Systems Approach to Scenario Generation for Automated Driving System

Dr Siddartha Khastgir CEng MIMechE
Head of Verification & Validation, Intelligent Vehicles
WMG, University of Warwick, UK
UK Technical Representative – ISO TC204/WG14, ISO TC22/SC33/WG9

WMG
THE UNIVERSITY OF WARWICK

ARCADE Workshop on Edge Cases for Automated Driving
11 May 2021

Agenda

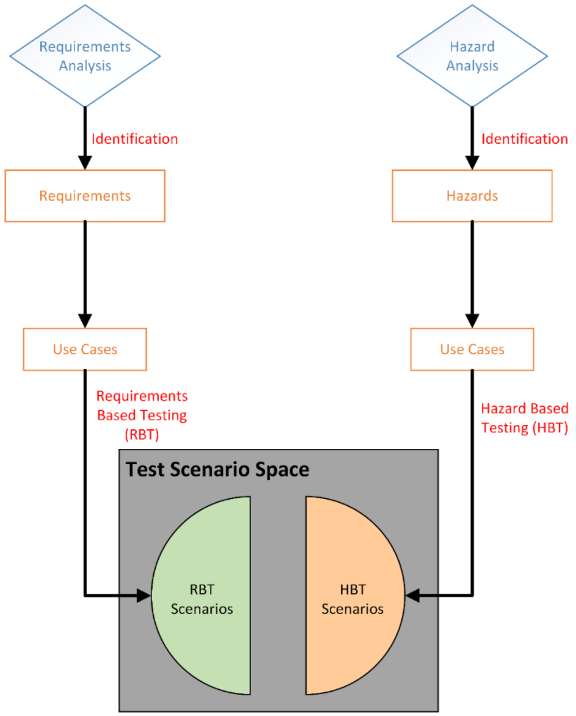
- Motivation
- STPA: Systems Theoretic Process Analysis
- Test Scenarios – STPA extension
- Safety Pool^{TM} Scenario Database
- Conclusions

Motivation: Identifying test scenarios

- Semi-structured interview study of Verification and Validation (V&V) experts in the industry from USA, Sweden, Germany, India, UK and Japan (across the automotive supply chain)

- Key findings [3]:
  - For ADAS and ADS: we need to test *"how a system fails"* as compared to *"how a system works"*
  - Need for a structure way to define test scenarios and test cases

- Proposed Hazard Based Testing



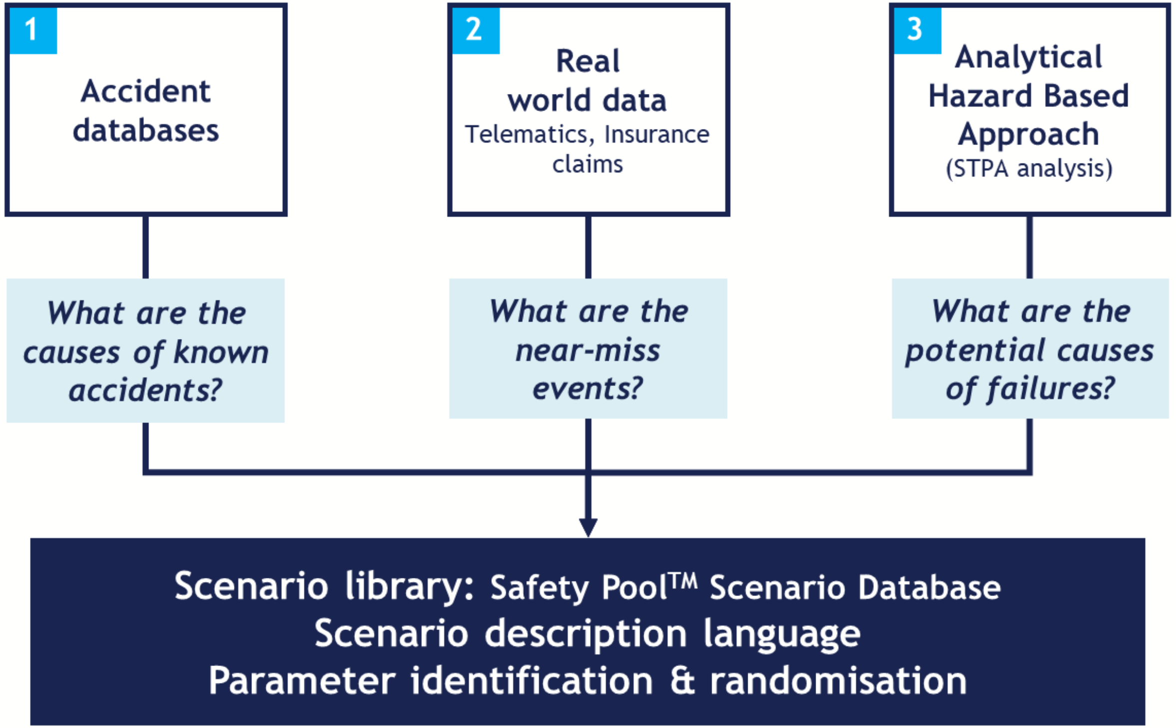
[3] Khastgir, S. et al., "The science of testing: an automotive perspective," SAE World Congress Experience 2018

Hazard Based Testing

Three step process:

- Identification of hazards
- Creating test scenarios for the identified hazards
- Pass criteria for the created test scenarios

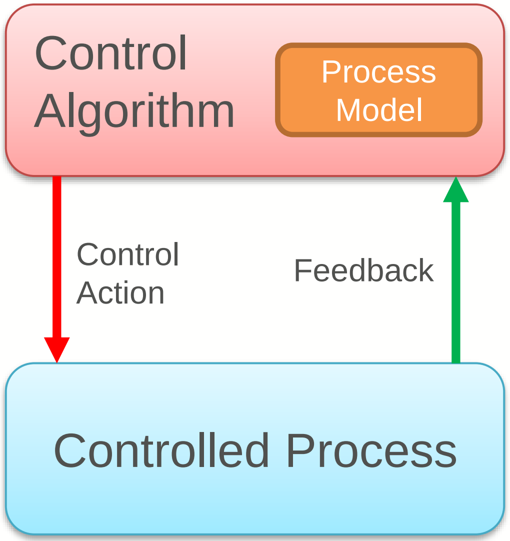
Scenario Generation



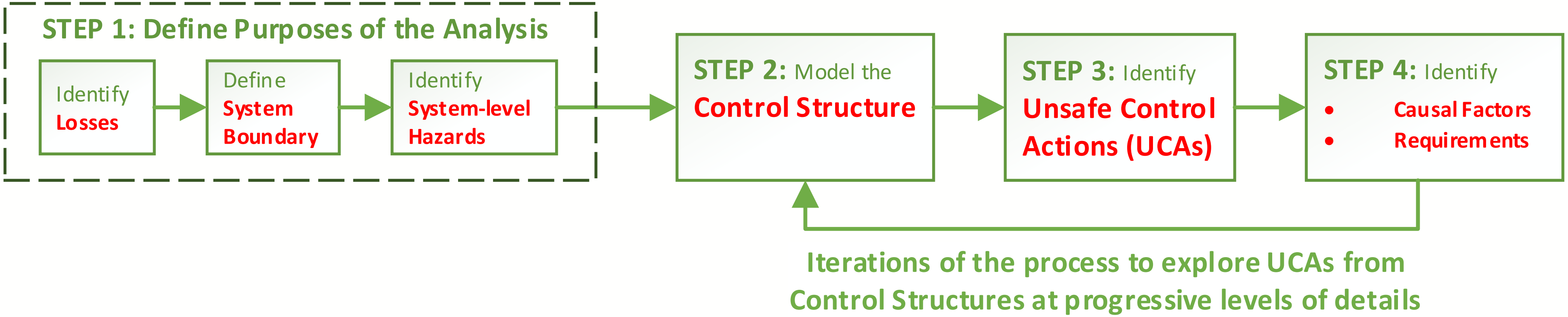
Reference: OmniCAV project: www.omnicav.com
Citation: OmniCAV: A Simulation and Modelling System that enables “CAVs for All” – Brackstone et. al., IEEE ITSC 2020

