
University of
Southampton

University of Southampton

# Developing a Trustworthy Integrated Mission Management System for Autonomous Vehicles

Son Hoang (University of Southampton)
joint work with many others

Exploring Formal Methods for Unmanned Aerial Vehicles (10/06/2025)

# Outline

University of Southampton

- Policing Function for UAV
  - Joint work between University of Southampton and Tekever Ltd.
- Integrated Mission Management System for Autonomous Vehicles
  - Joint work between University of Southampton and Thales, UK.
- Challenges and Opportunities

University of Southampton

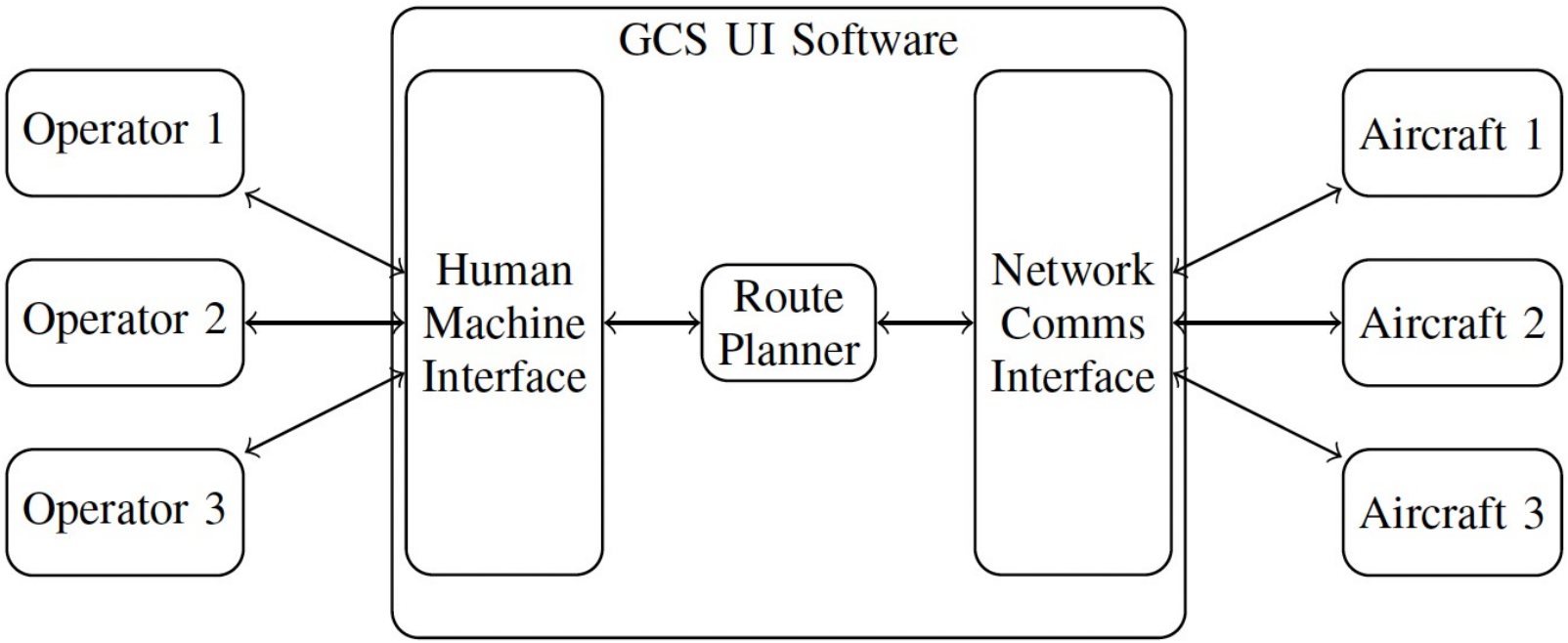
# Formal Development of Policing Functions for Intelligent Systems

