A Case Study for Assured Containment

Kelly Hayhurst, Jeff Maddalon, Natasha Neogi, NASA-LaRC

Harry Verstynen, Whirlwind Engineering LLC.

2015 International Conference on Unmanned Aircraft Systems

Denver, CO

June 10, 2015

Outline

- Motivation
- Hazard Partitioning and Confined Operations
- Containment and Assurance Issues
  - Geofencing and Assurance
  - Assured Containment
- Agricultural Case Study for Assured Containment
- Summary

UAS in the NAS

- UAS are authorized to operate commercially in the US National Airspace System (NAS) on a case-by-case basis
  - Part 21.25, Part 21.17(b), Section 333 Exemption, COAs, proposed sUAS rule etc.
- FAA Pathfinder Program
  - News Gathering (CNN): Urban Area, Visual Line of Sight (VLOS)
  - Agricultural Survey (PrecisionHawk): Rural Area, Extended VLOS (EVLOS)
  - Railway Line Inspection (BNSF): Isolated Area, Beyond VLOS (BVLOS)
  - FAA suggests "*developing design standards tailored to a specific UAS application and proposed operating environment*" [11]
- Incremental approach to gaining type-design and airworthiness approval

Motivation for Approach

- Wish to enable airspace access for commercial applications whose vehicle platform is not ‘small’, and/or who may wish to operate BVLOS
- Several commercial application domains have been identified:
  - Precision Agriculture, Inspection/Surveillance, Mapping/Surveying
- Applications may present limited set of hazards compared to Conventionally Piloted Aircraft (CPA), enabling development of a streamlined set of requirements for their type certification basis
- This will enable a ‘starting’ certification basis for (Operational Concept, Platform) pair.

Our Approach

- Provide provisional means for confined commercial operations that are not single –vehicle or -case limited
  - Operations fall outside small UAS (sUAS) parameters
  - Vehicle being used does not meet CPA airworthiness standards
  - Large scale substitution of operational limits for airworthiness requirements
- *Assured Containment System*
  - Includes localization system independent of the autopilot system
  - acts to keep Unmanned Aircraft (UA) within given bounds
  - realized by smaller set of functions than in a typical autopilot →facilitates certification quality safety arguments
- May ease overall effort required to regulate some special purpose UAS, expediting market entry

Barriers to Assurance Arguments for Containment

- Inadequate understanding of effect of conventional Hazards on Airworthiness Standards for UAS
- Lack of Assurance Arguments for Commercial Off The Shelf Components (COTS) in safety critical roles
- Lack of Component (e.g., sensors, actuators) Quality Assurance Data
- Lack of relevant C2 Datalink Standards
  - Mission differences between Global Hawk and Ag operations
- Lack of Ground Based Equipment Standards
  - Ground Station, Ground Based Detect and Avoid, etc.
- Lack of Ground Crew/Operator procedures
- Lack of guidance for certifying infrastructure systems

HAZARD PARTITIONING AND CONFINED OPERATIONS

Hazards for UAS Under Confined Operations

- Hazard space for CPA (on which current regulation is based):
  - Hazards to people onboard aircraft
  - Hazards to people on other aircraft
  - Hazards to people and property on ground
- Lack of people onboard removes significant portion of CPA hazard space
- Rote removal of corresponding regulation may act to expose secondary hazards
- Must account for *coupling* between hazards

Hazard Partitioning

- CPA has inherent coupling of mitigations for onboard and ground hazards
  - Mitigations for people on board also act to protect people on ground (e.g., hull integrity)
- Hazard partitioning provides potential means to analyze and mitigate groupings of hazards independently of one another
- Mitigating common hazards over entire partitions requires less effort than individually mitigating each hazard
  - e.g., operational restrictions for crop dusting

Confined Operations

- Further partition ground hazards with respect to operational area
  - Hazards to people on the ground within operational area
  - Hazards to people on ground outside operational area
- Can use different strategies to mitigate these partitions if:
  - Partition is maintained (no explicit coupling across these hazard partitions)
  - Any implicit coupling across partitions is managed by mitigation technique
- If partition scheme decouples hazards → Enable development of mitigations whose impact can be mapped onto relevant hazards
- Eases complexity of assurance argument

CONTAINMENT AND ASSURANCE ISSUES

Containment Schemes: Class U Airspace [1]

- Confined operations in well-defined airspace volumes designated for particular tasks
- Class U: Surface to 500 feet above ground level below existing Class G airspace
  - mechanisms to enforce this partition are airspace rules and/or operational procedures
- Sub-classifications
  - property ownership (private or public)
  - type (rural, suburban, and urban)
- Certified geofence required to keep UA in designated operating area