Systems Theoretic Process Analysis (STPA)

- After going through literature, we found STAMP/STPA the most exhaustive list of hazards capturing system interactions
- STAMP/STPA is based on Systems Engineering and considers system safety as a control problem
  - *Safety* is a control problem (property of a system as a whole, not individually)
  - Breach of control laws (constraints) cause accidents
- Basis of STAMP:
  - Constraints, control loops and process models, and levels of control



STPA: Four step process



System Definition

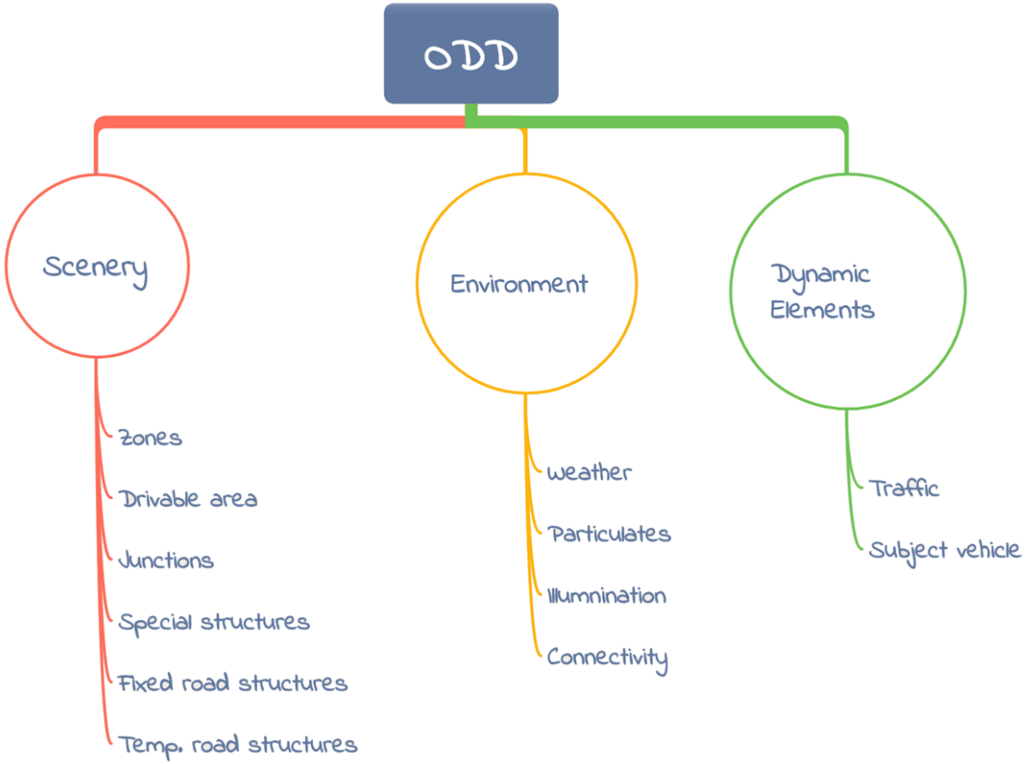
- Fully autonomous low-speed shuttle (SAE Level 4)
- Limited ODD
- Sensor suite
- Remote dispatcher
- Electric propulsion

STPA: Step 1: Losses and Hazards

Losses	
L1	Collision with objects outside the vehicle or damage to vehicle
L2	Not completing the journey with passenger and cargo
L3	**Time of journey being too long, i.e., service target not met**
L4	Loss of life or serious injury to people

Hazards	
H1	Vehicle does not maintain safe distance from nearby objects - L1
H2	Vehicle enters dangerous area/region – L1
H3	Vehicle exceeds safe operating envelope for environment (speed, lateral/longitudinal forces) - L1, L2, L3
H4	Vehicle occupants exposed to harmful effects and/or health hazards (e.g. fire, excessive temperature, inability to escape, door closes on passengers, etc.) – L4
H5	**Vehicle does not follow an efficient, complete path to destination – L2, L3**

