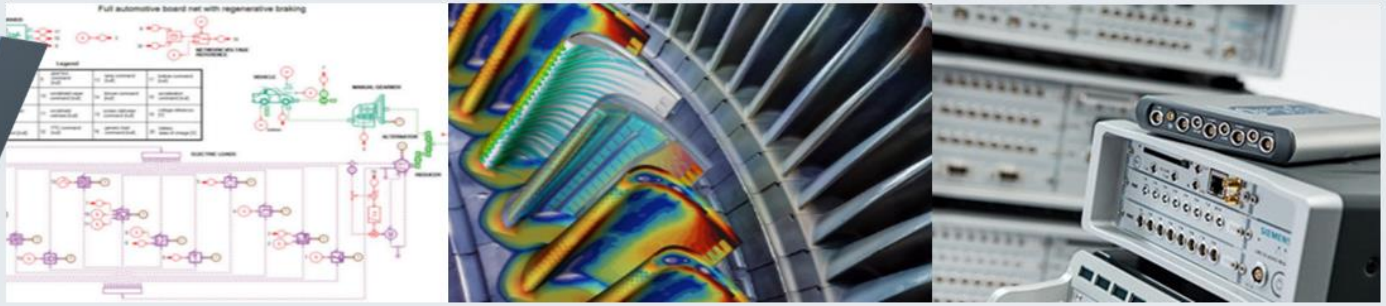
SIEMENS
Ingenuity for life

Verification and Validation at Component, Sub-system and System Level

Design



Simcenter™ Portfolio



System Simulation | CAE Simulation | Physical Testing

Design space exploration

Teamcenter - Traceability, Change and Configuration Management

Presentation Outline

Automated driving systems - main challenges

Verification and validation of automated valet parking system

ISO 26262 perspective

Verification and validation of automated valet parking system

SOTIF perspective

Remarks, conclusions and discussions

EIT Urban Mobility is supported by the EIT, a body of the European Union

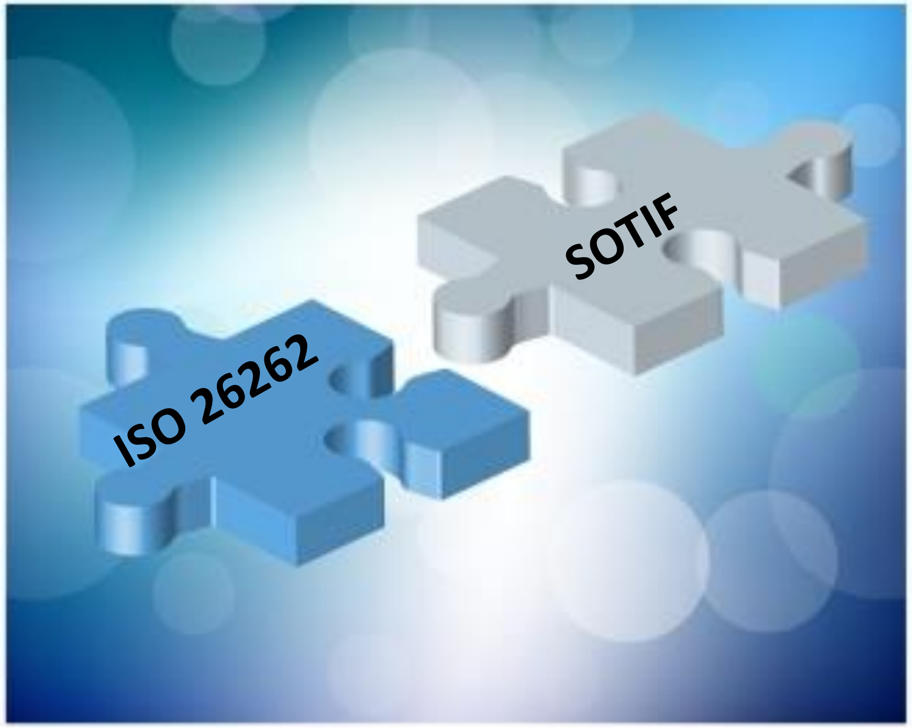
Functional Safety Standards

SIEMENS
Ingenuity for life

ISO26262 – functional safety standard - **how the system should detect and respond to failures**, errors, or off-nominal performance of the self-driving system.