Containment Schemes: Geofencing

- Geofence algorithm detects when UA has transgressed preset boundary (or if transgression is imminent)
  - alert pilot or issue control command
- This requires a reliable and fault tolerant algorithm [2-4]
- Implementation must consider:
  - computational platform upon which algorithm is implemented
  - underlying operating system [5]
  - communications architecture [6-7]
- Often implemented through autopilot

Geofences and Assurance Arguments

- For assurance purposes, no single point of failure between autopilot and geofence
- Assurance argument requires independence
  - Cannot have common dependence on the global positioning system (GPS) and inertial measurement unit (IMU) for navigation
  - Cannot use same processor as for autopilot
  - Cannot use same actuators to implement resolution strategy
  - Must consider switching logic and timing (common clocks)

Assured Containment System

- Assured containment system acts to keep the UA within given bounds with a *certification quality safety argument*
- Safety argument must demonstrate that the UA will remain in a specified area in the presence of common vehicle, position sensing, autopilot, sensor and actuator failures
- Independence of assured containment system from UA primary avionics enables certification ease

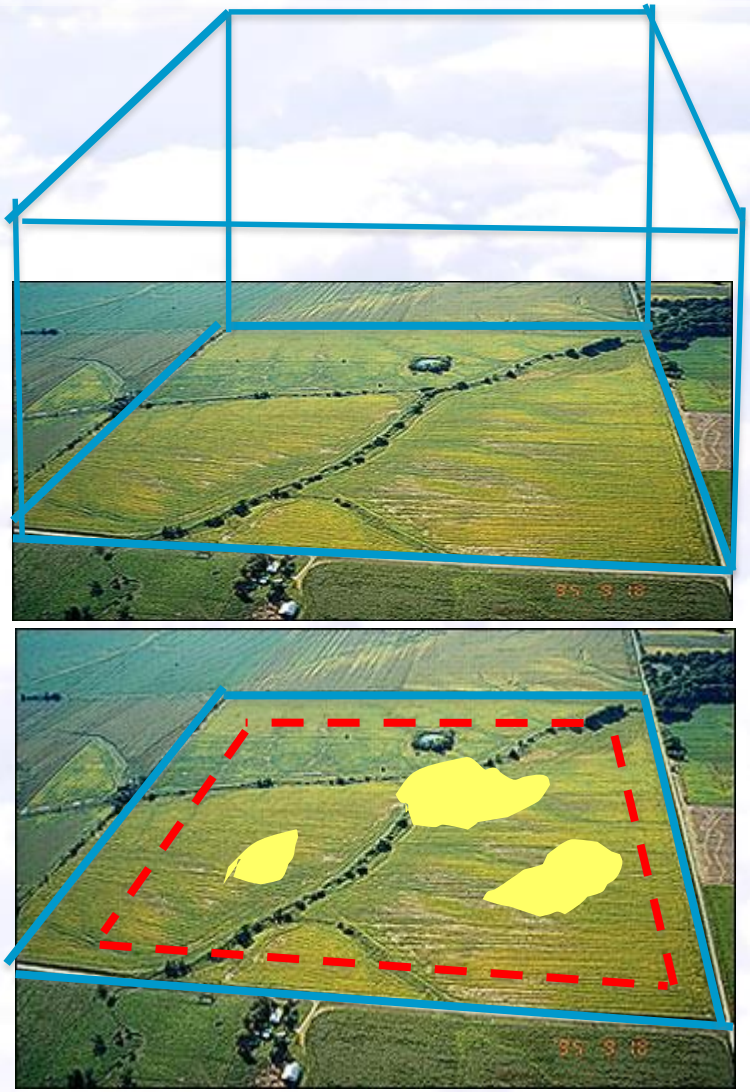
Assured Containment: Components

- Containment system consists of:
  - sensors that determine the vehicle state information,
  - decision logic to detect an anticipated breach of containment,
  - means to control the breach of containment (e.g., actuators for flight termination)
  - Also includes: operational procedures, human-machine interfaces, and software required to set and validate the containment area
- Assurance Argument consists of the following premises:
  - containment system will be independent of the UA autopilot system as well as other avionics,
  - containment system will have an independent means by which to ensure the geospatial containment of the UA in the event of onboard autopilot, sensor and servomotor connection failures.
    - e.g., independent servos for flight termination, independent processor for decision logic, GPS-independent means of determining position etc.
  - no single failure in the UA's autopilot systems results in an automatic failure of the containment system
- Limited functionality may aid in certification

AGRICULTURAL CASE STUDY FOR ASSURED CONTAINMENT

Define Concept of Operations [8]