STPA: Step 1: Define the ODD

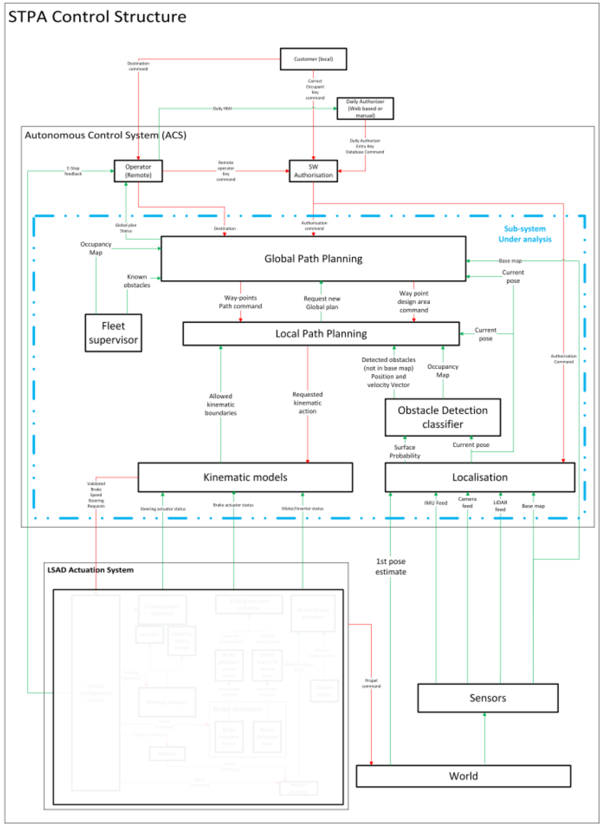


ODD Taxonomy as per BSI PAS 1883

WMG
THE UNIVERSITY OF WARWICK

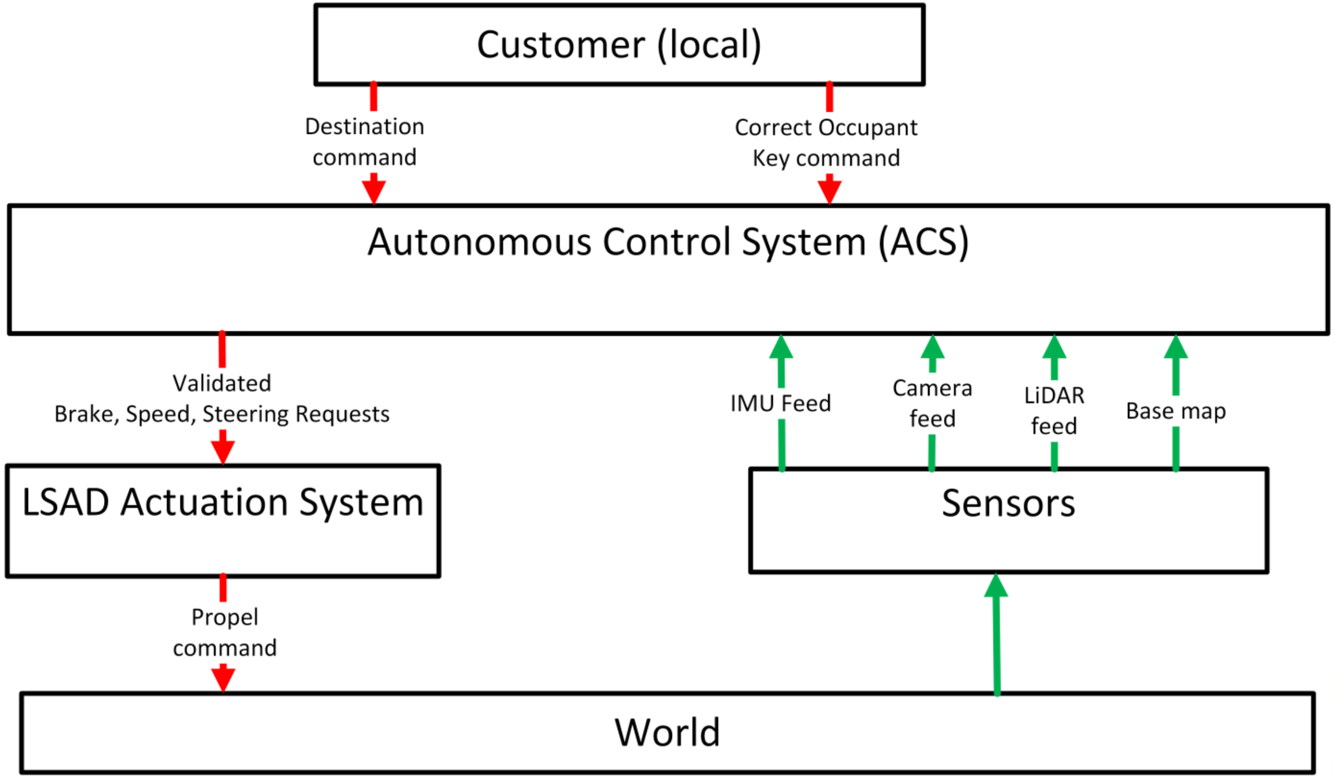
STPA: Step 2: Control Structure

- Identify a control structure for the system with control actions and feedback
- Control structure can be at various abstraction levels
- Control structure for fully autonomous vehicle (pod)
  - Red = control action
  - Green = feedback



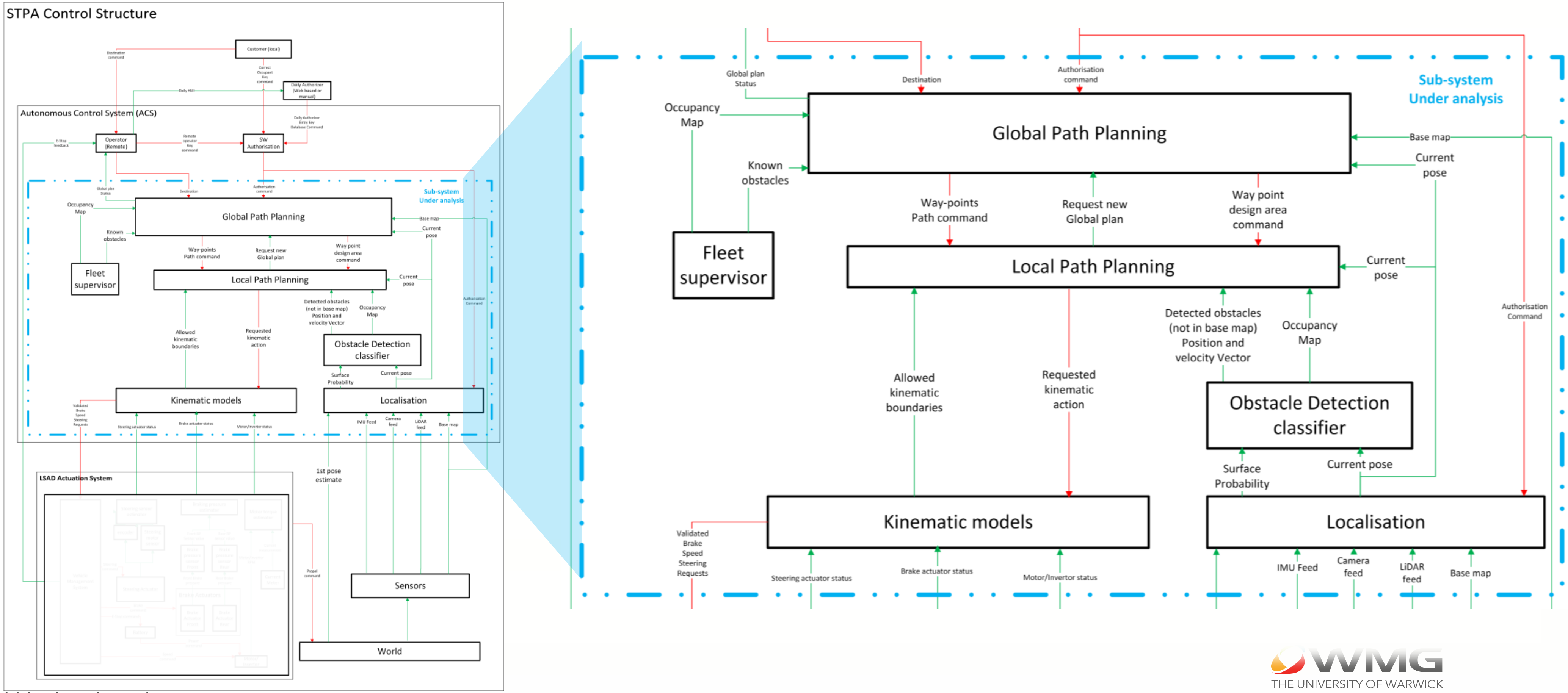
WMG
THE UNIVERSITY OF WARWICK

STPA: Step 2: Control Structure (high level)



