Overcoming the safety and security barriers to autonomous vehicle deployment

Colin Robbins. Principal Security Consultant, Nexor

Prof Carsten Marple. Professor of Cyber Systems Engineering, WMG

Contributors:

- Mike Bartley, T&VS
- Rajesh, T&VS
- Mark Brackstone, Aimsun.
- Pete Sykes, Aimsun.
- Tuan Le, WMG
- Ivan Ivanov, WMG
- Bristol Robotics Laboratory
- Loughborough University

IoT SF Conference, London.

December 4th, 2018

Capri Consortium

£4.2 million of funding from:

- Innovate UK
- Centre for Connected & Autonomous Vehicles
- Industry

Pilot scheme that could pave the way for the use of connected and autonomous vehicles to move people around airports, hospitals, business parks, shopping and tourist centres.

Capri

Capri Vision

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

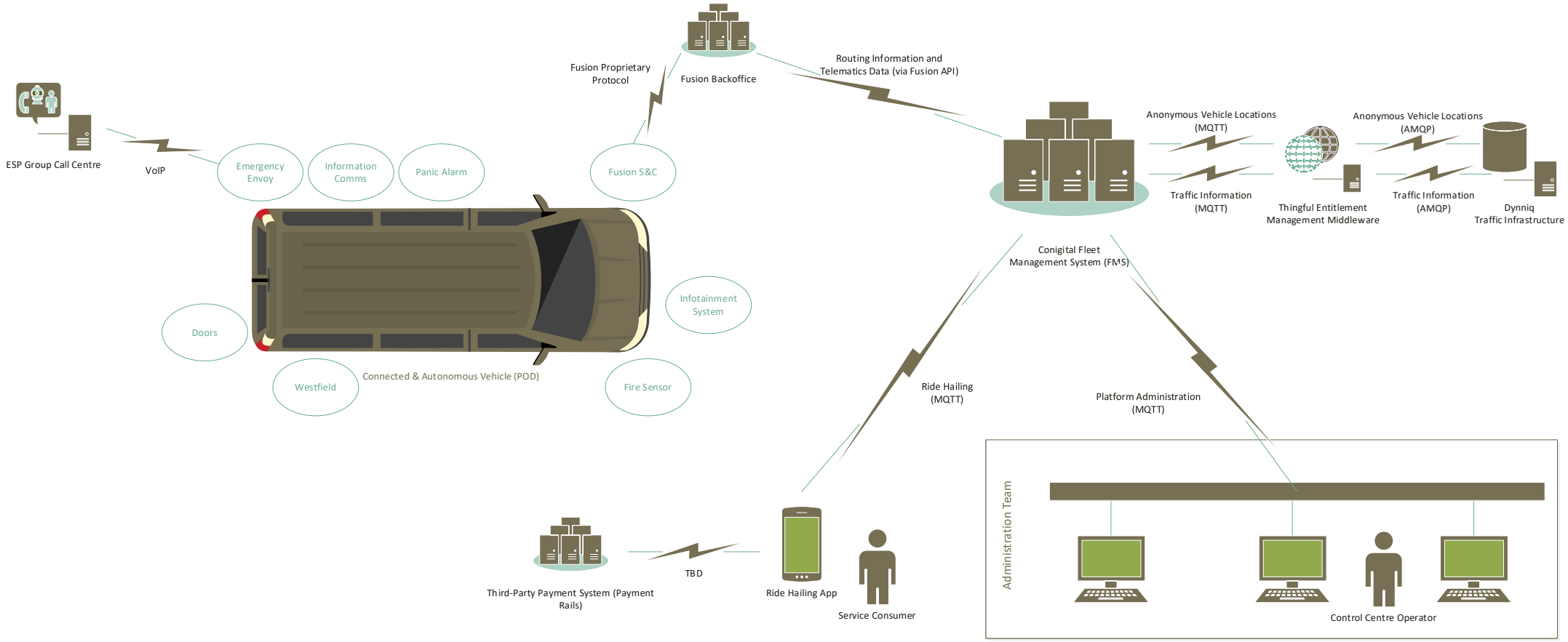
Reducing the barriers to market for a commercial autonomous pod service by:

- 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

This presentation focuses on Cyber Security and how it could impact operational safety.

