Safety and Security Driven Design. Unmanned Aircraft-National Airspace System Integration Case Study

Kip Johnson

Prof. Nancy Leveson

See accompanying abstract:

Johnson, K., Leveson, N. "Investigating Safety and Cybersecurity Design Tradespace for Manned-Unmanned Aerial Systems Integration Using Systems Theoretic Process Analysis." in *Proceedings of the Gesellschaft für Informatik*, 2014.

Disclaimer

- This work is sponsored by the Department of the Air Force under Air Force Contract #FA8721-05-C-0002.

- The views expressed in this presentation are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.
- Presentation approved for public release.
  - Case 88ABW-2014-4381

Overview

- **Introduction**
- Background
- Application of STAMP-STPA
- Conclusions

Introduction

Problem Statement.

- How to assess and design Unmanned Aircraft System (UAS) integration into the National Airspace System (NAS)?
  - Safety *and* (cyber) security are critical to system
  - What is the design space for safety and security?
  - What is the Human-Automation ontology necessary for safe and secure flight operations?

Introduction

Motivation. Real world.

- Today, laborious *accommodation* of unmanned aerial systems (UAS) within the National Airspace System (NAS), or use in *isolated* military operations
  - 545 UAS Certificate of Authorizations, Dec 13 [1]
  - Exponential UAS use in DoD past decade ->
- Recent Projections [2]
  - Teal Group (2013). Research & Development / Procurement $5.2-$11.6B annually next decade
- Future, *seamless* UAS integration into manned operations.
- FAA on UAS-NAS integration [4]
  - "Ultimately, UAS must be integrated into the NAS without reducing existing capacity, decreasing safety, negatively impacting current operators, or increasing the risk to airspace users or persons and property on the ground…"

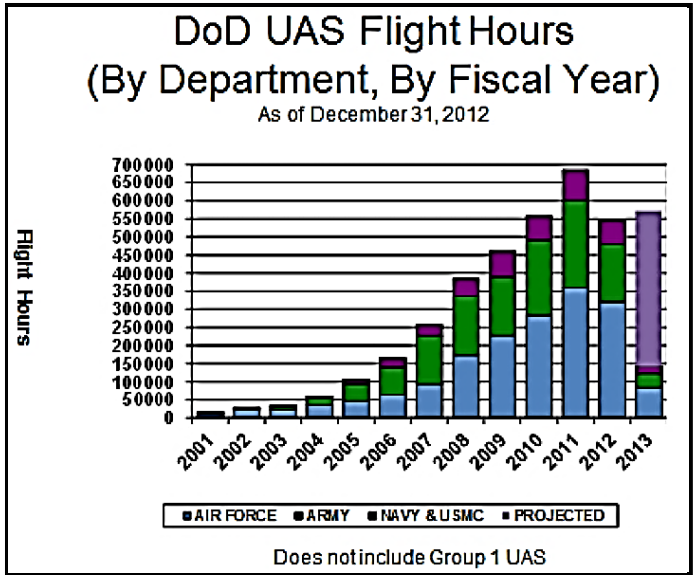

Fig. 1. DoD UAS Flight Hour Summary.
Fig. 1 adapted from [3]

Motivation. Intellectual.

- Systems Theory applied to Systems Engineering (SE)
  - UAS Integration is a Complex Sociotechnical System
  - Safety and Security are emergent properties; framed and analyzed as a control problem. Leveson and Young [6]
- Application of SE to UAS integration
  - STAMP-STPA, and Safety and Security Driven Design
    - Iterative relationship. Assess ↔Design
  - Most benefit in conceptual design and requirements generation
  - Aids in comprehension of system complexity

