Technology and Tool Development to Support Safety and Mission Assurance

Ewen Denney and Ganesh Pai

ISRDS 2
SGT Technology Day, Houston, TX
Oct. 30, 2017
Summary

• How we are (and have been)
  – Defining the state of the art
    ▪ Foundational research in assurance technology
  – Pushing the state of the practice
    ▪ Application of research to enable application of emerging technologies
    ▪ Unmanned aircraft systems (UAS) missions
  – Developing supporting tools and technologies
    ▪ AdvoCATE (Assurance Case Automation Toolset)
    ▪ Proven application in unmanned aircraft systems (UAS) missions
Outline

- Motivation
- Assurance Cases
- Example
- Tool support
- Outlook
Outline

• Motivation

• Assurance Cases

• Example

• Tool Support

• Outlook
Research Motivation

• High-hazard industries are moving to *active safety management*
  – Safety management system (SMS) in aviation
  – Need to
    ▪ Unify reasoning about technical aspects of safety
    ▪ Support safety-related decision making

• *Goals-based* regulation is attractive for novel applications
  – When performance standards are absent
    ▪ Unmanned aircraft systems (UAS), Autonomous systems, …
  – Increases flexibility for regulated entity
  – Evidence-based assurance → *safety case*

Foundational research in languages, methodology, and automation support
Practical Motivation

• MIZOPEX (2013)
  – NASA Earth science mission with Sierra UAS off Alaska coast
  – Flight in combination of US National Airspace + Oceanic Airspace
  – Use of air defense radar for detect and avoid
  – Project needed FAA approval through submission of safety case – a detailed safety justification

• UTM (2016 – Ongoing)
  – Fleet of small UAS demonstrating low-altitude traffic management system
  – Flight in US national airspace, over sparsely populated land
  – Use of ground-based radar for detect and avoid
  – Project needed FAA approval through submission of safety case

Practical application of our research solutions in response to customer needs

Oct. 30 - 31, 2017 SGT Technology Day. Houston, TX
Outline

- Motivation
- Assurance Cases
- Example
- Tool support
- Outlook
‘A safety case is a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment’

- UK MOD, DS-00-56 Issue 4 (2007)

• Essentially, a safety risk management artifact
  – Other compatible definitions and guidance on content
    ▪ Based on application domain, standard, regulatory paradigm, etc.
      – FAA: Order 8900.1, FSIMS, vol. 16, UAS
      – NAVAIR: Instruction 13034.4
      – ICAO and Eurocontrol: Safety case development manual
      – Automotive: ISO 26262
      – FDA: Infusion pumps total product lifecycle guidance
Safety Case Content

- FAA (8900.1, FSIMS, vol. 16, UAS)
  - Core content
    - Environment (airspace system) description
    - System description and system change description
    - Airworthiness description of affected items
    - Aircraft capabilities and flight data
    - Accident / incident data
    - Pilot / crew roles and responsibilities
    - Hazard analysis and details of risk analysis, risk assessment, and risk control
    - Emergency and contingency procedures
  - Safety risk management plan
    - Hazard tracking and treatment
    - Safety performance monitoring
• In general,
  – Explicit statement of safety assurance objectives
  – Heterogeneous evidence
    ▪ Datasheets, design and analysis, verification, operational testing,…
  – Structured argument
    ▪ Capturing rationale why evidence supports the claims made

• Additionally,
  – Safety architecture providing a risk basis
  – Hazard log and hazard analyses
  – Evidence model
  – Monitoring and update
Assurance Cases

‘A documented body of evidence that provides a convincing and valid argument that a specified set of critical claims regarding a system’s properties are adequately justified for a given application in a given environment’

- MITRE (2005)

‘A reasoned and compelling argument, supported by a body of evidence, that a system, service, or organization, will operate as intended for a defined application, in a defined environment’

- Goal Structuring Notation Standard (2011)

‘A structured set of arguments and a body of evidence showing that an (information) system satisfies specific claims with respect to a given quality attribute’

- National Institute of Standards and Technology (2013)

Generalization of safety cases to other assurance properties: security, dependability, …
Safety Risk Management Approach

System Analysis
- Concept of Operations
- System/change description
- Regulations, ...

HazID
- Hazards
  Operational, functional, ...

