Quantitative SOTIF Analysis for highly automated Driving Systems

Conference Paper · November 2017

1 author:

Wilhard Wendorff
Mentor Graphics

AUTOMOTIVE INFOCOM MOBILITY, ENERGY & ENVIRONMENT AERONAUTICS SPACE DEFENCE & SECURITY

safetronic.2017
Functional Safety in Automotive

Quantitative SOTIF Analysis for highly automated Driving Systems

Dr. Wilhard von Wendorff, IABG - Center of Competence Safety

Stuttgart, November 8th, 2017

Contents

Contents

Different Aspects of Safety Functionality

Safety in use — Gebrauchs-Sicherheit

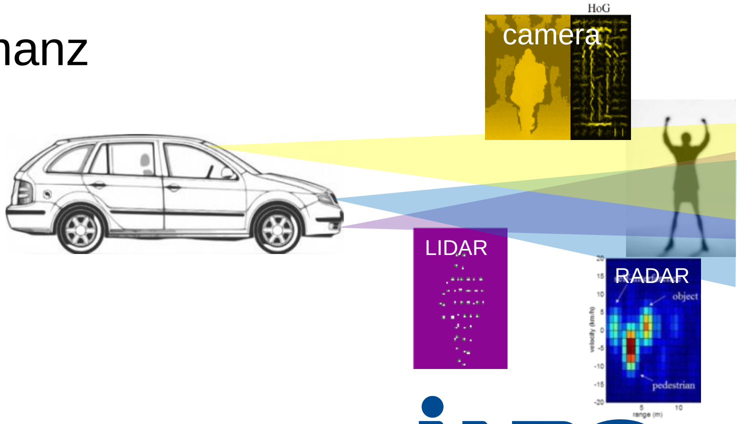
- preventing or reducing the risk of injuries resulting from the use of an electronic system

Functional Safety — Funktionale Sicherheit

- absence of unreasonable risk due to hazards caused by erroneous (random faults) parts
  - Is it safe when wearing out?

Functional Performance — Funktionale Performanz

- The ability of the system in case of absence of random faults to behave safe



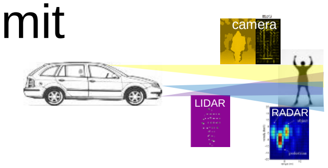
Some Examples regarding Aspects of Safety Functionality

Specified safety function (ISO 26262 functional safety goal)

- **Safe in Use**: User expects more than the specified function (foreseeable/not foreseeable (mis)use)
  e.g. highway assist is expected by driver to work on rural road

- **Functional Safety**: System integrator is not aware of a limit EE system (unknown limitations) systematic functional safety failure
  e.g. not specifying US traffic signs

- **Functional Performance**: System integrator is aware of system limit (accepted risk, specified limitation)
  e.g. Radar only detects object having absolute speed