SOTIF – safety of the intended functionality - **how the system should detect and respond to functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons**.

The objective is to validate the automated function in all relevant scenarios, especially in difficult conditions for both sensors and algorithms.

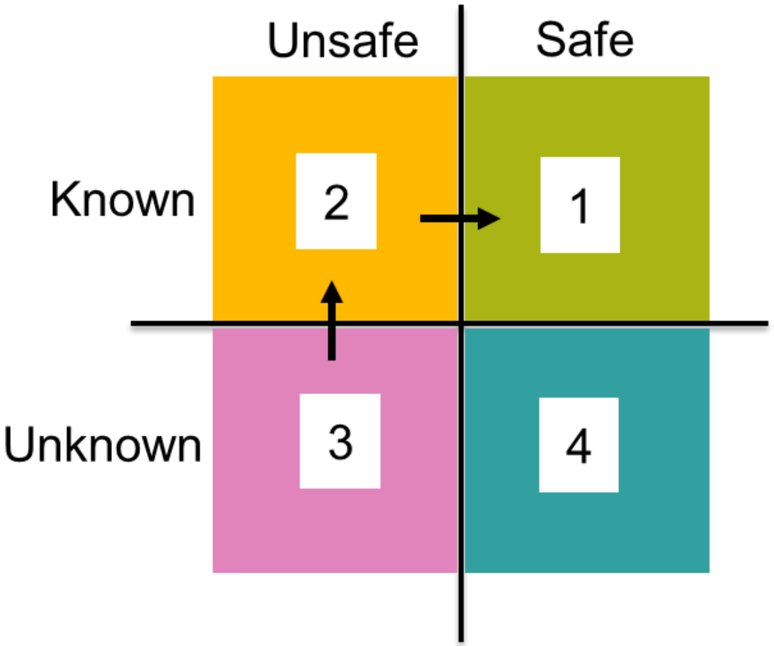


SOTIF **is complementing** ISO26262

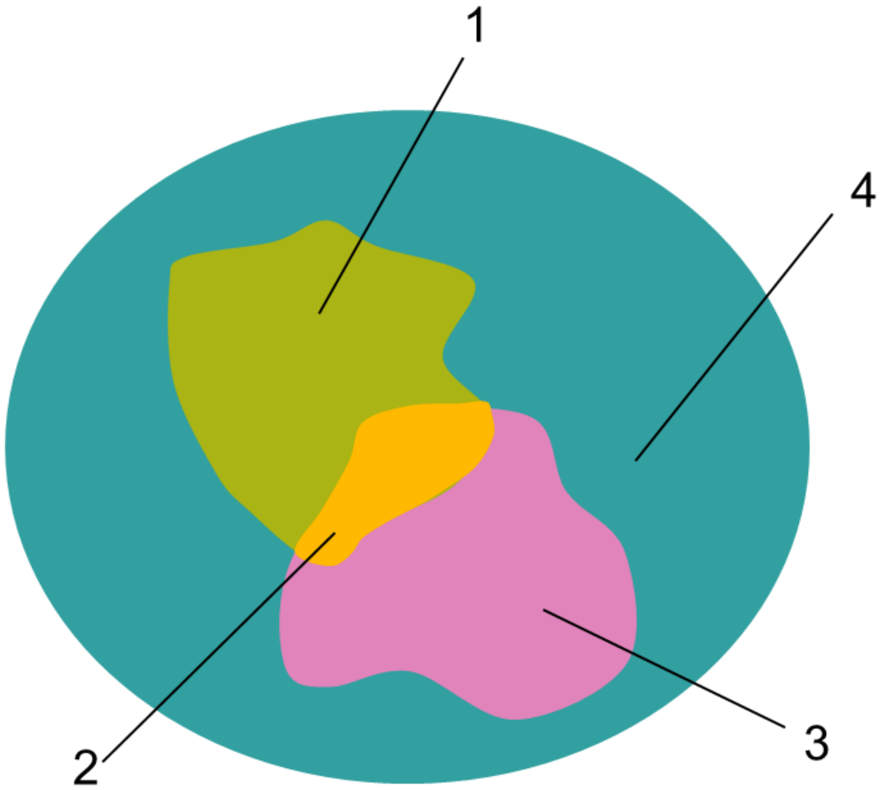
SOTIF: Scenario Space and Scenario Categories