Uni. of Southampton:
T. Wilkinson, J. Snook, S. Hoang, M. Butler

Tekever Ltd.:
C. Bogdiukiewicz, X. Waldron, M. Paxton

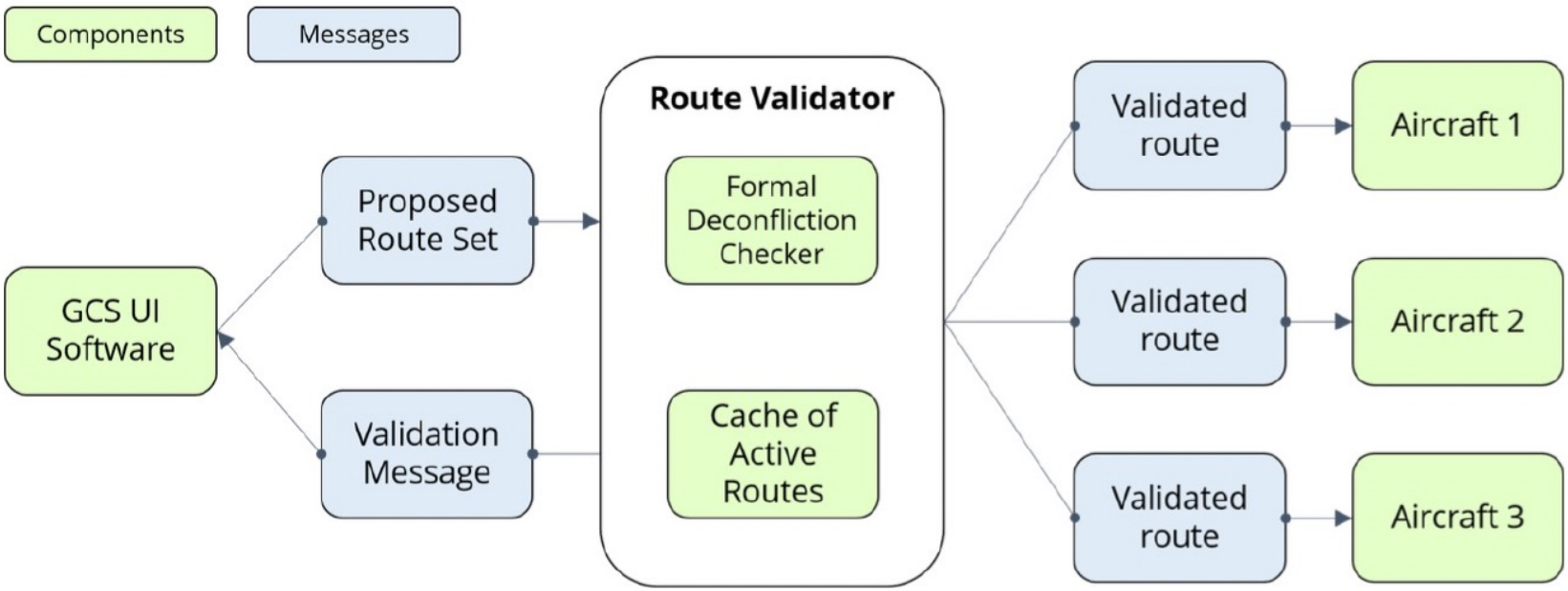
ISSRE 2017

# System Overview



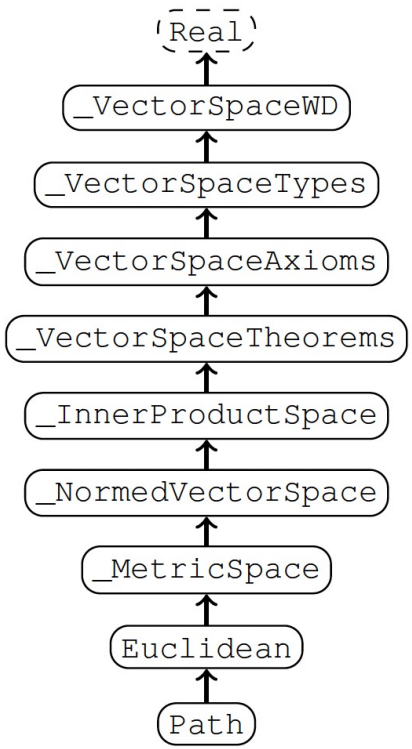
# Route Validator

## Architecture



# Route Deconfliction Validator

## Formal Development




Theories based on Real

```
constants r len min_sep
axioms
  "2 ≤ len"
  "r ∈ 0 .. len − 1 → ROUTE_T"
  "zero ≤ min_sep"
events
  get_conflicts
  any cflts where
    "cflts = (⋃ m,n · m ∈ 0 .. len − 1 ∧
                          n ∈ m+1 .. len − 1
      | route_pair_conflicts(r(m), r(n), min_sep))"
  then
    skip
  end
```