WMG THE UNIVERSITY OF WARWICK

STPA: Step 2: Control Structure



THE UNIVERSITY OF WARWICK

STPA: Step 3: Unsafe Control Actions

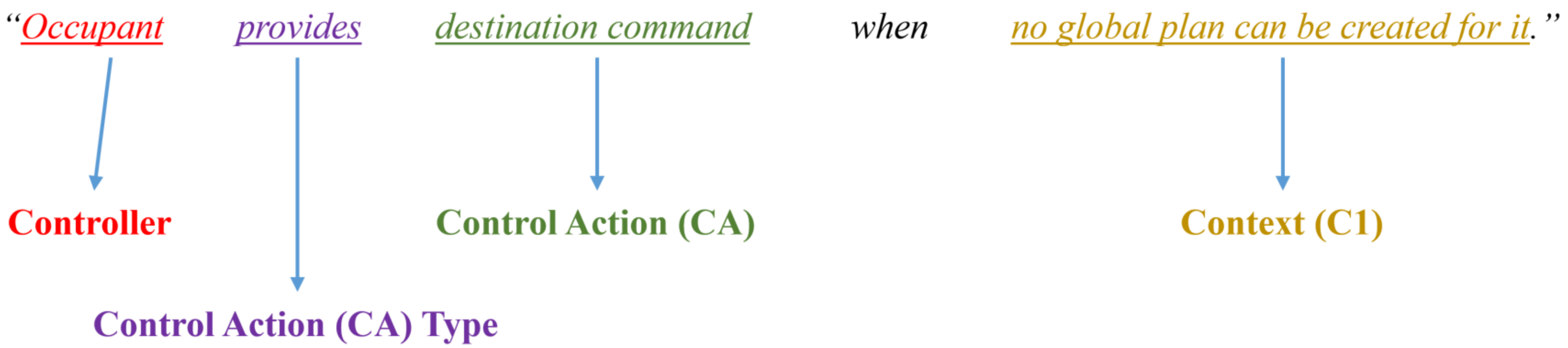
- 12 Control Actions led to 70 Unsafe Control Actions
- Essential to maintain the UCA structure

Control Action	Not Providing causes a loss	Providing causes a loss	Too early, too late, out of sequence causes a loss	Stopped too soon or applied too long causes a loss
Requested kinematic command	[UCA# 15a] Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front. – [H1, H2, H4, H5] [..]	[..]	[UCA# 15c1] LPP provides kinematic action (braking) too late after conflict is unavoidable when there is an obstacle in front and pod is moving. – [H1, H2, H3] [..]	[..]

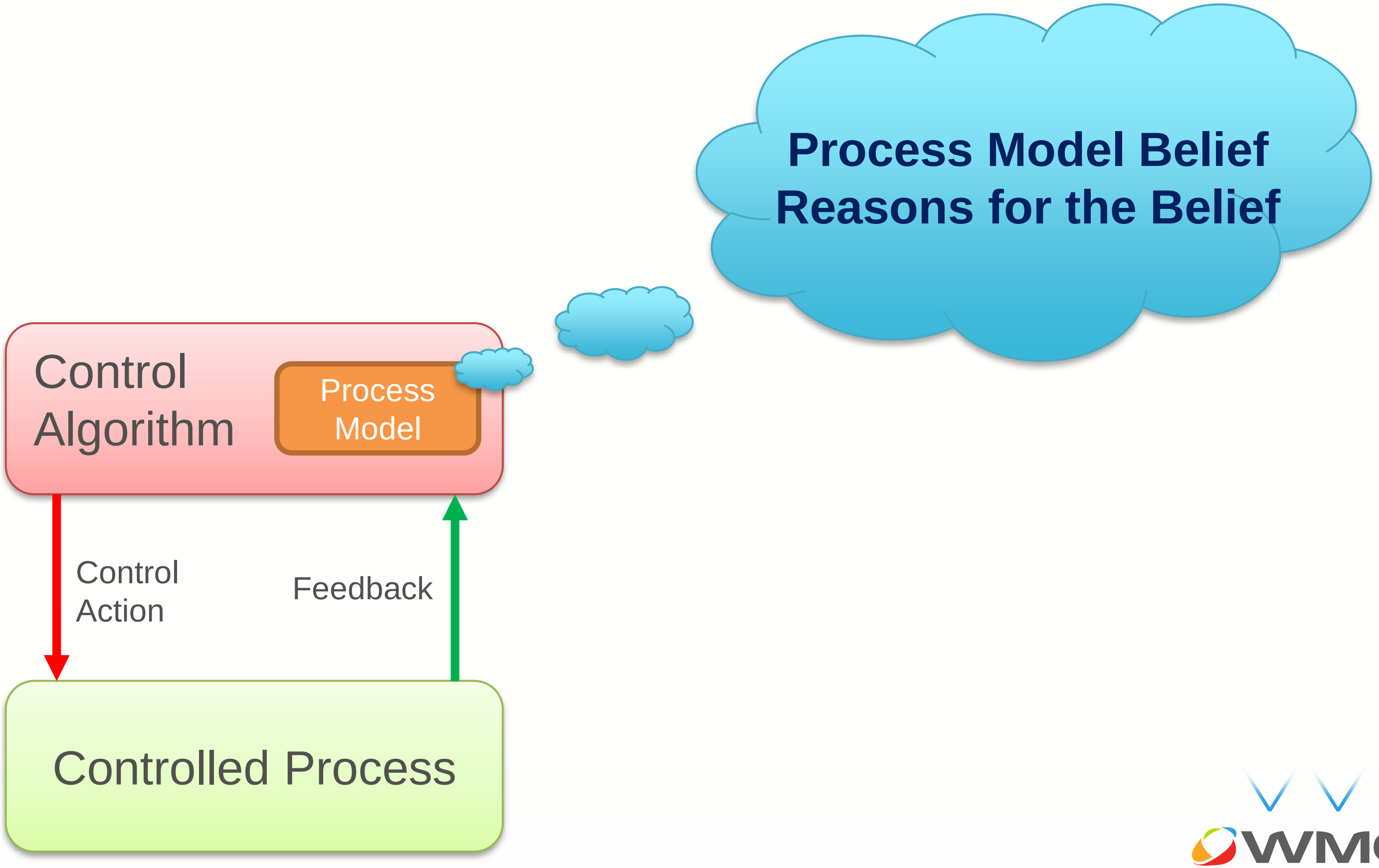
WMG THE UNIVERSITY OF WARWICK

STPA: Step 3: Unsafe Control Actions

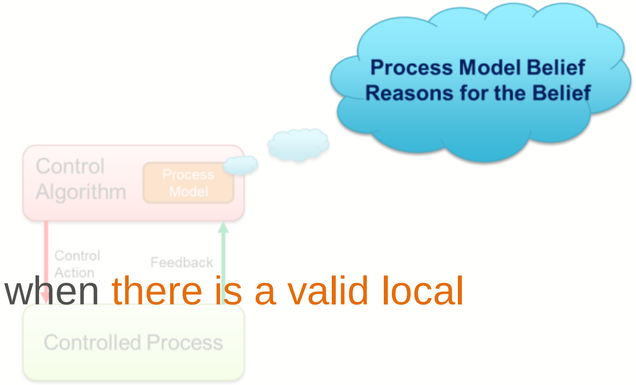
- 12 Control Actions led to 70 Unsafe Control Actions
- Essential to maintain the UCA structure



STPA: Step 4: Loss Scenarios

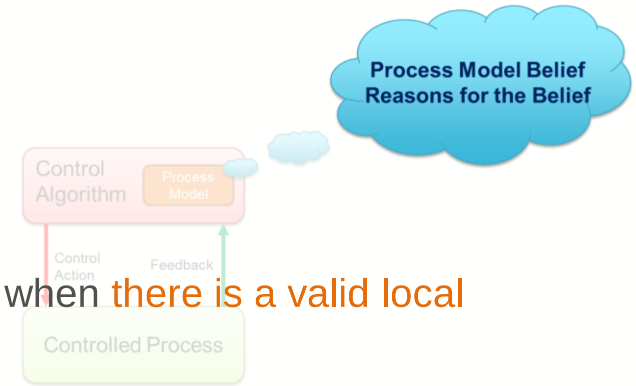


STPA: Step 4: Loss Scenarios



UCA: Local Path Planning (LPP) doesn’t provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.

