NASA/TM-2007-214539

Preliminary Considerations for Classifying Hazards of Unmanned Aircraft Systems

Kelly J. Hayhurst, Jeffrey M. Maddalon, Paul S. Miner, and George N. Szatkowski
Langley Research Center, Hampton, Virginia

Michael L. Ulrey
The Boeing Company, Seattle, Washington

Michael P. DeWalt
Certification Services, Inc., East Sound, Washington

Cary R. Spitzer
AvioniCon, Williamsburg, Virginia

February 2007

The NASA STI Program Office … in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the lead center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that complement the STI Program Office's diverse offerings include creating custom thesauri, building customized databases, organizing and publishing research results ... even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at ***http://www.sti.nasa.gov***

- E-mail your question via the Internet to help@sti.nasa.gov

- Fax your question to the NASA STI Help Desk at (301) 621-0134

- Phone the NASA STI Help Desk at (301) 621-0390

- Write to:
  NASA STI Help Desk
  NASA Center for AeroSpace Information
  7115 Standard Drive
  Hanover, MD 21076-1320

NASA/TM-2007-214539

Preliminary Considerations for Classifying Hazards of Unmanned Aircraft Systems

Kelly J. Hayhurst, Jeffrey M. Maddalon, Paul S. Miner, and George N. Szatkowski
Langley Research Center, Hampton, Virginia

Michael L. Ulrey
The Boeing Company, Seattle, Washington

Michael P. DeWalt
Certification Services, Inc., East Sound, Washington

Cary R. Spitzer
AvioniCon, Williamsburg, Virginia

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

February 2007

Acknowledgments

The work documented in this report contains technical contributions from joint work between government and industry representatives participating in NASA's Access 5 program. In particular, Robin Cahhal-Simpson from General Atomics, Jamie Ferensic from Northrop Grumman Corporation, and Paul Myer and Russell Morris from the Boeing Company contributed to discussions about classification of hazards for unmanned systems, and also contributed to conducting a preliminary functional hazard assessment of a generic unmanned aircraft system. Our thanks go to each of them for their contributions to this work.

Available from:

NASA Center for AeroSpace Information (CASI)
7115 Standard Drive
Hanover, MD 21076-1320
(301) 621-0390

National Technical Information Service (NTIS)
5285 Port Royal Road
Springfield, VA 22161-2171
(703) 605-6000

Table of Contents

Acronyms

AC	Advisory Circular
AGT	Air/Ground Transition
ARP	Aerospace Recommended Practices
ATC	Air Traffic Control
ATM	Air Traffic Management
CCA	Common Cause Analysis
CFR	Code of Federal Regulations
C2	Command and Control
FAR	Federal Aviation Regulations
FHA	Functional Hazard Assessment
FP	Flight Path
FTA	Fault Tree Analysis
FMEA	Failure Modes and Effects Analysis
FMES	Failure Modes and Effects Summary
GP	Ground Path
HIRF	High Intensity Radiated Fields
NAS	National Airspace System
PSSA	Preliminary System Safety Assessment
SAE	Society of Automotive Engineers
SEU	Single Event Upset
SSA	System Safety Assessment
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
US	United States

Abstract

The use of unmanned aircraft in national airspace has been characterized as the next great step forward in the evolution of civil aviation. To make routine and safe operation of these aircraft a reality, a number of technological and regulatory challenges must be overcome. This report discusses some of the regulatory challenges with respect to deriving safety and reliability requirements for unmanned aircraft. In particular, definitions of hazards and their classification are discussed and applied to a preliminary functional hazard assessment of a generic unmanned system.

1 Introduction

Military interest in unmanned aircraft systems (UASs) dates back to the early 1900's with the experimental development of the Curtiss/Sperry "Flying Bomb" in 1915 by the United States (US) Navy, and the US Army's development of the Kettering "Bug" in 1918 (ref. 1, 2). From those humble beginnings, unmanned aircraft have become an integral component in military operations today. As of September 2004, some twenty types of unmanned aircraft, large and small, have flown over 100,000 total flight hours in support of military operations, especially in Afghanistan and Iraq (ref. 3). There is little doubt that unmanned aircraft are transforming military operations.

Buoyed by the success in the military sector, UAS vendors are looking to civil and commercial applications for their aircraft, especially applications characterized as dull, dangerous, or dirty. A wide-range of applications such as pipeline inspection, border control, fire fighting, agricultural management, communications relay, and air-freight operations seem ideally suited for unmanned aircraft. Many believe that the time is rapidly approaching when unmanned aircraft will be commonplace in our national airspace system (NAS), and that now is the time for the formulation of governing standards.

A comprehensive safety argument for unmanned aircraft will be necessary for formulating these standards. That safety argument will differ from that of conventional aircraft in at least two fundamental aspects. First, unlike manned aircraft, an unmanned vehicle[1] can be lost without necessarily endangering any human life. Second, because the pilot is not on board the vehicle, reliance will be placed on automation to a much greater degree than in conventional aircraft—especially in unusual situations. The NAS already accommodates some degree of autonomous operation, as described by Hadden (ref. 4):

> Except during take-off and the final stages of landing, the modern commercial aircraft is routinely being flown by computers, monitored by human pilots. The systems in the latest generation of commercial aircraft commonly have fault monitoring and diagnostic functions which can cope with many failure conditions without pilot intervention. Automatic landing including flare and ground roll has been commonplace for many years. When automation of the take-off segment of

[1] The terms unmanned aircraft and unmanned vehicle are used interchangeably to refer specifically to an air vehicle that does not have an on-board crew. For this paper, we are not considering such aircraft with passengers on board. Conversely, manned aircraft refers to an air vehicle that does have an on-board crew.

> flight also becomes common it may be the norm for airliners to complete their missions without operation of the primary flying controls by a human pilot at any stage.
>
> It is expected that automatic systems for civil aircraft will become ever more capable and demonstrate increasing reliability. As a consequence the severity of the effect of a flight crew becoming incapacitated whilst airborne will tend to diminish. Whilst the remoteness of the pilot/controller of a UAV raises major issues for aircraft operations in terms of air traffic management, compliance with the Rules of the Air etc, it can be seen that the regulatory process for airworthiness certification is already proven to be able to cope with high levels of automation.

Technological advances, such as reliable command and control, and sense and avoid capability, will play a key role in enabling access to civil airspace. Equally important, and perhaps more difficult, is development of the regulatory framework that will provide the guidance necessary to assure safety. This report focuses attention on one part of the regulations necessary for establishing the airworthiness of a UAS, namely standards for reliability and safety.