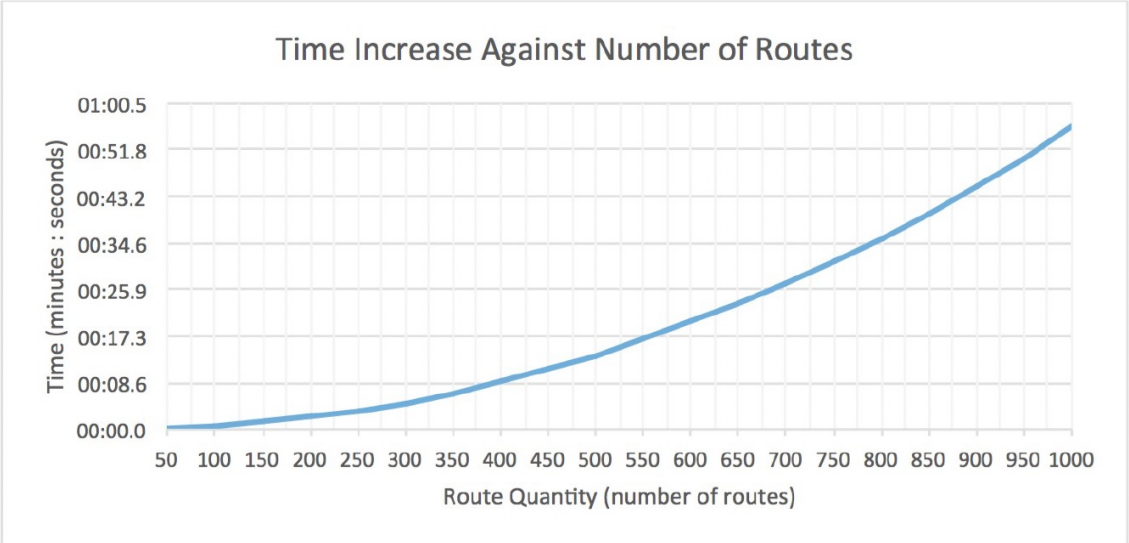
Event-B Formal Specification

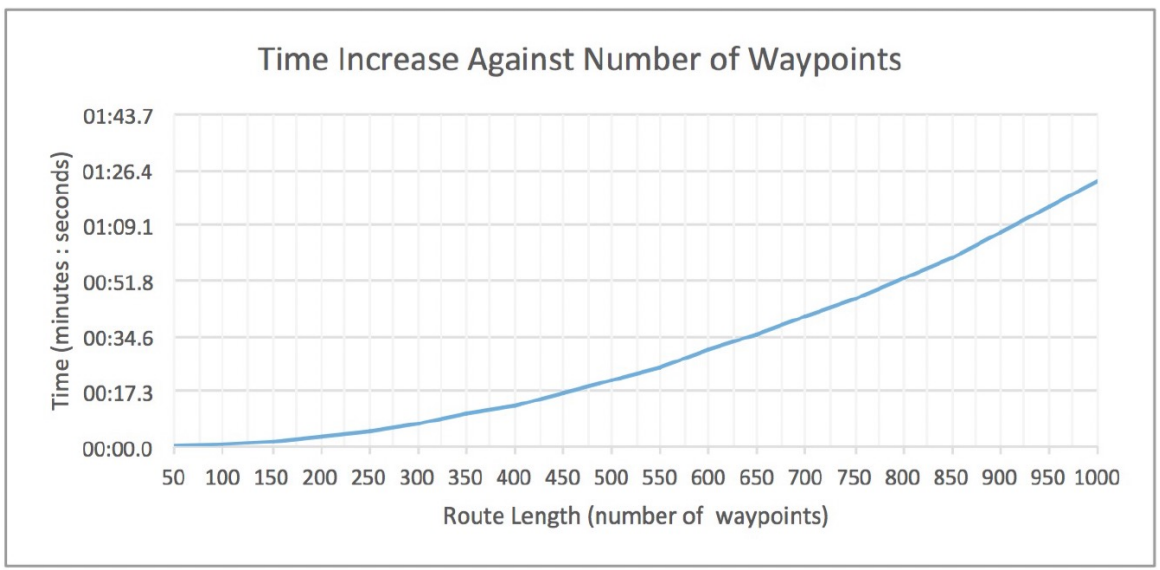
```
separation_conflicts_t *get_conflicts(route_t *r,
          int len,
          distance_t min_sep) {
 ....
 separation_conflicts_t *conflicts = sc_create();

 for (int i = 0; i < len; ++i)
 {
   for (int j = i + 1; j < len; ++j)
   {
     if (r[i].id == r[j].id)
     {
       /* An aircraft is never in conflict with itself. */
       continue;
     }

     route_pair_conflicts(conflicts,
       r[i],
       r[j],
       min_sep);

   }
 }
}
```

Systematic translation into C

# Some Experimental Figures

University of Southampton



University of Southampton

# Integrated Mission Management System

Uni. of Southampton (School of Engineering & ECS):
J. Downes, S. Turnock, J. Scalan, M. Ferraro,
S.J. Ossont, D. Dghaym, A. Salehi-Fathabadi,
S. Hoang, M. Butler, E. Rogers