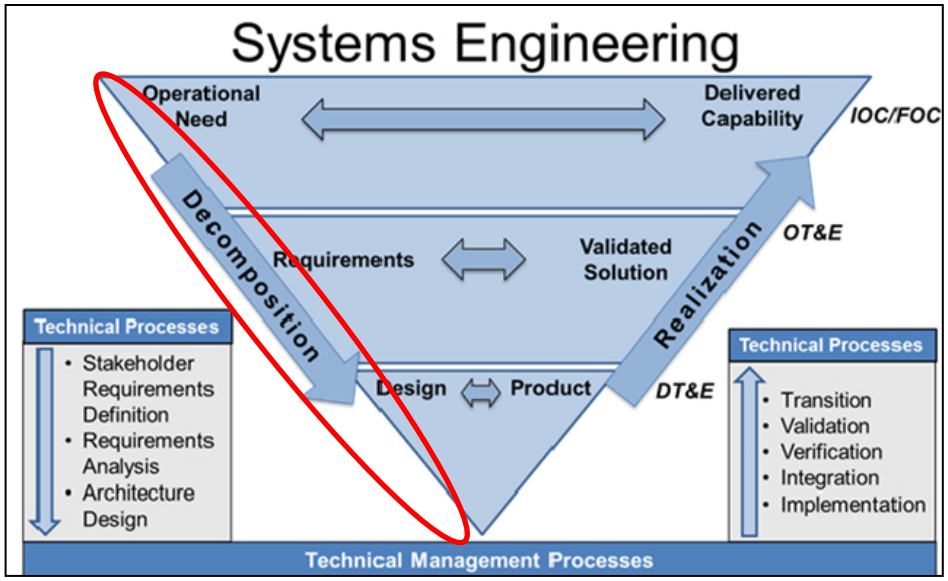

Fig. 2. Systems Engineering.

Fig. 2 adapted from Defense Acquisition Guidebook, Chpt 4 [7]

Introduction

Hypothesis:

- A systems-theoretic process analysis can be applied to the design and evaluation of safe and cyber-secure integrated manned-unmanned aerial system operations.
- A coupled safety and cybersecurity SE assessment will demonstrate system design and evaluation benefits over independent analyses.
- UAS automation ontology for safe and secure integrated operations can be derived from SE analyses.

Method.

- Systems engineering approach
- Adaptation of Systems Theoretic Accident Model and Processes for system hazard and vulnerability analyses.

Overview

- Introduction
- **Background**
- Application of STAMP-STPA
- Conclusions

Background

UAS-NAS Integration. Challenging Problem

- International efforts
  - Began in the 1990s
  - International Civil Aviation Organization
- US efforts
  - Vision 100 – Century of Aviation Reauthorization Act (NextGen), 2003
    - Congress mandated FAA to accommodate UAS operations.
  - 2012, FAA Modernization & Reform Act
    - Small UAS rule by Sep 2014
    - UAS integration into the NAS, Sep 2015
- European Efforts
  - European Organization for Civil Aviation Equipment (EUROCAE)
- Current efforts.
  - Radio Technical Committee for Aeronautics
  - RTCA Steering Committee-228 to develop performance standards for key UAS technologies
    - Detect and Avoid (DAA)
    - Communications and Control (C2)
    - Safety Assessment key effort for the NAS-level change

Background

- Current safety assessment efforts [8][9]
  - Goal. Integration does not decrease safety
  - Accident of interest. Mid-air collisions (MAC)
  - System safety metric.
    - Target level of safety, collision rate (λ). e.g. $1x10^{-9}$ MAC/hr
  - Detect and Avoid safety metric. Risk ratio of λ.
    - $\lambda_{mitigated} / \lambda_{unmitigated}$, Mitigated = λ w/ Detect & Avoid System
    - Many efforts-human factors studies, model and simulation (M&S), etc.-feed these quantitative safety assessments
  - Traditional methods used, such as Bow-Tie model, fault and event trees.

Background

- Current safety barrier paradigm
  - Air traffic control perspective
  - US airspace does not completely match (dotted oval)
- UAS-NAS integration
  - Lose See & Avoid
  - What about C2?