STPA: Step 4: Loss Scenarios

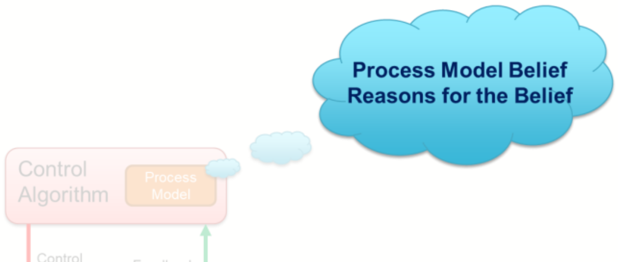


UCA: Local Path Planning (LPP) doesn’t provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.

Process Model Belief (B1):

- LPP believes that obstacles are not in vehicle trajectory

STPA: Step 4: Loss Scenarios



UCA: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.

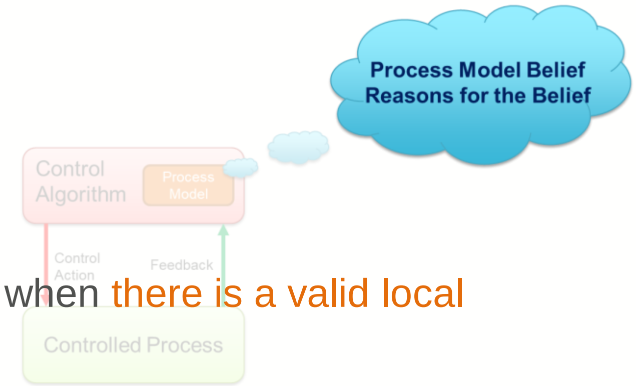
Process Model Belief (B1):

- LPP believes that obstacles are not in vehicle trajectory

Reason for the Belief (B2):

- LPP believes that because the Obstacle Detection Classifier doesn't provide detected obstacles vector when obstacle is in vehicle trajectory

STPA: Step 4: Loss Scenarios



UCA: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.

Process Model Belief (B1):

- LPP believes that obstacles are not in vehicle trajectory

Reason for the Belief (B2):

- LPP believes that because the Obstacle Detection Classifier doesn't provide detected obstacles vector when obstacle is in vehicle trajectory

Causal Factors

- This could be because historical data of the pose and the surface probability shows no collision and the Covariance Error is low (i.e., sensor data is coherent). This could be because all sensor feeds are delayed in time leading to a low covariance error as they are coherent.

THE UNIVERSITY OF WARWICK

STPA: Step 5: Extension: Test Scenario creation

STPA: Step 5: Extension: Test Scenario creation

- Every scenario will have:
  - Scenery
  - Dynamic elements

  } Library
  - Depend on ODD, a library of base sceneries and dynamic elements have been created

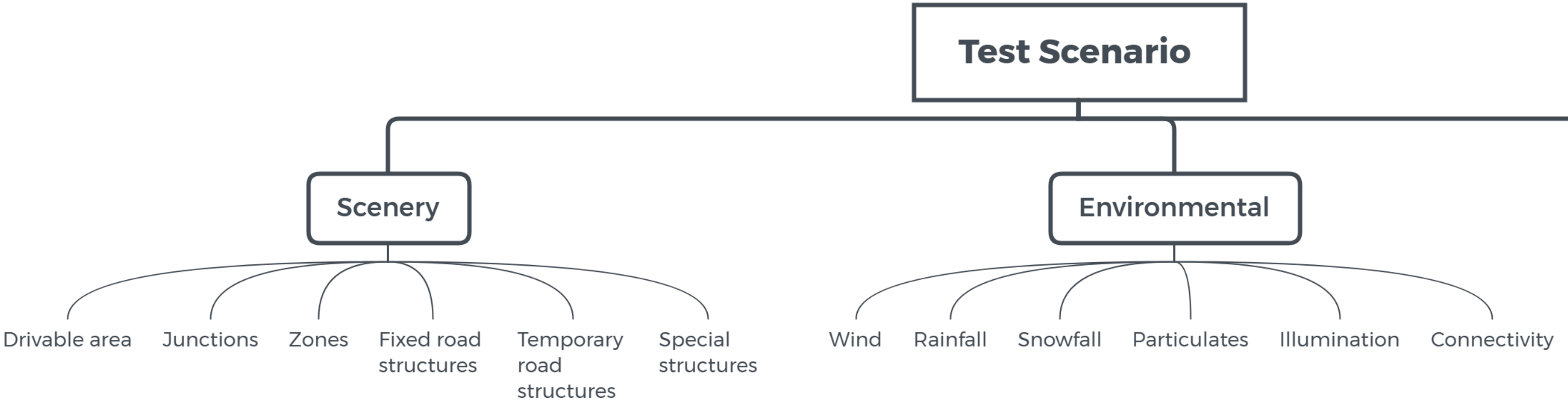
Additional Context:

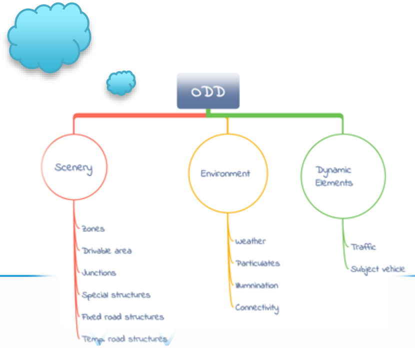
- Parametrise the “context element” (of UCA)
- Parametrise the “causal factors” (step 4)