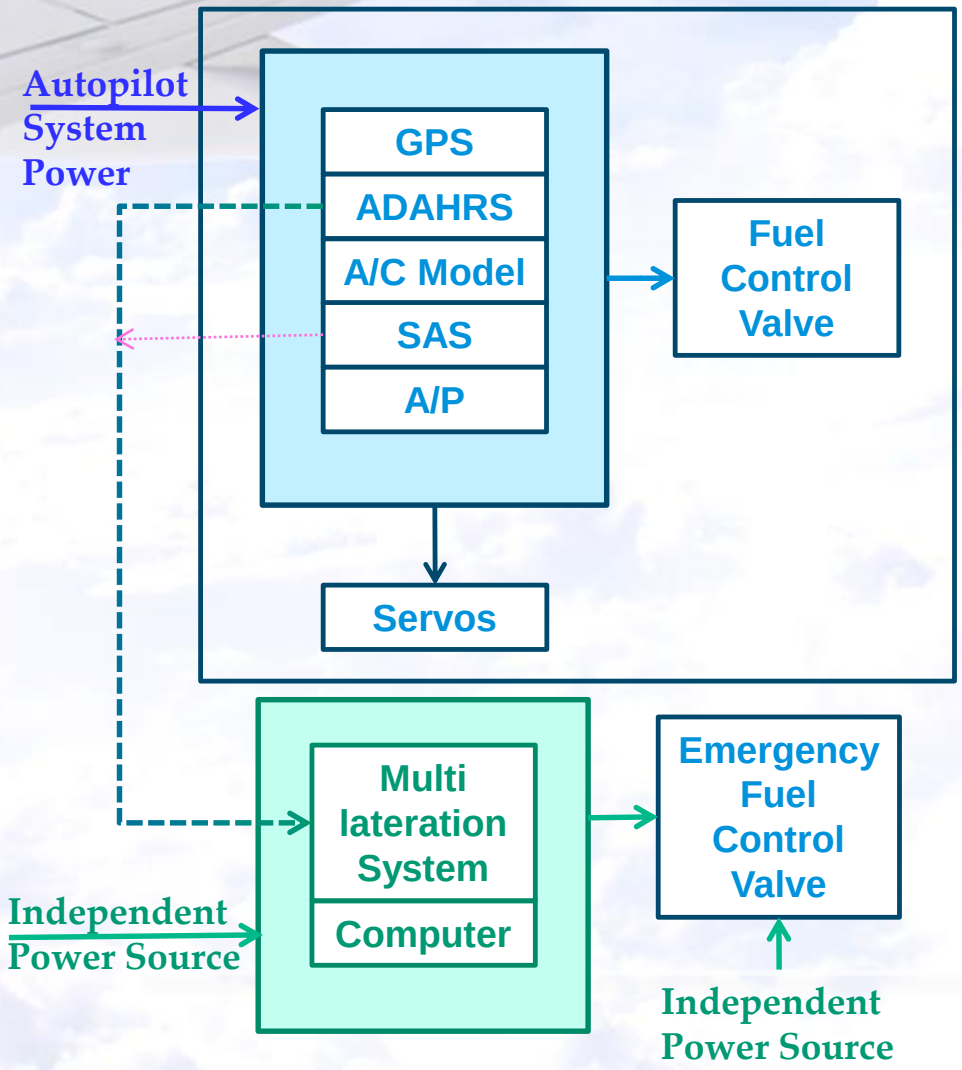
- Clearly define:
  - Operational Scenarios
  - Operational Environment
  - Assumptions
  - Functional Performance
  - Anticipated Safety Considerations
- Also Relevant: economic considerations



Vehicle Selection [9]

- Relevant Vehicle characteristics
  - e.g., range, endurance, speed
- Relevant Safety Concerns
  - Autorotative capability, etc.
- Economic Considerations

Architecture



- Assured Containment uses multi-lateration techniques [10]
  - GPS-degraded environments
- Position determined by separate onboard computer that operates independently of the primary navigation system
- Computer determines distance using ground-based sensors, compares to pre-loaded boundary
- Position and speed indicate boundary will be exceeded→ Signal generated to close emergency fuel control valve, forcing the UA to the ground

Hazard Analysis

- For the clearly defined Conops, an Operational Hazard Assessment (in conjunction with the selected vehicle) will yield relevant hazards
  - Evaluate with respect to severity
- Vehicle specific hazards (that are evinced in operational context) are then aggregated
  - Controllability, maneuverability, etc.
- In the context of operational and environmental assumptions, this forms the set of hazards to be mitigated (airworthiness, operational, training…)
  - Ground Station, Operator, Communication Links, etc.

