# Investigating Safety and Cybersecurity Design Tradespace for Manned-Unmanned Aerial Systems Integration Using Systems Theoretic Process Analysis

Kip Johnson[1], Nancy Leveson[2]

Department of Aeronautics and Astronautics
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, Massachusetts 02139
1. Graduate Student, johnskip@mit.edu
2. Professor, leveson@mit.edu

**Abstract:** Safety and cybersecurity are two emergent behaviors critical to mission success of Unmanned Aerial Vehicles (UAVs). This paper presents the concepts driving the initial research investigation of a hazard and vulnerability analysis for the integration of manned-unmanned aerial systems (UAS) using System-Theoretic Process Analysis (STPA). The motivation for this analysis is the need to engineer safe and secure UAS integration into the National Airspace System, or any system where manned and UASs will operate together. In contrast to more traditional safety and vulnerability assessments, this research aims to develop systems engineering methods and processes that are beneficial for initial design space exploration and developing system design requirements from the beginning of systems engineering phases. It is expected that research results will provide system architecture and design engineers the system framework and requirements necessary to engineer safe and secure integrated flight operations.

## 1 Introduction

The integration of manned-unmanned aerial systems is of critical and timely importance, especially for UAV integration into the United States (U.S.) National Airspace System (NAS). Interest and pressure is mounting for access to the NAS, and the Federal Aviation Administration (FAA) is responding. The FAA is under a U.S. congressional mandated deadline for UAV integration, due by the end of September 2015. [USC12] As highlighted by the FAA's 2013 Civil UAS Roadmap,

> "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 any more than the integration of comparable new and novel technologies." [FAA13a]

The motivation for this research is to develop UAS integration system-level safety and security requirements to help guide and intellectually manage the engineering and

development of this large complex sociotechnical system (CSS). It is imperative to have methods for bringing safety and cybersecurity to the mission concept and requirements development systems engineering stages as the mission is often one and the same with safety and security. Integrating manned-UAS operations is one of these safe and secure essential missions.

## 2 Systems Engineering Methods

### 2.1 Background

Traditional methods are being used assure safety for UAS integration in the NAS, based on reliability theory and underlying chain of events accident models. The Radio Technical Commission for Aeronautics (RTCA) steering committee (SC) 228 was charged by the FAA to develop the Minimum Operational Performance Standards for UASs, specifically Detect and Avoid (DAA) and Command and Control (C2) technologies. Based on the 2013 Sense and Avoid report, the community concluded that a risk ratio method would provide the "most effective" Target Level of Safety. [FAA13b] The C2 safety standards are in development and currently are envisioned to rely on a probability concept, the required communications performance metric. [RTC14]

This approach alone, we argue, is not the best suited for this large CSS. There is little to no historical flight integration data, human interaction is integral, and the system is heavily software dependent—all challenges for traditional safety and hazard analyses.

The safety effort is further complicated by the shear enormity and complexity of the task and the ability of decision makers to adequately comprehend the system, let alone define the safety requirements driving the system's regulatory and technical design efforts. [Di13] [GAO12] Efforts across the globe to integrate UAV operations began in the late 1990s and early 2000s within government, academia, and industry stakeholders. [De04] Accommodation of UAVs for the Next Generation transportation system was enacted into U.S. law through the Vision 100-Century of Aviation Reauthorization Act, 2003. [El12] The efforts continue today in 2014, over a decade after they began. Designing for safe and secure UAV integration operations is a difficult and challenging endeavor.

### 2.2 The Case for a Systems Approach to Design

A systems approach is fundamentally about two paired concepts. [Ch93] First is the concept of systems hierarchy and emergence. Safety and cybersecurity are emergent properties that cannot adequately be handled through decomposition. Second, there needs to be communication and control between the system levels. The idea of control is the foundation for recent developments in systems safety concepts, more specifically STAMP (Systems-Theoretic Accident Model and Processes). [Le11] Safety can be analyzed as a control problem, and it is hypothesized that the STPA (System-Theoretic

Process Analysis) method can be applied and extended to the design and development of safe and cybersecure integrated manned-UAS flight operations.

## 3 A New Approach for Qualitative Systems Analysis in Design

As conceptualized by STAMP, safety is an emergent or a systems level behavior. The analysis of such requires a systems approach, one that analyzes component interactions. The application of STAMP-STPA to another emergent property, cybersecurity, is currently being developed by researchers at the Massachusetts Institute of Technology. [YoLe14] For UAS integration, both safety and cybersecurity are both critical emergent properties.