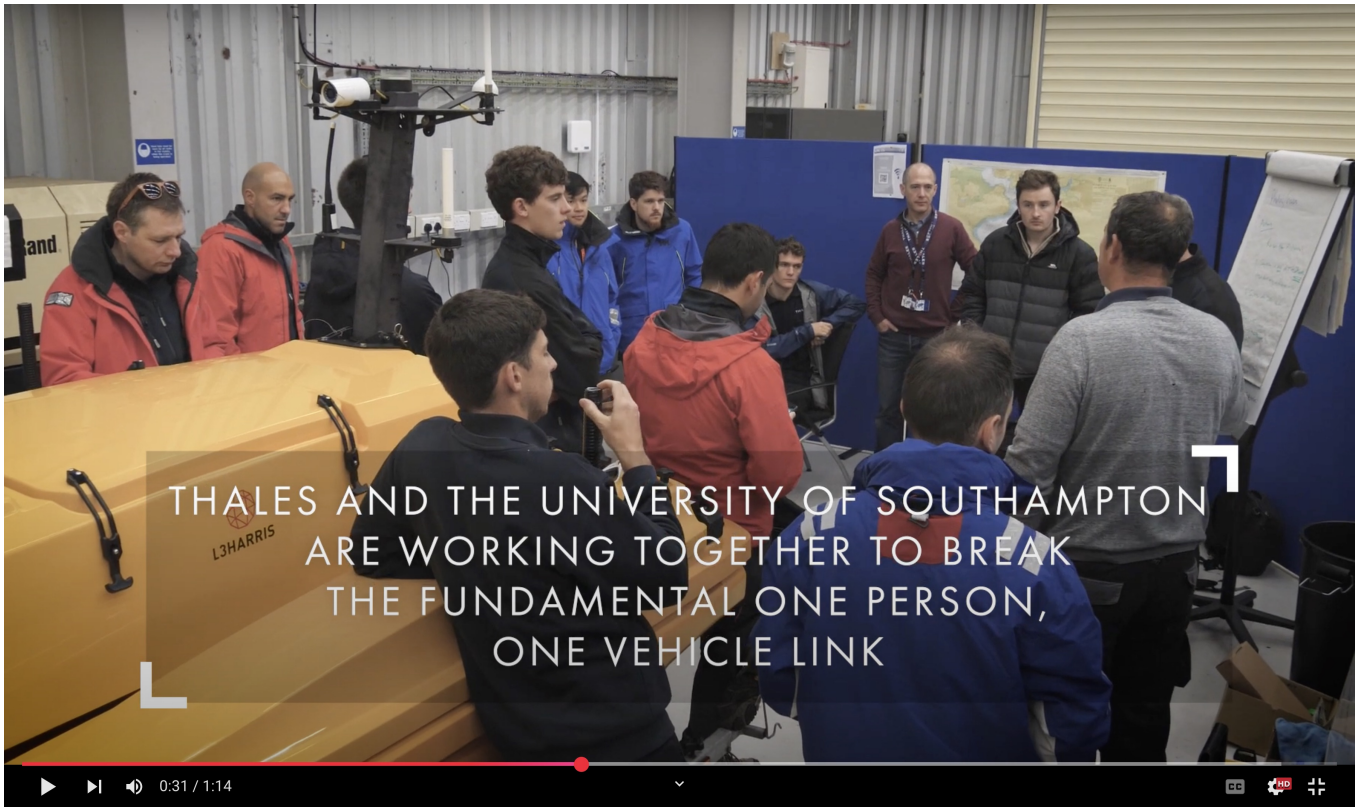
Thales UK:
J.Lam, B. Pritchard, C. Harding, J. Leech,
M. Shepheard