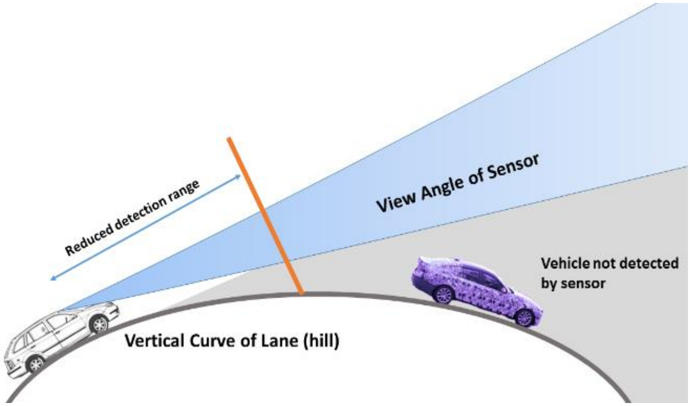


Contents

Goals of SotiF FMEDA

- SotiF FMEDA quantifies the Functional Performance of a system

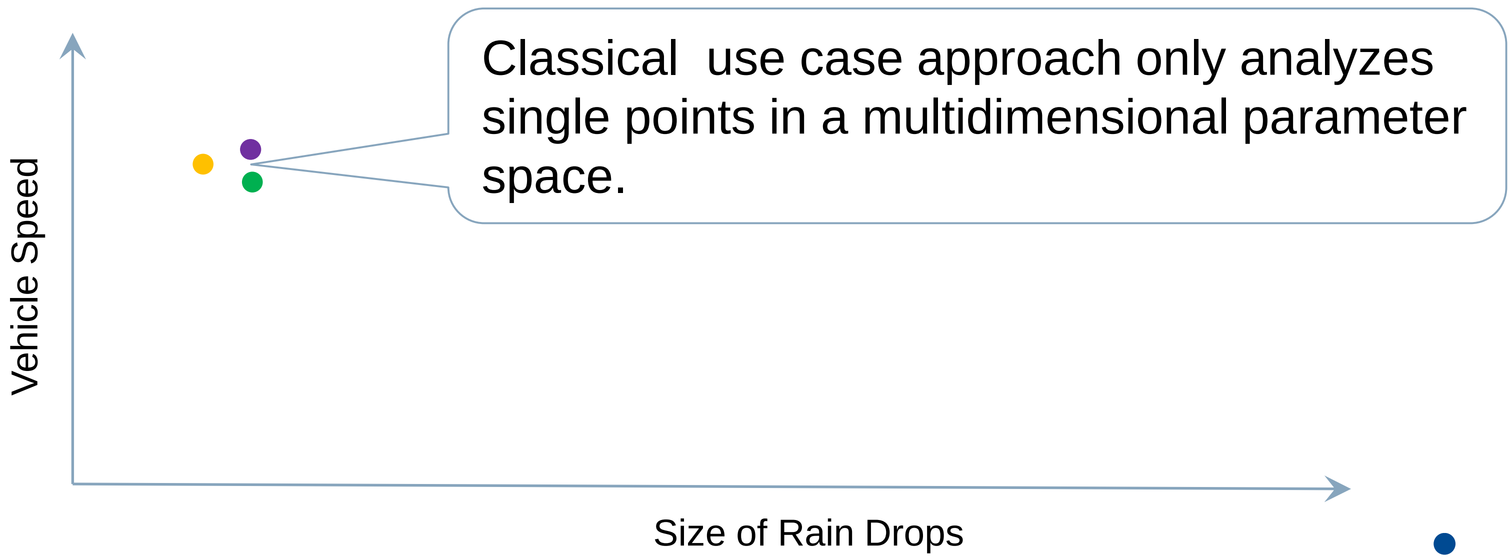
- Supports identifying Unknown Limitation



Contents

Use Case Approach

- Classical approach is to analyze complex problems is based on use cases (driving scenarios),
  e.g. driving while having fog in a tunnel and another car changes the lane…
- Figure assumes (clarification) only two physical parameters influencing safety of ADAS system.