The broad issue, informally speaking, is: how reliable does a UAS need to be to operate routinely and safely in civil airspace? Does such a system need to meet the most stringent reliability requirements, such as those levied on commercial transport (Part 25) aircraft? Or, is comparison with general aviation aircraft (Part 23) more appropriate? Answering these questions for a UAS is non-trivial. Unmanned aircraft in operation today range in size from vehicles capable of being hand-launched to vehicles with a wingspan comparable to transport aircraft, with fixed and rotary wings, and with radically different altitude and endurance capabilities. This report does not attempt to answer the reliability question associated with each distinct type of aircraft, but instead covers a few fundamental underpinnings of reliability and safety requirements that will be needed to eventually provide an answer. This report presents initial thinking about definitions of hazards and their classification for UASs, and how those definitions could be applied in a functional hazard assessment of a UAS. This work is preliminary and intended to encourage debate and discussion.

This report is organized as follows. Section 2 provides a brief overview of existing airworthiness guidance for manned aircraft with respect to regulating hazards. Section 3 discusses how terminology used to identify and classify hazards may be adapted for a UAS. In particular, new definitions for hazard classifications are proposed. Next, section 4 describes the hazard assessment process used in civil aviation, and how that process may be tailored to address unique aspects of a UAS. A functional decomposition of a generic UAS is described in section 5. The decomposition is an organized listing of the high-level functions required for the safe and routine flight of a generic UAS. This functional decomposition is used for conducting a preliminary functional hazard assessment (FHA), that is the subject of section 6. Because of its size, the FHA is included as an appendix. Section 7 provides preliminary thoughts on environmental protection from high intensity radiated fields and single event upset. Finally, a summary and concluding remarks are given in section 8.

2 Regulations Governing Design Hazards for Manned Aircraft

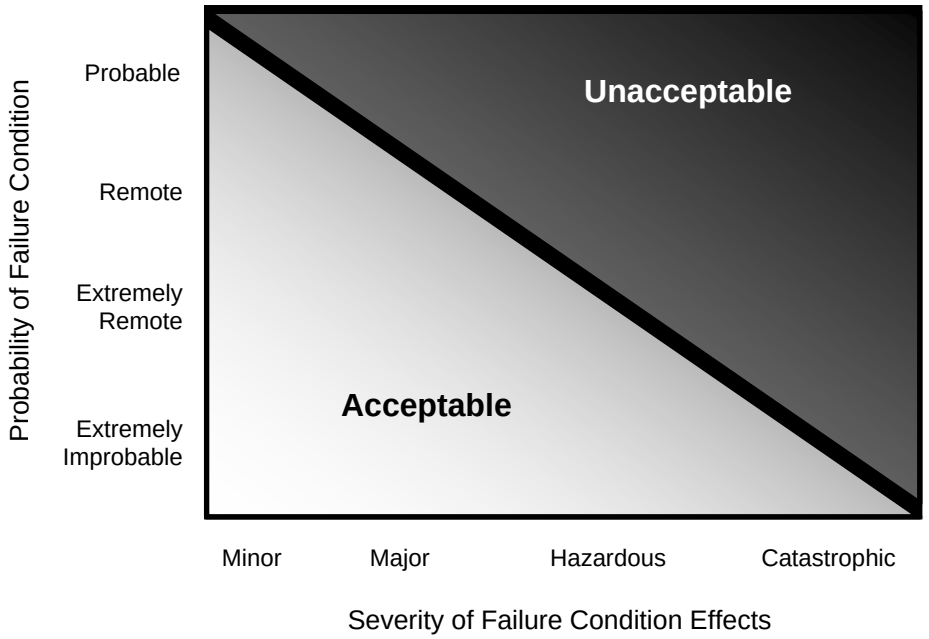
An intricate system of rules and regulations governs the design and operation of aircraft within the NAS. Title 14 of the Code of Federal Regulations (14 CFR, Chapter I) contains the Federal Aviation Regulations (FARs) (ref. 5) for the certification process for various product types: FAR Part 25 for large transport airplanes, FAR Part 23 for small airplanes, FAR Part 27 for small

helicopters, FAR Part 29 for large transport helicopters, FAR Part 31 for manned free balloons, and FAR Parts 33 and 35 for engines and propellers, respectively. The regulations promote safety of flight by setting minimum standards for the design, materials, workmanship, construction, and performance of aircraft, aircraft engines, and propellers as may be required in the interest of safety.

Current regulations define no category of aircraft that would apply rationally or completely to UAS design and certification. A reasonable assertion from which to start developing such regulations is that unmanned aircraft should pose no greater risk to persons or property in the air or on the ground than that presented by equivalent manned aircraft (ref. 4). Working from that assertion, two related issues come into play: hazard classification and likelihood of failure. Both are factors in evaluating risk.

FAR Sections 23.1309 and 25.1309 deal with hazards to equipment, systems, and installations. The regulations require justification that all probable failures or combinations of failures of any system will not result in unacceptable consequences. The justification is typically in the form of analysis that shows that the probability of a failure or combination of failures which could cause a significant hazard is acceptably low. The FAA recognizes five hazard categories: catastrophic, hazardous, major, minor, and no effect. Figure 1 shows the general relationship expected between likelihood of failure and the hazard categories (ref. 6).

Figure 1. Relationship Between Likelihood of Failure and Hazard Category



For decades, there was no formal distinction in treatment of hazards among aircraft types. For example, prior to 1999, single-engine general aviation aircraft were subject to virtually the same regulatory considerations as large jet transports with respect to definitions of allowable hazards (ref. 7). In 1999, however, the FAA acknowledged that imposing the same standards on transport and general aviation aircraft was inconsistent with the actual risks. That acknowledgement was

made in FAA Advisory Circular (AC) 23.1309-1C (ref. 6), that redefined many risks for small aircraft. As stated in AC 23.1309-1C,

> Incorporation of [standards developed for transport airplanes] into Part 23 resulted in a significant increase in equipment reliability standards. That is, they required much lower probability values for failure conditions than the existing operational safety history of different airplane classes. Current data indicates that these probability values were not realistic. Since most aircraft accidents are caused by something other than equipment failures, increasing the reliability of the installed systems to try to improve safety will have little positive effect on reducing aircraft accidents when compared with reducing accidents due to pilot error.

In accord with this, AC 23.1309-1C established a multi-tiered certification approach for four different classes of Part 23 aircraft: the smallest craft having a single piston engine to the largest being a multiengine commuter jet. Different criteria for probability of failure per flight hour were prescribed for each class, based on historical evidence from the airline industry's existing safety record. Table 1 compares current requirements for hazard probabilities between Part 23 and other FAR Parts. The probability numbers in table 1 represent only random hardware failures per flight hour.