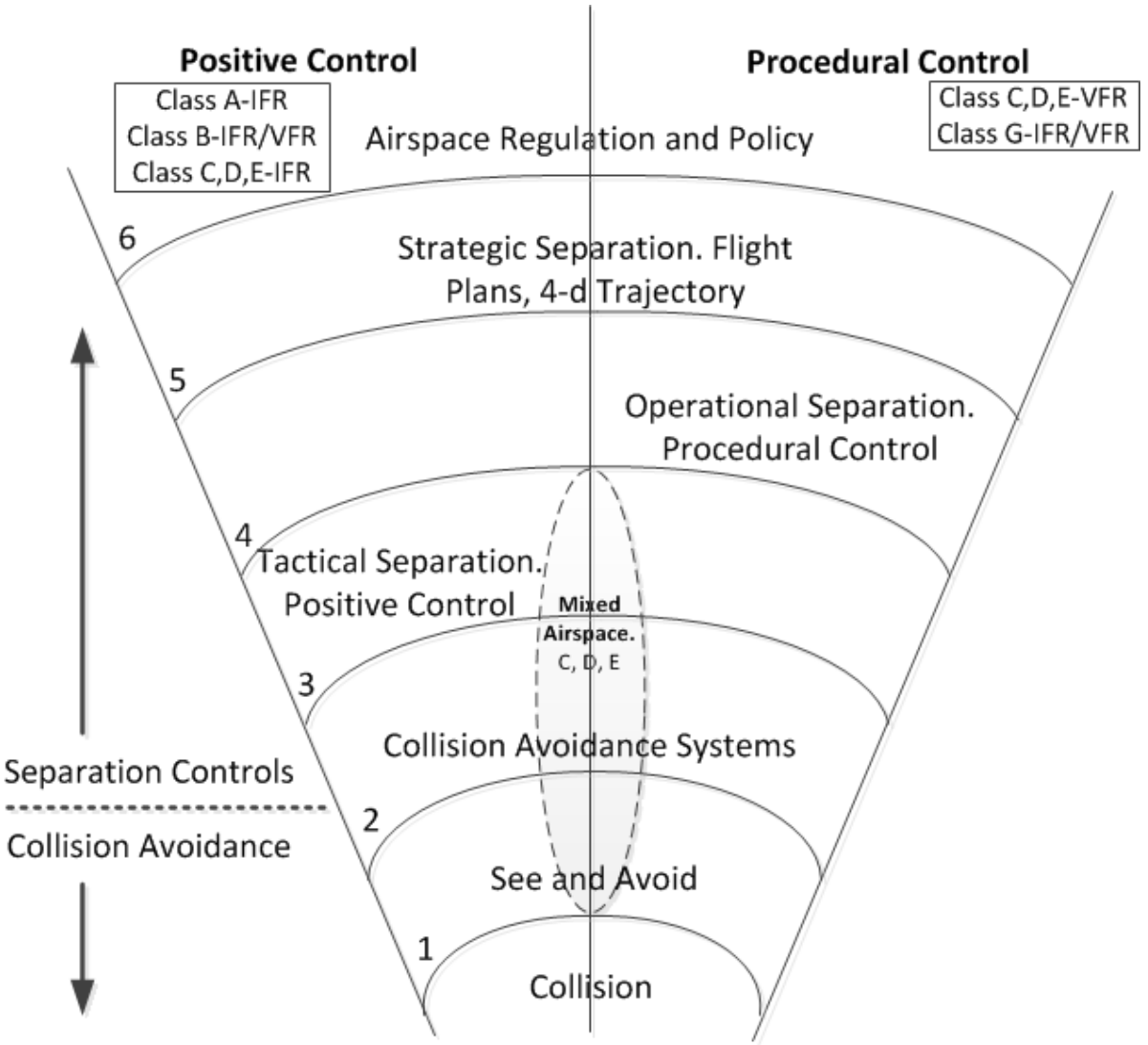

Fig 3. NAS Barriers to Collision

Overview

- Introduction
- Background
- **Application of STAMP-STPA**
- Conclusions

Application of STAMP-STPA

- System of interest.
  - Manned-Unmanned integrated flight operations
  - High level system safety control structure
  - System goal. Safe and secure integration
- Objectives.
  - No new hazards from introduction of UAS remote operations
- Accidents of interest.
  - Mid-air collision
  - Ground collision (not a focus)

