Overcoming the safety and security barriers to autonomous vehicle deployment

Mike Bartley
Founder and CEO, Test and Verification Solutions

AESIN Conference

October, 2nd, 2018
Agenda

- Objectives
- Overview of the simulation environment
- Scenarios – safety and security
- Simulation
- Test bench
Objectives

• To build passenger, regulatory and market trust in autonomous pods as a practical, safe and affordable way to travel.

• Capri is a £4.2 million pilot project that includes the design, development and testing of connected and autonomous pods, culminating in on-road public trials at London’s Queen Elizabeth Olympic Park.

• Reducing the barriers to market for a commercial autonomous pod service by:
  • Devising a procedure to certify the operational safety of autonomous pods
  • Assessing the infrastructure requirements for deployment
  • Addressing the legal and regulatory barriers to commercial use
  • Co-designing a service blueprint with real user input
  • Preparing a business case to support investment decisions

• Technical: Safety, Verification, Validation & Road Simulation
  • Develop a framework for Safety and Security Testing of Connected and Autonomous Vehicles
An overview of the simulation environment

Security Scenarios

Simulation

POD

Test Bench

Fleet Instructions

Test Outputs & Analytics

API

API
Real world evidence base

Grounded in reality – quantifying the premise that AV’s should be at least as ‘good’ as a human driver

Accidentology identifies situations where human drivers make errors (94% of collisions)

Accidentology approach is more transparent and justifiable than a purely taxonomic approach leading to greater user confidence
Identifying relevant scenarios

Application of general design principles - British Design Council Double Diamond

Defining the vehicle operating envelope through

- Specific conditions under which the AV is intended to operate (e.g. Road way type, geographic areas, speed range, environmental conditions)
- Vehicle functional specification

Identify the defined operating envelope within the accident data

Any scenario that ‘fits’ within the envelope is relevant
Pod example envelope definition

There is no pre-existing accident data for AVs e.g. pods

Identify accidents that occur within an anticipated “pod-like envelope” based upon knowledge of the pod operating conditions but drawn from human driven vehicles

These form the scenario specifications for virtual testing
Identifying the Relevant Attack Surfaces and Threats

The need to have a *reference architecture* that can cover the CAV systems comprehensively

Identify the attack surfaces of a specific cyber-physical CAV system or application through the general reference architecture

Specify the relevant threats in each attack surface
Testing and Validation: Flexibility Based on Available Testing Resources

Three levels of testing:
- Theoretical analysis
- Simulation
- Trial

When a threat has high requirements for testing: it will be more difficult to test, however, it will also be less likely to happen in real life (require more attack potential)

Public trial vs private trial
- Closer to reality but may have safety impact

Proprietary testing issue
- Cooperation via fuzzing test

Example of a typical testing plan and management
Dynamic Risk Consideration: Environment and System State

No vehicle operate without environments: CAV risk assessment needs to take environments into account because of their impacts on attack and defense potential as well as motivations.

- Environment risks can either reinforce or reduce vehicle risks.

Risk considerations when there are links between attack surfaces: vulnerabilities in one surface may open the chances for attacking other surfaces.

- Consequence: System’s security states affect significantly on risk assessment.

How to manage the dynamic risk assessment procedure effectively:

- Maintain risk profiles of environments and system states

![Diagram](attachment:diagram.png)
Cloud Security Objective

The Capri POD is connected to an Internet based Fleet Management Systems.

If the Fleet Management Systems is compromised, could an attacker affect the safety of the POD?

Area of Focus: Assume Cloud is compromised – what is the impact a Threat Actor could have?
Protecting the Cloud Elements: Risk Assessment

- Threat Model
  - Derived from NCC Group Automotive threat model
- Applied STRIDE risk model
- Recommended mitigations
  - Known “Cyber Security” science
  - Nothing “Special” for CAV
Cloud Security: Next Steps

Work with partners to implement appropriate security in the Cloud environment.
Feed risk assessment into overall Dynamic Risk Assessment model WMG are working on
Develop use cases for simulation, on the assumption the Cloud is compromised and the attacker can take full control of communications to the POD

- What happens when STOP signal is sent?
- What happens when STOP signal is sent *at a time when it would leave the POD in a dangerous position*
  - E.g., middle of a busy intersection
Aimsun Next

- Aimsun Next
  - Mobility Modelling Laboratory.
  - In use Worldwide for:
    - Transport Planning and Assessment
    - Operational Modelling
    - Predictive ITS
  - Models the interactions between vehicles and pedestrians.
  - Calibrated and validated vehicle behaviour algorithms.
  - Extensible, via API, to include alternative form of vehicle control.
Control of EGO Vehicle