Table 1. Relationship of Hazard Categories to Probability of Failure for Different Categories of Aircraft

Hazard Classification	Requirements for Probability of Failure Per Flight Hour	
	Part 23	Parts 25, 27, 29, and 33
Catastrophic	10^{-6} to 10^{-9}, plus no single functional failure	10^{-9}, plus no single functional failure
Hazardous	10^{-5} to 10^{-7}	10^{-7}
Major	10^{-4} to 10^{-5}	10^{-5}
Minor	10^{-3}	$>10^{-5}$
No Effect	None	None

FAA AC 23.1309-1C explains the rationale for these probability numbers for Part 23 aircraft as follows:

> Historical evidence indicates that the probability of a fatal accident in restricted visibility due to operational and airframe-related causes is approximately one per ten thousand hours of flight for single-engine airplanes under 6,000 pounds. Furthermore, from accident databases, it appears that about 10 percent of the total was attributed to Failure Conditions caused by the airplane's systems. It is reasonable to expect that the probability of a fatal accident from all such Failure Conditions would not be greater than one per one hundred thousand flight hours or 1×10^{-5} per flight hour for a newly designed airplane. It is also assumed, arbitrarily, that there are about ten potential Failure Conditions in an airplane that could be catastrophic. The allowable target Average Probability Per Flight Hour of 1×10^{-5} was thus apportioned equally among these Failure Conditions, which resulted in an allocation of not greater than 1×10^{-6} to each. The upper limit for the Average Probability per Flight Hour for Catastrophic Failure Conditions

would be 1 x 10^{-6}, which establishes an approximate probability value for the term "Extremely Improbable." Failure Conditions having less severe effects could be relatively more likely to occur. Similarly, airplanes over 6,000 pounds have a lower fatal accident rate; therefore, they have a lower probability value for Catastrophic Failure Conditions.

A similar derivation is given for the probabilities assigned for commercial transport aircraft (ref. 8), except that the probability of a fatal accident due to airplane system failures is assumed to be less than 10^{-7}, with approximately 100 potential failure conditions that could be catastrophic, and a mean flight duration of one hour—giving the 10^{-9} per flight hour requirement. This derivation becomes problematic for a UAS because little relevant historical data exists on failure of unmanned aircraft in civil applications[2]. Existing data from military operations (ref. 9) indicates that UAS reliability is about two orders of magnitude worse than the aircraft with the worst documented reliability, namely Part 23 Class 1 aircraft. Introducing a UAS with such low reliability into the NAS has the potential for creating unacceptable hazards.

Assuming that the public will expect new aircraft systems to be no more dangerous than current systems, specifically that a UAS should pose no greater risk than that presented by equivalent manned aircraft, then understanding potentially catastrophic failure conditions of a UAS becomes important to establishing system reliability requirements. But, what does catastrophic failure mean for a UAS? Answering this question for a UAS will help set the stage for airworthiness requirements, as well as system design and equipment requirements.

The next section examines terminology for describing failure conditions for a UAS.

3 Defining Hazard Classifications for a UAS

Hazard categories are defined in a number of regulatory documents. For example, the FAA System Safety Handbook (ref. 10) contains a general set of definitions, AC 23.1309-1C offers definitions specific for Part 23 aircraft, and AC 25.1309-1A (ref. 11) offers definitions for transport aircraft. The various definitions are similar, but not exactly the same. For the purposes of this paper, AC 23.1309-1C was chosen as a model for developing regulatory wording for hazards associated systems and equipment for a UAS. This choice was made, at least in part, because many unmanned aircraft of interest are similar in weight and performance characteristics to Part 23 aircraft. Also, it was assumed that definitions for UASs would more likely gain acceptance if they were similar to existing definitions. Hence, the work here in defining hazard classifications for a UAS started with the definitions of the five hazard classifications from AC 23.1309-1C, as shown in table 2.

The fundamental distinction for unmanned aircraft, of course, is that there are no people on board the aircraft. Hence, one approach to revising the definitions specific to UASs would be to delete references to the on-board flight crew and occupants. Although this may seem reasonable at first, this approach would obfuscate important collateral issues. One such issue is that regulations which aim to protect aircraft occupants by preventing crashes might also protect third parties (people in other aircraft and people on the ground). Most safety analyses, however, do not address this fully. Another issue concerns mitigating hazards. In conventional aircraft, the on-board pilot is willing and able to minimize or eliminate hazards to other aircraft or persons or property on the ground. That ability may be significantly different for a remote or autonomous pilot. Revised hazard definitions for UASs should consider these distinctions.

[2] There may be a small amount of data on civilian-like missions such as surveillance operations conducted by the Coast Guard. But, the context is insufficiently similar to be useful.

The definitions for hazard categories actually start with a definition of failure conditions, which include the specific definition of the terms catastrophic, hazardous, major, minor, and no safety effect. AC 23.1309-1C gives the following definition:

Failure Conditions: A condition having an effect on either the airplane or its occupants, or both, either direct or consequential, which is caused or contributed to by one or more failures or errors considering flight phase and relevant adverse operational or environmental conditions or external events. Failure Conditions may be classified according to their severity as follows: [as shown in table 2].

Table 2. Definitions of Hazard Categories for Part 23 Aircraft

No Safety Effect: Failure Conditions that would have no affect [*sic*]on safety (that is, Failure Conditions that would not affect the operational capability of the airplane or increase crew workload)
Minor: Failure Conditions that would not significantly reduce airplane safety and involve crew actions that are well within their capabilities. Minor Failure Conditions may include a slight reduction in safety margins or functional capabilities, a slight increase in crew workload (such as routine flight plan changes), or some physical discomfort to passengers or cabin crew.
Major: Failure Conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins or functional capabilities; a significant increase in crew workload or in conditions impairing crew efficiency; or a discomfort to the flight crew or physical distress to passengers or cabin crew, possibly including injuries.
Hazardous: Failure Conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be the following: 1. A large reduction in safety margins or functional capabilities; 2. Physical distress or higher workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or 3. Serious or fatal injury to an occupant other than the flight crew.
Catastrophic: Failure Conditions that are expected to result in multiple fatalities of the occupants, or incapacitation or fatal injury to a flight crewmember normally with the loss of the airplane. Notes: (1) The phrase "are expected to result" is not intended to require 100% certainty that the effects will always be catastrophic. Conversely, just because the effects of a given failure, or combination of failures, could conceivably be catastrophic in extreme circumstances, it is not intended to imply that the failure condition will necessarily be considered catastrophic. (2) The term "Catastrophic" was defined in previous versions of the rule and the advisory material as a Failure Condition that would prevent continued safe flight and landing.