Capri Architecture

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

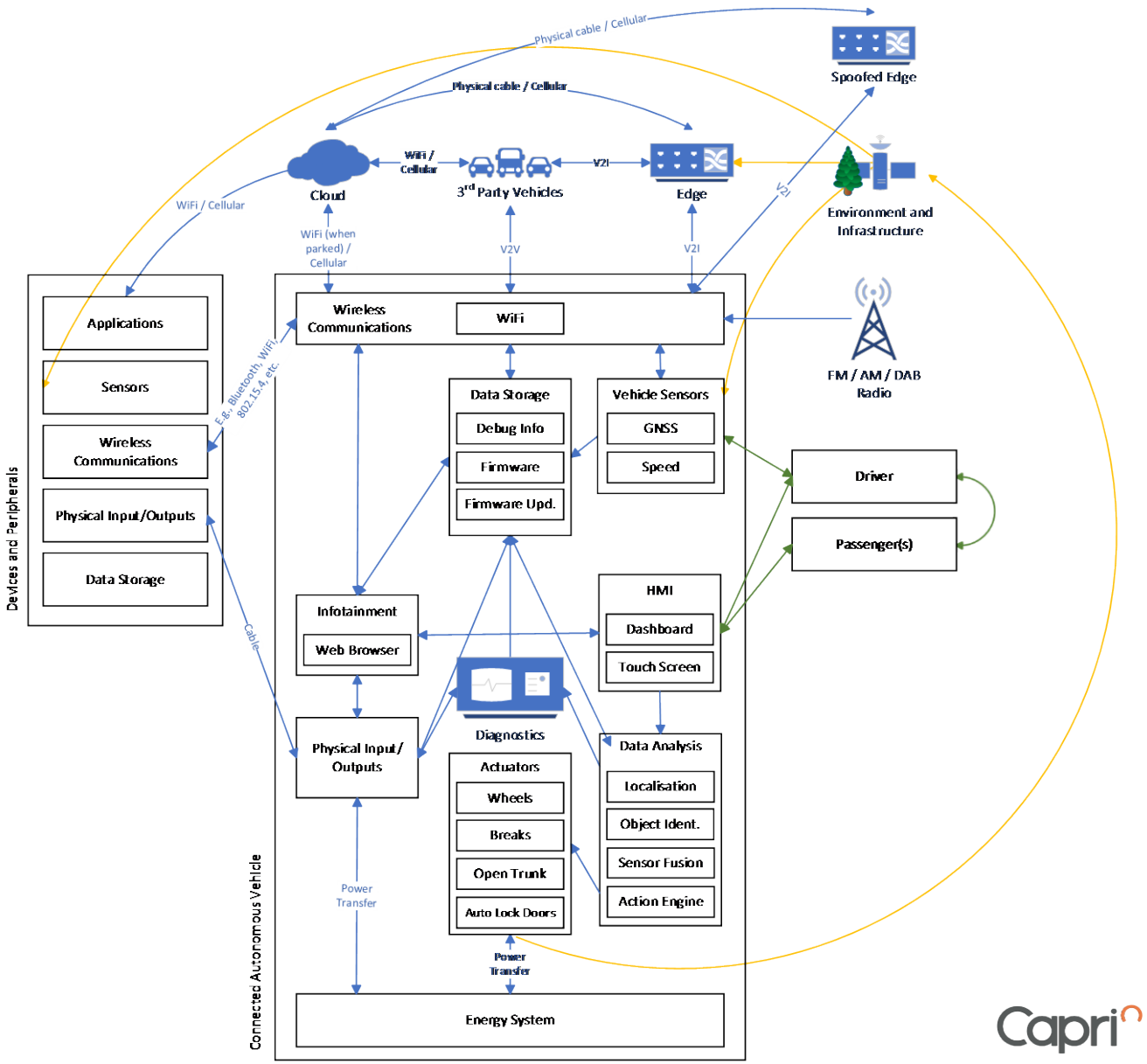


NEXOR

Capri

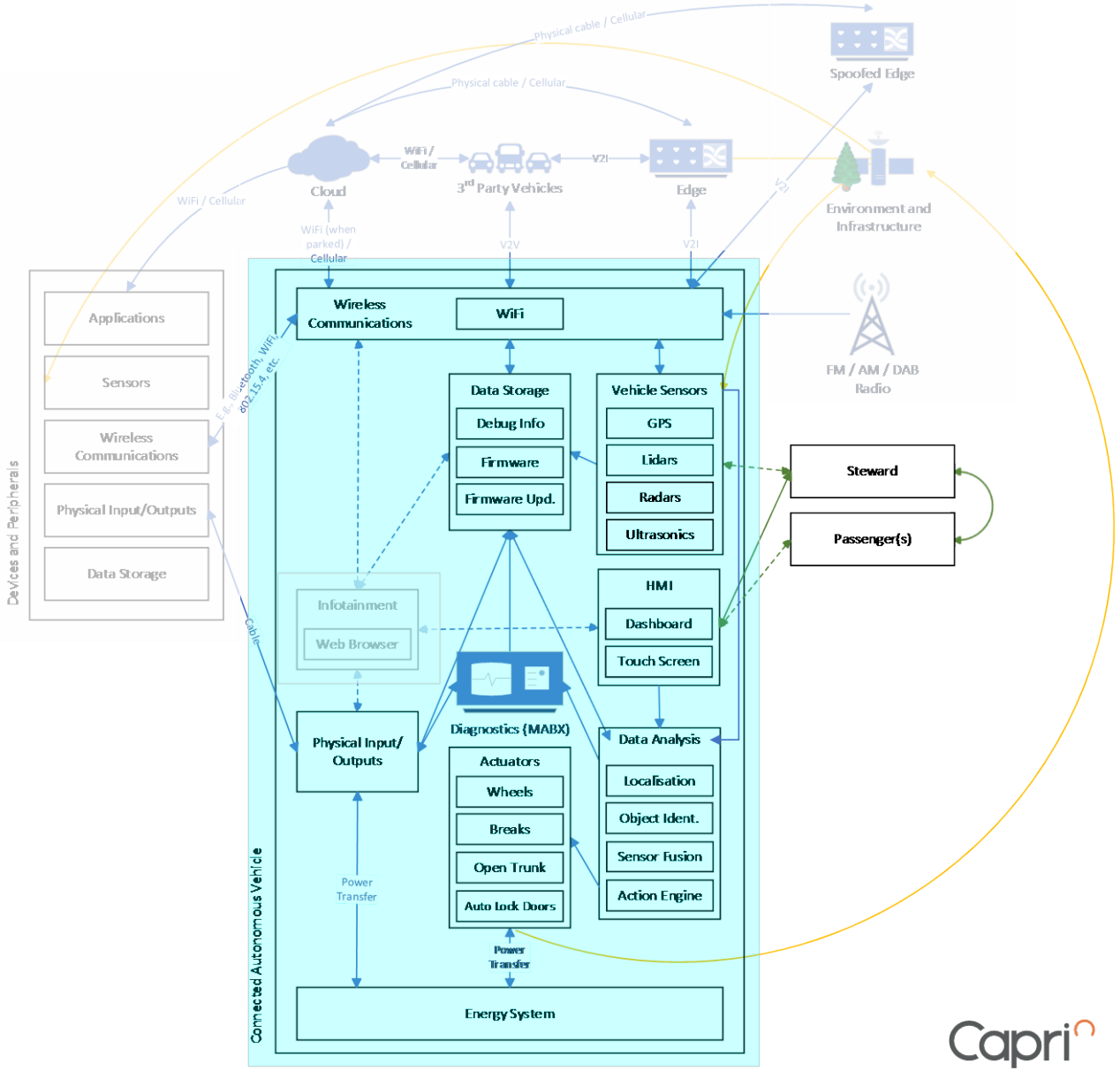
Cyber Security: CAV Reference Architecture

- A general CAV reference architecture that can understand CAV components, their functionalities and technologies in operation
- Identify the attack surfaces (potential threats) for components, functionalities, and technologies
- Shaping the focus of testing and validations through identifying most relevant threat agents and their goals