Develop Type Certification Basis

- Can develop regulation for each hazard that will result in desired level of mitigation
  - Can use available regulation for conventional hazards
  - Can modify available regulation to fit similar hazards in new context
  - Can abstract groups of requirements
  - Can simplify many requirements
  - Develop regulation for aspects of vehicle/operation that are novel
    - e.g., Communications Link , Containment Area

Proposed Containment System Requirements

- Preliminary requirements for a containment system must mitigate the hazards associated with escape from the containment volume.
- Additional requirements address:
  - The accuracy of the aircraft's location relative to the containment boundaries,
  - Situational awareness of the UA's location relative to the containment boundaries,
  - Failure of infrastructure related to position information (e.g., GPS, cell phone network),
  - Means of detecting impending boundary violations,
  - Means of alerting the pilot in command,
  - Means of ensuring the UA remains within the established containment boundaries at all times; and,
  - Release of high energy parts that may constitute a hazard to crewmembers bystanders outside the containment area.

SUMMARY

Assured Containment Concept Summary

- Assured containment system consists of:
  - hardware, software and operational procedures
  - evidentiary material (e.g., safety analysis, reliability data, proofs, etc.) that demonstrate the system performs its intended containment function at the required level of assurance
- Assured containment system must be analyzed as a whole (for airworthiness), including
  - documented, fixed design
  - failure modes that can be clearly understood, (and mitigated or controlled)
- Due to focused functionality, effort required to develop and certify assured containment system may be less than the effort required for conventional UAS autopilot and supporting systems

Perspectives

- Enabling access to airspace for a wide class of vehicles and applications will require either:
  - Case by case evaluation or
  - Reuse of assurance concepts and arguements to form a common certification basis across vehicles and operational concepts
- Concept of assured containment offers one possible approach to streamlined development of design standards tailored to UAS applications suitable for confined, rural operational environments

Implications

- Yields streamlined approach to airworthiness certification
  - Allows midsize UAS to operate near populated areas
- Could enable further commercial uses:
  - herd management, natural resource exploration, wind turbine, pipeline, and power line inspections etc.,
- Industry and regulators gain valuable experience with UAS while carefully controlling access and potential harm to the aviation system as a whole
- Use of operationally driven type certification bases may provide relief while maintaining safety, and begin to build a foundation for certification over other classes of operations and vehicles

Questions?

Natasha.A.Neogi@nasa.gov

References

[1] Ella M. Atkins, “Autonomy as an enabler of economically-viable, beyond-line-of-sight, low-altitude UAS application with acceptable risk,” AUVSI Unmanned Systems 2014, Orlando, FL, pp.200-211.

[2] Iman Sadeghzadeh and Youmin Zhang, “A Review on Fault-Tolerant Control for Unmanned Aerial Vehicles (UAVs),” Infotech@Aerospace 2011, AIAA 2011-1472, 29 - 31 March 2011, St. Louis, Missouri.

[3] K. Bhamidipati, Daniel Uhlig, and Natasha Neogi, “Engineering Safety and Reliability into UAV Systems: Mitigating the Ground Impact Hazard,” University of Illinois, Urbana-Champaign, Urbana, IL, 61822, 2008.

[4] E. N. Johnson and D. P. Schrage, “System Integration and Operation of a Research Unmanned Aerial Vehicle,” Journal of Aerospace Computing, Information, and Communication, vol. 1, January 2004, Georgia Institute of Technology, Atlanta, GA, USA.

[5] E. A. Marconato, D. F. Pigatto, K.R.L.J.C. Branco, and L.H.C. Branco, “LARISSA: Layered architecture model for interconnection of systems in UAS,” 2014 International Conference on Unmanned Aircraft Systems (ICUAS), May 2014, Orlando, FL, pp. 20-31.

References

[6] D. F. Pigatto, G. Freire Roberto, L. Gonçalves, J. F> Rodrigues Filho, A. S. Roschildt Pinto, and K.R.L.J. Castelo Branco, “HAMSTER - Healthy, mobility and security-based data communication architecture for Unmanned Aircraft Systems,” 2014 International Conference on Unmanned Aircraft Systems (ICUAS), May 2014, Orlando, FL, pp. 52- 63.

[7] Shengxiang Jiang, Petros G. Voulgaris, and Natasha Neogi, “Distributed control over structured and packet-dropping networks,” International Journal of Robust and Nonlinear Control, vol. 18, Issue 14, pp. 1389–1408, 25 Sept. 2008

[8] Kelly J. Hayhurst, Jeffrey M. Maddalon, Natasha A. Neogi, and Harry A. Verstynen, “Concept of operations for UAS use in precision agriculture for targeted aerial application”, in preparation.