SIEMENS
Ingenuity for life

- (Area 1) – Known safe scenarios
- (Area 2) – Known unsafe scenarios
- (Area 3) – Unknown unsafe scenarios
- (Area 4) – Unknown safe scenarios



Scenario space



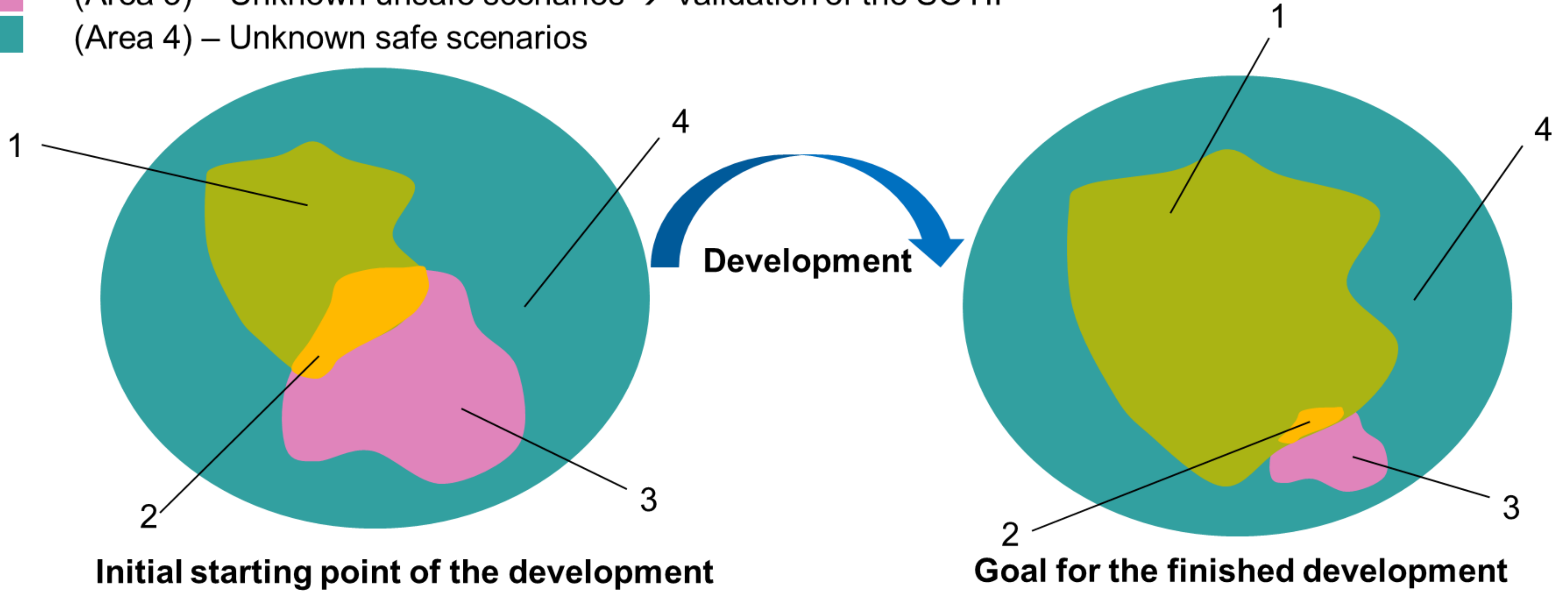
Scenario space

SOTIF - ISO PAS 21448