	INTEGRATION SYSTEM HAZARD
H1	System control actions lead to loss of aircraft minimum separation standards
H2	System control actions induce or contribute to a controlled flight into terrain maneuver
H3	System control actions induce or contribute to loss of aircraft controlled flight

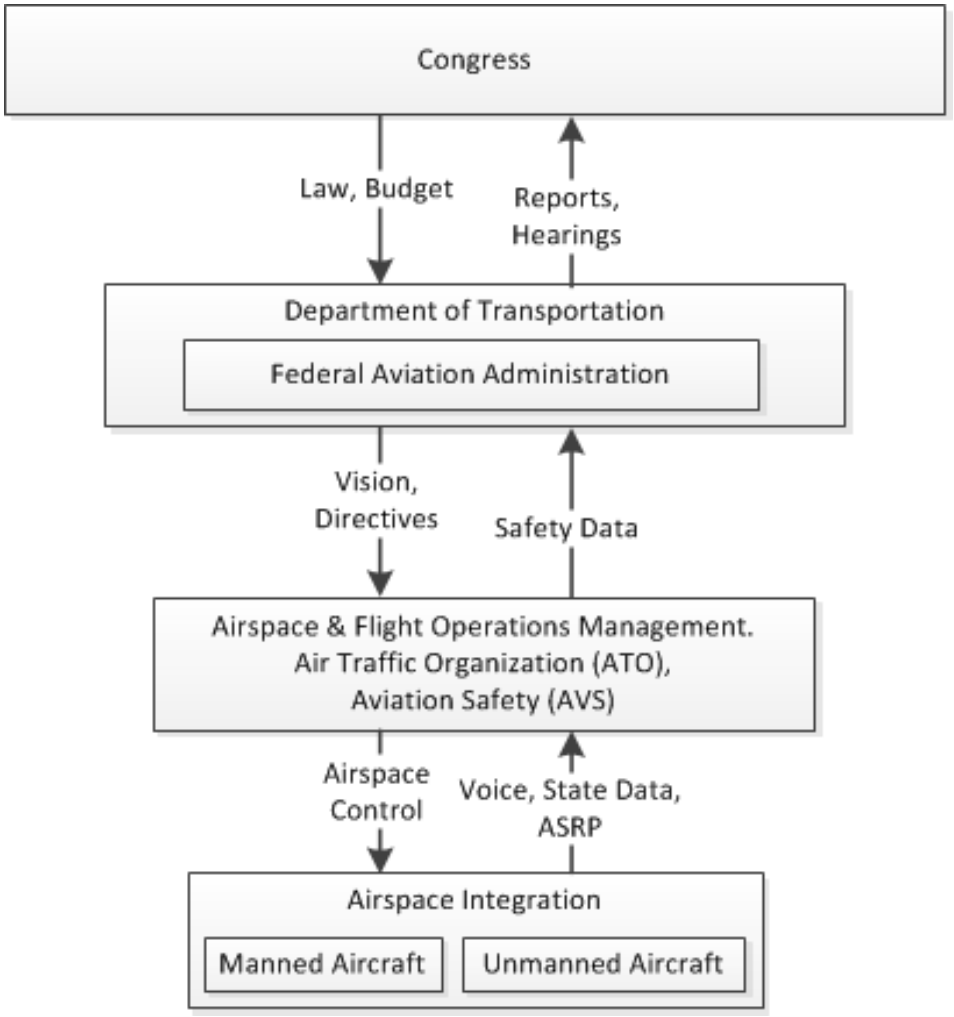

Fig 4. UAS Integration Safety Control Structure

Application of STAMP-STPA

- Major assumptions
  - Manufacturing, certification, airworthiness, maintenance, training are nominal
  - No airspace changes, working with current US airspace designations
  - Communications spectrum available to support UAS
- Concept of operations (CONOPS)
  - File and fly under Instrument flight rules
  - ATC does not have direct link to the UA for flight control
  - Fully autonomous operations not permitted
  - Separation services will be provided to UAS
  - Two separation thresholds. Self Separation (SST) and Collision Avoidance (CAT)