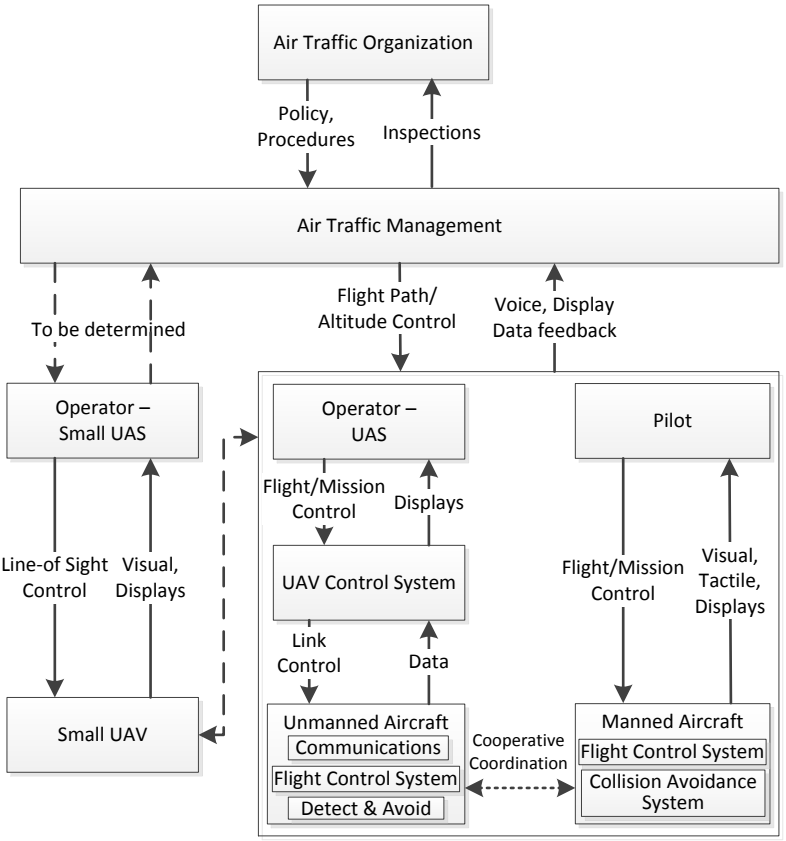


Figure 1: Representative Manned-Unmanned Aerial System Safety Control Structure

Figure 1 is a representative STAMP safety control structure modeling the manned-UAS integration system for flight operations in a controlled environment. The dotted lines represent current unknown controls, feedback, and information coordination. The Detect

and Avoid, and C2 systems are the perspectives of interest, but not independent from the more complete complex sociotechnical system represented in Figure 1.

Inspired by multidisciplinary systems design optimization methods, we are investigating the design space, potential tradespace, and concept of a potential qualitative Pareto tradeoff between safety and cybersecurity for manned-UAS integrated systems. A design is optimal, or on the Pareto frontier, if improving one design objective must diminish the other. [PaWi00] Demonstrating true Pareto optimality is not the goal here, nor is it possible. Rather, what can be learned about the design space, potential tradespace, and relationships during an STPA-Safety Driven Design analysis in pursuit of a qualitative Pareto?

The research aims to answer what is the qualitative system design tradespace for safety and cybersecurity, and can the concept of an approximate qualitative Pareto tradeoff be demonstrated on manned-UAS integration to benefit system design? The authors will investigate framework and methodology to characterize the design space using STPA for the hazard and vulnerability systems engineering analysis.

## 4 Conclusions

The accompanying presentation at the Second European STAMP Workshop (ESW2014) will present the initial hazard and vulnerability STPA analyses conducted on manned-UAS integration enabling technologies and concepts, both UAS DAA and C2. Research findings on the development of multi-objective systems engineering design methods to analyze and evaluate system emergent properties will also be discussed.

It is hypothesized that the application and extension of STPA will be successful for both safety and cybersecurity alone. Systems theoretic design methods and processes to characterize the bi-objective design space should have immediate impact on the development of requirements and standards for engineering UAV integration complex sociotechnical systems. In addition, the research more broadly develops STPA-SDD (Safety-Driven Design) by integrating safety and security requirements earlier into the systems engineering design and analysis processes. [Le11]

Unmanned aircraft integration is a complex and difficult endeavor. A systems-theoretic approach to the design and analysis of manned-UAS integration systems should prove beneficial to the realization of safe and secure integrated flight operations.

## Acknowledgments

This work is sponsored by the Department of the Air Force under Contract #FA8721-05-C-0002. The views expressed in this article are those of the authors and do not reflect the official policy or position of the Massachusetts Institute of Technology Lincoln Laboratory, United States Air Force, Department of Defense, or the U.S. Government.

## References


[USC12] United States Congress, FAA Modernization and Reform Act of 2012. 2012.

[FAA13a] Federal Aviation Administration, "Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap," 2013.

[FAA13b] Federal Aviation Administration, "Sense and Avoid (SAA) for Unmanned Aircraft Systems (UAS). Second Caucus Workshop Report," 2013.

[RTC14] RTCA SC-228, "Command and Control (C2) Data Link White Paper," 2014.

[Di13] G. L. Dillingham, "Government Accountability Office Report to Congress-Unmanned Aircraft Systems: Continued Coordination, Operational Data, and Performance Standards Needed to Guide Research and Development," 2013.

[GAO12] U.S. Government Accountability Office, "Report to Congress - Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System," 2012.

[De04] M. T. DeGarmo, "Issues Concerning Integration of Unmanned Aerial Vehicles in Civil Airspace," 2004.

[El12] B. Elias, "Pilotless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace System," 2012.

[Ch93] P. Checkland, Systems Thinking, Systems Practice. Chichester: John Wiley & Sons, Inc., 1993.

[Le11] N. Leveson, Engineering a Safer World: Systems Thinking Applied to Safety. Cambridge: The MIT Press, 2011.

[YoLe14] 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.

[PaWi00] P. Y. Papalambros and D. J. Wilde, Principles of Optimal Design: Modeling and Computation, Second. Cambridge: Cambridge University Press, 2000.