National Aeronautics and Space Administration

A Formal Model for Assurance Case Development and Efficient Testing

Principal Investigator: Ben Smith (397)
Martin Feather (5125) and Terry Huntsberger (347)
Program: Strategic Initiative

Project Objective:

Improve confidence in autonomous systems by developing a new assurance methodology based on a combination of Assurance Cases and High Throughput Testing.

Benefits to NASA and JPL:

Enable more effective and confident V&V of autonomy. Provide higher confidence in assurance claims and generate highly efficient test suites.

FY19 Results:

Evaluated the Autonomy Assurance approach against a mission case study, specifically the MEXEC autonomy experiment on the ASTERIA CubeSat.

- Applied AAC approach to the MEXEC experiment on ASTERIA
- The approach was effective at uncovering potential issues
- Assurance cases provided structure; STPA identified hazard; HTT provided efficient test suites.
- Evaluated approach in context of case study

Case Study: ASTERIA

ASTERIA: a CubeSat in Earth orbit

- Primary mission completed
- **Hosting further experiments**

Artist's impression of ASTERIA in orbit
Credit: NASA/JPL-Caltech

MEXEC (Multi-mission EXECutive)

- A "lightweight on-board planning and execution system that monitors spacecraft state to robustly respond to current conditions"
- **First in-flight use of MEXEC is on ASTERIA**

Software Assurance for Autonomy

Techniques:

- Assurance Cases to make the assurance argument
- Hazard Analyses appropriate to autonomy software
- Efficient testing to show hazards mitigated

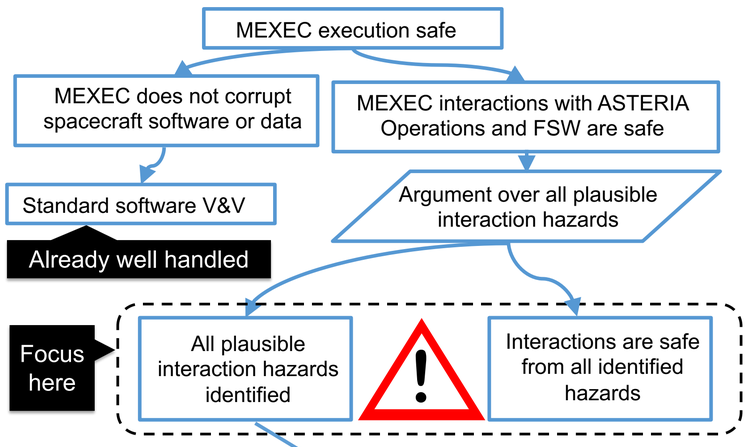
Objective

Assure that:

- **MEXEC will operate *correctly***
- **MEXEC will operate *safely***

Approach

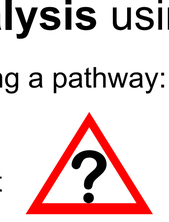
Assurance Case to guide focus



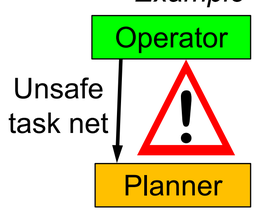
Hazard Analysis using STPA

For each action along a pathway:

- Wrong
- Missing
- Early or Late Start
- Early or Late End



Example



Unsafe control action	Scenario	Safety constraint
Operator's unsafe task net	Operator specifies task net with an unsafe execution	Check for unsafe execution paths before upload