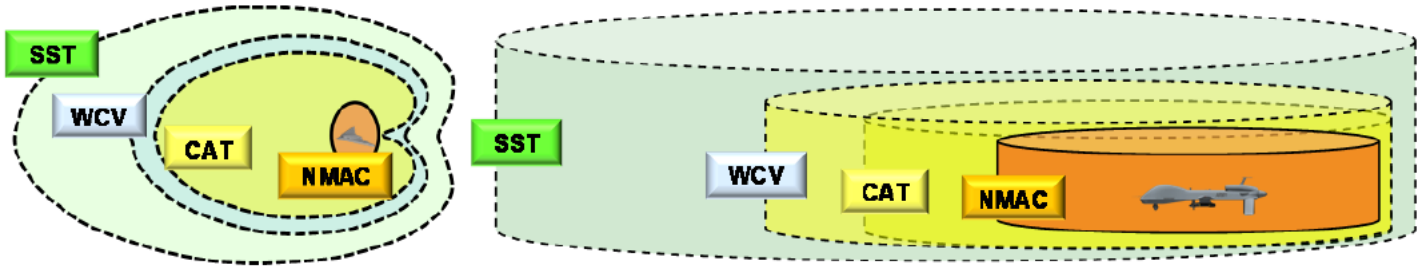

Figure 5. Self-Separation Functional Boundaries and System Thresholds, SST to WCV

Fig. 5. Adapted from [10, p. 3-21]

Application of STAMP-STPA

Scope.

- Analysis and design of flight operations only
- Techno-human changes, challenges introduced to the NAS
  - Air traffic management
    - May not have control when UAS is operating autonomously (lost link) or under malevolent control (hacking)
  - UAS operator & remote UAS operations
    - Operator needs a way to see and avoid -> Detect and Avoid (DAA)
    - Operator needs a way to communicate and control (C2) -> C2 Data Link
  - Human Factors
    - Loss of visual, auditory, motion (angular & linear accelerations)
    - Motivation for self-preservation

Application of STAMP-STPA

- STPA on Techno-human level and control agents
  - Note. System model shows importance and relationship of both C2 and DAA
  - Safe and secure integration analysis of much more than simply C2 and DAA