Revising the definition of "failure condition", without the classification definitions, is relatively simple. For this particular term, removing the reference to occupants and replacing "airplane" with "UAS" are easy modifications. It is important to keep in mind that by UAS, we mean all essential systems for safe flight including the aircraft itself, any external components of the system, such as a ground control station, and the command, control, and communication links between the external components and the aircraft. With that in mind, a failure condition for a UAS could be defined as: *a condition having an effect on the UAS, either direct or consequential, which is caused or contributed to by one or more failures or errors considering flight phase and relevant adverse operational or environmental conditions or external events.*

Modifying the definitions for each hazard classification is more challenging, especially the definition for catastrophic. For this study, we made two assumptions: (1) the severity classifications used for a UAS should be consistent with those used for manned aircraft, and (2) changes to existing definitions should be minimized as much as possible. To that extent, the considerations for revising the definitions included thinking about the effects of failure on three entities: the UAS itself, the flight crew of the UAS (which likely resides in a ground control

station), and third parties (any people external to the UAS either on the ground or in other aircraft). These three considerations are comparable to those in AC 23.1309-1C for the effects of failure on the airplane, flight crew, and occupants.

Most of the proposed changes to the definitions deal with references to passengers and cabin crew. One change is to use the term "flight crew" in place of "crew". Here, the term "flight crew" is defined as individuals authorized to command and control the UAS. Although the flight crew for a UAS would likely be located in a ground control station, issues of workload and physical distress, injury, incapacitation, or death are still relevant. Implicit in this discussion is the assumption that a person or persons are responsible for control of the vehicle—completely autonomous vehicles are not considered. Table 3 shows proposed changes to the original AC 23.1309-1C definitions in table 2 for all of the hazard categories, except catastrophic. Additions to the AC 23.1309-1C definitions are indicated in bold italics font, and deletions are indicated by striking through the original text.

Table 3. Proposed Revisions to the Definitions of Four Hazard Categories

No Safety Effect: Failure Conditions that would have no effect on safety (that is, Failure Conditions that would not affect the operational capability of the airplane or increase ***flight crew*** workload).
Minor: Failure Conditions that would not significantly reduce ~~airplane~~ ***UAS*** safety and involve ***flight crew*** actions that are well within their capabilities. Minor Failure Conditions may include a slight reduction in safety margins or functional capabilities ***or*** a slight increase in ***flight crew*** workload (such as routine flight plan changes)~~. or some physical discomfort to passengers or cabin crew.~~
Major: Failure conditions that would reduce the capability of the ~~airplane~~ ***UAS*** or the ability of the ***flight crew*** to cope with adverse operating conditions to the extent that there would be: a significant reduction in safety margins or functional capabilities; a significant increase in ***flight crew*** workload or in conditions impairing ***flight crew*** efficiency; a discomfort to the ***flight crew***~~, or physical distress to passengers or cabin crew,~~ possibly including injuries; or ***a potential for physical discomfort to persons***
Hazardous: Failure Conditions that would reduce the capability of the ~~airplane~~ ***UAS*** or the ability of the ***flight crew*** to cope with adverse operating conditions to the extent that there would be the following: 1. A large reduction in safety margins or functional capabilities; 2. Physical distress or higher workload such that the ***UAS flight crew*** cannot be relied upon to perform their tasks accurately or completely; or 3. ~~Serious or fatal injury to an occupant other than the flight crew.~~ ***Physical distress to persons, possibly including injuries.***

Revising the definition of catastrophic failure posed more of a challenge. A unique concern for a UAS, especially within the FAA, is the persistent loss of the ability to control the flight path of the aircraft. The worst case assumption is that loss of the aircraft will normally follow at some point after permanent loss of control. Unmanned aircraft have the unique ability to potentially provide controlled loss of the aircraft, without loss of life; for example, controlled flight termination at a pre-designated crash location. The key factor is control, without which no guarantees can be made about safe flight termination.

Because FAA recognizes the seriousness of lost-link situations, current authorizations for a UAS to fly under a Certification of Authorization (ref. 12) or Experimental Certificate predominantly limit operations to unpopulated areas, and, in many cases, require airspace

restrictions to reduce potential interference of UAS with other aircraft. Procedures are typically put in place such that "should loss of link occur, the UAS pilot must immediately alert air traffic control (ATC) and inform the controllers of the loss of control link. Information about what the aircraft is programmed to do and when it is programmed to do it is pre-coordinated with the affected ATC facilities in advance of the flight so that FAA can take the appropriate actions to mitigate the situation and preserve safety." (ref. 13)

With these thoughts in mind, the following revised definition for "catastrophic" was proposed:

> Catastrophic: Failure conditions that are expected to result in ~~multiple fatalities of the occupants, or incapacitation or fatal injury to a flight crewmember normally with the loss of the airplane.~~ ***one or more fatalities or serious injury to persons, or the persistent loss of the ability to control the flight path of the aircraft normally with the loss of the aircraft.***
> Notes: (1) The phrase "are expected to result" is not intended to require 100% certainty that the effects will always be catastrophic. Conversely, just because the effects of a given failure, or combination of failures, could conceivably be catastrophic in extreme circumstances, it is not intended to imply that the failure condition will necessarily be considered catastrophic. ~~(2) The term "Catastrophic" was defined in previous versions of the rule and the advisory material as a Failure Condition that would prevent continued safe flight and landing.~~

In addition to the definitions of severity levels, the advisory circular provides additional guidance about the relationship between the severity levels and the effects of failure on the airplane, flight crew, and occupants. Some changes to that guidance are essential for a UAS. Table 4 shows the relationships specified in AC 23.1309-1C, with proposed changes highlighted. Additions to the original text are indicated in bold italics font, and deletions are indicated by striking through the text.

Table 4. Relationship Between Severity Levels and Effects for a UAS

Classification of Failure Conditions	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Effect on ~~Airplane~~ ***UAS***	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with ~~*hull loss*~~ ***uncontrolled loss of aircraft***
~~Effect on Occupants~~	~~Inconvenience for passengers~~	~~Physical discomfort for passengers~~	~~Physical distress to passengers, possibly including injuries~~	~~Serious or fatal injury to an occupant~~	~~Multiple fatalities~~
Effects External to UAS	***No effect***	***No effect***	***Potential for physical discomfort***	***Physical distress, possibly including injuries***	***Potential for one or more fatalities and/or severe injuries***
Effect on ***UAS*** Flight Crew	No effect on flight crew.	Slight increase in workload or use of emergency procedures	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatal injury or incapacitation

One obvious change involves modifying the guidance for the effect on *airplane* to be guidance for the effect on *UAS*. As shown in table 4, the effect on UAS is very similar to the effect on airplane, except that catastrophic failure for a UAS is concerned with *uncontrolled* hull loss. An

uncontrolled hull loss, for example, may result from a permanent lost-link situation. On the other hand, the automatic destruction of the UAS, in a safe circumstance, or controlled flight into a designated crash location may be considered examples of acceptable *controlled* hull loss.