- Pass criteria

WMG
THE UNIVERSITY OF WARWICK

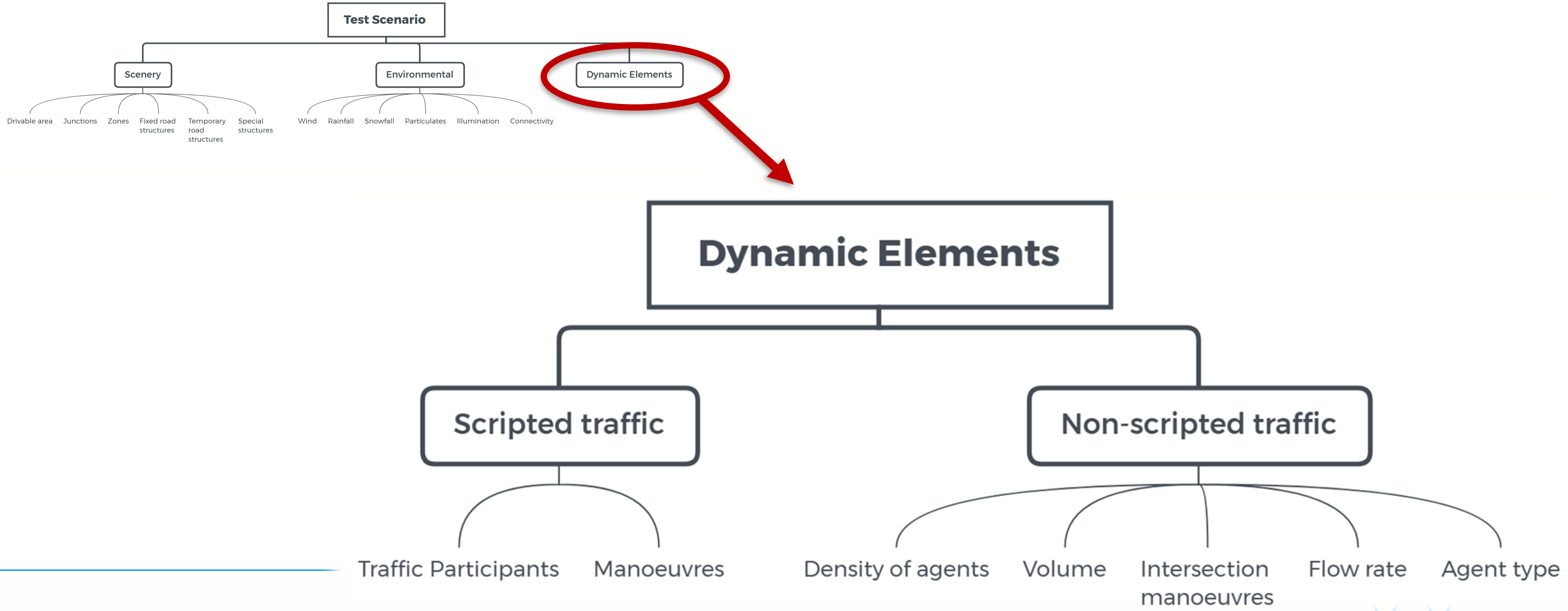
Test Scenarios structure





WMG
THE UNIVERSITY OF WARWICK

Test Scenarios structure



STPA: Step 5: Additional Context

UCA: *Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.*

STPA: Step 5: Additional Context

***UCA**: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.*

- Parametrise the "context element" (of UCA)
  - *there is a valid local path and the pod is moving and there is an obstacle in front*
  - Parameters: Velocity, obstacle position

WMG
THE UNIVERSITY OF WARWICK

STPA: Step 5: Additional Context

***UCA**: Local Path Planning (LPP) doesn't provide kinematic action (braking) when there is a valid local path and the pod is moving and there is an obstacle in front.*

- Parametrise the "context element" (of UCA)
  - *there is a valid local path and the pod is moving and there is an obstacle in front*
  - Parameters: Velocity, obstacle position

- Parametrise the "causal factors" (step 4)
  - This could be because all sensor feeds are delayed in time leading to a low covariance error as they are coherent.
  - Parameters: Delay time, type of sensor feed

WMG
THE UNIVERSITY OF WARWICK

Case study overview: STPA & extension

Case study overview: STPA & extension

WMG
THE UNIVERSITY OF WARWICK

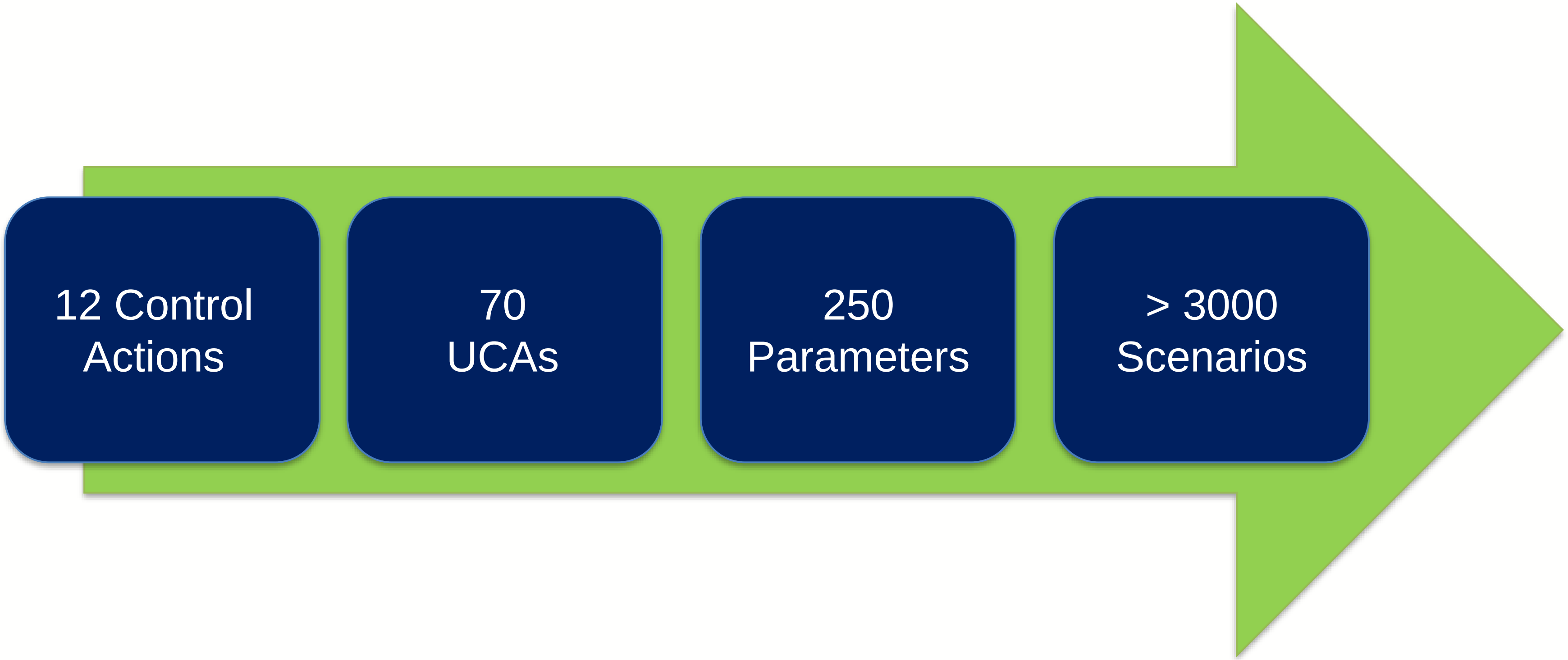
Case study overview: STPA & extension

12 Control Actions

70 UCAs

250 Parameters

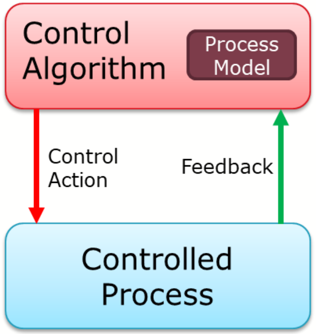
Case study overview: STPA & extension



WMG
THE UNIVERSITY OF WARWICK

STPA: Extension: An overview

1-2. Identify control actions, feedback and high level losses



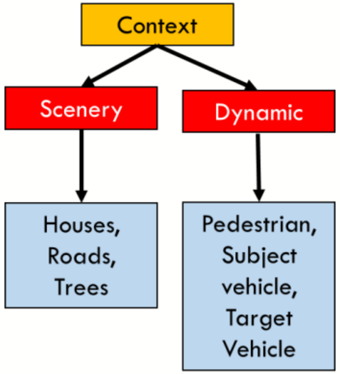
3. Identify Unsafe Control Actions

1) Not providing a control action
2) Not providing a control action
3) Providing a control action too late, too early or out of sequence
4) Control action stopped too soon or applied too long.