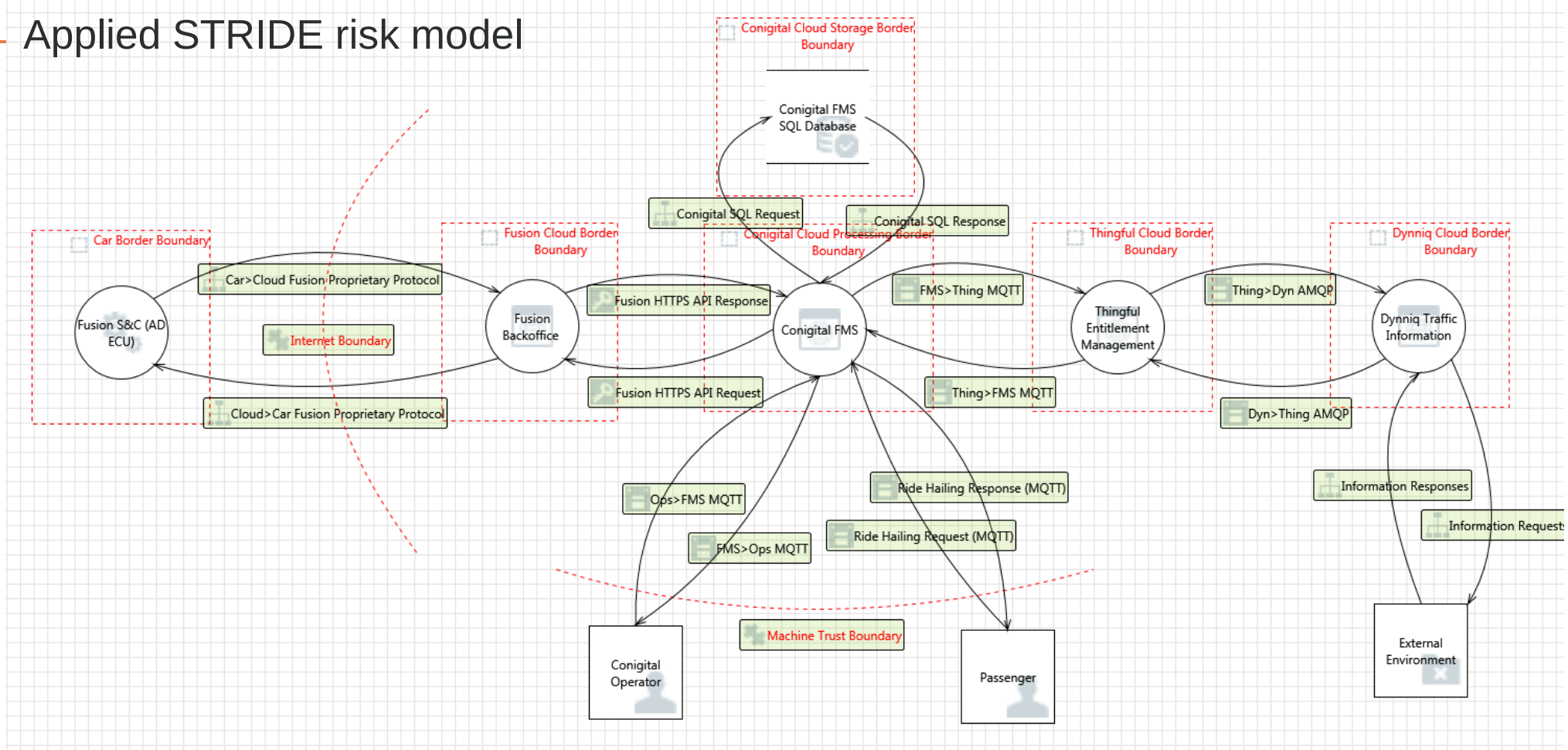
CAPRI Internal POD Architecture

- Remove irrelevant components and functions (POD has no Infotainment; having a steward instead of the driver for safety control only)
- Elaborating components and functions (adding Lidars, Radars and Ultrasonic sensors)
- Main threat agents: organised crime, hacktivists, transport infrastructure attackers, mischief makers



Cyber Security: Threat Modeling – Cloud

- Threat Model: Derived from NCC Group Automotive threat model
- Applied STRIDE risk model