The effect on flight crew is proposed to be the same, regardless of whether the flight crew supports a manned or unmanned aircraft. However, for unmanned aircraft, the effect on flight crew may not necessarily be tightly coupled with the effect on a UAS. For example, a system failure with a catastrophic consequence to the UAS, may not be catastrophic for the flight crew, although that would likely be the case with a manned aircraft. For example, an uncontrolled loss of a UAS would not likely cause fatal injury or incapacitation to the ground crew. On the other hand, hazards limited to the ground station, such as a fire, may have catastrophic consequences for the crew, but not for the vehicle.

The final change is that guidance for effect on occupants was deleted, and new guidance for effects external to a UAS was added. This new row considers the potential effect of a failure to persons on the ground or in other aircraft. The effects specified here are specific to physical discomfort, injury or death to third parties. As shown in table 4, the severity of each potential effect has been increased with respect to third parties, as compared with the effect on occupants. For example, potential for physical discomfort is considered to be major for third parties, but only minor for aircraft occupants. The rationale for increasing the severity is that the third parties are, in effect, innocent bystanders, whereas aircraft occupants assumed some level of risk by boarding the aircraft.

Table 4 does not include guidance about effects on air traffic management (ATM). Such guidance is not included in AC 23.1309-1C. But, considering the potential effect on ATM may be worthwhile because unmanned aircraft may increase demand on various elements of the civil ATM system, particularly surveillance and communications. Ideally, we would not want unmanned aircraft to place a burden on the system greater than the burden imposed from an equivalent number of manned aircraft. “In essence, the function of maintaining safe separation, passing instructions and providing efficient tactical management of traffic flow should be no more labour intensive, or less safe.” (ref. 14) This may require the adaptation of additional forms of safety analysis such as described in RTCA DO-264, Guidelines For Approval Of The Provision And Use Of Air Traffic Services Supported By Data Communications, (ref. 15) to supplement the traditional aircraft oriented techniques. For the purposes of this report, however, only aircraft oriented techniques are explored.

It is important to note that the hazard definitions presented in this section are intended to be a starting point for thinking about the effects of failures. Further modifications will likely be warranted as potential UAS failures and their effects are better understood.

4 Applying Functional Hazard Assessment to a UAS

Given a starting set of hazard definitions, a next step is to see how they might apply in the assessment of UAS hazards. Functional hazard assessment (FHA) is a systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity. SAE ARP 4761 (ref. 16) provides guidance for the FHA process used in civil aviation.

According to SAE ARP 4761, the FHA process:

- provides the top-level design criteria for a system
- determines the depth of further analysis
- allows for derivation of the system architecture
- is independent of hardware and software

The FHA process, in general, is intended to be iterative and becomes more defined and fixed as a system evolves. The output of the FHA is an identification of the potential failure modes, associated hazards, and their criticalities. This output is the starting point for the generation and allocation of safety requirements of a system.

Some special considerations are worth noting when applying FHA to a UAS. Traditional FHA for manned aircraft is concerned with the functions on board the vehicle and its systems. For a UAS, functions integral to safe operation, such as command and control functions resident with a remote pilot, may not necessarily reside on the vehicle. An FHA of a UAS should include all functions integral to the safe operation of the vehicle, regardless of where those functions reside. Though, where a function resides may affect the possible failure conditions and their consequences and severities.

It is also worth noting that the functions described in our FHA process were for a generic UAS, as opposed to a specific UAS platform. Although there is considerable variation among UAS platforms, there presumably is a core set of functions that most aircraft, including unmanned aircraft, will need to operate routinely and safely within the NAS. For this study, we used colloquial tenets of piloting; namely, to fly the plane (*aviate*), fly it in the right direction (*navigate*), and, state your condition or intentions to other people (*communicate*) to provide a rudimentary framework for organizing functions of a UAS. A fourth category, *mitigate hazards,* was also added to the framework. This category is intended to capture those actions necessary to (1) stay clear of hazards, including other air traffic, flight or ground path obstructions, and adverse weather conditions, and (2) manage contingency situations that may arise. Managing contingencies (or mitigate in general) is not typically specified as a separate function for manned aircraft, but is included as part of other functions. This category was included here to highlight a class of functions that are performed implicitly by the on-board pilot in a manned aircraft, but may be performed by automation in a UAS. As such, new hazards may arise. The core set of functions used in our FHA is given in a functional decomposition of the generic UAS discussed in the next section.

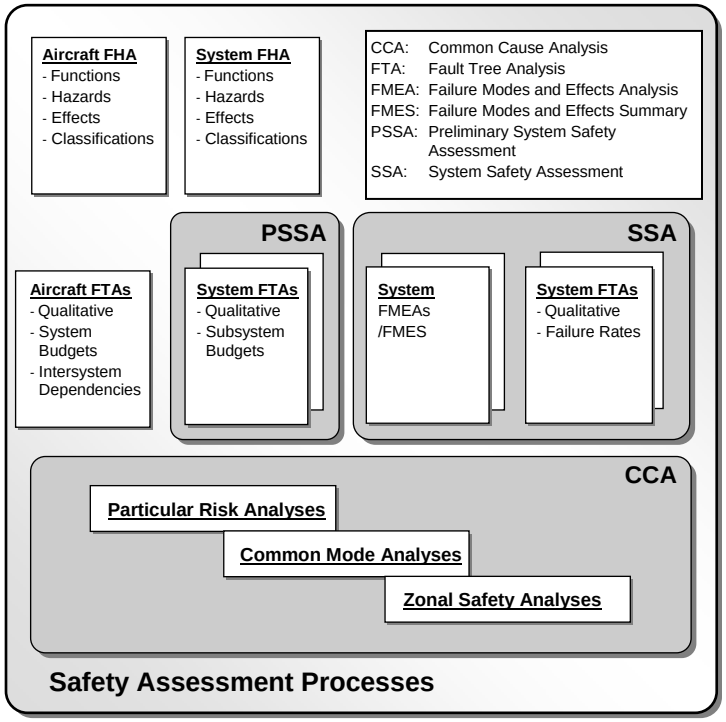
A final consideration worth noting relates to the types of hazards applicable to a UAS. For manned aircraft, hazards associated with the safety of the crew and passengers are the primary concern. For a UAS, hazards involving impact with people or property on the ground and impact with other aircraft are the primary concern. Reliance on a remote pilot, as well as on-board automation, also introduces different considerations for failure conditions.

In this section, fundamental aspects of the FHA process are described in brief, along with specific tailoring of the process to accommodate unique aspects of unmanned aircraft.

4.1 FHA Fundamentals

The FHA process described in this report is based on the safety assessment methodology specified in SAE ARP 4761. Figure 2 shows a top-level view of the system safety assessment process described in that document. For this project, the “Aircraft FHA” shown in figure 2 is actually a “UAS FHA”.