Risk Analysis and Assessment
- Design target
- Risk scenarios, design targets, risk evaluation

Risk Control
- Threats / Causes / Initiating Events or States
- Prevention / Preventative Barriers
- Loss of Control State
- Accident / Loss / Harmful States or Events
- Recovery / Mitigative Barriers

Barrier Modeling – Abstract Safety Architecture

Assurance Rationale
(Structured Argument)
- Assurance claims, strategies, context, rationale, ...

Evidence Artifacts
- Design, Analysis, Verification Testing,

Operational Safety Assurance
(Monitoring and Update)
- Operational Evidence
  Verification of safety performance targets
  Assumption corroboration
- Hazard tracking, Precursors, ...

Safety Requirements Implementation
- Mitigations
  Safety requirements
  Barrier and Control functions

Operational Evidence
- Safety performance measures, monitors, ...

Event Log
- All identified hazards acceptably mitigated
- Assurance claims, strategies, context, rationale, ...

Evidence Artifacts
- Design, Analysis, Verification Testing,

Operational Safety Assurance
(Monitoring and Update)
- Operational Evidence
  Verification of safety performance targets
  Assumption corroboration
- Hazard tracking, Precursors, ...

Safety Requirements Implementation
- Mitigations
  Safety requirements
  Barrier and Control functions

Oct. 30 - 31, 2017
SGT Technology Day. Houston, TX

Motivation
- ASSURANCE CASES
- Example
- Tool Support
- Outlook

HazID
- Hazard
  Effect
  Severity
  Unidentified
  Initial Risk Level
  Hazard Control
  Residual Risk Level

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Effect</th>
<th>Severity</th>
<th>Unidentified</th>
<th>Initial Risk Level</th>
<th>Hazard Control</th>
<th>Residual Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>Low</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>H2</td>
<td>Stall</td>
<td>CFT</td>
<td>3</td>
<td>High</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>
This Talk

System Analysis
Concept of Operations,
System/change description,
Regulations, ...

HazID
Hazards
Operational, functional, ...

Risk Analysis
and Assessment

Hazards
Operational, functional, ...

Risk Control

Barrier Modeling – Abstract Safety Architecture

Evidence Artifacts
Design, Analysis, Verification, Testing,

Operational Safety Assurance
(Monitoring and Update)

Safety performance measures, monitors, ...

Mitigations
Safety requirements
Barrier and Control functions

Assurance claims, strategies, context, rationale, ...

Operational Evidence
Verification of safety performance targets
Assumption corroboration
Hazard tracking, Precursors, ...

Assurance Rationale
(Structured Argument)

Evidence Artifacts
Design, Analysis, Verification, Testing,

Operational Safety Assurance
(Monitoring and Update)

Safety performance measures, monitors, ...

Mitigations
Safety requirements
Barrier and Control functions

Assurance claims, strategies, context, rationale, ...

Operational Evidence
Verification of safety performance targets
Assumption corroboration
Hazard tracking, Precursors, ...

…”
Barrier Modeling

- Collection of barrier models providing a *risk basis*
  - Collection of all factors affecting risk
  - Model for risk qualification/quantification

---

**Event chain / accident trajectory**

- **Barrier compromise/breach**

---

**Figure:**
- **Prevention Barriers**
- **Recovery Barriers**
- **Hazard**
- **Loss of Control State**
- **Accident / Loss / Harmful States or Events**
- **Threats / Causes / Initiating Events or States**
Bow Tie Diagram (BTD)

- **Motivation**
- **ASSURANCE CASES**
- **Example**
- **Tool Support**
- **Outlook**

**Prevention Barrier**
- Prevention Control (2)
- Barrier Integrity: 0.999

**Hazard**
- Top Event:
  - IR: 5B (Low)
  - RR: 5E (Low)

**Threat**
- Likelihood: Probable

**Escalation Factor**

**Prevention Barrier**
- Prevention Control (1)
- Barrier Integrity: 0.99

**Consequence**
- IL: B (Probable)
- IS: 5 (Minimal)
- IRL: 5B (Low)
- RL: E (Extremely Improbable)
- RS: 5 (Minimal)
- RRL: 5E (Low)