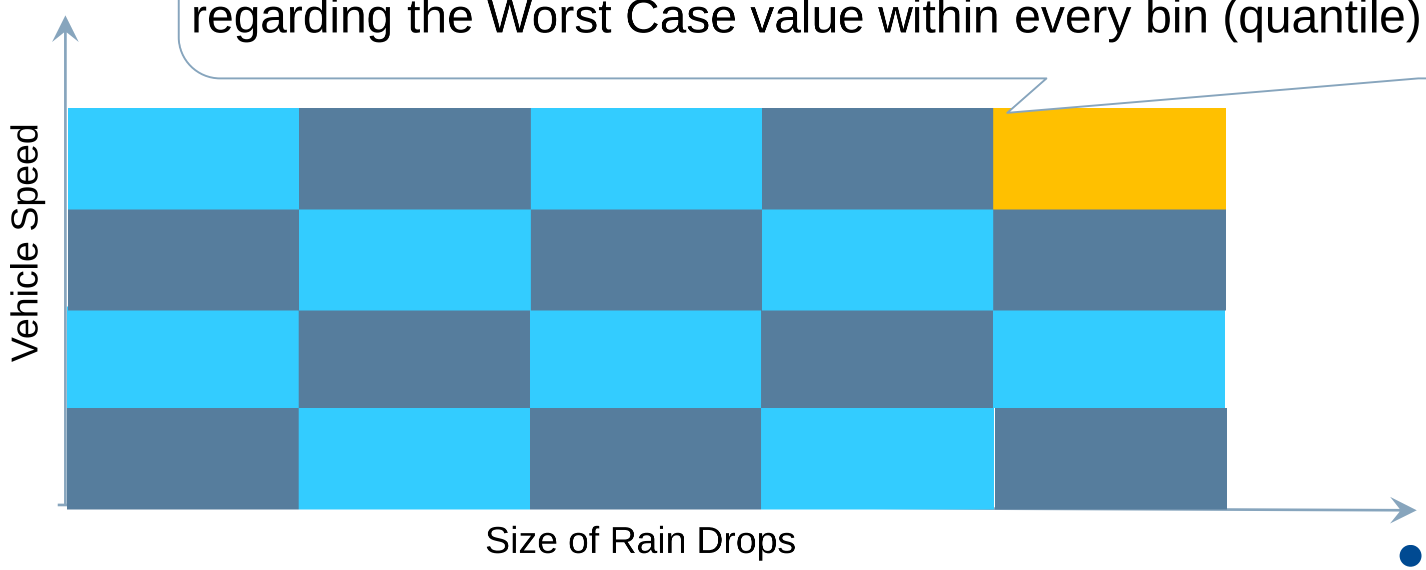
Issues with Use cases

- This approach base on engineering assumptions therefore is not systematic.
- Use cases may be all “nearby” instead being distributed over a large multidimensional data space“
- No evidence can be provided that chosen use cases are relevant

Space Segment Approach

- This approach uses physical parameters instead of driving scenarios, as the amount of physical parameters is limited, the driving scenarios not.
- Following figure assumes (clarification) only two physical parameters influencing safety of ADAS system.

SotiF FMEDA breaks the multidimensional parameter space into space segments (quantile) and determines the vehicle controllability regarding the Worst Case value within every bin (quantile).



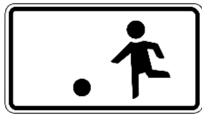
Contents

SotiF FMEDA Calculations (modelling)

For each space segment the SotiF FMEDA calculates:

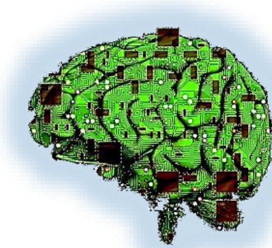
- Detecting capabilities of environmental conditions (**environment model**)
  (e.g. curve having small curve radius, road friction µ=0,3 due to ice)
  - ➢ Calculation of consequence by driving strategy, e.g. speed reduction

- Capabilities of obstacle detection (**obstacle model**)
  (e.g. detecting person / small RADAR cross section in a lane curve)
  - ➢ Calculation of detection distance regarding obstacle



- Detecting capability of vehicle state (**vehicle model**)
  (e.g. vehicle speed, centripetal forces, changing lanes)
  - ➢ Calculation of brake deceleration and crash velocity (severity)

- Reaction of driving system (**driving & reaction strategy**)
  (e.g. reducing driving speed, initiating lane change)
  - ➢ Implementing driving strategy



Examples of Physical Parameters

Environmental Model

- Dry Friction
- Curve Radius
- Vision Range
- RADAR Attenuation
- (vertical) Curves (hills)
- RADAR Interference
- Visual Backlighting

