Application of Falsification Methods on the UxAS System

Cumhur E. Tuncali, Georgios Fainekos
Arizona State University

Bardh Hoxha
Southern Illinois University
bhoxha@cs.siu.edu
www.bhoxha.com

Guohui Ding, Sriram Sankaranarayanan
University of Colorado Boulder

NASA Formal Methods 2018
Newport News, Virginia, USA, April 18

Summer Of Innovation 2017

AFRL
THE AIR FORCE RESEARCH LABORATORY
LEAD I DISCOVER I DEVELOP I DELIVER

WRIGHT BROTHERS INSTITUTE

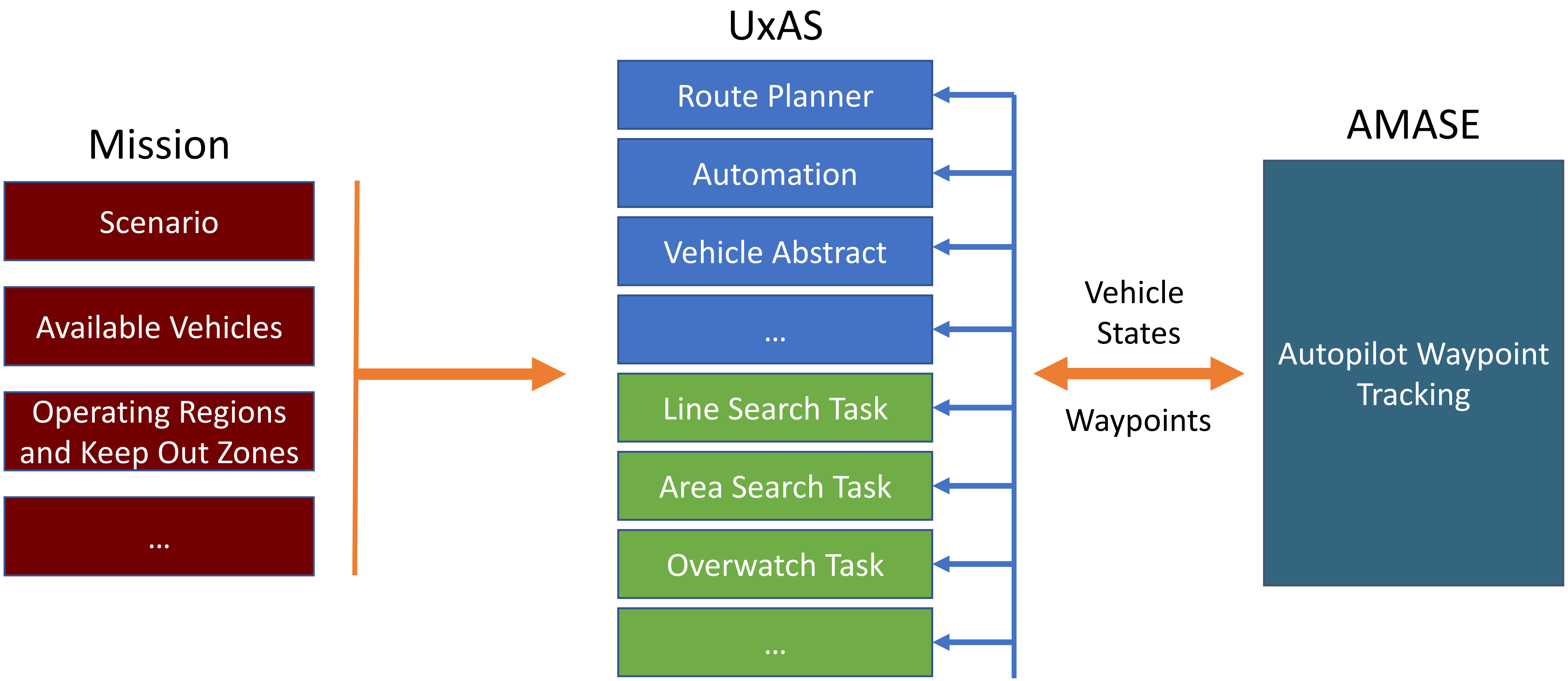
Participants from the industry, academia, and the government

Apply formal methods to the AFRLs UAV mission planning software UxAS

Requirement formalization • Formal architecture description • Methods for proving correct and safe behavior • Cyber-security considerations • Real-time scheduling/enforcement • Automated test generation • Argumentation and assurance cases • Run-time assurance • Hybrid systems analysis • Improvements in mission and task planning