**Recovery Barrier**
- Recovery Control
- Barrier Integrity: 0.99

**Escalation Factor Barrier**
- Escalation Factor Control
Rationale Capture

Safety / Dependability Claims

Chain of reasoning

Developed claims

Documentation and Details

Item of Evidence

Goal Structuring Notation (GSN)
Example Structured Argument

- Motivation
- ASSURANCE CASES
- Example
- Tool Support
- Outlook

G1
LiPo battery system failures are acceptably tolerated

C1
FMEA of LiPo Battery System

J1
LiPo battery system failures are characterized by the different failure modes

S1
Show toleration over all identified failure modes

S2
Usage of redundancy

G2
Battery system short circuits are eliminated

G3
Thermal runaway of the battery packs is mitigated

E1
Results of short circuit analysis

A1
Independence in failures of the primary and the spare battery systems
## Tiered Assurance Framework

<table>
<thead>
<tr>
<th>Tier</th>
<th>Core Assurance Concerns and Scope</th>
<th>Additional Assurance Qualities</th>
</tr>
</thead>
</table>
| Safety Objectives | **System Safety**  
  - Safe concept (safety designed-in)  
  - Safety in design  
  - Safety in implementation  
  - Safe transition into service  
  - Safety in operations  
  - TLOS / Acceptable level of risk  
  - Safe disposal  
  **Due diligence**  
  **Reduction of risk**  
  - ALARP  
  - SFAIRP  
  - ASARP  
  **Compliance with Aviation Regulations** | **Processes**  
  - Maturity, ...  
  **Input data**  
  - People;  
  - Competence, ...  
  **Method and Tools**  
  - Qualification, ...  
  **Safety management system**  
  - Lifecycle |
| 1 | **Overall Assurance**  
  All hazards / hazard risk statements, i.e., combination of hazardous situation, hazard release.  
  **All relevant consequences** across all BTDs.  
  **All applicable regulatory requirements** | **Coverage**  
  - Independence of threats;  
  **Effectiveness**; ... |
| 2 | **Profile of Risks**  
  For each hazard, all risk scenarios (consequences), e.g., midair collision, near midair collision, ground collision, ...  
  **Specific consequence**, e.g., midair collision  
  All causal chains, threats, and dangerous interactions across all hazards. | **Coverage (function, environment, interactions, scenarios, ...)**;  
  **Independence**; ... |
| 3 | **Individual Risks**  
  **Specific risk scenario**, i.e., causal chain of consequence, top event, threats, causes/precursors  
  **Applicable system of barriers / safety measures** | **Depth**;  
  **Independence**;  
  **Proactiveness**: Prevention vs. Recovery; ... |
| 4 | **Barriers**  
  Functional safety / fitness for purpose  
  Delivery of required service | **Depth**;  
  **Independence**;  
  **Common causes/modes**, ... |
| 5 | **Controls**  
  Functional safety / fitness for purpose  
  Delivery of required service | **Reliability and effectiveness**;  
  **Availability**; Functional / safety integrity;  
  **Resilience**; Fail safety; Data integrity;  
  **Verifiability**; ... |
Outline

- Motivation
- Assurance Cases
- Example
- Tool support
- Outlook
Factors Affecting UAS Safety

Diverse environment
- Populated / urban / built-up areas
- Uncontrolled / controlled airspace
- Low / high density airspace

Combination of operating modes
- Visual line of sight (VLOS)
- Beyond visual line of sight (BVLOS)
- Beyond radio line of sight (BRLOS)

Varying mission concepts
- Package delivery
- Surveillance
- Aerial inspection
- Mapping, …

Different configurations
- Airborne sensors (Lidar, sonar, FPV camera, Radar)
- Ground sensors (Radar)
- Multiple GCS, Roaming GCS, …

Varying access profiles
- Operating range
- Terminal airspace
- Transit (vertical / lateral)

Increasing complexity in mission and operations

Motivation
- Assurance cases
- EXAMPLE
- Tool Support
- Outlook

Oct. 30 - 31, 2017

SGT Technology Day. Houston, TX
UAS Safety Assurance

- **Scope of UAS safety**
  - Design assurance
  - Prior to deployment
  - Engineering evidence from development of fitness for purpose

- **Operational assurance**
  - Post-deployment, runtime evidence
  - Corroboration of expected safety performance

- Safety measures should be commensurate with the risk posed by the intended operations
  - Level of risk posed dictates safety measures employed and the extent of assurance provided

- Preferred form of safety justification (FAA Order 8900.1)
  - Safety Case
  - Assessment of Acceptable Level of Safety (ALoS)
**UTM / UAS Safety**