4. Identify the causes of Unsafe Control Action

- Process Model Belief
- Reason for the belief
- Negate this to obtain pass criterion

5. Extension: Provide context to obtain bounds on the scenario



- Test Scenario Parameters
- Pass Criteria

THE UNIVERSITY OF WARWICK

Acknowledgement

Centre for Connected & Autonomous Vehicles

AURRIGO

WMG THE UNIVERSITY OF WARWICK

MIT

UKRI Future Leaders Fellowships

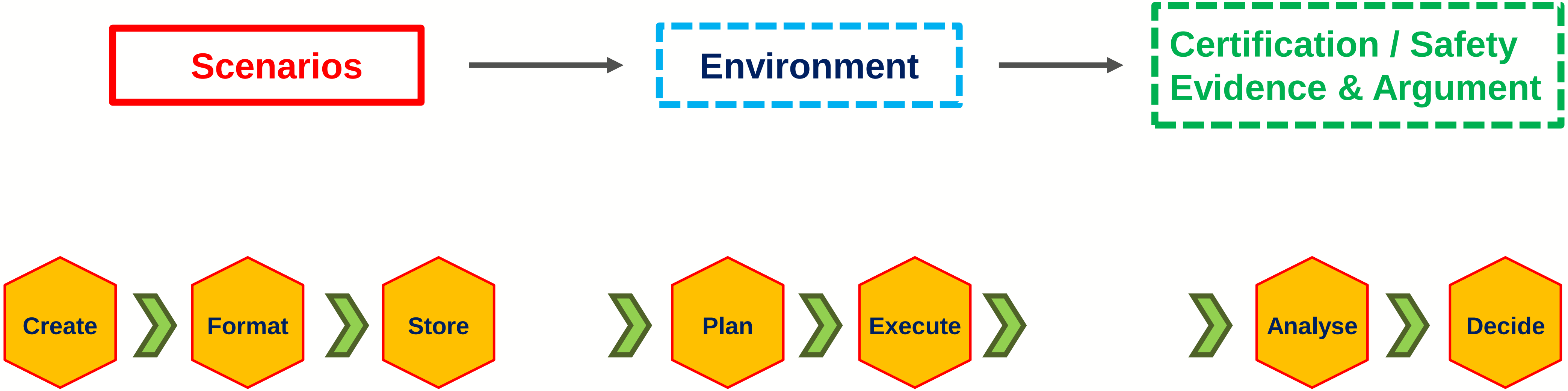
For more details:

Khastgir, S., Brewerton, S., Thomas, J., & Jennings, P. (2021). Systems Approach to Creating Test Scenarios for Automated Driving Systems. *Reliability Engineering & System Safety*, 107610.

Implementing the Evaluation Continuum

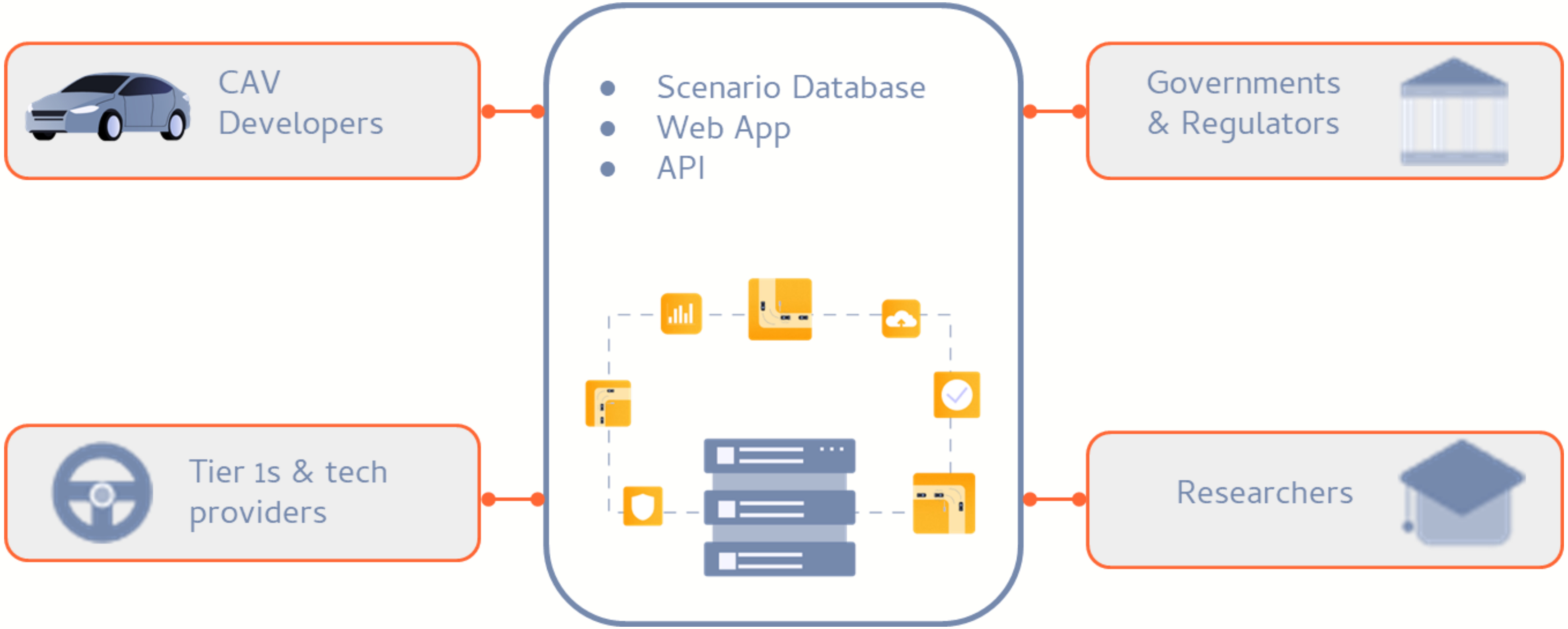
Scenarios → Environment → Certification / Safety Evidence & Argument