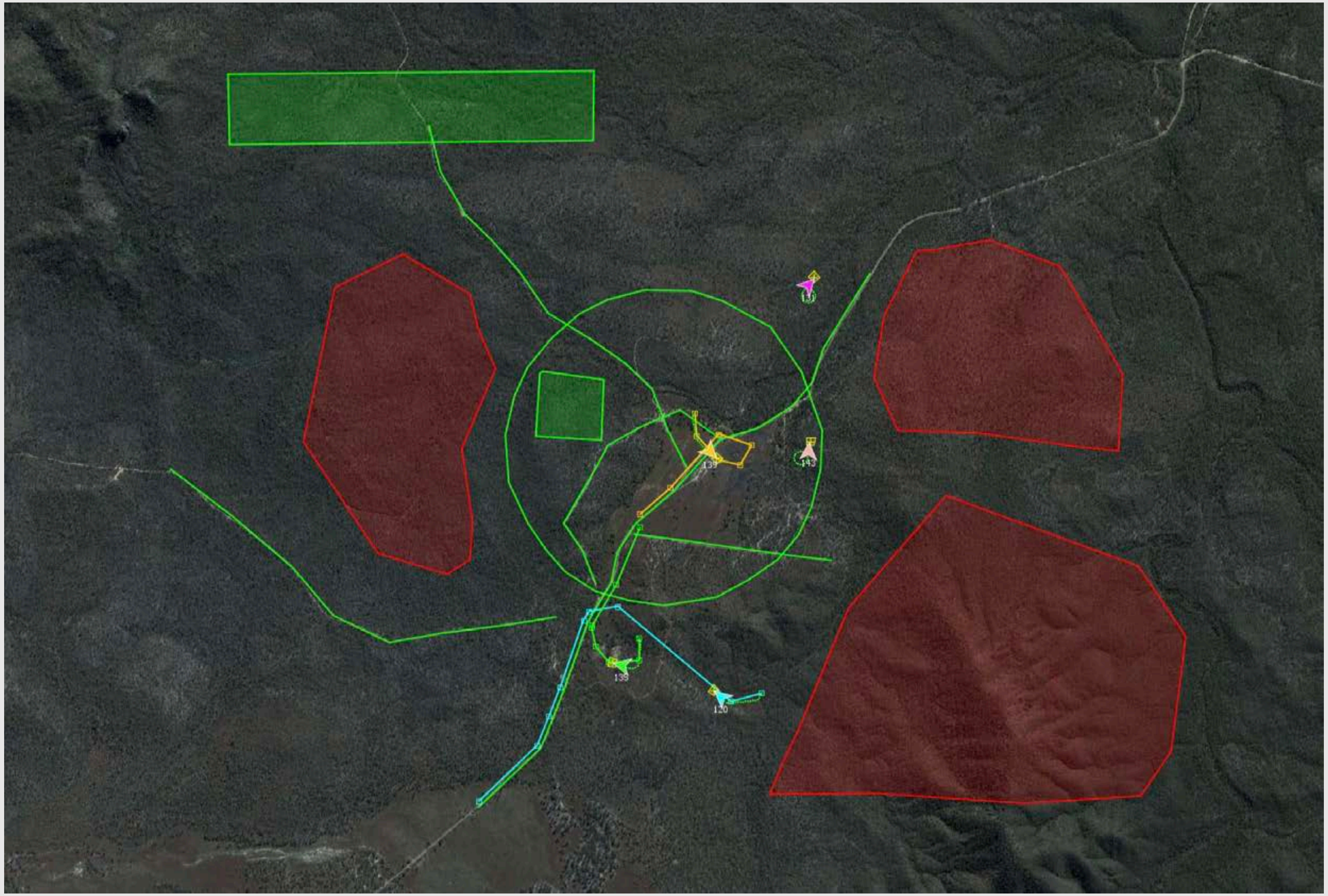
1. UxAS and AMASE

From Mission Scenarios to Simulation



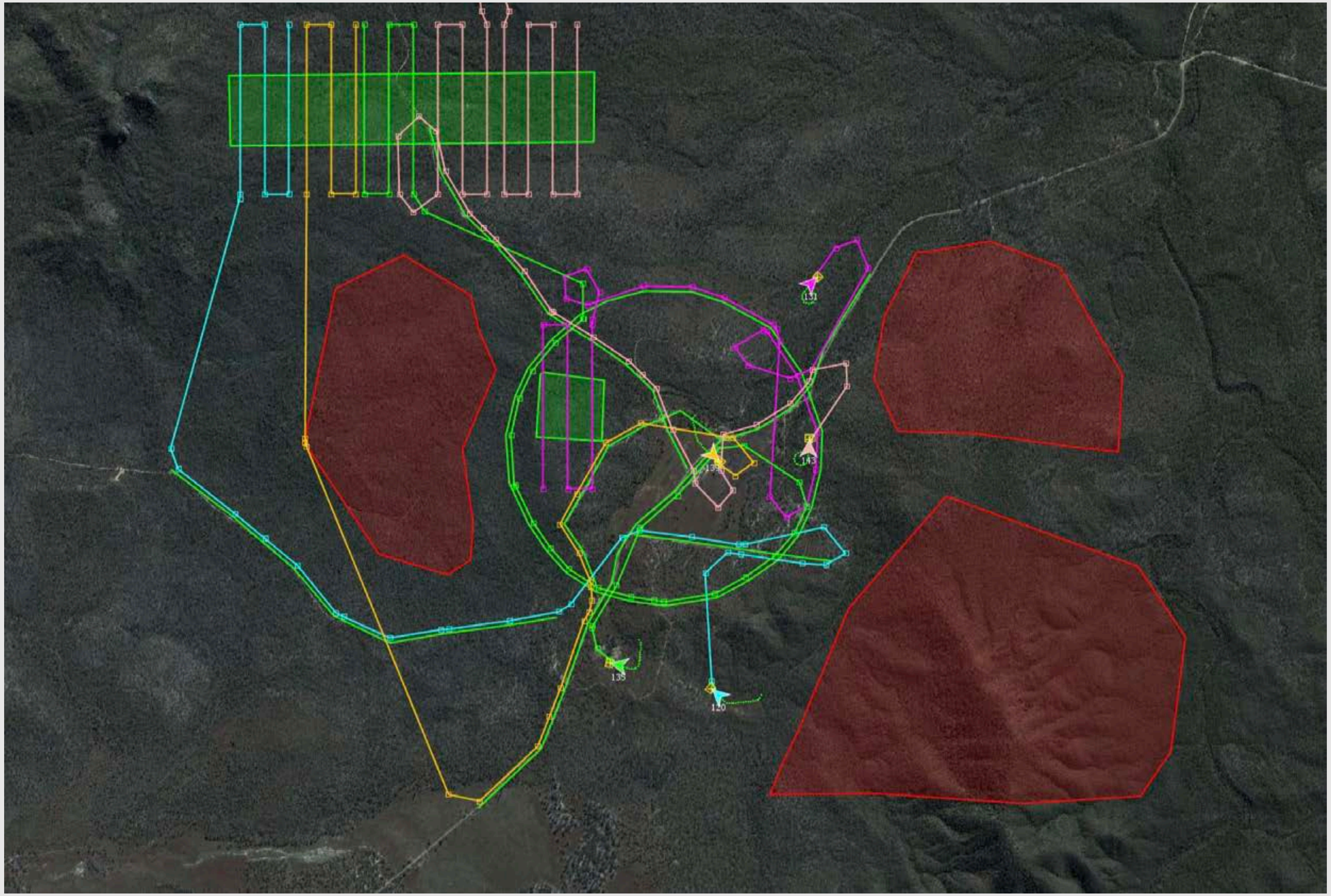