Evolution of Scenario Categories

SIEMENS
Ingenuity for life

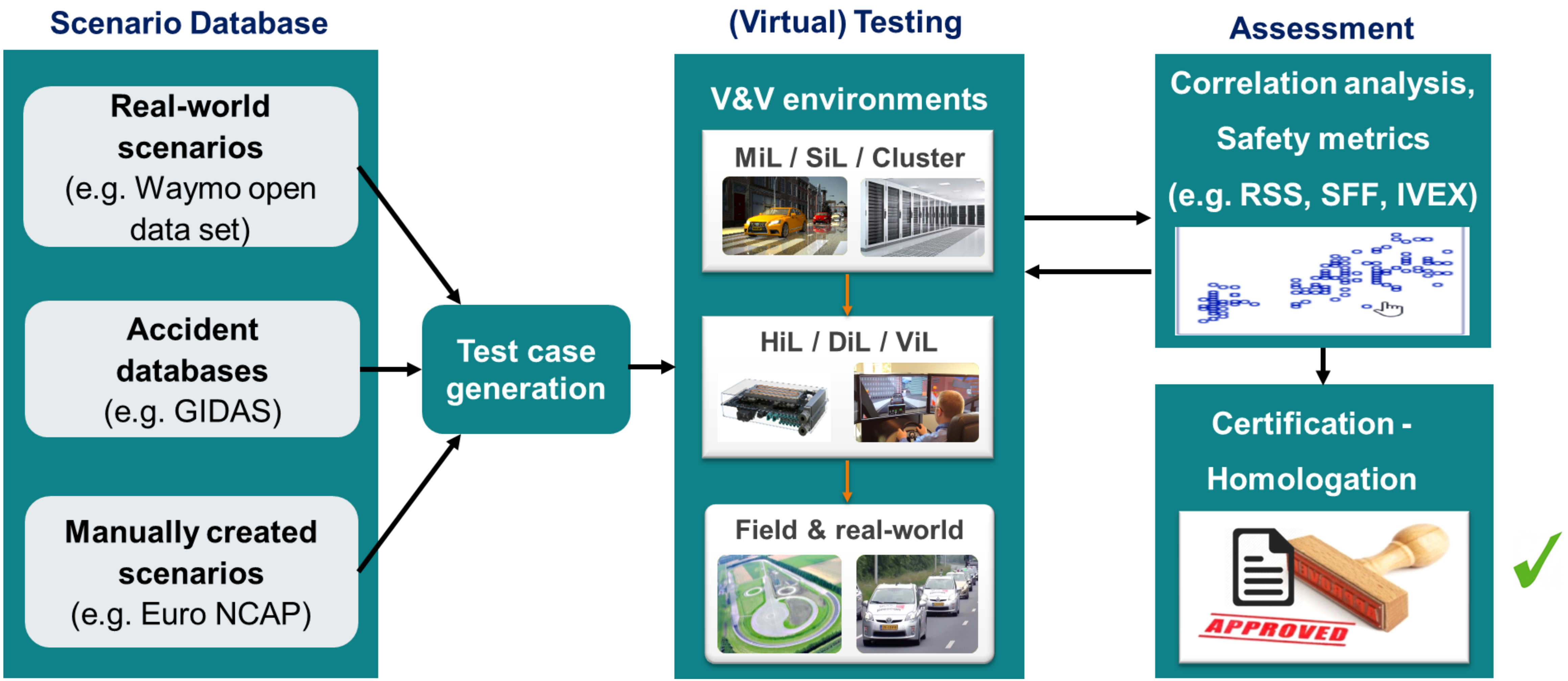
(Area 1) – Known safe scenarios
(Area 2) – Known unsafe scenarios → Verification of the SOTIF
(Area 3) – Unknown unsafe scenarios → Validation of the SOTIF
(Area 4) – Unknown safe scenarios