[9] Dragonfly Pictures, Inc., (undated), “DP-14 Hawk”, [Online], Available:

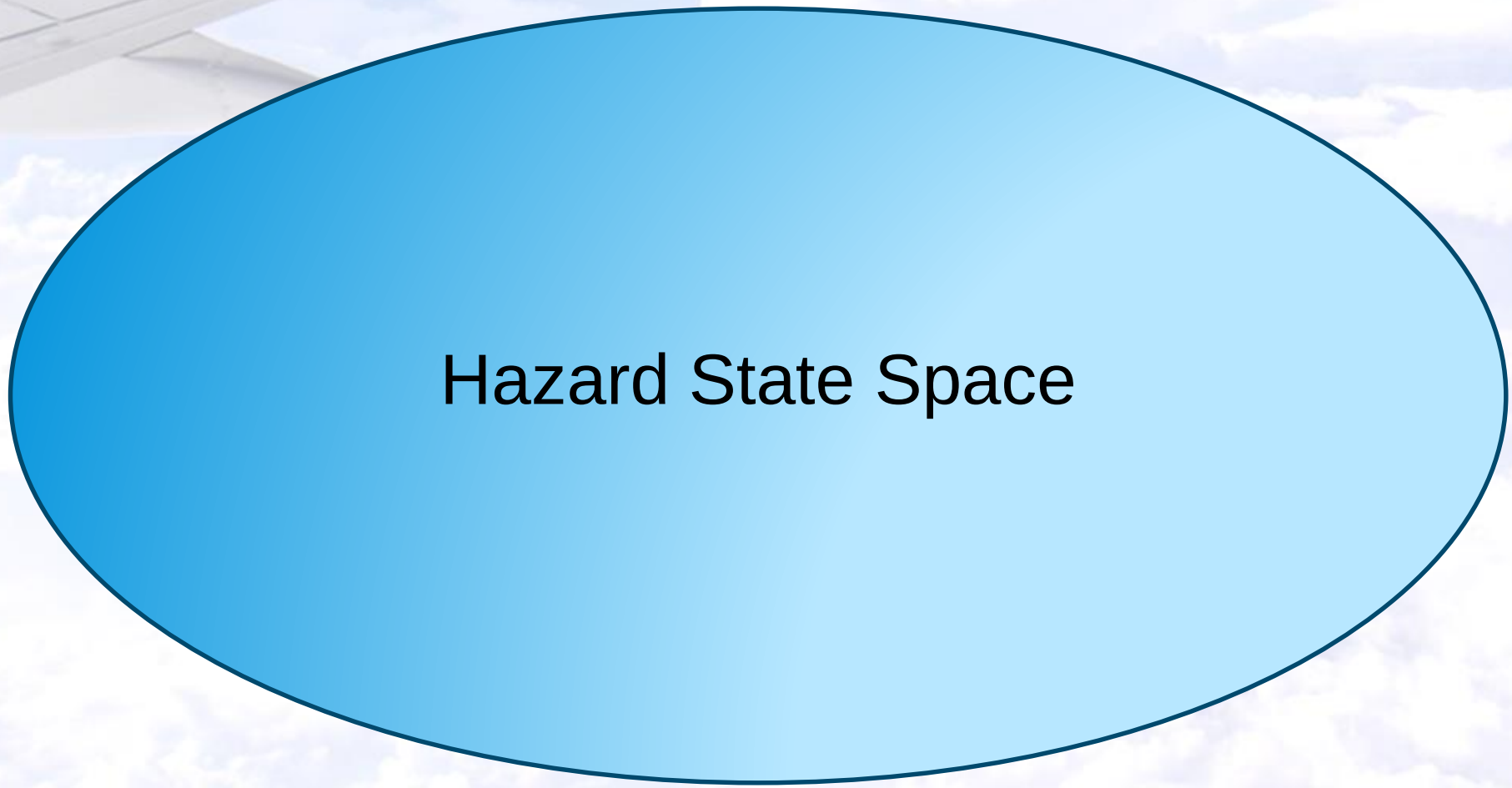
http://www.dragonflypictures.com/ products/unmanned- vehicles/dp-14-hawk/

[10] “Multilateration & ADS-B, Executive Reference Guide”, (undated), [Online], Available: http://www.multilateration.com.

[11] FAA, “FAA UAS Roadmap”, https://www.faa.gov/uas/legislative_programs/uas_roadmap/media/UAS_Roadmap_2013.pdf

BACKUPS

Hazard Partitioning



Hazard Partitioning