https://github.com/cmcghan/OpenUxAS
https://github.com/cmcghan/OpenAMASE

Tasks



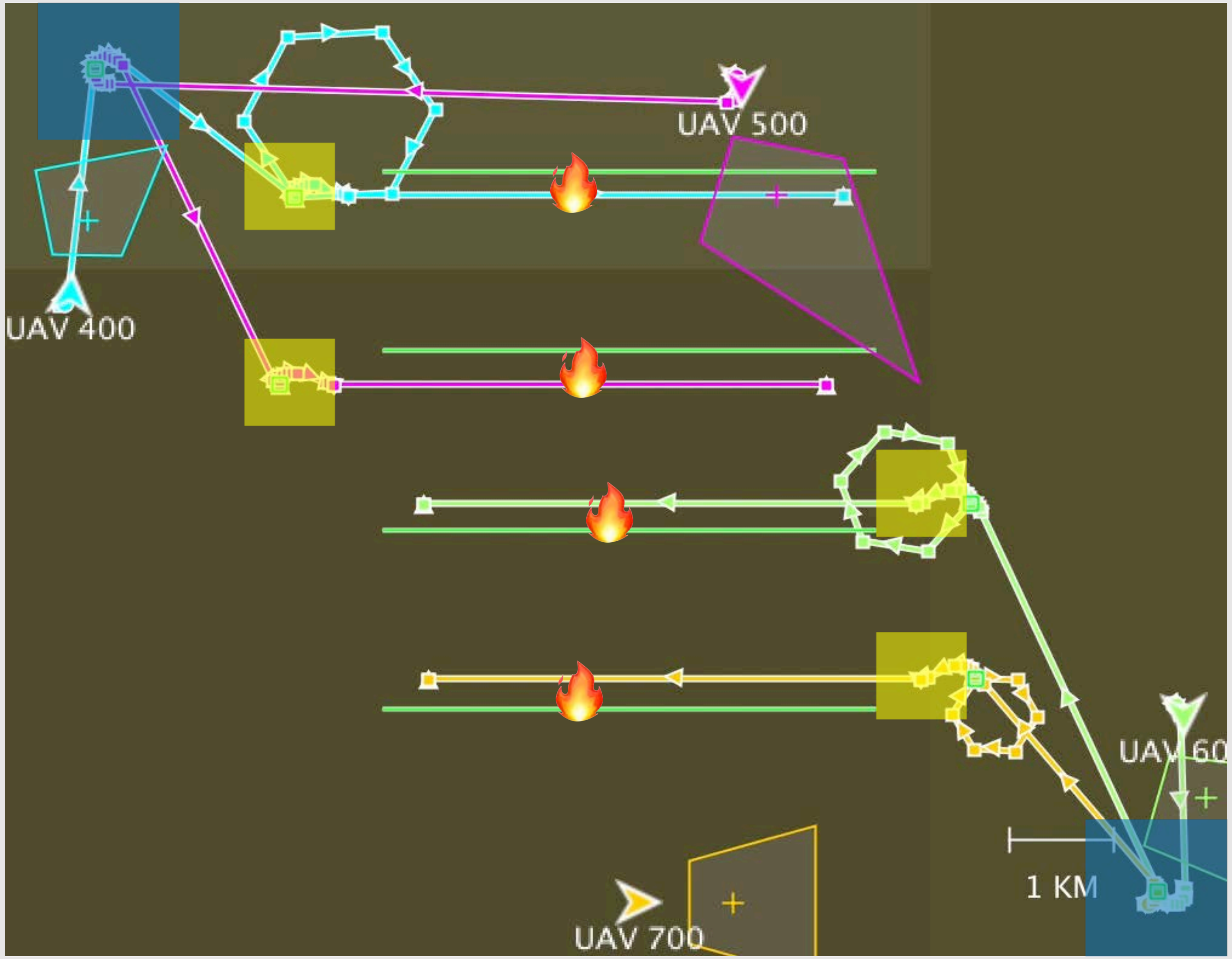
[Slide adopted/modified from D. Fisher, S5 2017]

