Iowa State University
of Science and Technology

CAREER: Theoretical Foundations of the UAS in the NAS Problem (Unmanned Aerial Systems in the National Air Space)

PI: Kristin Yvonne Rozier

In order to address the UAS in the NAS problem, we must take a holistic view, integrating advances in the state of the art from three intertwined perspectives: from on-board the UAS, from the environment (NAS), and from the underlying theory enabling their formal analysis.

Theoretical Advancements Enabling Formal Analysis

FuseIC3:
An Algorithm for Checking Large Design Spaces

The design of safety-critical systems often requires *design space exploration*: comparing several system models that differ in terms of design choices, capabilities, and implementations. Model checking can compare different models in such a set, however, it is continuously challenged by the state space explosion problem. Therefore, learning and reusing information from solving related models becomes very important for future checking efforts. For example, reusing variable ordering in BDD-based model checking leads to substantial performance improvement. FuseIC3 is a SAT-based algorithm for checking a set of models. FuseIC3 extends IC3 to minimize time spent in exploring the common state space between related models. Specifically, FuseIC3 accumulates artifacts from the sequence of over-approximated reachable states, called *frames*, from earlier runs when checking new models, albeit, after careful repair. It uses bidirectional reachability; forward reachability to repair frames, and IC3-type backward reachability to block predecessors to bad states.

Assumption 1

The different models in the design space are related, i.e., have overlapping reachable states.

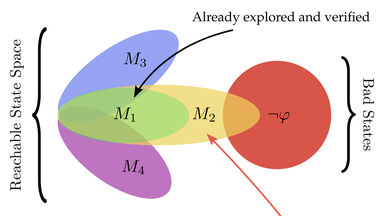
Assumption 2

The models in the design space are checked sequentially.

Intuition

Set of related models $\{M_1, M_2, M_3, M_4\}$

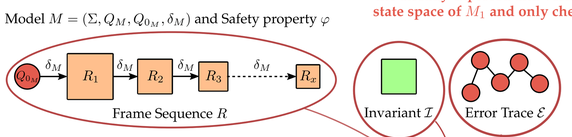
Safety property φ



1. Check M_1 with $\varphi \longrightarrow$ $M_1 \models \varphi$
2. Check M_2 with $\varphi \longrightarrow$

When checking M_2, FuseIC3 reuses the already explored and verified state space of M_1 and only checks

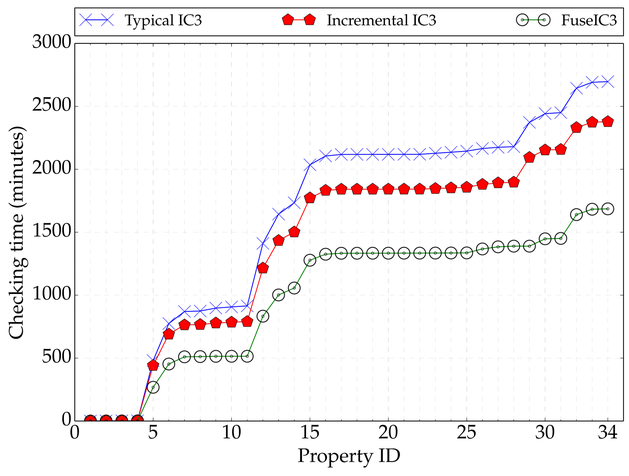
Model $M = (\Sigma, Q_M, Q_{0_M}, \delta_M)$ and Safety property φ



Model $N = (\Sigma, Q_N, Q_{0_N}, \delta_N)$ and Safety property φ

Information Reuse

Goal: Compute frame sequence S for model N



Model checking the **34 safety properties** over the **1,620 models** comprising the design space for **NASA's NextGen Automated Air Traffic Control design** with FuseIC3 is on-average 5.48x (median 1.75x) faster than checking each model individually, and up to 3.67x (median 1.72x) faster than the state-of-the-art incremental IC3 algorithm.