IMMS 2019 & 2022

# Integrated Mission Management System

University of Southampton

## Purpose

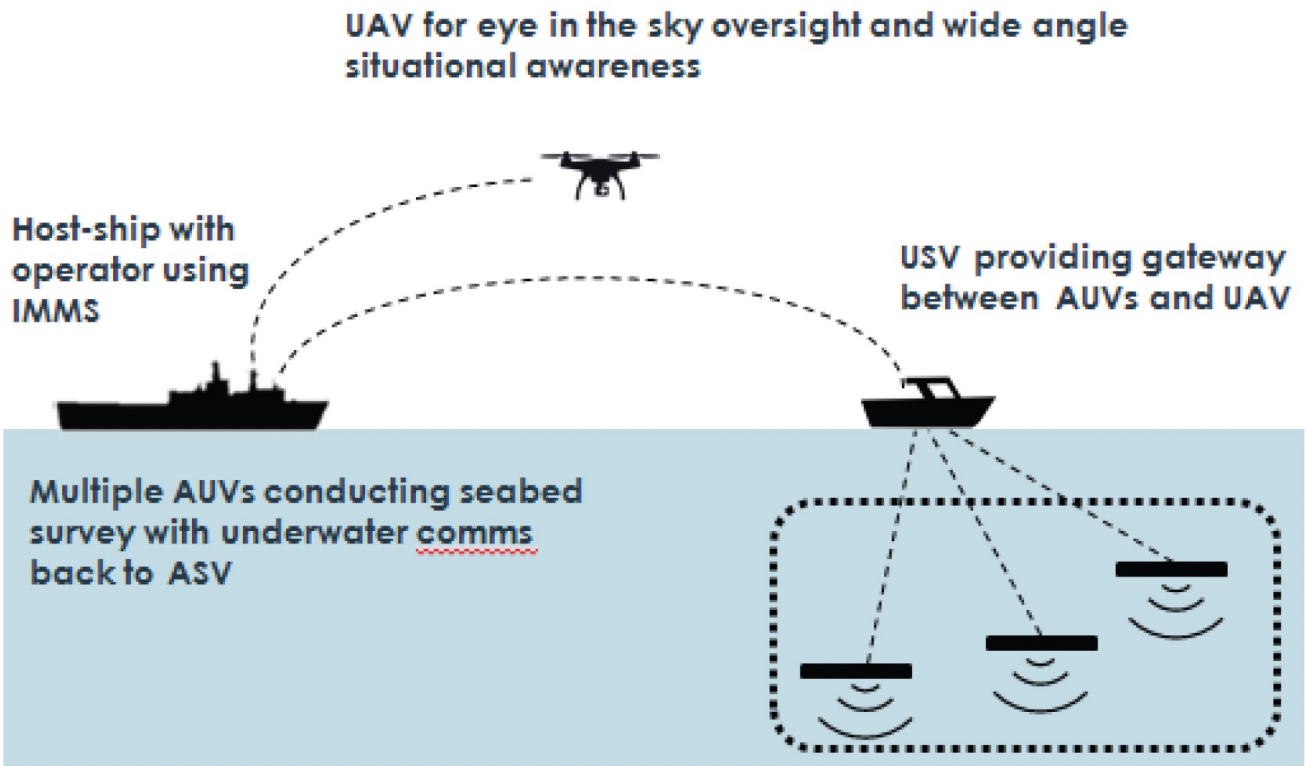



https://www.youtube.com/watch?v=QYpjZZsIe-A

# Integrated Mission Management System

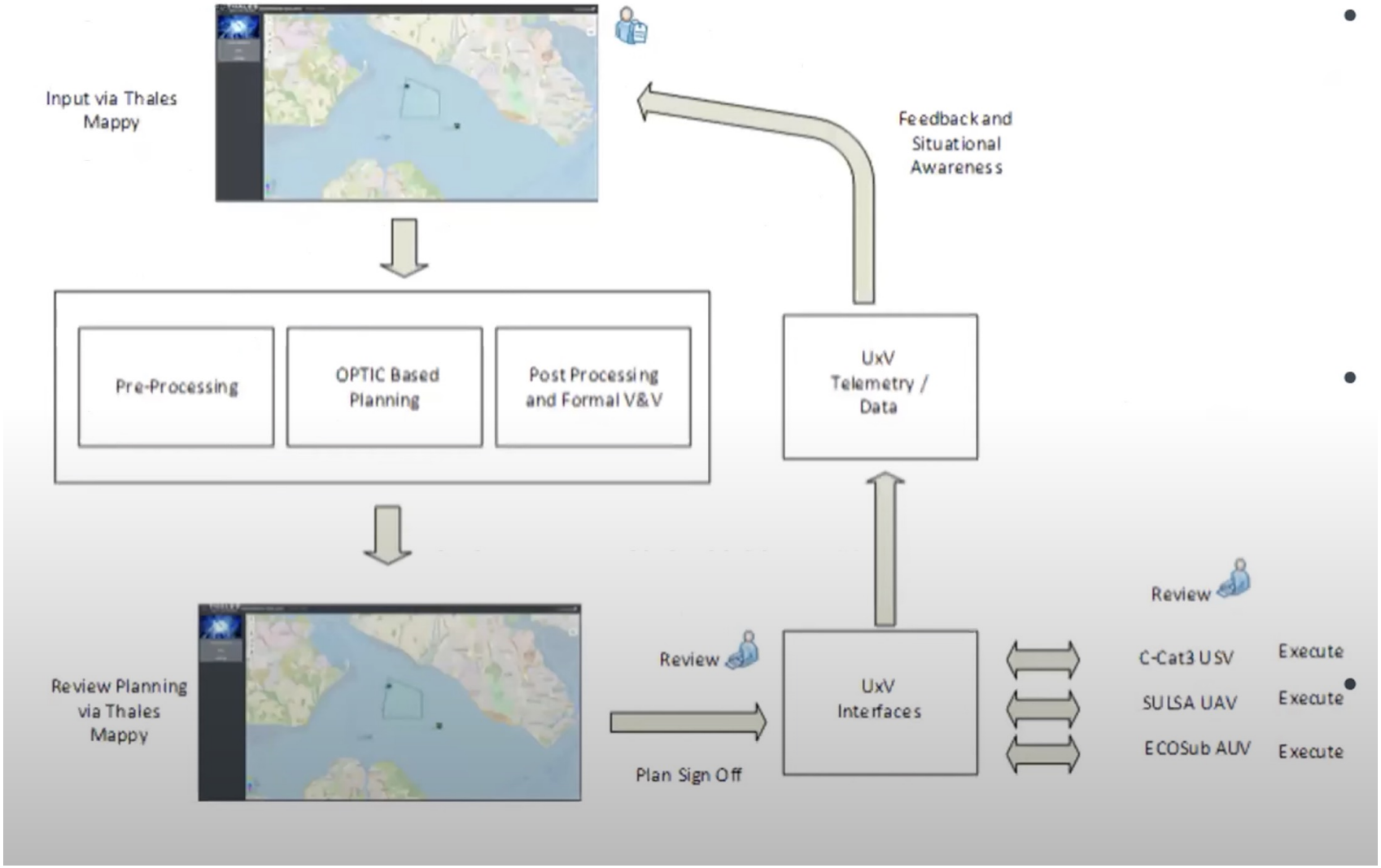
University of Southampton

## Scenario



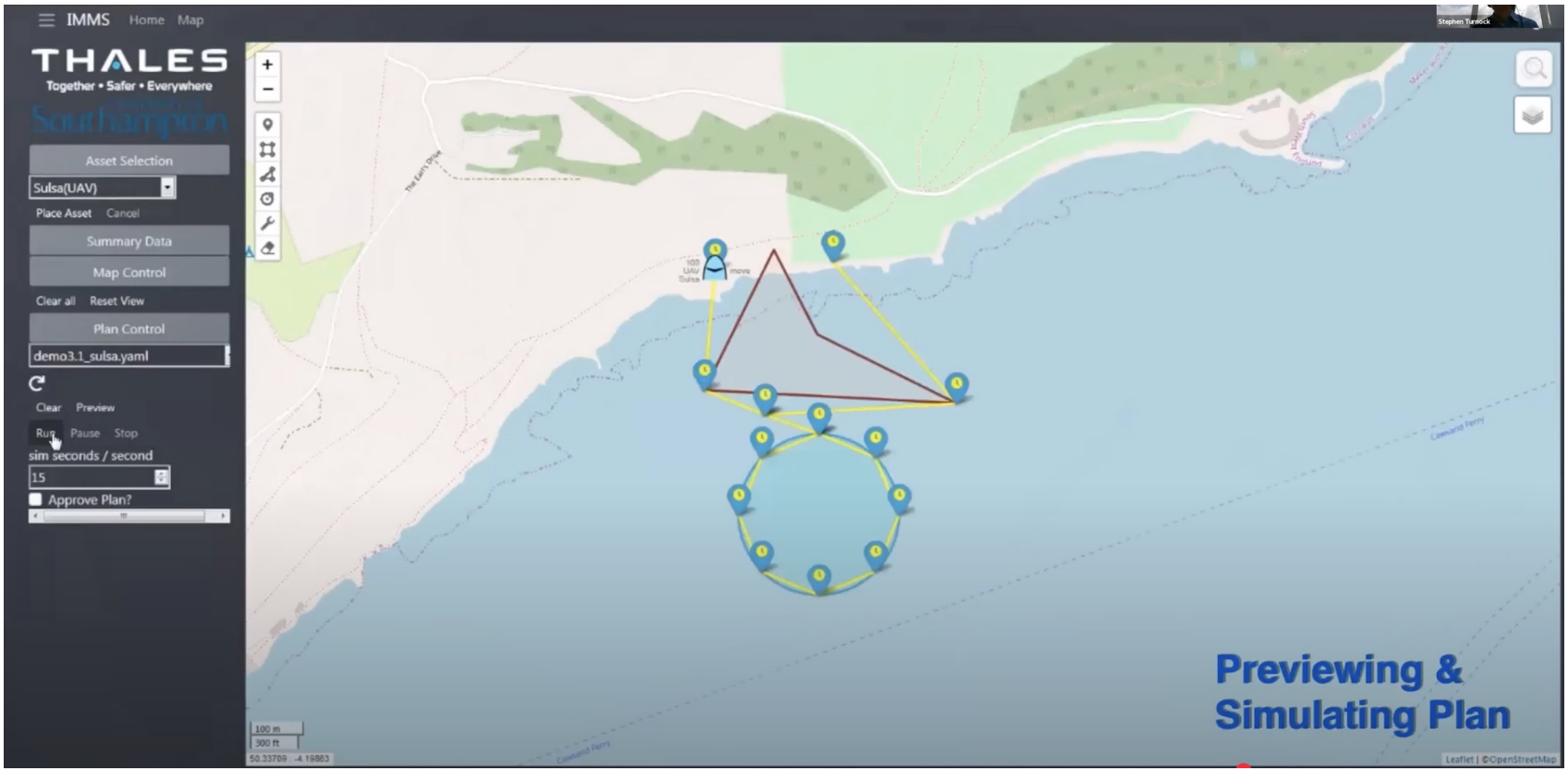