Figure 2. System Safety Assessment Processes from SAE ARP 4761



According to SAE ARP 4761, the objectives of the FHA are to consider functions at the most appropriate level and to identify failure conditions and the associated classifications while considering both loss of functions and malfunctions. The FHA should identify the failure conditions for each phase of flight when the failure effects and classifications vary from one flight phase to another. The FHA should also establish derived safety requirements needed to limit the function failure effects which affect the failure condition classification. The safety requirements may include such things as design constraints, annunciation of failure conditions, or recommended flight crew or maintenance actions.

The FHA process is a top down approach for identifying the functional failure conditions and assessing their effects. This assessment proceeds through the following steps:

a. identifying all functions associated with the system under study (given in this report in the functional decomposition)

b. identifying and describing failure conditions associated with these functions, considering single and multiple failures in normal and degraded environments

c. determining the effects of the failure condition

The essential prerequisite for conducting an FHA is a description of the high level functions of the system. For this study, those functions were captured in the UAS functional decomposition presented in Section 5. This functional decomposition was based on functional requirements for a generic UAS as specified in a functional requirements document developed under NASA's Access 5 program (ref. 17). It is important to note that a preliminary FHA is performed before the functions have been allocated to equipment, procedures or people; that is, it considers what

the proposed system will do, rather than how the functions may be implemented. Preliminary FHA results can be used to support function allocation.

Other aspects of the UAS are important to the FHA process in addition to the functions themselves. These aspects include a description of operational scenarios (how the system will be used and in what environment) and relevant regulatory policy and guidance. For this project, much of that information is given in the Access 5 Concept of Operations (ref. 18). The final output of the FHA process is a comprehensive description of the system to be assessed. Here, that description is mostly embodied in the functional decomposition.

Once the system functions are defined, the next step is to identify possible failure modes or conditions for each function, and what the consequences of those failures might be. Hazards are the results of failures within the system, the combination of failures and interactions with other systems, and external events in the operational environment. To identify potential hazards, it is necessary to consider the various ways each individual function of the system can fail (that is the failure mode). Given each failure mode, the consequence of that failure should be described. Consequences of failures may include effects on the functional capability of the UAS, air traffic management operations, and the operator; e.g., workload. Figure 3 shows the template used in this project for documenting the functions, failure conditions, their consequences, and criticality classification.

Figure 3. FHA Template

Record #	Function	Flight Phase	Failure Conditions	Operational Consequences	Criticality	Remarks

Much of the FHA process as described in SAE ARP 4761 can be applied directly to assessment of a UAS. A few areas, however, need special consideration due to the unique aspects of a UAS, namely, failure conditions and phases of flight.

4.2 Failure Conditions for a UAS

Two approaches to enumerating failure conditions of a UAS were considered. The first approach is shown in the appendix of AC 23.1309-1C, and the second approach is taken from examples in SAE ARP 4761. The example FHA for Class I general aviation aircraft in Appendix A of AC 23.1309-1C identifies failure conditions in three categories: (1) total loss of function, (2) loss of primary means of providing function, and (3) misleading and/or malfunction without warning. Implicit in the example FHA is that the pilot is ultimately responsible for redundancy management. That is, the pilot appears to be responsible for managing the switch between primary and secondary functions. This view of the system also implicitly assumes a systems architecture that may not adequately capture the complexities of highly automated UAS.

SAE ARP 4761 takes a slightly broader approach to failure conditions, identifying failure conditions specific to a single abstracted aircraft function. In an example from Appendix L of that document, failure conditions for the function “Decelerate Aircraft on Ground” are as follows:

- Loss of all deceleration capability
- Reduced deceleration capability
- Inadvertent deceleration
- Loss of all auto stopping features
- Asymmetrical deceleration

These failure conditions reveal an implied classification: there are two different cases of function degradation, and two types of malfunction. None of these failure conditions is architecture specific (except perhaps for the existence of an "auto stopping" capability).

For the preliminary UAS FHA, the functional failure conditions were listed in a manner similar to the example given in Appendix L of SAE ARP 4761. The functional failure condition classification considered the following potential effects of failures on function capabilities:

- Total loss of function
  - Detected and undetected
  - Example includes: loss of all deceleration capability
- Partial loss of function/degraded functional capability
  - Detected and undetected
  - Generic and specific
  - Examples include: reduced deceleration capability (generic loss), loss of all auto stopping features (specific loss), loss of accuracy for navigation information, and reduced control authority
- Malfunction (including misleading information)
  - Detected and undetected
  - Generic and specific
  - Examples include: inadvertent deceleration (specific malfunction), asymmetric deceleration (specific malfunction), asymmetric thrust, unintended control action (e.g., in-flight thrust reversal), and persistent offset from correct navigation information

As in the SAE ARP 4761 example, some functions may have several types of degradation and several potential malfunctions. Consequently, each function may have several rows in the FHA, and different functions may have a different number of failure conditions to consider than other functions. In the FHA, each row identifies some degradation of function combined with flight phase and degree of system knowledge about the failure, and a specific hazard classification (i.e., minor, major, hazardous, or catastrophic).

4.3 Phases of Flight for a UAS

The last aspect of the FHA process worth mentioning is the phase of flight when a failure occurs. In some cases, a particular function may be used throughout the entire flight; while in other cases a function may only be used during one phase of flight. According to SAE ARP 4761, "the FHA should identify the failure conditions for each phase of flight when the failure effects and classifications vary from one flight phase to another." In some cases, the phase of flight for a particular function may be "all" if the same failure conditions are consistent throughout all flight phases.

A typical FHA includes common phases of flight such as taxi, take-off, climb, enroute, approach, and landing. For the purposes of this study, only those failure conditions relevant to the enroute phase of flight were considered, due specifically to time limitations on the project. Follow-on work might consider extending the FHA for the other phases of flight.

An interesting phase of flight to consider for future work, and one that might be unique to a UAS, is loitering. A number of potential commercial applications involve this phase of flight

where the UAS remains within a relatively small local area for an extended period of time. It may be worthwhile to examine whether there are any unique failure conditions to be considered in a loitering phase of flight.

The next section covers the functional description of a generic UAS and the process used for organizing the functions.

5 Functional Decomposition of a Generic UAS

For this study, a functional decomposition refers to a hierarchical organization of all the functions of a system. A simple tree structure is used to represent the basic relationship between the functions. The decomposition proceeds from the top (in our case, UAS) to various levels of functions. When decomposing functions, it is not always obvious when to stop. Following the guidance in AC 23.1309-1C, the decomposition continues until "the lowest defined level of a specific action…that, by itself, provides a complete operational capability" is reached. There are several key points in this criteria. One is that a function refers to a specific action. There are many legitimate requirements that are not functions. For instance, a UAS may be required to comply with certain FARs, but this is not a function because a function must perform some action. Another point is that functions must include a complete operational capability. This means that a function must be observable at the operational level. The effect of this is that the functional decomposition cannot proceed indefinitely. For example, the calculation of navigation accuracy violations is not, by this definition, a function. Conveying navigation state to the flight crew is a function because it is observable at the operational level. In addition, the guidance of SAE ARP 4754 (ref. 19) states that a function includes its interface (human or machine).