Assurance Process

Six 1-hour meetings with ASTERIA + MEXEC team

Interim activities by SR&TD team: studies, analyses, documentation

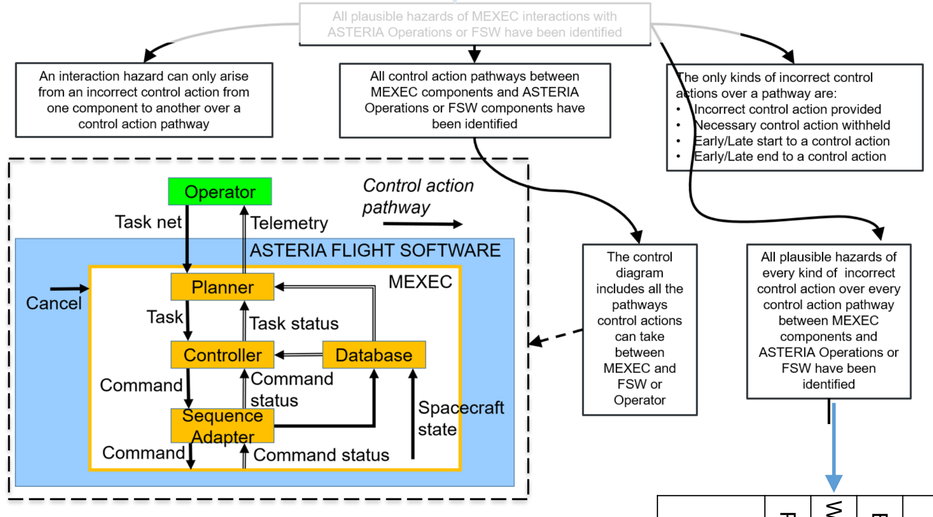
11/28	• Understand MEXEC and ASTERIA's MEXEC experiments • Draft of MEXEC-in-ASTERIA control diagram
12/6	• Identify control action discrepancies & consequences • Completed control diagram; beginning of STPA hazard analysis
12/17	• Confirm discrepancies, identify scenarios that would cause them • Assembled the majority of discrepancy-causing scenarios
1/17	• Confirm discrepancies & scenarios, identify safety constraints • Completed scenarios, started on safety constraints
2/10	• Start walk-through of entire STPA table of 26 scenarios+constraints • Started identification of means to meet the safety constraints
2/28	• Complete walk-through entire STPA table • Completed identification of means to meet safety constraints

Purpose
Outcome

Conclusions

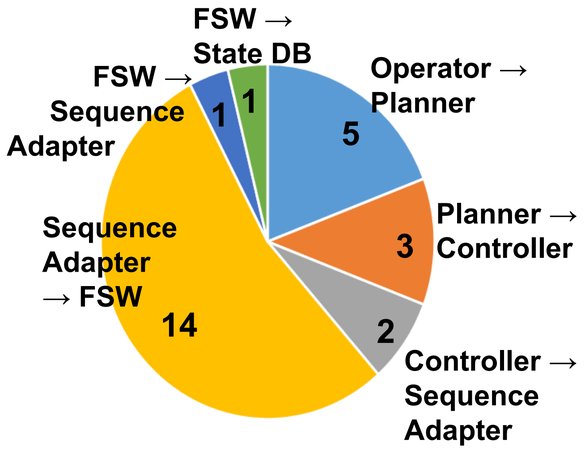
Assurance Case

- Improves confidence by systematically relating many forms of evidence—requirements, design, tests—into a comprehensive assurance argument.



Systematic analysis of 26 potential interactions

- Identified key hazards and mitigations
- Analysis effort compatible with scale of project



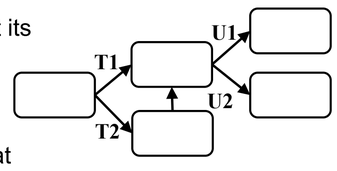
Module	Provides	Withholds	E/L Start	E/L End	Unsafe Control Action	Scenario	Safety Constraint / Control
Operator	P	-	-	-	Task net	Operator specifies task net with an unsafe execution.	Check for unsafe execution paths before upload

(25 more rows not shown)

Combinatorial/High-Throughput Testing

- Generates efficient test suites with known coverage of input space.
- Some component behaviors are best described by statecharts. HTT also generates efficient test suites that cover statechart interactions:

1. Add constraints to HTT to limit its test generation to valid paths through the statechart



2. Use HTT to find test paths that achieve desired coverage, e.g., pairwise combinations of T1/T2 and U1/U2

Publications:

B. Smith, M. Feather, T. Huntsberger, and R. Bocchino "Software Assurance of Autonomous Spacecraft Control", Reliability and Maintainability Symposium (RAMS) 2020; in final review.

PI/Task Mgr. Contact: Benjamin.D.Smith@jpl.nasa.gov, x35371

Poster No. RPC-138

National Aeronautics and Space Administration
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

www.nasa.gov