Assignment



[Slide adopted/modified from D. Fisher, S5 2017]

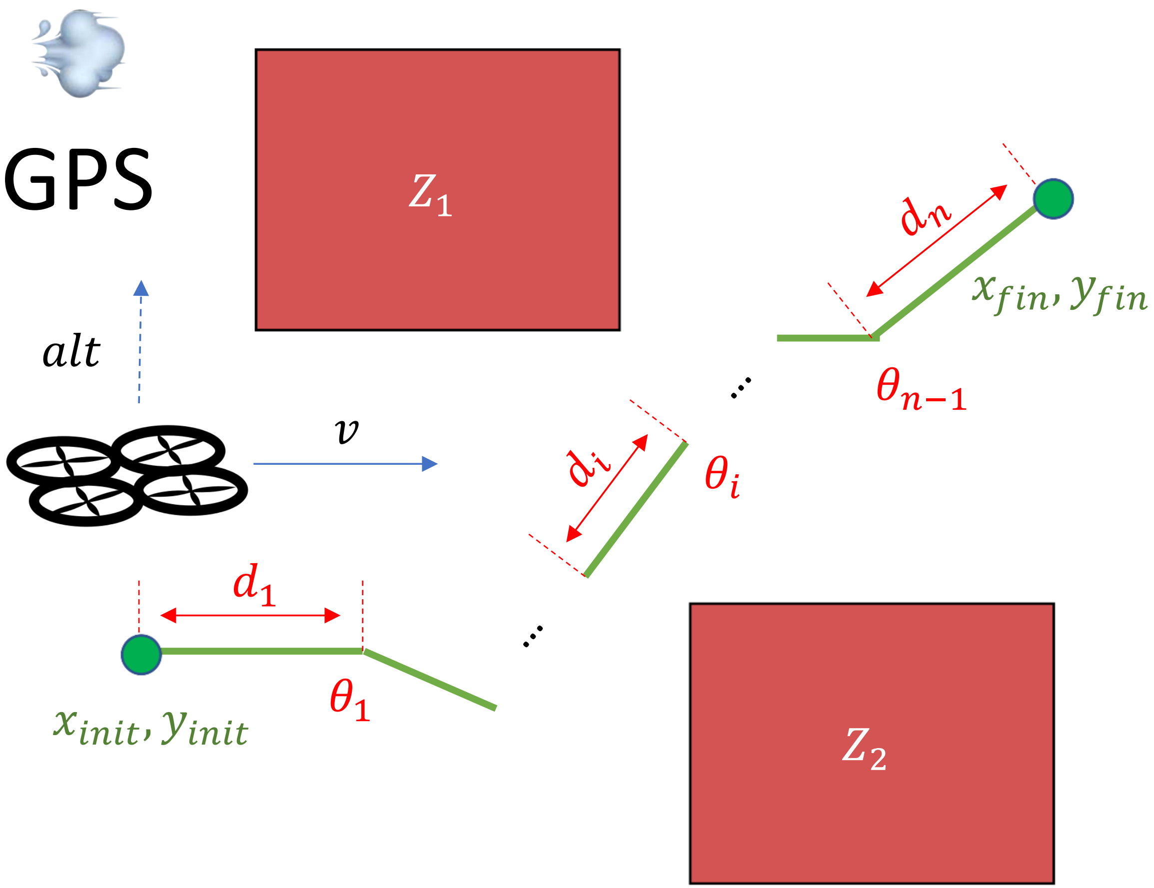
Synchronized Firefight



https://youtu.be/rgerTBylMsc

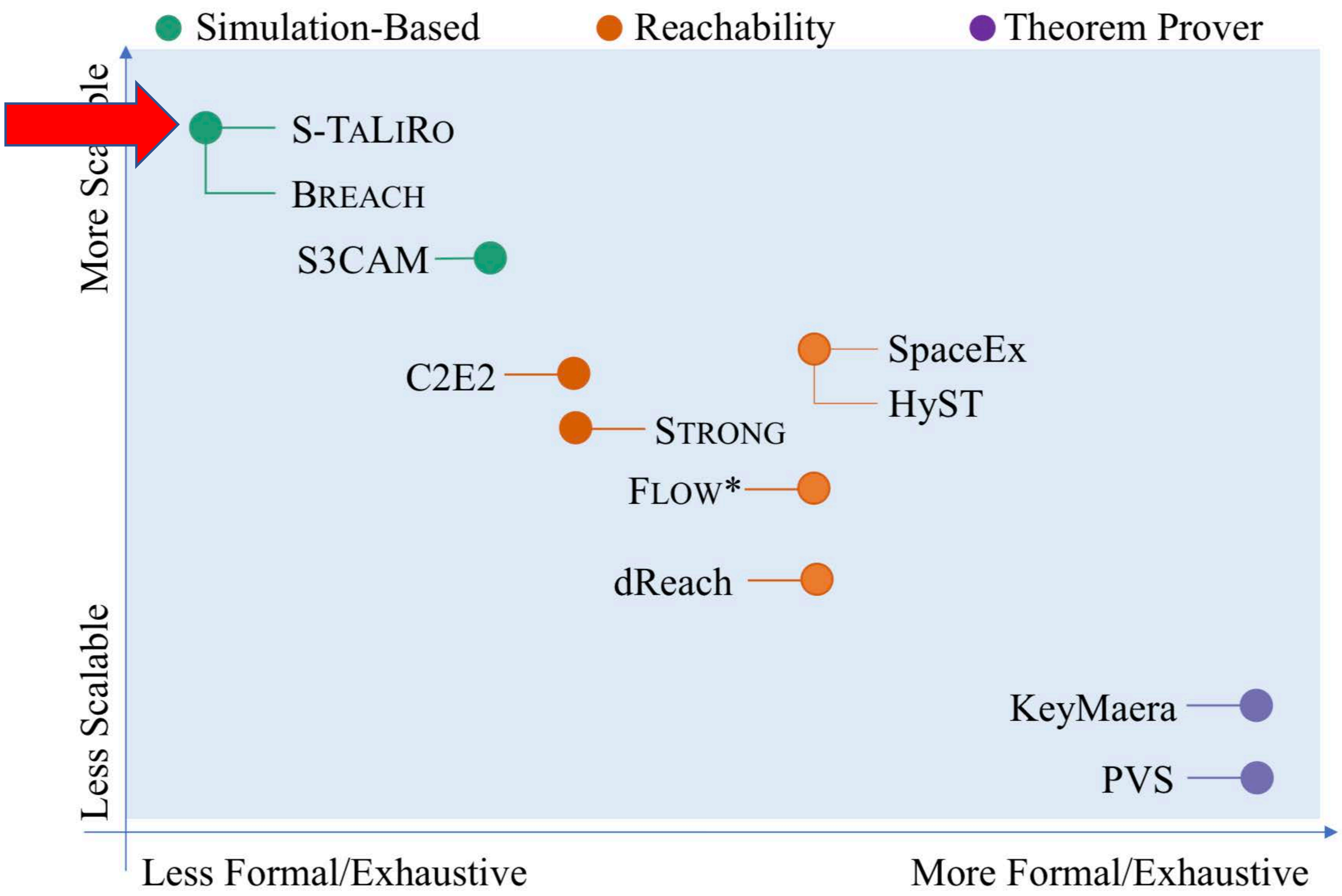
[ASU – SIU – VU] [ADHS2018]

Testing UxAS: Keep Out Zone Violations

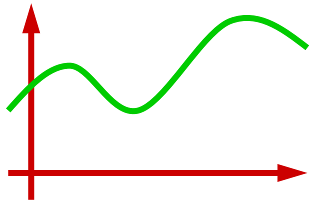


2. Robustness-Guided Testing

Methods and Tools

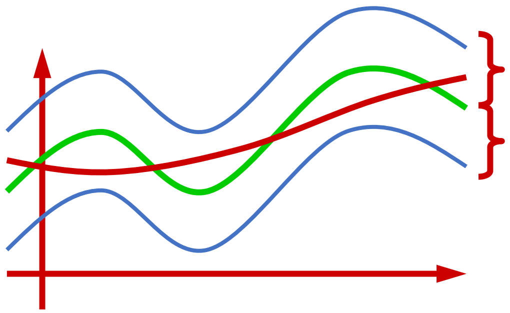


Falsification By Optimization



MTL ϕ

Robustness Metric
$\varepsilon \in \mathbb{R} \cup \{\pm\infty\}$



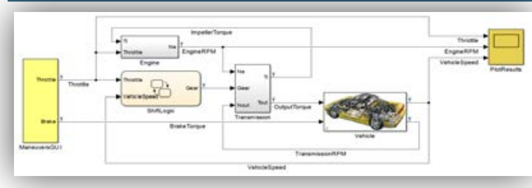
positive robustness → signal satisfies the formula

negative robustness → signal falsifies the formula

[Fainekos and Pappas, TCS]