5.1 Purpose of Functional Decomposition

Hazard analysis is used to answer questions about the safety of a system. These analyses presume that if all hazards have been adequately addressed, then the system will be safe. Therefore, a major issue with hazard analyses is ensuring that all hazards have been captured. The basic technique used to ensure coverage is one of partitioning the hazards.

The FHA approach, described throughout this document, first partitions the system into functions, then assesses the hazards associated with each function. Because functions have a smaller scope than the system as a whole, it is assumed that if all hazards for all functions have been captured, then all hazards for the system have been captured[3]. If all hazards for each identified function have been addressed, the question then arises, have all the functions been identified?

The functional decomposition attempts to answer this question. The functional decomposition is a structured way to identify all functions in the system. As should be expected, the functional decomposition is not guaranteed to identify all functions, but it is a tool to help that effort.

5.2 The SAE ARP 4761 Approach to Functional Decomposition

Examples in SAE ARP 4761 served as a model for separating the functions of a system. Figure 4 shows the SAE ARP 4761 view of a functional decomposition.

[3] The validity of this assumption should not be taken for granted. It is typically very hard to identify hazards that arise from situations where there are small deviations from expected behavior.

Figure 4. Example Function Decomposition from SAE ARP 4761

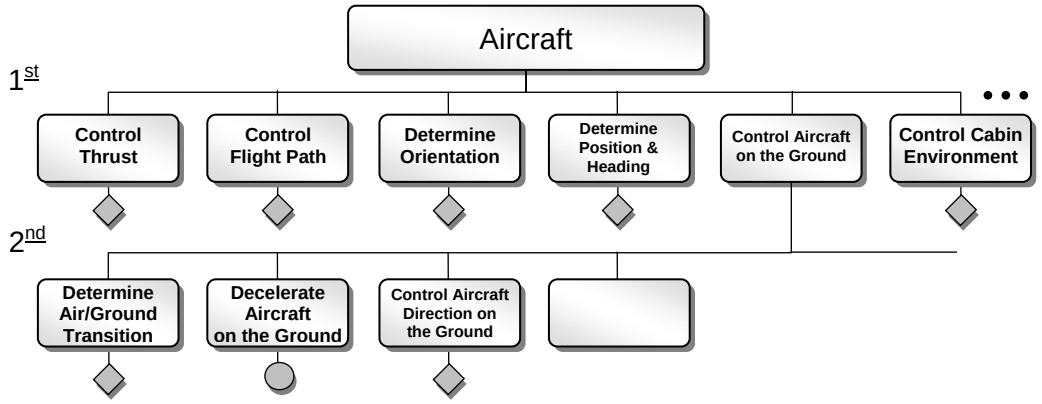


Figure 4 provides a guide for the granularity of the functions in a functional decomposition. The notation in this figure is as follows: the boxes followed by diamonds indicate that the decomposition of that function continues, but is not shown; boxes followed by a circle indicate the lowest level functions that cannot be decomposed further. In this example, actions such as controlling thrust, controlling flight path, and determining orientation are relatively high-level actions that can be refined further, whereas the function "decelerate aircraft on the ground" is the lowest level action that is operationally visible and is not decomposed further.

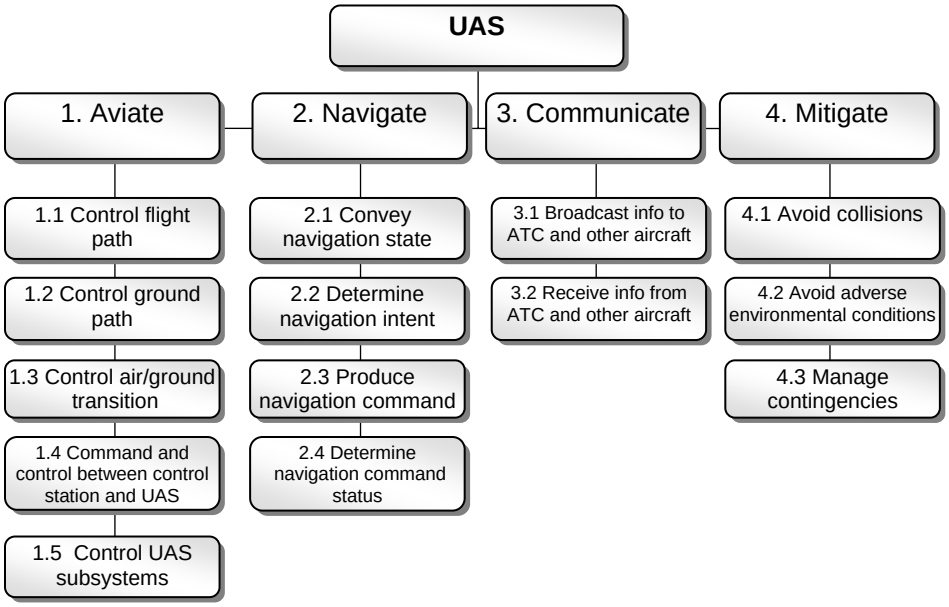
The process described in SAE ARP 4761 assumes that the functional decomposition is for a specific vehicle. For this example, decelerating aircraft on the ground is the lowest-level operational action. On other aircraft, there may be multiple ways for pilots to decelerate the aircraft on the ground such as braking, parachute, or thrust reversers. For this alternate vehicle, "decelerate aircraft on the ground" would not be the lowest-level action and this function would need to be decomposed further.

The functional decomposition presented here is intended to be as generic as possible, while capturing the significant functions necessary for safe flight of any UAS. A number of aircraft function lists from major transport and general aviation aircraft venders were reviewed in the development of the decomposition to provide a check for consistency and completeness of the function list. Because of the wide variation in UAS types and operations, no single functional decomposition of a UAS can possibly cover the range of functions of all vehicles. The functional decomposition in this report leans more towards those unmanned aircraft that are similar to conventional transport or general aviation aircraft.

5.3 UAS Functional Decomposition

The full functional decomposition is relatively large, with 69 functions at the lowest level under the major functions of aviate, navigate, communicate, and mitigate. Figure 5 shows a top level view of these functions.