Laboratory for Temporal Logic

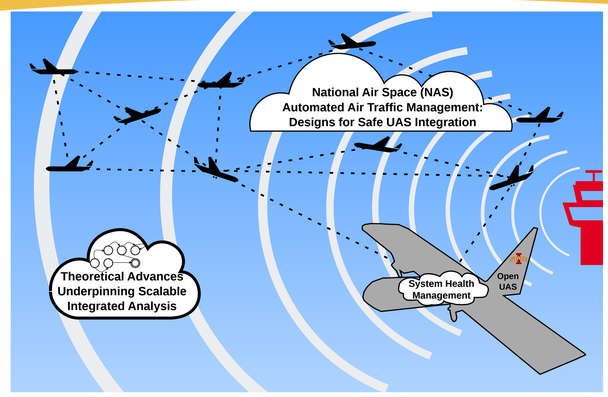


Figure 1: Overview of CAREER trajectory, a holistic view of the UAS in the NAS problem in three integrated thrusts: advancingon-board UAS capabilities, fleet-level reasoning, and theoreticalunderpinnings needed to advance the state of the art for the broader problem of UAS in the NAS. Research is facilitated by an educational open UAS design.

Overview

Due to increasing use by civil and federal authorities and vast commercial and amateur applications, Unmanned Aerial Systems (UAS) will be introduced into the National Air Space (NAS); the question is only how we can do this safely. NASA and the FAA are designing a new automated air traffic control system (NextGen) for all aircraft, manned or unmanned. New algorithms and tools need to be developed to enable computation of the complex questions inherent in designing such a system while proving adherence to rigorous safety standards. We must grow the tools of formal analysis to be able to address the UAS in the NAS problem, reason about UAS integration during the design phase of NextGen, and tie this design to on-board capabilities to provide runtime System Health Management (SHM), ensuring the safety of people and property. To address the UAS in the NAS problem, we take a holistic view, integrating advances in the state of the art from three intertwined perspectives: on-board the UAS, the environment (NAS), and the underlying theory enabling their formal analysis. Despite advances in formal methods, few are grounded in real-world avionics systems. There has been rapid development of UAS technologies yet few of them are formally mathematically rigorous to the degree needed for FAA safety-critical system certification. This CAREER proposal bridges that gap, integrating new UAS and air traffic control designs with advances in formal analysis. In the wealth of promising directions for autonomous UAS capabilities, this CAREER proposal fills a unique need, providing a direct synergy between on-board UAS SHM, the NAS environment in which they operate, and the theoretical foundations common to both of these.

Intellectual Merit

From the perspective of the NAS environment, this CAREER proposal will conduct a comparative analysis of NASA's designs for an automated NAS, model cutting-edge ideas for UAS integration, and address questions of scalability to include the relevant details of NextGen architectures via exploring options such as compositional verification, contract-based design, and new encodings of the system specifications. This includes new modeling algorithms and tools to enable analysis of the safety of UAS integration into the NAS, taking into account relationships with other aircraft, communications, and air traffic control. Advances from the UAS and the NAS perspectives will require theoretical research into scalable model checking and debugging of safety properties. Safety properties express the sentiment that "something bad does not happen" during any system execution; they represent the vast majority of the requirements for NextGen designs and all requirements we can monitor on-board a UAS for system heath management during runtime. From the UAS perspective, this CAREER proposal will develop new capabilities for runtime SHM that complies with current and expected future FAA regulations for UAS with a focus on increasing scalability, automation, and industrial utility over the current state of the art. Specification patterning and synthesis from physical UAS platforms will be essential for enabling real-world implementation of any SHM platform; this research will tackle these new frontiers in embedding health management capabilities on-board UAS.

Broader Impact

This work will help to build a safer NAS with increased capacity for UAS and create critical capabilities for SHM on-board UAS. Collaborations with aerospace system designers at NASA and tool designers at FBK will aid real-life utility and technology transfer. Current small UAS platforms are difficult to re-configure for missions requiring different sensor suites, have payload capacities that are too oddly shaped and cramped to facilitate the instrumentation required for real-time SHM, restrict internal airflow in a way that causes overheating, have battery lives that are too short to enable rigorous experimental field evaluation in complex environments, and are too restricted or expensive for use in academic environments. Broader impact will be achieved by involving undergraduate students in the design of an open-source, affordable, all-COTS and 3D-printable UAS, which will facilitate flight testing of this proposal's research advances. An open-UAS design for academia will be useful both for classroom demonstrations and as a research platform. Further impact will be achieved by using this UAS and the research it enables in interactive teaching experiences for K-12, undergraduate, and graduate students and in mentoring outreach specifically targeted at girls achieving in STEM subjects.

