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

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

**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”
### Safety in Different Industry Sectors

<table>
<thead>
<tr>
<th>System complexity</th>
<th>Pick and place robot</th>
<th>Chemical plant</th>
<th>Elevators</th>
<th>Airplane</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mid-complexity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High-complexity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mid-complexity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High-complexity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Safe state (in case of malfunction)

<table>
<thead>
<tr>
<th>Safe state</th>
<th>Pick and place robot</th>
<th>Chemical plant</th>
<th>Elevators</th>
<th>Airplane</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sudden stop</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safe stop within $\Delta T$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stop nearest floor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Land nearest airport</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Operational environment

<table>
<thead>
<tr>
<th>Environment</th>
<th>Pick and place robot</th>
<th>Chemical plant</th>
<th>Elevators</th>
<th>Airplane</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known &amp; Defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Known &amp; Controlled</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Known &amp; Defined</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown-Predicted</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## System and Operational Environment

<table>
<thead>
<tr>
<th>Operational environment</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known</td>
<td>Simple: ✓</td>
</tr>
<tr>
<td></td>
<td>Complex: ✓</td>
</tr>
<tr>
<td>Unknown</td>
<td></td>
</tr>
</tbody>
</table>

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

*Operational env. shall be known/monitored/predicted – otherwise operational safety cannot be assured.*
Automated Driving System

Goal

Sense
Perception

Plan
Decision/Control

Execute
Actuation

System
under control

Noise

Disturbances
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.
Automated driving systems - main challenges

**Verification and validation of automated valet parking system**

- ISO 26262 perspective

- SOTIF perspective

Remarks, conclusions and discussions
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:

2\textsuperscript{nd} 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 = Severity * Probability of Exposure = S * E

Residual risk = Severity * Probability of Exposure * (1-Controllability) = S * E * (1- C)

Remark: it is required to minimize the risk at least to the accepted (tolerable) risk.
The absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E systems

Systematic failures
(Bugs in S/W, H/W design and Tools)

Random H/W failures
(permanent faults, transient faults occurring while using the system)

Functional Safety Standards used in different industry sectors

IEC 61800-3
Electr. Drives

IEC 61513
Nuclear Sector

IEC 61511
Process Sector

IEC 61508

EN 50128
Railway applications

IEC 50156
Furnaces

ISO 62061
Machinery

ISO 26262
Automotive

.....etc.
Systematic Failures (SW, Process, Tools)

Failures distribution during development & deployment

- Specification: 44%
- Design & Implementation: 15%
- Installation & Setting into operation: 20%
- Operation and Maintenance: 15%
- Modification after setting into operation: 6%

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.
How to assure safety? Safety by design, which means how we Define → Design → Develop → Deploy.
Random (Hardware) Failures

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)

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

- **Sense Perception**
- **Plan Decision/Control**
- **Execute Actuation**

**Goal**

- **System under control**

**Noise**

**Disturbances**

- **Goal**

Siemens
Ingenuity for life
Verification and Validation Process

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
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

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

SOTIF - ISO PAS 21448
Evolution of Scenario Categories

(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

Development

Initial starting point of the development

Goal for the finished development

SOTIF - ISO PAS 21448
Verification and Validation Framework

**Scenario Database**
- Real-world scenarios (e.g. Waymo open data set)
- Accident databases (e.g. GIDAS)
- Manually created scenarios (e.g. Euro NCAP)

**Test case generation**

**(Virtual) Testing**
- V&V environments
  - MiL / SiL / Cluster
  - HiL / DiL / ViL
  - Field & real-world

**Assessment**
- Correlation analysis, Safety metrics (e.g. RSS, SFF, IVEX)
- Certification - Homologation

**UrbanSmartPark**

16-Dec-2020 | USP Event | 24

EIT Urban Mobility is supported by the EIT, a body of the European Union
Real-World Parking Area in Hamburg
From Real-World to Virtual-World

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

Simcenter Prescan360
Physics-based Simulation Platform – Simcenter Prescan
AVP Field Tests – 2020, Helmond, The Netherlands
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
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
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