System Σ

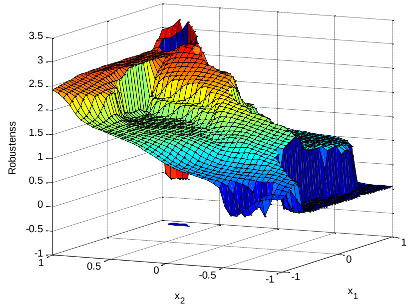
$y = \Delta(x_0, u)$ $\quad x_0 \in X_0$, $u \in U$



ϕ

Stochastic Optimizer

Next
$x_0 \in X_0$
$u \in U$



Minimum Robustness after termination condition met

[Abbas et al. TECS]

Metric Temporal Logic

- Propositional logic + Temporal Operators with timing intervals
- Interpreted over traces/trajectories
- Ex. $G_{[0,5]}p \wedge F_{[2.4]}b$:

"*always* from 0 to 5, p is true and *eventually* from 2 to 4, b is true"

Model

Simulink/Stateflow
User-defined functions

S-TALIRO

Stochastic Optimization Engine

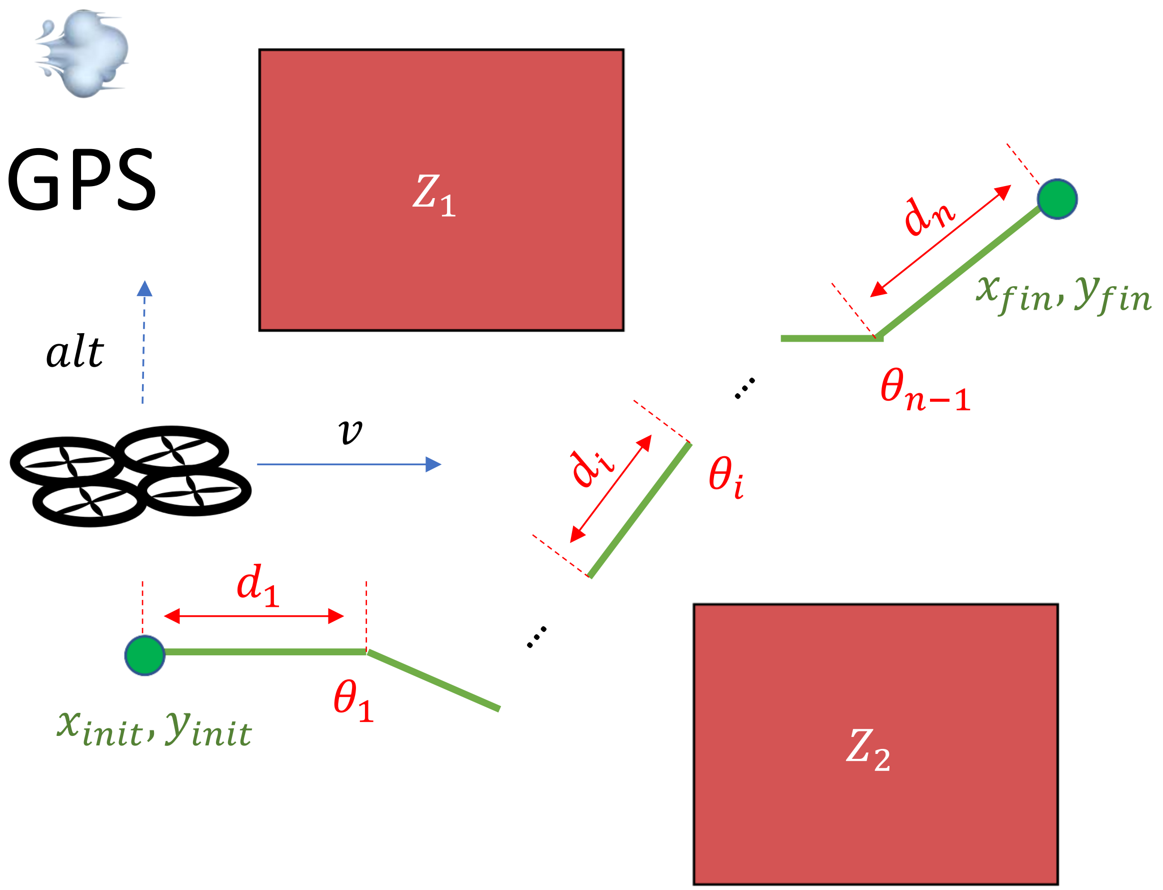
Simulated Annealing
Cross Entropy
Ant-colony
Gradient Descent
Flexible initial condition and input signal generation