Publications

[1] Marco Gario, Alessandro Cimatti, Cristian Mattarei, Stefano Tonetta, and Kristin Yvonne Rozier. ``Model Checking at Scale: Automated Air Traffic Control Design Space Exploration.'' In *Proceedings of the 28th International Conference on Computer Aided Verification (CAV)*, Springer-Verlag, Toronto, Ontario, Canada, July 17-23, 2016. (acceptance rate <27%; received ``Artifact Evaluated Stamp'' (highest mark from Artifact Evaluation Review Committee: http://barghouthi.github.io/cav16-aec/); CORE A*-ranked conference)

[2] Kristin Yvonne Rozier. ``Specification: The Biggest Bottleneck in Formal Methods and Autonomy.'' In *Proceedings of the 8th Working Conference on Verified Software: Theories, Tools, and Experiments (VSTTE)*, Toronto, Canada, July 17--18, 2016. (Invited)

[3] Kristin Yvonne Rozier. "On the Evaluation and Comparison of Runtime Verication Tools for Hardware and Cyber-Physical Systems." In International Workshop on Competitions, Usability, Benchmarks, Evaluation, and Standardisation for Runtime Verication Tools (RV-CUBES), held in conjunction with the 17th International Conference on Runtime Verication (RV), Springer-Verlag, Seattle, Washington, USA, September 13--16, 2017.

[4] Kristin Yvonne Rozier, and Johann Schumann. "R2U2: Tool Overview." In International Workshop on Competitions, Usability, Benchmarks, Evaluation, and Standardisation for Runtime Verication Tools (RV-CUBES), held in conjunction with the 17th International Conference on Runtime Verication (RV), Springer-Verlag, Seattle, Washington, USA, September 13{16, 2017.

[5] Rohit Dureja and Kristin Yvonne Rozier. "FuseIC3: An Algorithm for Checking Large Design Spaces." In Formal Methods in Computer-Aided Design (FMCAD 2017), IEEE/ACM, Vienna, Austria, October 2--6, 2017. (acceptance rate 29%; CORE A-ranked conference)

[6] Rohit Dureja and Kristin Yvonne Rozier. "More Scalable LTL Model Checking via Discovering Design-Space Dependencies (D3)." (under submission)

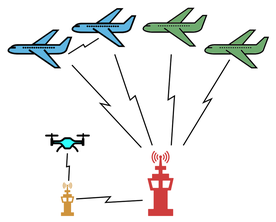
UAS in the NAS from the NAS Perspective

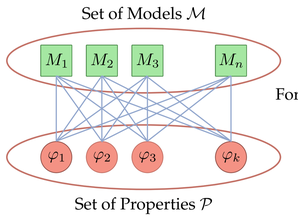
- Comparative symbolic analysis of designs
- Modeling for UAS-specific designs
- Specializing formal tools for aerospace analysis

Defining and Modeling the Design Space:

Name	Possible Values	Possible Size	Considered Values	Considered Size
SSEP TS SA	ATC, SELF, SATC	3	ATC, SELF, SATC	3
SSEP SS SA	ATC, SELF, SATC	3	ATC, SELF, SATC	3
Aircraft Mix	h4, 0i, h3, 1i, h2, 2i, h1, 3i, h0, 4i	5	h4, 0i, h3, 1i, h2, 2i, h1, 3i, h0, 4i	5
Burdening Rules	Undef, GSEP, SSEP	3	Undef, GSEP, SSEP	3
GSEPs to SSEPs Info	None, Current, Near, Mid, Far	5	Current, Far	2
SSEPs to ATC Info	None, Current, Near, Mid, Far	5	Far	1
Com Steps	1, 2, ...	2	1, 2	2
ACDR Implementations	Simple, Asymmetric, Non-Receptive	3	Simple, Asymmetric, Non-Receptive	3
TOTAL		20,250		1,620

Summary of possible and considered design dimensions comprising the design space for **NASA's NextGen Automated Air Traffic Control design.** The *design space* consists of **1,620 nuXmv models**.