NEXOR

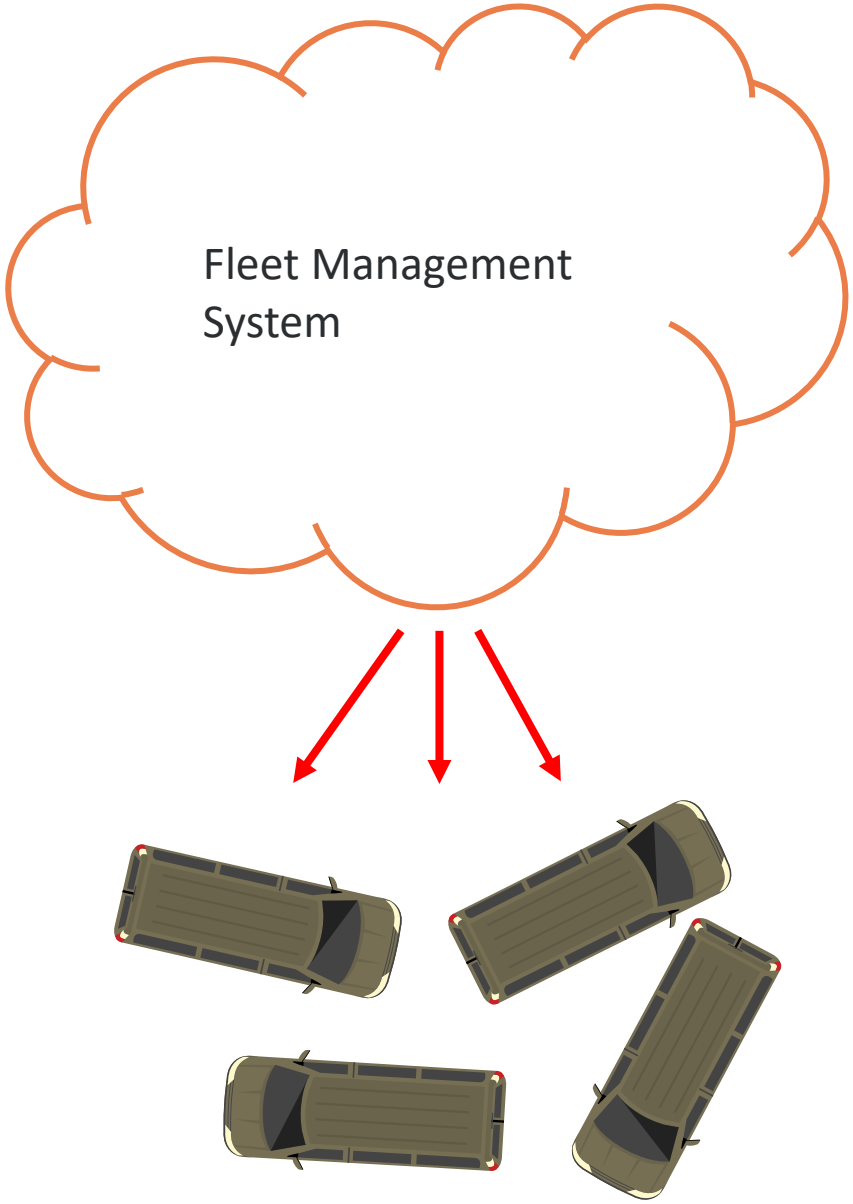
Capri

Cloud Security Scenario

Assume Fleet Management Systems is compromised…

- What happens when STOP signal is sent?
- What happens if STOP signal is sent at a time when it would leave the POD in a dangerous position?
  - E.g., middle of a busy intersection
- Can you send all PODs to the same point, then tell them to stop?
  - Denial or Service

Capri approach: Simulation



NEXOR

Capri

Testing & Validation: Developing Knowledge of Attack and Defence Potential

For each attack, testing and validation should investigate the following essential knowledge:

- Attack potential: minimum requirements for the attack to be successful: Elapsed time, expertise, knowledge, opportunity, equipment
- Defence potential: available controls and their effectiveness
- High probability threat agents and their relevant goals to initiate that attack

Three levels of testing:

- Theoretical analysis
- Simulation
- Trial
- → Balance between testing resource and requirements

Trial testing issues:

- Public trial vs private trial: Closer to reality but may have safety impact
- Proprietary testing issue: Cooperation via fuzzing test

Attack surface	Threat modelling: STRIDE					
	Spoofing	Tampering	Repudiation	Information disclosure	DoS	Elevation of Privilege
Camera	M3	M2	M2	M3	M3	N/A
GPS	M3	M2	M2	M3	M3	N/A
Radar	M3	M1	M1	M1	M3	N/A
Lidar	M3	M1	M1	M1	M3	N/A
Blindspot sensors	M3	M1	M1	M1	M3	N/A
Ultrasound sensors	M3	M1	M1	M1	M3	N/A
Decision making system	M3	M2	M2	M3	M3	N/A
Curtis controller	M3	M2	M2	M3	M3	N/A
MABX	M3	M2	M2	M3	M3	N/A
Digital Concentrator Measurement Unit	M3	M2	M2	M3	M3	N/A
Cradle point	M3	M2	M2	M3	M3	N/A
Tire sensors	M3	M2	M2	M3	M3	N/A
		M1: Analyis		Completed		
		M2: Simulation		In Progress		
		M3: Trial		Planning		
				Not Applicable		