Features

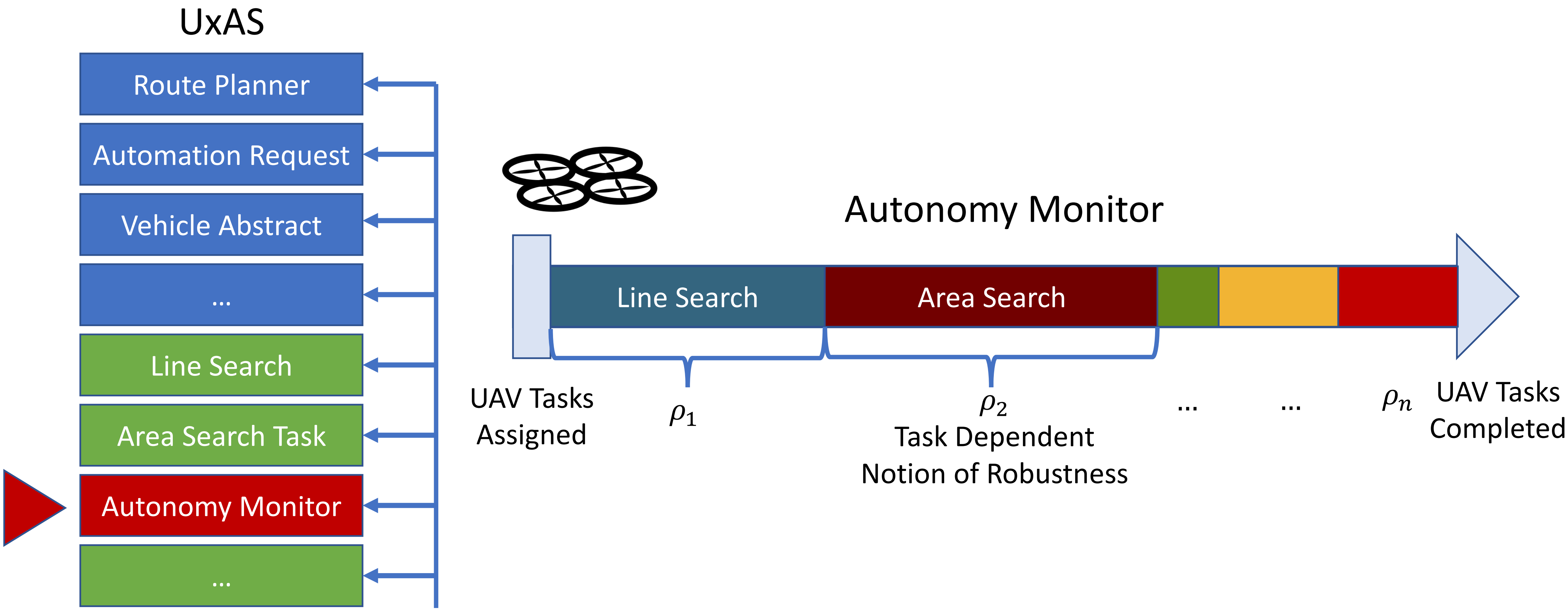
Falsification
Parameter Mining
Requirement Engineering with ViSpec
Runtime Verification
Conformance Testing
…

