STPA Evaluation of Potential Conflicts Between Large Commercial Air Traffic and Small Uncrewed Aircraft Systems in the Terminal Airspace

Paul Stanley
Victor Arcos Barraquero
Overview

▪ Background
  ▪ Small UAS (sUAS) and emerging hazards
  ▪ Goals, scope and assumptions
  ▪ Literature review

▪ STPA Details and Observations
  ▪ Control Structure
  ▪ Overview of losses, hazards, UCAs, loss scenarios

▪ Enabling Communication of STPA Results
  ▪ Refinement and allocation of requirements to system components
  ▪ Validation & verification of requirements
  ▪ Distillation to key recommendations
Background

- FAA estimates ~1.5M recreational/hobby sUAS in use by 2025
  - Additional 800k commercial sUAS estimated
  - Similar growth expected worldwide

- Current mitigations to avoid collisions are primarily procedural
  - UAS Operator must be aware of and abide by limitations
  - Some built-in geofencing for sUAS

- Some related losses have already been realized
  - Disruptive UAS operations (or reported operations) near airports
  - Collisions and near-collisions with aircraft

Background

- **Goals**
  - Provide an analytical basis for engagement with other stakeholders
    - Traditional engagements
      - Airspace & Airport Regulators, Air Navigation Service Providers, Airlines, Airport Operators
    - Emerging stakeholders
      - Public Safety Agencies, UAS Flight Approval Providers, UAS Operators

- **Scope & Assumptions**
  - Small mass-produced UAS
    - Most common UAS in use
  - Current state
    - Technology, regulation, operations, etc.
  - Terminal Airspace
    - Commercial airplanes at low altitude
  - Single airport, airplane, and UAS
Literature Review

- Extensive research has shown that an sUAS collision could cause significant damage to airplane structure
  - FAA ASSURE UAS Airborne Collision Severity Evaluation
  - EASA Research Project: Vulnerability of Manned Aircraft to Drone Strikes

- “Detect and avoid” solutions for small UAS are in development
  - Electro-optical, radar, acoustic, cooperative (ACAS sXu)

- Emerging guidance to standardize response after detection of sUAS in restricted airspace near airports
  - EASA’s “Drone Incident Management at Aerodromes” manual

- Limited published research regarding potential causes of sUAS incursions into terminal airspace or effective mitigations to deter and prevent such incursions
STPA Details & Observations

- Eight Losses

- Nine Hazards
  - Pictorial depiction of hazards helped supplement text

- 94 Unsafe Control Actions

- 400+ Loss Scenarios
  - Important to maintain structured approach to loss scenarios
    - Focused on maintaining connection and terminology related to inputs/feedback, process model, control algorithm, and controlled process
    - Aids consistent balance of generality/specificity, particularly for human controllers
Refinement & Allocation of Requirements

- For each loss scenario, requirements identified and allocated to system elements
  - Engineering judgement needed to identify appropriate requirement and allocation
  - Supporting rationale recorded for each scenario to maintain traceability
  - A single requirement may help mitigate several loss scenarios
    - 80 requirements identified and allocated

- Alternate requirement proposals easily evaluated within STPA structure
Evaluation of System Requirements

- Requirements were evaluated through a lens of validation and verification maturity
- Evaluation of current state, with intent to identify potential gaps in the system
- Examples:
  - *(ATC-01)*: *ATC shall have accurate indications of airplane location and path*
    - Standardized two-way communication protocols with worldwide implementation
    - Millions of commercial flights have been conducted in accordance with the established protocols and standards
    - Automatic components are designed to established standards and have effective error detection and alerting
    - Backup procedures are well established and proven to be effective
    - Observation: Requirement is well validated and implementation well verified
  
  - *(ATC-11)*: *ATC shall be informed of sUAVs that could present an airspace conflict*
    - Related standards that could contribute (but not complete) implementation are emerging (e.g. Remote ID)
    - Implementations are not widespread or thoroughly validated
    - Backup procedures are not well defined
    - Observation: Validation of the requirement and verification of implementations are incomplete
Distillation to key recommendations

- Ten observations based on V&V evaluation
- Three key recommendations to support prioritized stakeholder engagement
- All fully traceable throughout STPA documentation
  - Enables evaluation of alternate hazard mitigation strategies
  - Enables potential further research
Conclusions

▪ STPA proved to be an effective analysis tool for this study
  ▪ Complex interactions managed through relatively high level of abstraction
    – Allowed analysis of interactions without necessarily understanding internal details of each element
    – Hardware, software, and human elements
  ▪ Generated insight and solid analytical basis for recommendations to stakeholders
  ▪ Pictorial depiction of hazards aided organization and communication

▪ Allocation and evaluation of requirements helped distill results
  ▪ Enabled focus on key recommendations
  ▪ Facilitates communication with stakeholders
  ▪ Full traceability maintained within STPA structure
    – Supports evaluation of alternate mitigation strategies
    – Supports further research expanding scope or increasing level of detail
    – Supports revision as “current state” evolves