- **Notional CONOPS**
  - Surveillance Requirements
  - Avoidance maneuvers, Procedures, etc.
  - Justification and Rationale

- **Airspace / Threat Modeling**
- **Traceability from Hazards to Mitigation Barriers**

**Identified Hazards**
- Primary hazards:
  - PH1: NMAC with non-cooperative airborne entities
  - PH2: NMAC between UAs
  - PH3: Collision into ground structures / people / vehicles
  - PH4: Rapid onset of inclement weather
  - PH5: GPS signal outage
  - PH6: UAs exiting the QR
- Secondary hazards:
  - SH1: Lithium fire and/or explosion

**Contributory hazards**
- CH1: Loss of surveillance
- CH2: Loss of command and control (C2) links
- CH3: Loss of ground control station (GCS)
- CH4: Unrecoverable UA failures/malfunction in flight
- CH5: UA deviation from approved flight path and/or exiting the QR
- CH6: Human factors
- CH7: Loss of voice communication links

**Cross References**

**Mitigation Barriers**

**Primary and Secondary Hazards**

**Evidence Artifacts**
- Design, Analysis, Verification Testing,
  Assurance claims, strategies, context,
  rationale,

**Operational Safety Assurance**
- Monitoring and Update
- Safety performance measures, monitors,
  ...

**Operational Evidence**
- Verification of safety performance targets
- Assumption corroboration
- Hazard tracking, precursors,
  ...

**System Analysis**
- Concept of Operations, System/change description,
  Regulations,
  ...

**Barrier Modeling**
- Abstract Safety Architecture

**Safety Requirements**
- Implementation
- Safety requirements
- Barrier and control functions

**Risk Control**
- Risk scenarios, design targets, risk evaluation

**Risk Analysis and Assessment**
- Hazards, risk analysis, system functions

**Operational Safety Assurance**
- Monitoring and Update
- Safety performance measures, monitors,
  ...

**Safety Requirements Implementation**

**Hazard Analysis**
- Hazard Analysis Reports
  - Table 9, Table 10, Table 11, Table 12, Table 13, Table 14

**Motivation**
- Assurance cases
- Example
- Tool Support
- Outlook

Oct. 30 - 31, 2017

**SGT Technology Day, Houston, TX**
Risk Assessment

- Residual risk = Consequence probability \times severity
  - Probability of disjunction of all paths leading to consequence
    - Inclusion exclusion principle
  - Path probability = Joint probability of all events on path
    - Barrier *integrity*, threat event probability
  - Assumptions and data
<table>
<thead>
<tr>
<th>Tier</th>
<th>Core Assurance Concerns and Scope</th>
<th>Additional Assurance Qualities</th>
</tr>
</thead>
</table>
| Safety Objectives | System Safety  
- Safe concept (safety designed-in)  
- Safety in design  
- Safety in implementation  
- Safe transition into service  
- Safety in operations  
  - TLOS / Acceptable level of risk  
- Safe disposal | Due diligence  
Reduction of risk  
- ALARP  
- SFAIRP  
- ASARP | Compliance with Aviation Regulations  
Processes;  
- Maturity, ...  
Input data;  
People;  
- Competence, ...  
Method and Tools;  
- Qualification, ...  
Safety management system;  
Lifecycle |
| 1 | Overall Assurance  
All hazards / hazard risk statements, i.e., combination of hazardous situation, hazard release.  
All relevant consequences across all BTDs. | All applicable regulatory requirements |
| 2 | Profile of Risks  
For each hazard, all risk scenarios (consequences), e.g., midair collision, near midair collision, ground collision, ...  
Specific consequence, e.g., midair collision  
All causal chains, threats, and dangerous interactions across all hazards. | Coverage;  
Independence of threats;  
Effectiveness;  
.... |
| 3 | Individual Risks  
Specific risk scenario, i.e., causal chain of consequence, top event, threats, causes/precursors  
Applicable system of barriers / safety measures | Depth;  
Independence;  
Proactiveness: Prevention vs. Recovery;  
.... |
| 4 | Barriers  
Functional safety / fitness for purpose  
Delivery of required service | Depth;  
Independence;  
Common causes/modes, ... |
| 5 | Controls  
Functional safety / fitness for purpose  
Delivery of required service | Reliability and effectiveness;  
Availability; Functional / safety integrity;  
Resilience; Fail safety; Data integrity;  
Verifiability;  ... |
# Argument-based Assurance