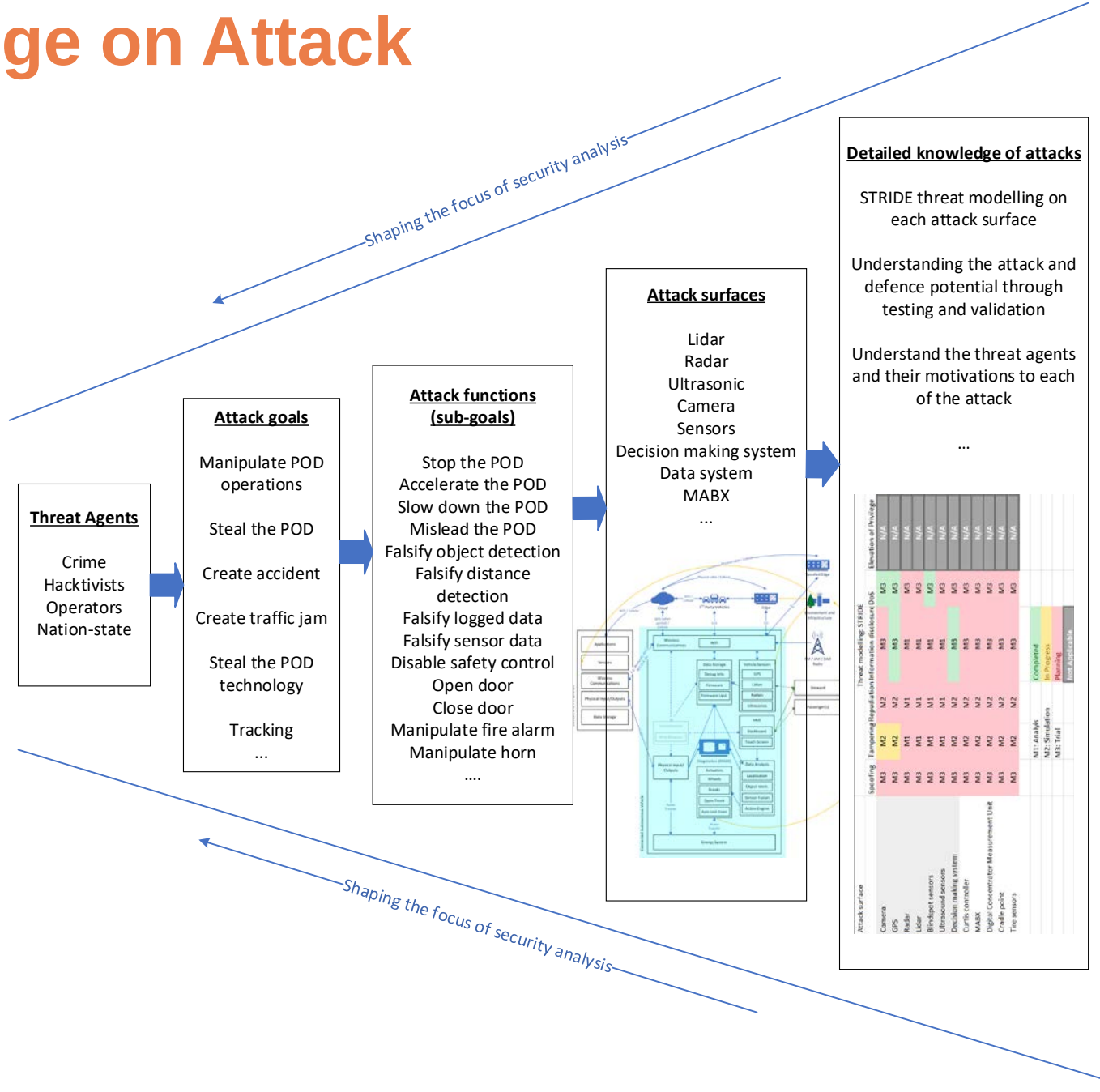
Example of a typical testing plan and management

Manage the Knowledge on Attack

Issue of large and expanding attack surfaces

- Analysing all the attacks is infeasible
- Attack tree to shape the focus of security analysis
- Attacks come from several threat agents, aiming at specific functions and surfaces

→ Identifying the most likely threat agents and goals to reduce the set of attacks to analyse