SOTIF - ISO PAS 21448

Verification and Valiation Framework

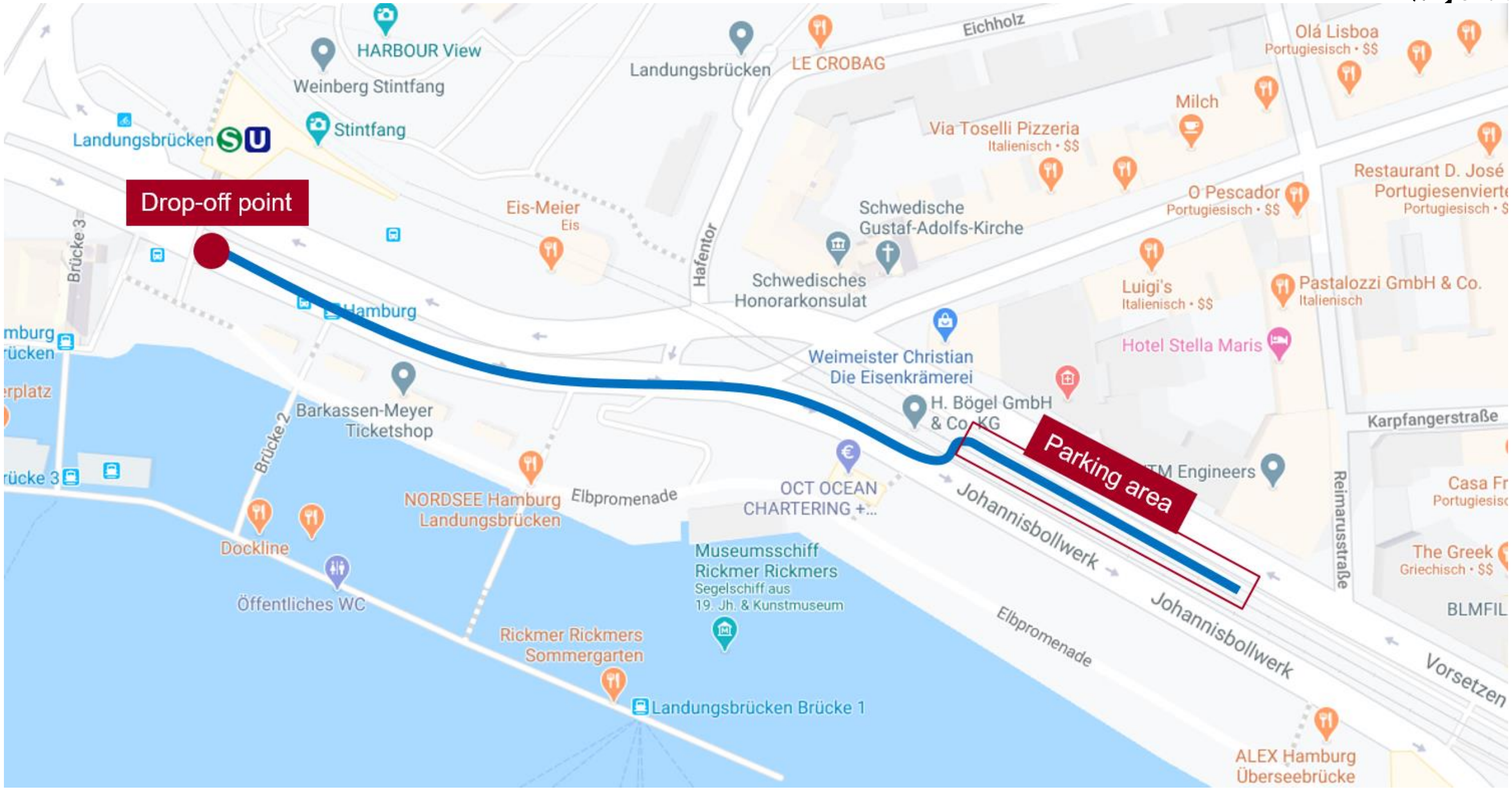
SIEMENS
Ingenuity for life



EIT Urban Mobility is supported by the EIT, a body of the European Union
eit Urban Mobility