<table>
<thead>
<tr>
<th>Tier</th>
<th>Core Assurance Concerns and Scope</th>
<th>Additional Assurance Qualities</th>
</tr>
</thead>
</table>
| Safety Objectives | **System Safety**  
- Safe concept (safety designed-in)  
- Safety in design  
- Safety in implementation  
- Safe transition into service  
- **Safety in operations**  
  - TLOS / Acceptable level of risk  
  - Safe disposal  
Due diligence  
Reduction of risk  
- ALARP  
- SFAIRP  
- ASARP | Compliance with Aviation Regulations  
Processes;  
- Maturity, ...  
Input data;  
People;  
- Competence, ...  
Method and Tools;  
- Qualification, ...  
Safety management system;  
Lifecycle |
| 1 | **Overall Assurance**  
All hazards / hazard risk statements, i.e., combination of hazardous situation, hazard release.  
All relevant consequences across all BTDs. | All applicable regulatory requirements  
Coverage;  
Independence of threats;  
Effectiveness;  
... |
| 2 | **Profile of Risks**  
For each hazard, all risk scenarios (consequences), e.g., midair collision, near midair collision, ground collision, ...  
**Specific consequence**, e.g., midair collision  
All causal chains, threats, and dangerous interactions across all hazards. | Coverage (function, environment, interactions, scenarios, ...);  
Independence;  
... |
| 3 | **Individual Risks**  
Specific risk scenario, i.e., causal chain of consequence, top event, threats, causes/precursors  
Applicable system of barriers / safety measures | Depth;  
Independence;  
Proactiveness: Prevention vs. Recovery;  
... |
| 4 | **Barriers**  
Functional safety / fitness for purpose  
Delivery of required service | Depth;  
Independence;  
Common causes/modes, ... |
| 5 | **Controls**  
Functional safety / fitness for purpose  
Delivery of required service | Reliability and effectiveness;  
Availability; Functional / safety integrity;  
Resilience; Fail safety; Data integrity;  
Verifiability; ... |
Barrier Fitness for Purpose

- Motivation
- Assurance Cases
- EXAMPLE
- Tool Support
- Outlook

C31 Ground-based surveillance system; LSTAR V2; radar, ADS-B ground receiver, integrated range safety display (RSD), visual observation (VO), and radar operator (RO)

C32 Ground-based surveillance detects and tracks airborne targets that are a credible threat to UA operations sufficiently early

C16 Definition of OR: A prismatic volume of class G airspace, whose base is a quadrilateral and height is 1200 ft, AGL.

Q2 Definition of credible threat: Air traffic of the size of a single engine Cessna (or larger), at the boundary of or within the threat volume (TV)

G18 Airborne targets in the radar cone of silence that pose a credible threat are detected and tracked

Use of visual surveillance

G16 Definition of sufficiently early: No less than 10s should elapse after detection for the intruder to arrive at the OR boundary, i.e., time to breaching OR boundary ≥ 10 seconds

G11 The RSD provides the situational picture of the airspace of operations and its surroundings, consistent with reality

Q3 LSTAR V2 radar system adequately detects and tracks noncooperative/cooperative intruder aircraft that can pose a credible threat

Q2 Use of onboard equipment

Q10 Use of onboard equipment

Q16 ADS-B ground receiver detects and tracks UA's operating within the OR

Q8 Reason over surveillance system organization

Q1 Definition of credible threat: Air traffic of the size of a single engine Cessna (or larger) at the boundary of or within the threat volume (TV)

Q2 Definition of sufficiently early: No less than 10s should elapse after detection for the intruder to arrive at the OR boundary, i.e., time to breaching OR boundary ≥ 10 seconds

Q3 Use of onboard equipment

Oct. 30 - 31, 2017

SGT Technology Day. Houston, TX
Barrier Fitness for Purpose

Ground-based surveillance can adequately detect and track intruders.