WMG THE UNIVERSITY OF WARWICK

Capri

Dynamic Risk Consideration: Environment and System State

Environment risks can either reinforce or reduce vehicle risks, because they have:

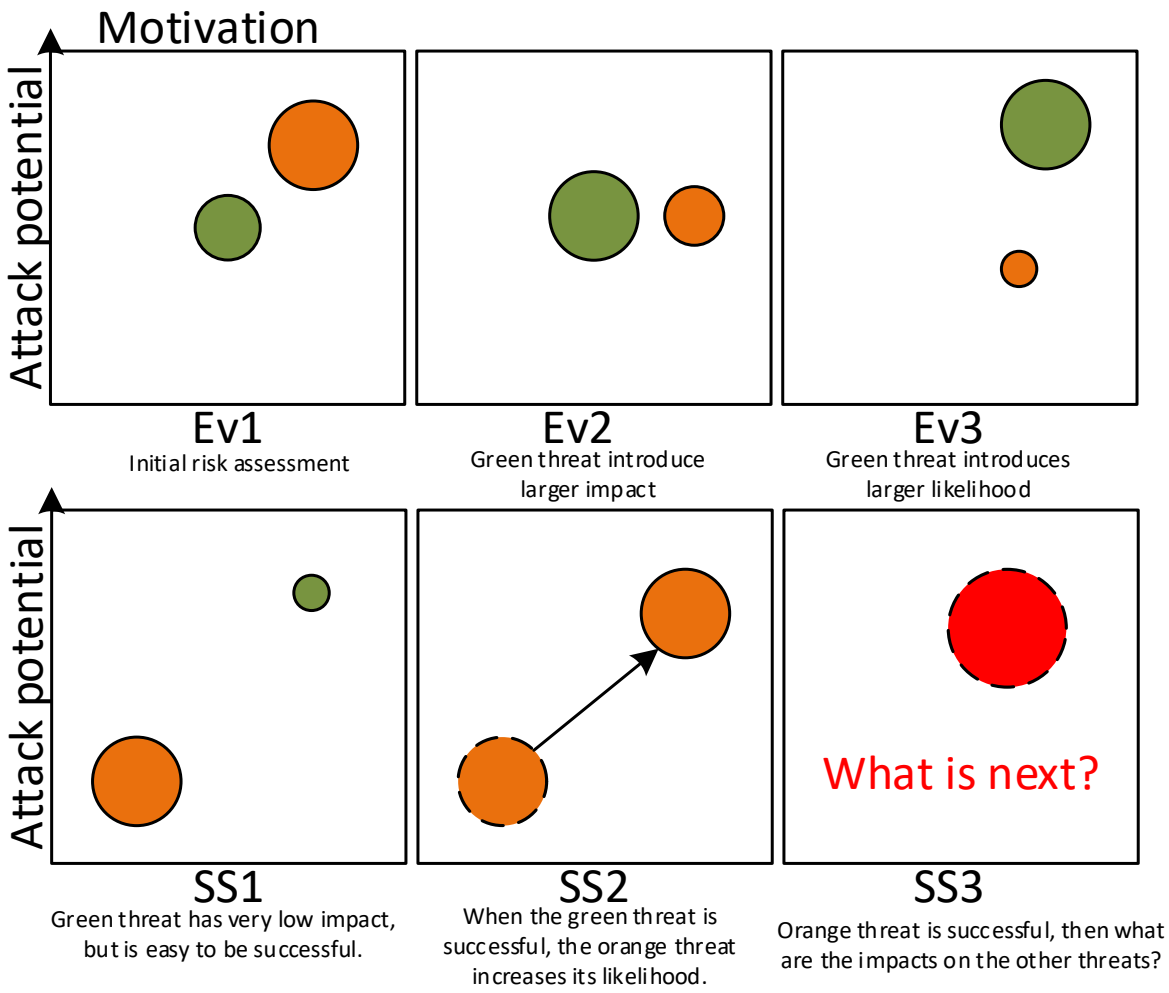
- Impacts on attack and defence potential
- Impacts on threat agents and their motivations.

System's security state affects risk assessment

- Vulnerabilities in one surface may open the chances for attacking other (linked) surfaces.