# Integrated Mission Management System

## Flow Diagram



# Integrated Mission Management System

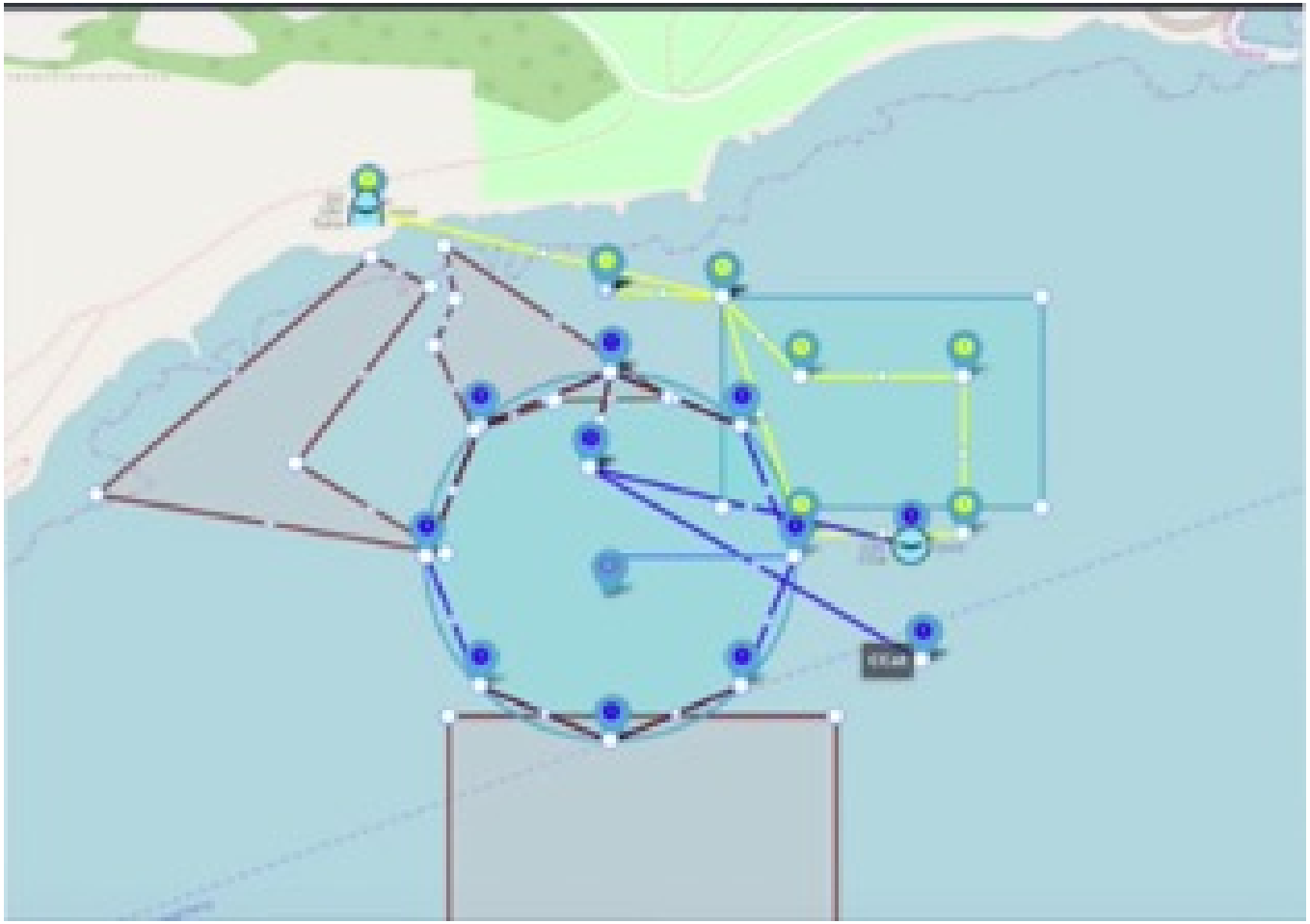
## Practical Trial



# Integrated Mission Management System

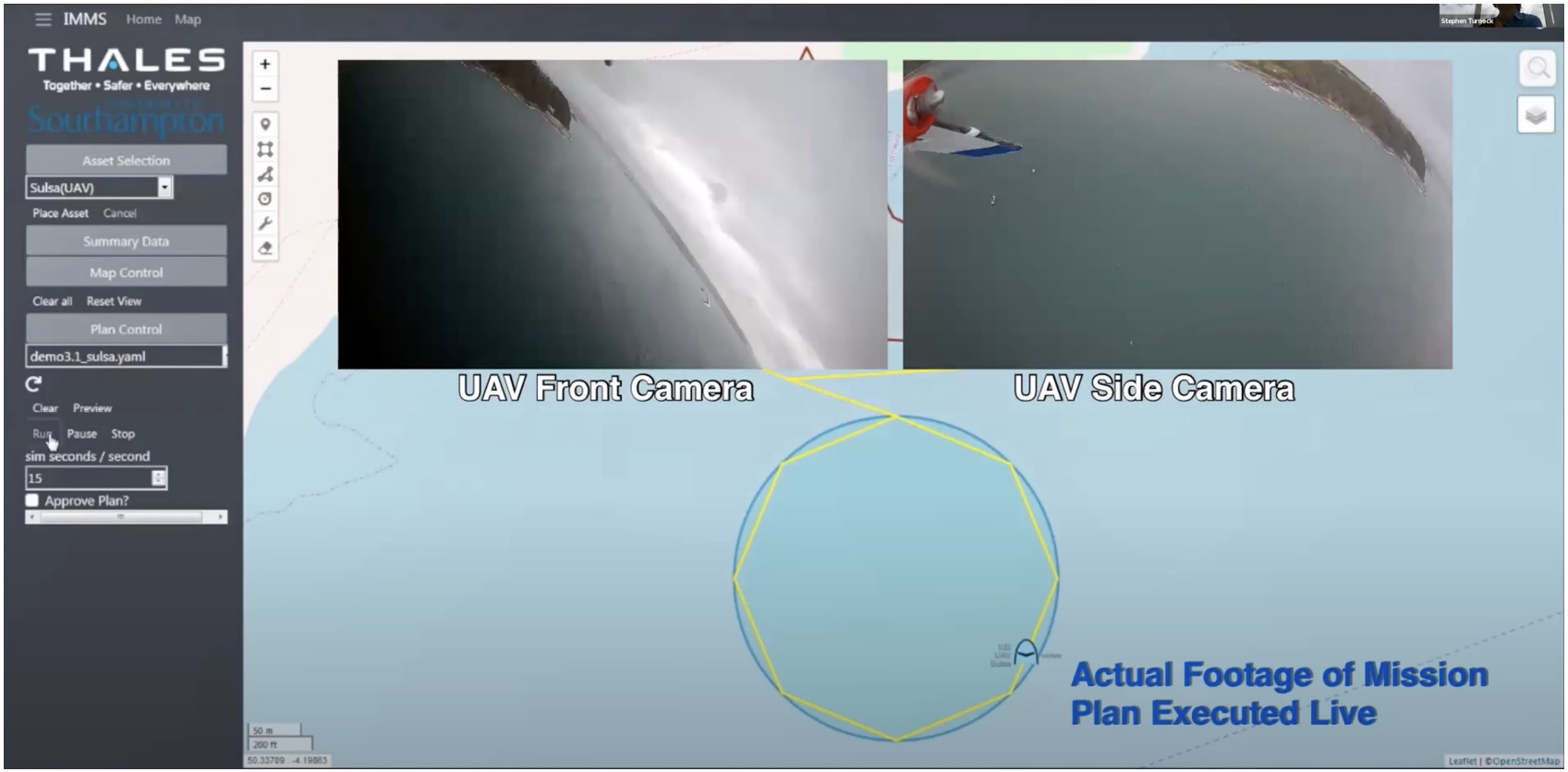
University of Southampton

## Route Validation



# Integrated Mission Management System

## UAV Cameras



University of Southampton