Real-World Parking Area in Hamburg

SIEMENS
Ingenuity for life



UrbanSmartPark

EIT Urban Mobility is supported by the EIT, a body of the European Union

eit Urban Mobility

From Real-World to Virtual-World

SIEMENS
Ingenuity for life

Simcenter Prescan360

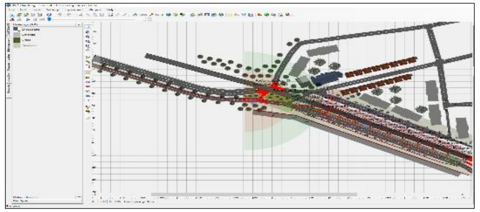
1 Real World into Database

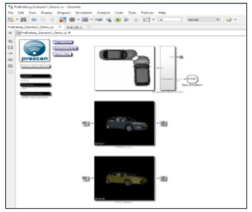
2 Import Static Env. into Simcenter Prescan

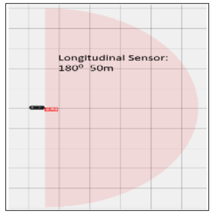
3 Insert EGO Vehicle + Controller + Sensors

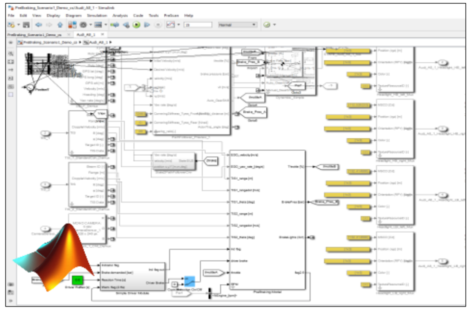
4 Run Scenario Variants Automate Tests

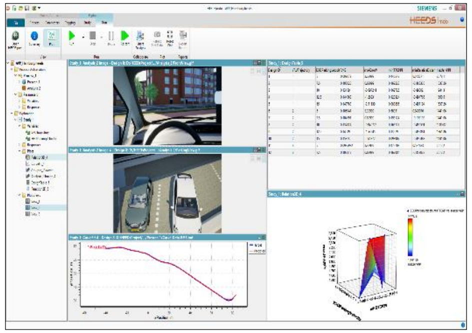
Open Street Map

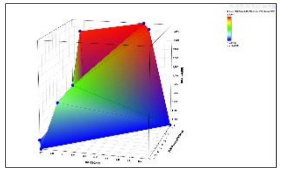


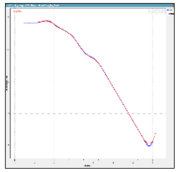












EIT Urban Mobility is supported by the EIT, a body of the European Union

eit Urban Mobility

Virtual Verification and Validation

Physics-based Simulation Platform – Simcenter Prescan

SIEMENS
Ingenuity for life

EIT Urban Mobility is supported by the EIT, a body of the European Union

Urban Mobility

AVP Field Tests – 2020, Helmond, The Netherlands

Presentation Outline

SIEMENS
Ingenuity for life

Automated driving systems - main challenges

Verification and validation of automated valet parking system

ISO 26262 perspective

Verification and validation of automated valet parking system

SOTIF perspective

Remarks, conclusions and discussions

EIT Urban Mobility is supported by the EIT, a body of the European Union

eit Urban Mobility

Remarks, Conclusions and Discussion

SIEMENS
Ingenuity for life

Siemens project goals:

- develop a unified framework/methodology for verification and validation of automated driving systems
- follow and demonstrate the validity of the V&V framework in case of automated valet parking system

Safety assurance of complex systems:

- if the operational environment is unknown operational safety is a very difficult (impossible) task
- verification and validation shall be performed at each level of the system
- there is no unified standard for certification of automated driving systems

EIT Urban Mobility is supported by the EIT, a body of the European Union

eit Urban Mobility

Thank you for your attention!

Contact Information

- **Alexandru Forrai, Ph.D.**
  Fellow Engineer & Consultant

- Business Development & RTD
  Simulation and Testing Solutions

- Siemens Digital Industry Software
- Automotive Campus 10
- 5708JZ Helmond, The Netherlands
- alexandru.forrai@siemens.com

EIT Urban Mobility is supported by the EIT, a body of the European Union