Effective dynamic risk assessment at scale:

– Maintain risk profiles of environments and system states to reuse the analysis

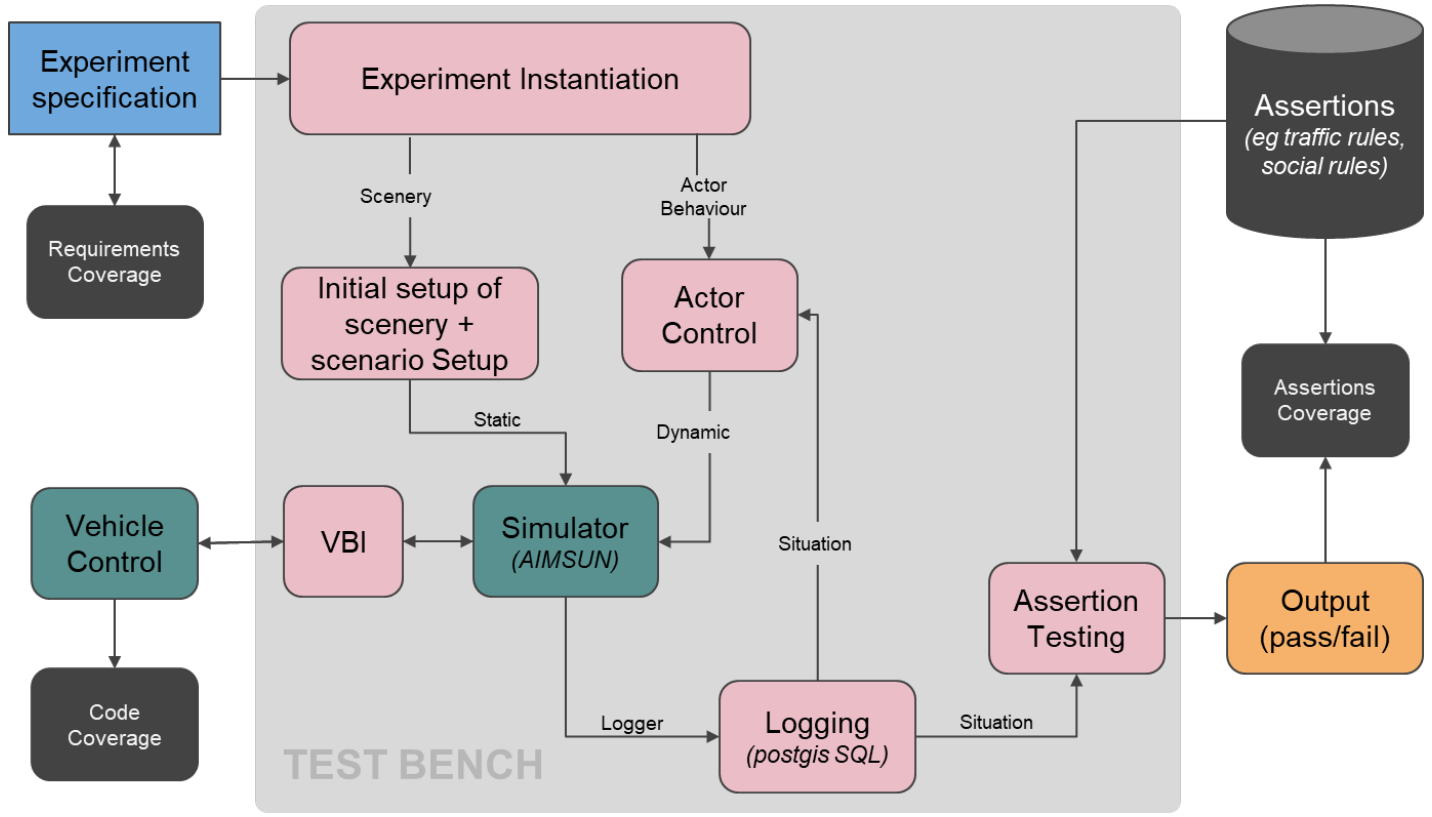


Simulator Testbench: Safety and Cyber Security

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



Summary

Final trials:

- Queen Elizabeth Olympic Park
- Jan 2020

Blend of approaches to assure Cyber Safety

- Traditional threat assessment
- Simulation
- Trial

Results will feed longer term pilots

Capri

Thank you

Capri

For more information: http://caprimobility.com/

NEXOR

Colin Robbins.
Principal Security Consultant
Colin.Robbins@Nexor.com

WMG
THE UNIVERSITY OF WARWICK

Prof Carsten Marple.
Professor of Cyber Systems Engineering
CM@warwick.ac.uk