Obstacle Model

- Distance to Obstacle
- Relative Speed of obstacle
- Lane change of obstacle.
- Lane of obstacle
- Vision Cross Section.
- RADAR Cross Section

Vehicle Model

- Dry Friction
- Vehicle Speed
- Lane change of vehicle
- Curve Radius

Contents

SotiF FMEDA Results

The SotiF FMEDA calculates:

- The probability of an incident for each severity over life time of vehicle
- Possible targets values may be found in:
  COMMISSION DECISION of 16 December 2009 laying down guidelines for the management of the Community Rapid Information System ‘RAPEX’ established under Article 12 and of the notification procedure established under Article 11 of Directive 2001/95/EC (the General Product Safety Directive) (notified under document C(2009) 9843)

SotiF FMEDA Target Values

Risk level from the combination of the severity of injury and probability

Probability of damage during the foreseeable lifetime of the product		Severity of injury			
		1	2	3	4
High	> 50 %	H	S	S	S
	> 1/10	M	S	S	S
	> 1/100	M	S	S	S
	> 1/1 000	L	H	S	S
	> 1/10 000	L	M	H	S
	> 1/100 000	L	L	M	H
	> 1/1 000 000	L	L	L	M
Low	< 1/1 000 000	L	L	L	L

S — Serious Risk
H — High risk
M — Medium risk
L — Low risk

Contents

Examples I

- Current example analyses 959.040 combinations of parameters (scenarios).
- The Physical parameters and physical parameter distribution

Physical Parameters

Quantile Bins

Distribution of Quantile

Friction Tire to Road	(horizontal) Curve Radius of Lane	Visibility in visible and infrared light	Attenuation at 24/77GHz	Angle Vehicle to slope surface (vertical curve)	Longitudinal Speed of Vehicle (EGO speed)	Width of Obstacle
Friction µ: 0,3	lane radius: 100m	visibility 20m	RADAR attenuation 1,0dB/km -	0° slope angle	Vehicle longitudinal Speed: 0 - 30km/h	obstacle width: 0,3m
Friction µ: 0,5	lane radius: 200m	visibility 60m	RADAR attenuation 10,0dB/km -	3° slope angle	Vehicle longitudinal Speed: 30 - 60km/h	obstacle width: 0,5m
Friction µ: 0,7	lane radius: 400m	visibility 100m		6° slope angle	Vehicle longitudinal Speed: 60 - 90km/h	obstacle width: 2,0m
	lane radius: 1.200m	visibility 1.000m			Vehicle longitudinal Speed: 90 - 130km/h	obstacle width: 3,0m
						obstacle width: 4,0m
8%	1,16%	_1;1;2,72211203969778%_1;2;2,72211203969778%_1;3;0,427252167491747%	_3;4;100%	84,27229%	13,8%	1,128%
38%	3,17%	_1;1;18,6224097152064%_1;2;18,6224097152064%_1;3;2,92290133495925%	_3;1;100%_3;2;100%_3;3;100%	15,26215%	16,2%	4,509%
53%	15,61%	_1;1;78,6554782450959%_1;2;78,6554782450959%_1;3;12,3454593621533%		0,46556%	35,0%	68,573%
	80,07%	_1;3;84,3043871353957%			35,0%	5,481%
						20,309%

Examples II

- Pull-down menus configure features.

LIDAR providing vehicle speed
FALSCH
FALSCH
WAHR

- Look-up tables configure sensor capabilities (environmental model)