For every $M \in \mathcal{M}$ and $\varphi \in \mathcal{P}$ check if $M \models \varphi$?

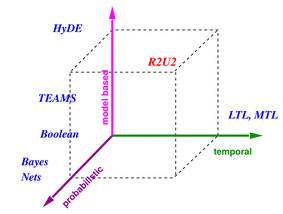
UAS in the NAS from the UAS Perspective

http://temporallogic.org/research/R2U2/

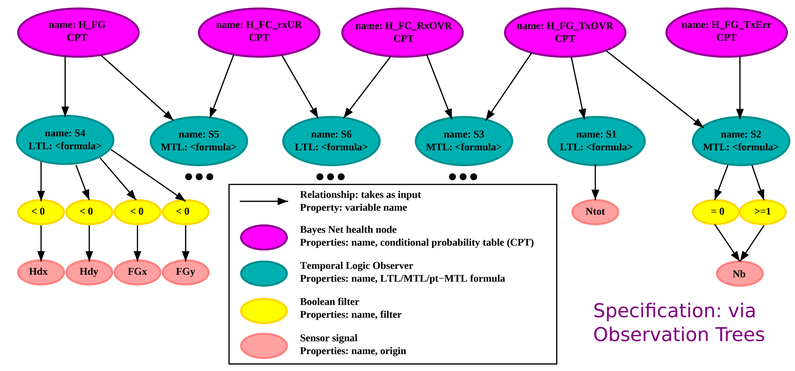
- Design for Runtime System Health Management (SHM)
- UAS specification patterns
- Synthesis of runtime requirements

R2U2 Observation Tree Specifications Combine:

1. **Signal Processing**: sensor readings
   * **Filtering**: processing of incoming data
   * **Discretization**: generation of Boolean outputs
   * **Prognostics**: predict component life
2. **TL Observers**: Efficient temporal reasoning
   (a) **Asynchronous**: output <t,{0,1}>
   (b) **Synchronous**: output <t, {0,1,?}>
   * **Logics**: MTL, pt-MTL, Mission-time LTL
   * **Variables**: Booleans (from system bus), sensor filter outputs
3. **Bayes Nets**: Efficient decision making
   * **Variables**: outputs of TL observers, sensor filters, Booleans
   * **Output**: most-likely status + probability

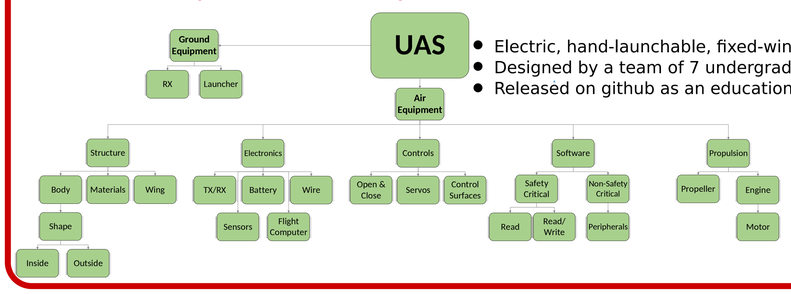


The on-board, real-time **R**ealizable, **R**esponsive, and **U**nobtrusive **U**nit (**R2U2**) provides SHM capabilities for a UAS in a certifiable way that complies with FAA regulations.



Specification: via Observation Trees

OpenUAS: An Open-Source, COTS/3D-Printed, Reconfigurable Testbed



- Electric, hand-launchable, fixed-wing, inexpensive
- Designed by a team of 7 undergraduate students
- Released on github as an educational project

L-R: Alexander Harpenau, Logan Gross, Madison Harrington, Kristin Yvonne Rozier (PI), Catherine Sener, Joshua Wallin, Abigail Gries. Not pictured: Mandy Kewitsch.

NSF