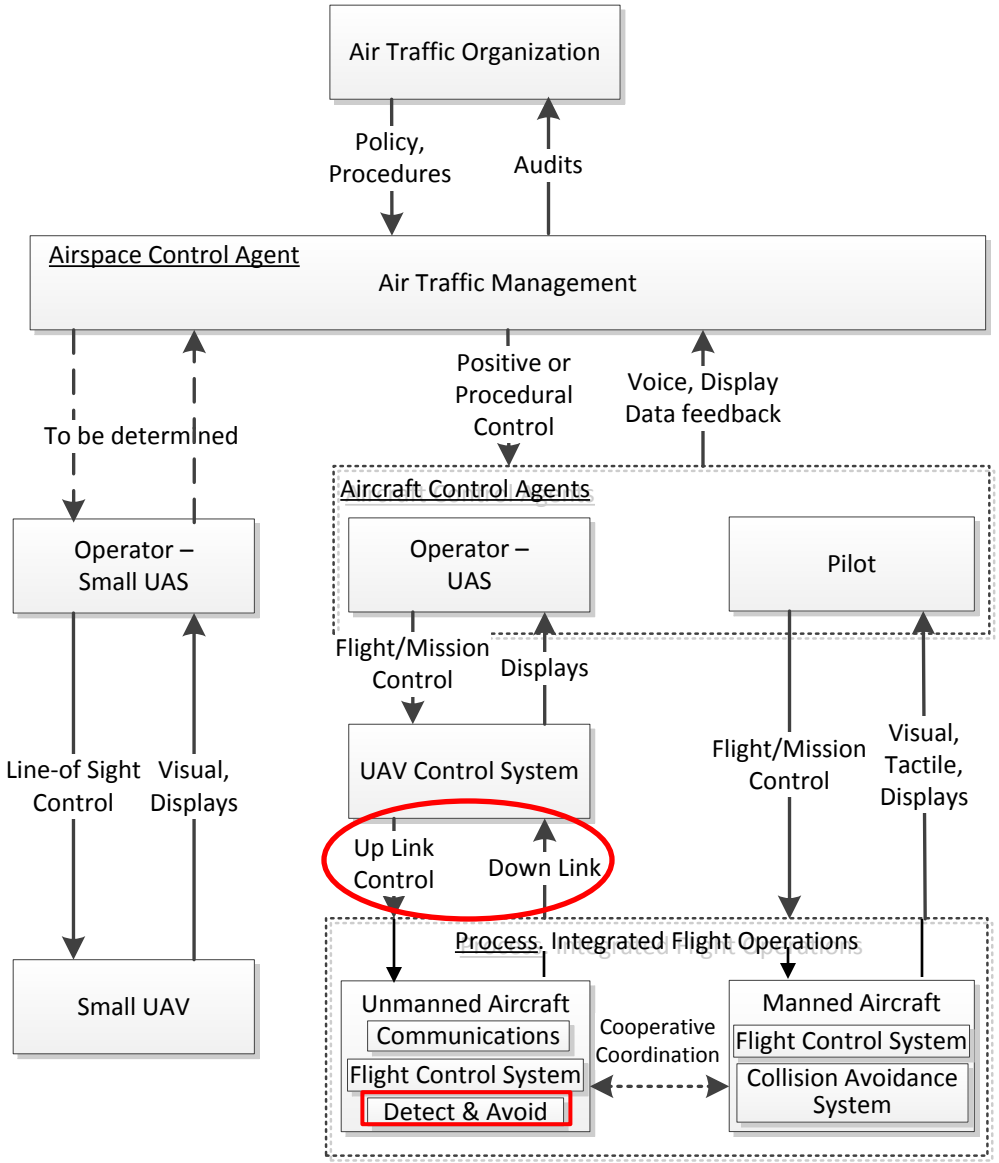

Fig 6. Techno-Human Safety Control Structure

Overview

- Introduction
- Background
- Application of STAMP-STPA
- **Conclusions**

Conclusions

- We can successfully apply STAMP-STPA to the UAS-NAS integration system.
  - STPA derived high level constraints, requirements for integration system and associated control agents
  - UAS operator and DAA STPA Step 2 control loop models developed
- Effort to assist standards making committees in framing, designing, and assessing system safety
- Next research phase.
  - Defining UAS human-automation ontology from STPA
  - Develop process and method for analytical design space characterization of safety and security

Bibliography & Acknowledgments

Bibliography

- [1] http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14153, accessed 22 Sept 2014.
- [2] S. J. Zaloga, D. Rockwell, and P. Finnegan, "World Unmanned Aerial Vehicle Systems. Market Profile and Forecast 2013 Edition.," Fairfax, 2013.
- [3] D. D. Weatherington, "Post Iraq and Afghanistan: Current and Future Roles for UAS and the Fiscal Year," 2013.
- [4] Federal Aviation Administration, "Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap," 2013.
- [5] P. Checkland, *Systems Thinking, Systems Practice*. Chichester: John Wiley & Sons, Inc., 1993.
- [6] W. Young and N. G. Leveson, "An integrated approach to safety and security based on systems theory," *Commun. ACM*, vol. 57, no. 2, pp. 31–35, Feb. 2014.
- [7] https://acc.dau.mil/docs/dag_pdf/dag_ch4.pdf, accessed 2 Sept 14
- [8] RTCA SC-228, "Detect and Avoid (DAA) White Paper," Washington, DC, 2014.
- [9] Federal Aviation Administration, "Sense and Avoid (SAA) for Unmanned Aircraft Systems (UAS). Second Caucus Workshop Report," 2013.

Acknowledgments

- The authors thank Dr. Roland Weibel, MIT Lincoln Laboratory Technical Staff, for research collaboration.