3. Testing UxAS

Keep Out Zones



Autonomy Monitors



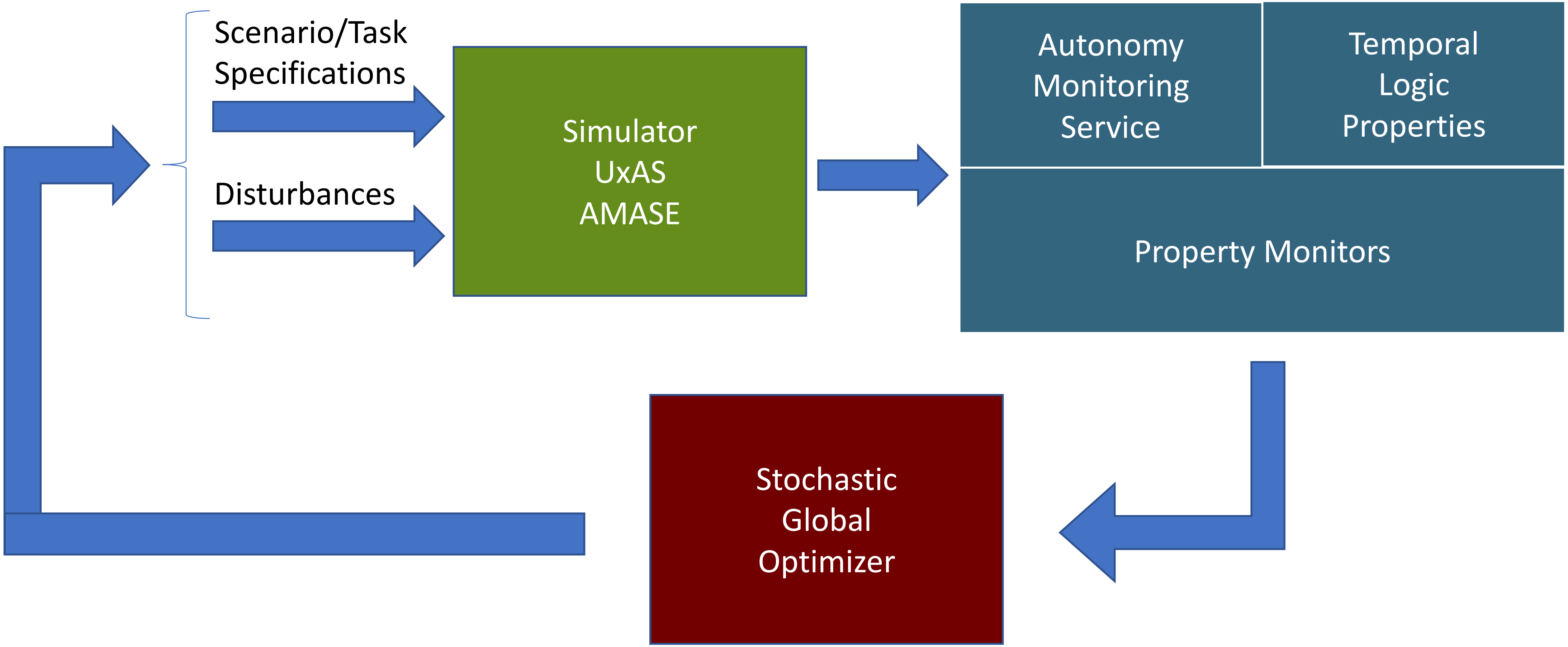
Testing UxAS with S-TaLiRo

Keep Out Zones: $$\phi_Z = \bigwedge_{i=1}^{n} G(r_i \rightarrow F_{[0,10]} \neg r_i)$$

Autonomy Monitors: $$\phi_M = \bigwedge_{i=1}^{k} M_k$$

Specification ϕ: $$\phi = \phi_Z \wedge \phi_M$$

Stochastic Optimization



Result: Falsification

https://youtu.be/tVB9TgwrCEc

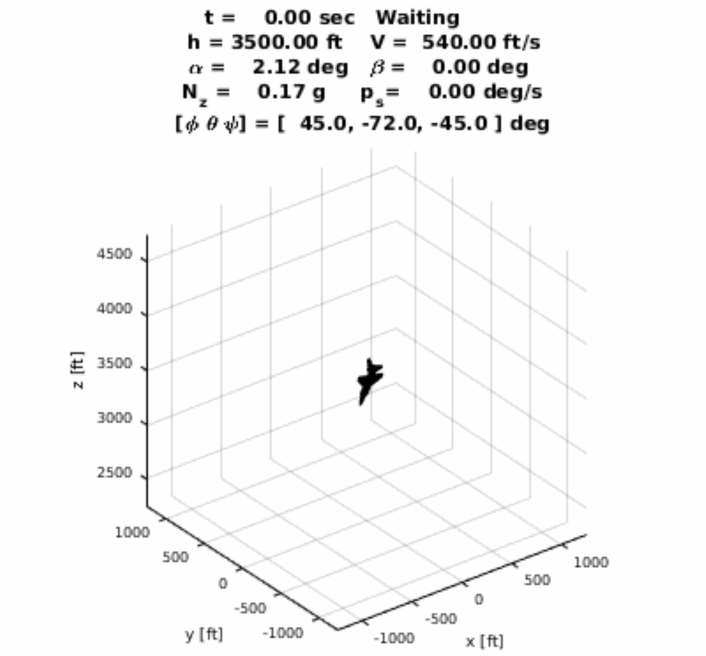
Future Work

1. Parameter Mining of MTL Specs [Hoxha et al. STTT]

What is the value of θ?

$$\phi_Z = \bigwedge_{i=1}^{n} G(r_i \rightarrow F_{[0,\theta]} \neg r_i)$$

2. More complex vehicle dynamics
Ex: F16 Aircraft Model
[Bak and Heidlauf]



github.com/pheidlauf/AeroBenchVV

Southern Illinois University
CARBONDALE

Acknowledgments

Cumhur E. Tuncali

Georgios Fainekos

Guohui Ding

Sriram Sankaranarayanan

ASU Arizona State University

University of Colorado Boulder

Sponsors:

AFRL THE AIR FORCE RESEARCH LABORATORY LEAD | DISCOVER | DEVELOP | DELIVER

WRIGHT BROTHERS INSTITUTE

AFRL:
- Derek Kingston
- Laura Humphrey

VU:
- Taylor Johnson
- Luan Viet Nguyen

UT Austin:
- Ufuk Topcu
- Mohammed Alshiekh

ASU:
- Adel Dokhanchi
- Shakiba Yaghoubi

Thank You
Questions?

MTL Survey

Test hypothesis that formal methods experts can write correct MTL specifications from NL

www.bit.ly/2HKsMQK