- **Timestep**
  - Report positions of nearby actors
  - Evaluate simulated actor actions
  - Update all actor positions
  - Time $T = T+1$

- **Evaluating EGO vehicle action**

Aimsun, Simulation

Actors = vehicles, bikes, pedestrians...
Experiment and Scenario Environment

- In each Experiment
  - Modify the Map
  - Trees
  - Buildings

- In each Scenario
  - Modify the Scenery
  - Parked cars
  - Traffic management and works
  - Modify the Actors
  - Vehicle presence
  - Relative positions
  - Behaviour and reactions
**Testbench**

- **Objectives**
  - Codify corner cases from accidentology & security, measure coverage
  - Automate checking for correctness
  - Control simulation and communications with POD

- **Concerns**
  - Fidelity
  - Hitting corner cases
  - Pass/fail automation

- **Solution**
  - Correlation with real world trials
  - Constrained random test generation
  - Intelligent, model-based test generation (e.g. agent-based or formal methods-based) for corner cases
  - Assertions and functional coverage

---

**T&VS, Testbench**

```
<table>
<thead>
<tr>
<th>Data structure</th>
<th>Layout/Sceneries</th>
<th>Navigator &amp; other algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenery/Scenario configuration module</td>
<td></td>
<td>Results Checker Coverage</td>
</tr>
<tr>
<td>Constraint Randomizer</td>
<td></td>
<td>Log</td>
</tr>
<tr>
<td>Cloud security</td>
<td>VBI</td>
<td></td>
</tr>
<tr>
<td>Decision making software (Fusion)</td>
<td></td>
<td>TVS Interface Lib (client socket)</td>
</tr>
<tr>
<td>Capri Simulator (Aimsun)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

- **Safety Scenario** (parameters, ranges, layout etc.)
- **Cloud security data**
- **Server Socket**

---

**Objectives**
- Codify corner cases from accidentology & security, measure coverage
- Automate checking for correctness
- Control simulation and communications with POD

**Concerns**
- Fidelity
- Hitting corner cases
- Pass/fail automation

**Solution**
- Correlation with real world trials
- Constrained random test generation
- Intelligent, model-based test generation (e.g. agent-based or formal methods-based) for corner cases
- Assertions and functional coverage
Testbench Summary

- We can achieve the following
  - A larger range of scenarios
  - More easily hit the corner cases and know when we have hit them
  - Have higher levels of control over the testing environment
  - Easily repeat tests
- The solution is focused on
  - Constrained-random stimulus
  - Well-defined APIs
- We are investigating the following concerns
  - Fidelity through qualification on real trials
  - Coverage of corner cases through model-based test generation
  - Pass/fail through assertions
- Sign off with regulatory organisations will be further investigated
- Reuse on other projects: Robopilot
  - bring autonomous racing technology to the light commercial vehicle market and demonstrate SAE level 4 autonomy
Status of WP4

- The accident data was analysed to generate the possible use cases and safety critical scenarios
- POD test scenarios & performance requirements defined
- Identified the Initial set of parameters for the simulation
- Developing the core test framework
  - Data structure like vehicle classes, road geometry, obstacles, speed, time, coordinate, dimensions
  - Enumeration for road type, junction type, obstacles etc.
  - Interprocess communication - socket
  - Test engine to constraint randomize the parameter value
- Defined how to protect POD systems based on an analysis of the threats and risk assessment with respect to cyber and cloud security
- The required information was gathered with respect to the Capri Architecture to support the POD trails, including
  - POD to cloud communications
  - Fleet management system
To do

- Develop the final scenario methodology in context of simulation and testing
- Integration of simulator and POD decision-making software with the test bench
- Develop a comprehensive framework for testing all possible scenarios for the various parameter ranges
- Develop use cases for simulation from a cloud perspective
- Compare data from the trial with results from the virtual test environment (test bench qualification)
- Design security countermeasures based on the security analysis for cyber and cloud system
- Generate the V&V report which will include coverage and test results
- Regulatory requirements for PODs
Contributors

Mike Bartley and Rajesh, T&VS
Mark Brackstone and Pete Sykes, Aimsun Ltd.
Tuan Le, Ivan Ivanov and Carsten Maple, WMG Warwick
Colin Robbins, Nexor
Kerstin Eder, University of Bristol and Bristol Robotics Laboratory
Laurie Brown and Steven Reed, Loughborough University
Pete Thomas, Ruth Welsh, Loughborough University, UK
For more information about Capri please go to http://caprimobility.com/
For more information on WG4 please contact Mike Bartley
  mike@testandverification.com
  07796 307958

Thank you