Detection and tracking in the radar cone of silence

Radar detection and tracking

Threats visible

Equipment

VFR / VMC

UA minimum equipment list

Range safety display functionality

Range safety display provides adequate situational picture

Display calibration

Pre-flight checks

• Motivation
• Assurance cases
• EXAMPLE
• Tool Support
• Outlook

Oct. 30 - 31, 2017

SGT Technology Day. Houston, TX

34
Outline

• Motivation
• Assurance Cases
• Example
• Tool support
• Outlook
Developing Structured Arguments

AdvoCATE

Assurance Case Automation Toolset (AdvoCATE)

Oct. 30 - 31, 2017
• Hazard analysis and safety requirements capture

• Structured arguments
  – Pattern specification and automated pattern instantiation
  – Integration of formal methods and formal tool-based evidence
  – Hierarchical and Modular refactoring
  – Argument queries and views
  – Argument verification
  – Metrics
  – Report generation

• Safety architectures
  – Bow tie modeling
  – Views
  – Transformations (event and barrier split / merge)

• Evidence management

• Safety, Mission Assurance, and Risk management (SMART) Dashboard
Outline

- Motivation
- Assurance Cases
- Example
- Tool support
- Outlook
• NASA adoption of safety case paradigm

• Promulgated by Office of Safety and Mission Assurance (OSMA)
  – Objective hierarchies (OHs)
    ▪ Decomposition of assurance objectives
      – Safety, reliability and maintainability, software assurance, range safety, …
  – Risk informed safety case (RISC)
    ▪ System Safety Handbook, vols. 1 & 2
    ▪ Elaborates
      – NASA acquisition process based on safety performance
      – Supplier requirements for justification of safety performance
      – Argumentation for rationale capture
      – Risk assessment and cost-benefit analysis for decision making
RISC and OHs

- Software assurance research program funding (FY18)
  - Retrospective characterization of assurance afforded by RISC and Software OH against an assurance baseline

  - Assurance baseline from NASA ARC BioSentinel mission
    - CFS/CFE
    - V&V artifacts
    - Current NASA assurance standards and guidelines

  - Mapping to RISC and OH to assurance artifacts
    - Analysis of potential gaps and assurance deficits

  - Tool support via AdvoCATE
Conclusions and Future Work

- Development of end-to-end assurance methodology and tool support
- Foundational research, informed by and corroborated in practical application
- Safety cases created were the first of their kind
  - MIZOPEX: First civil safety case to be approved
    - NASA Honor Award
  - UTM Safety Case: First civil safety case to be approved for using ground-based detect and avoid to conduct BVLOS operations in the NAS
Conclusions and Future Work

• Ongoing focus on design-time assurance
  – Artifacts and rationale from development, prior to release-into-service

• Outlook towards operational assurance through lifecycle
  – In-service safety performance monitoring

• Dashboard for stakeholder-specific assurance

• Current focus on safety
  – Expansion in focus to mission assurance
  – Expansion in application domain to spaceflight
    ▪ Initially robotic
    ▪ Eventually, human spaceflight

Looking for opportunities to infuse our technology into other SGT customer projects
The Assurance Case approach is being adopted in a number of safety-/mission-critical application domains in the U.S., e.g., medical devices, defense aviation, automotive systems, and, lately, civil aviation. This paradigm refocuses traditional, process-based approaches to assurance on demonstrating explicitly stated assurance goals, emphasizing the use of structured rationale, and concrete product-based evidence as the means for providing justified confidence that systems and software are fit for purpose in safely achieving mission objectives. NASA has also been embracing assurance cases through the concepts of Risk Informed Safety Cases (RISCs), as documented in the NASA System Safety Handbook, and Objective Hierarchies (OHs), as put forth by the Agency's Office of Safety and Mission Assurance (OSMA). This talk will give an overview of the work being performed by the SGT team located at NASA Ames Research Center, in developing technologies and tools to engineer and apply assurance cases in customer projects pertaining to aviation safety. We elaborate how our Assurance Case Automation Toolset (AdvoCATE) has not only extended the state-of-the-art in assurance case research, but also demonstrated its practical utility. We have successfully developed safety assurance cases for a number of Unmanned Aircraft Systems (UAS) operations, which underwent, and passed, scrutiny both by the aviation regulator, i.e., the FAA, as well as the applicable NASA boards for airworthiness and flight safety, flight readiness, and mission readiness. We discuss our efforts in expanding AdvoCATE capabilities to support RISCs and OHs under a project recently funded by OSMA under its Software Assurance Research Program. Finally, we speculate on the applicability of our innovations beyond aviation safety to such endeavors as robotic, and human spaceflight.