Probability not detecting a physical parameter	Short-Range RADAR	Long-Range RADAR	LIDAR	Omniview Cameras	Stereo Camera	Long Range Camera
Friction µ: 0,3	1	1	1	1	1	1
Friction µ: 0,5	1	1	1	1	1	1
Friction µ: 0,7	1	1	1	1	1	1
Vehicle longitudinal Speed: 0 - 30km/h	1	1	1E+0	1	1	1
Vehicle longitudinal Speed: 30 - 60km/h	1	1	1E+0	1	1	1
Vehicle longitudinal Speed: 60 - 90km/h	1	1	1E+0	1	1	1
Vehicle longitudinal Speed: 90 - 130km/h	1	1	1E+0	1	1	1
obstacle distance (longitudinal): 20m	2E-1	1	1E+0	4E-1	1E+0	1E-2
obstacle distance (longitudinal): 39m	2E-1	2E-1	1E+0	4E-1	1E+0	1E-2
obstacle distance (longitudinal): 59m	1E+0	2E-1	1E+0	4E-1	1E+0	1E-2
obstacle distance (longitudinal): 85m	1E+0	2E-1	1E+0	1E+0	1E+0	1E-2
obstacle distance (longitudinal): 200m	1E+0	2E-1	1E+0	1E+0	1E+0	1E-2
Obstacle relative longitudinal Speed: -130 — -90km/h	2E-1	2E-1	1E+0	1E-1	1E+0	1E-1
Obstacle relative longitudinal Speed: -90 — -60km/h	2E-1	2E-1	1E+0	1E-1	1E+0	1E-1
Obstacle relative longitudinal Speed: -60 — -30km/h	2E-1	2E-1	1E+0	1E-1	1E+0	1E-1
Obstacle relative longitudinal Speed: -30 — 0km/h	2E-1	2E-1	1E+0	1E-1	1E+0	1E-1

- Look-up tables enable configuration regarding degradation of sensor capabilities due to environmental conditions (obstacle model)

Table regarding obstacle detection failure rate				LIDAR	Omniview Cameras	Stereo Camera	Long Range Camera
obstacle width: 0,3m or Radar Cross Section: 5,0dB	visibility 20m or RADAR attenuation 1,0dB/km	20% RADAR Saturation or 10% Saturation (IR) or 20% Saturation (visible)	obstacle distance (longitudinal): 200m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 85m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 59m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 39m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 20m	1E+0	1E+0	1E+0	1E+0
		50% RADAR Saturation or 20% Saturation (IR) or 50% Saturation (visible)	obstacle distance (longitudinal): 200m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 85m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 59m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 39m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 20m	1E+0	1E+0	1E+0	1E+0
		80% RADAR Saturation or 80% Saturation (visible)	obstacle distance (longitudinal): 200m		1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 85m		1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 59m		1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 39m		1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 20m		1E+0	1E+0	1E+0
	visibility 60m or RADAR attenuation 10,0dB/km	20% RADAR Saturation or 10% Saturation (IR) or 20% Saturation (visible)	obstacle distance (longitudinal): 200m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 85m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 59m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 39m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 20m	1E+0	1E+0	1E+0	1E+0
		50% RADAR Saturation or 20% Saturation (IR) or 50% Saturation (visible)	obstacle distance (longitudinal): 200m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 85m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 59m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 39m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 20m	1E+0	1E+0	1E+0	1E+0
		80% RADAR Saturation or 80% Saturation (visible)	obstacle distance (longitudinal): 200m		1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 85m		1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 59m		1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 39m		1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 20m		1E+0	1E+0	1E+0
		20% RADAR Saturation or 10% Saturation (IR) or 20% Saturation (visible)	obstacle distance (longitudinal): 200m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 85m	1E+0	1E+0	1E+0	1E+0
			obstacle distance (longitudinal): 59m	1E+0	1E+0	1E+0	1E+0

Examples III

- Pull-down menus configure erroneous sensors (limb home evaluation)

Short-Range RADAR	Long-Range RADAR	LIDAR	Omniview Cameras	Stereo Camera	Long Range Camera	Unused0
6 Instantiations	1 Instantiations	0 Instantiations	4 Instantiations	0 Instantiations	1 Instantiations	0 Instantiations
6 Fault Free Instantiations	ult Free Instantiations	0 Fault Free Instantiations	4 Fault Free Instantiations	0 Fault Free Instantiations	1 Fault Free Instantiations	0 Fault Free Instantiations