# Challenges and Opportunities

# Challenges and Opportunities

University of Southampton

- Not all safety properties can be specified/formalised
  - Combine with other techniques, e.g., metamorphic testing
- System complexity
  - Compositional verification
- Scalability of verification
  - Need abstraction
- Large Language Models (Challenge?/Opportunity?)

# EASA CoDANN

University of Southampton

- Concepts of Design Assurance for Neural Networks (CoDANN)

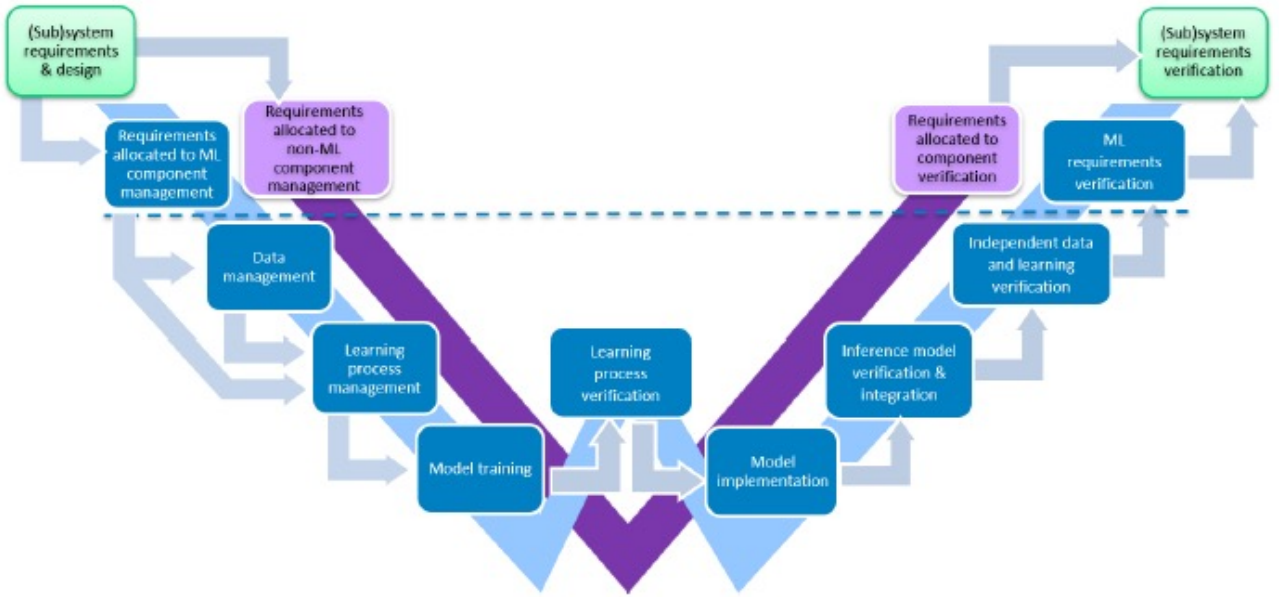



*Figure 8 — Global view of learning assurance W-shaped process, non-AI/ML component V-cycle process and safety assessment process*

# References I