Implementing the Evaluation Continuum

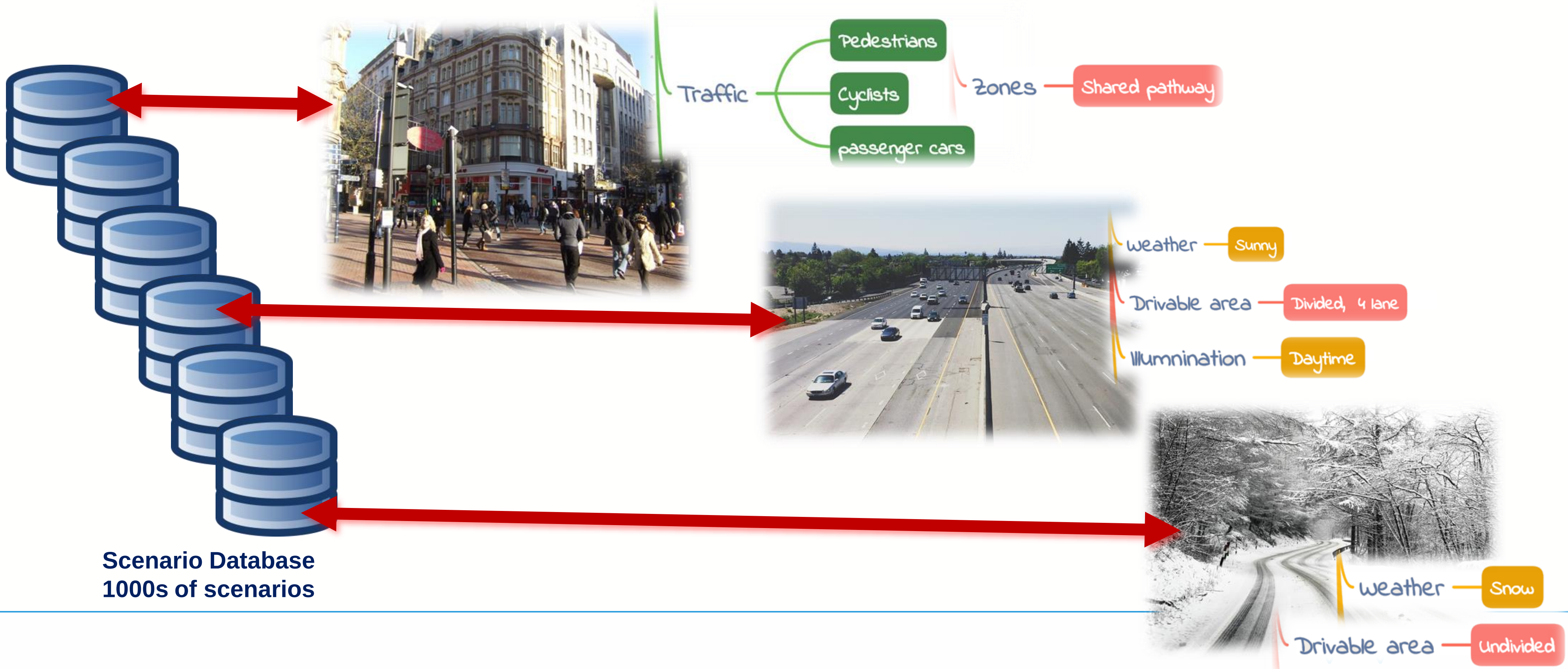


THE UNIVERSITY OF WARWICK

What is Safety Pool™ Scenario Database?



Scenario mapping to ODD



Safety Pool™

Powered by: deepen & WMG THE UNIVERSITY OF WARWICK

Founders

deepen

WMG THE UNIVERSITY OF WARWICK

Supported by

WORLD ECONOMIC FORUM

ZENZIC SELF-DRIVING REVOLUTION

UKRI Innovate UK

Summary

For Automated Driving, It is not about the number of miles, but about the number of *"smart"* miles...

Hazard based testing to identify the *"interesting"* scenarios

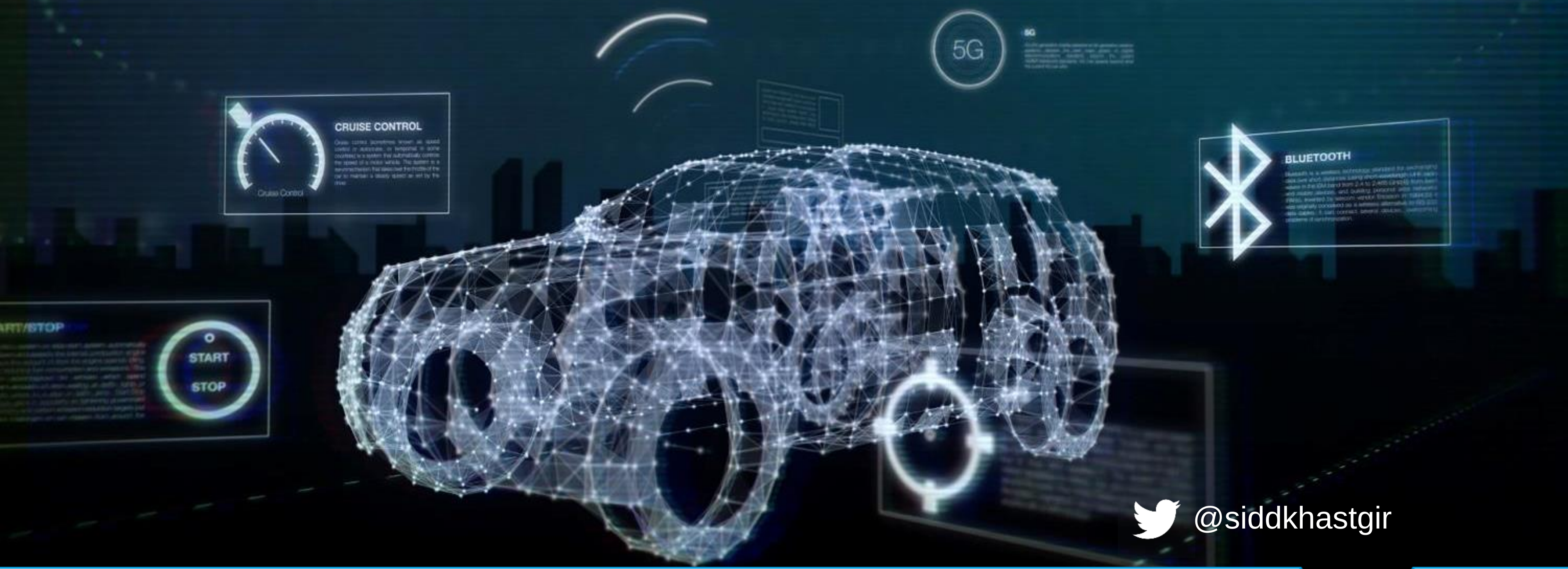
STPA facilitates Hazard Based Testing. STPA applied on a SAE Level 4 system

An extension to STPA proposed to solve two key challenges: test scenarios and pass criteria

STPA identifies the parameters to be fuzzed along with the pass/fail criteria for the test case

WMG
THE UNIVERSITY OF WARWICK

Thank you…
Discussions…



@siddkhastgir

Dr Siddartha Khastgir CEng MIMechE
S.Khastgir.1@warwick.ac.uk

WMG
THE UNIVERSITY OF WARWICK