0 Instantiations
1 Instantiations
2 Instantiations
3 Instantiations
4 Instantiations
5 Instantiations
6 Instantiations

- Look-up tables configure driving strategy (driving & reaction strategy)

Maximum Speed Strategy		0° slope angle						
		visibility 20m		visibility 60m		visibility 100m		visibility
		RADAR attenuation 1,0dB/km	RADAR attenuation 10,0dB/km	RADAR attenuation 1,0dB/km	RADAR attenuation 10,0dB/km	RADAR attenuation 1,0dB/km	RADAR attenuation 10,0dB/km	RADAR attenuation 1,0dB/km
Friction µ: 0,3	lane radius: 100m	0km/h	0km/h	0km/h	0km/h	0km/h	0km/h	0km/h
	lane radius: 200m	0km/h	0km/h	0km/h	0km/h	0km/h	0km/h	0km/h
	lane radius: 400m	0km/h	0km/h	0km/h	0km/h	0km/h	0km/h	0km/h
	lane radius: 1.200m	0km/h	0km/h	0km/h	0km/h	0km/h	0km/h	0km/h
Friction µ: 0,5	lane radius: 100m	60km/h	60km/h	60km/h	60km/h	60km/h	60km/h	60km/h
	lane radius: 200m	90km/h	90km/h	90km/h	90km/h	90km/h	90km/h	90km/h
	lane radius: 400m	130km/h	130km/h	130km/h	130km/h	130km/h	130km/h	130km/h
	lane radius: 1.200m	130km/h	130km/h	130km/h	130km/h	130km/h	130km/h	130km/h
Friction µ: 0,7	lane radius: 100m	90km/h	90km/h	90km/h	90km/h	90km/h	90km/h	90km/h
	lane radius: 200m	130km/h	130km/h	130km/h	130km/h	130km/h	130km/h	130km/h
	lane radius: 400m	130km/h	130km/h	130km/h	130km/h	130km/h	130km/h	130km/h
	lane radius: 1.200m	130km/h	130km/h	130km/h	130km/h	130km/h	130km/h	130km/h

- Look-up tables configure crash severity (obstacle model)

Crash Severity	Collision Velocity			
	passenger car↔Ego-vehicle	Truck↔Ego-vehicle	Motorcylce↔Ego-vehicle	Pedestrian↔Ego-vehicle
S1	≥ 20 km/h	≥ 15 km/h	≥ 10 km/h	≥ 5 km/h
S2	≥ 65 km/h	≥ 50 km/h	≥ 30 km/h	≥ 20 km/h
S3	≥ 75 km/h	≥ 60 km/h	≥ 50 km/h	≥ 40 km/h

	Probability			
	passenger car↔Ego-vehicle	Truck↔Ego-vehicle	Motorcylce↔Ego-vehicle	Pedestrian↔Ego-vehicle
obstacle width: 0,3m				100%
obstacle width: 0,5m			100%	
obstacle width: 2,0m	100%			
obstacle width: 3,0m		100%		
obstacle width: 4,0m	80%	11%	5%	4%

Examples IV

- Detailed analysis for every scenario:

Velocity distribution due to environmental model

Detection distribution due to obstacle mode

Severity distribution due to vehicle model

Probability of Safety Performance Flaws

Transversal Distance of Obstacle	Exposure	Probability for speed					Probability of obstacle detection						Probability for Crash Severity				Exposure for Crash Severity			
		0km/h	30km/h	60km/h	90km/h	130km/h	200,0m	84,5m	58,5m	39,0m	19,5m	0m	S0	S1	S2	S3	S0	S1	S2	S3
obstacle transversal distance: 0,0m	2E-8																2E-8		8E-22	
obstacle transversal distance: 3,6m	1E-10										1E+0	2E-6	1E+0		3E-14		1E-10		5E-24	
obstacle transversal distance: 7,1m	9E-11																9E-11		3E-24	
obstacle transversal distance: 0,0m	2E-10																2E-10		8E-24	
obstacle transversal distance: 3,6m	2E-12	1E+0	2E-8								1E+0	2E-6	1E+0		3E-14		2E-12		5E-26	
obstacle transversal distance: 7,1m	9E-13																9E-13		3E-26	
obstacle transversal distance: 0,0m	3E-9																3E-9		9E-23	
obstacle transversal distance: 3,6m	2E-11										1E+0	2E-6	1E+0		3E-14		2E-11		6E-25	
obstacle transversal distance: 7,1m	1E-11																1E-11		3E-25	

The table build-up is automated by script

Examples V

- Quantitative Results

Total Exposure:
100,0%
Dangerous Undetected Exposure S0
9,430E-02
Dangerous Undetected Exposure S1
2,166E-03
Dangerous Undetected Exposure S2
2,166E-03
Dangerous Undetected Exposure S3
2,058E-02
Number of Combinations (scenarios):
959.040

Summary

- A Methodology has been presented Quantifying the Safety Performance of Highly Automated Driving System
- The Methodology is based on an environmental model, an obstacle model, a vehicle model and a driving & reaction strategy
- This Methodology quantifies the entire multidimensional space into quantile (brute force method)
- The Methodology quantifies the probability not meeting safety performance
- The Tool Identifies Test Case for Driving Tests
- The Tool may be tailored to different analysis topics as it is built by scripts
- The Methodology is independent from Vendors (enables confirmation review)

Your contact

IABG mbH

Innovation Center Human Factors and Safety

Dr. Wilhard von Wendorff

Einsteinstrasse 20

85521 Ottobrunn

Germany

Phone +49 89 6088-2856

Fax +49 89 6088-13-2856

wendorff@iabg.de

www.iabg.de

Overview Business Area

Tests & Analyses

Overview Competence Center

Center of Competence Safety & Human Factors

Consulting and support

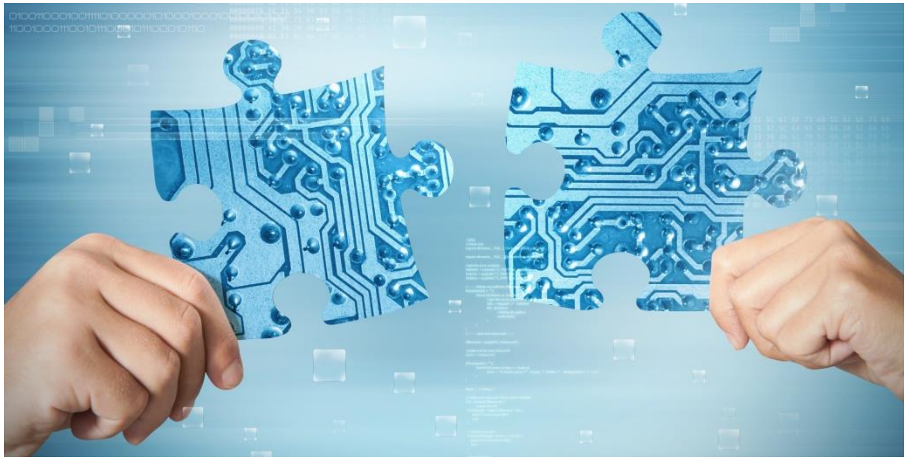
- Functional safety
- Safe in Use
- Mechanical, electronic & software safety aspects
- Human factors (Interaction humans and machines)

Services

- Process consulting
- Safety engineering
- Audits and assessments
- Partner for outsourcing development services
- Training / Safety academy

Expertise regarding industry standards

- Automotive: ISO 26262
- Defence: MIL-STD-882, IEC EN 61508
- Aeronautics: RTCA/DO-178, RTCA/DO-254
- Railway: EN 50128/9



IABG