Figure 5. Top-level of the Functional Decomposition



Aviate includes not only actions involved in flying the aircraft, but also actions for moving the aircraft on the ground, providing command and control, and managing sub-systems. Navigate includes actions involved in the management and execution of a flight plan. Communicate provides functionality for the communication between the UAS, ATC and other aircraft. All actions associated with the command and control link to the vehicle are contained within the Aviate category. Mitigate includes actions such as avoiding traffic, avoiding ground objects, avoiding weather or other types of environmental effects, and handling contingencies. The motivation for this particular top-level decomposition is to capture, as a category, each of the basic actions that pilots perform in a manned aircraft.

The Mitigate function is not typically included as a top level aircraft function. The common saying is that when pilots are taught to fly, they are taught to aviate, navigate, and communicate. By explicitly calling out a mitigate function, the hope was to capture a category of functions that in many aircraft are performed by the pilot, but will likely be performed by automation in a UAS. To help ensure these functions are adequately emphasized for discussion and debate, the Mitigate category was created. Figures 6 through 11 give the complete decomposition under each of the four major functions.

Figure 6. Aviate Functions

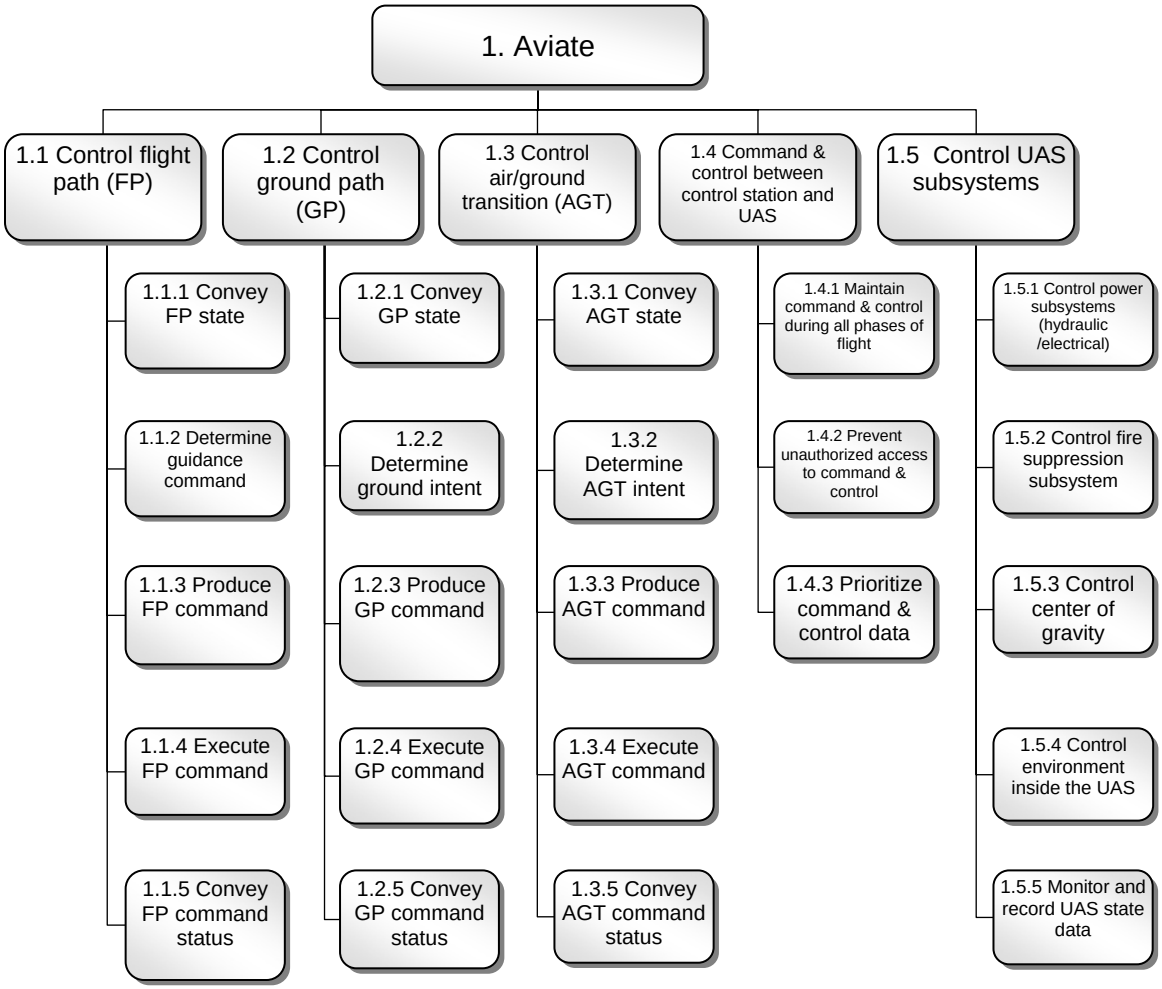


Figure 7. Navigate Functions

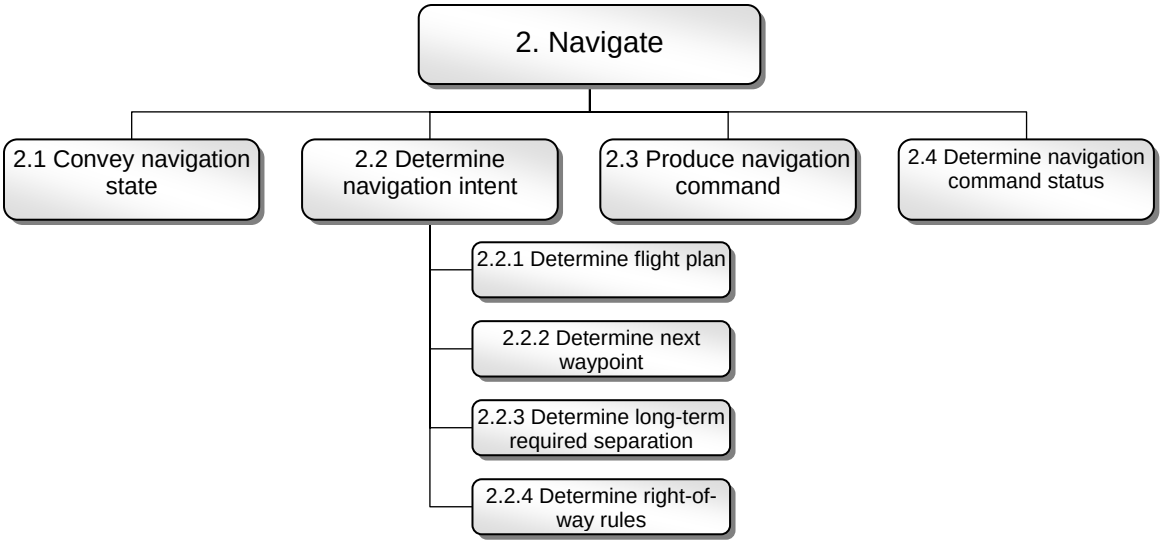


Figure 8. Communicate Functions

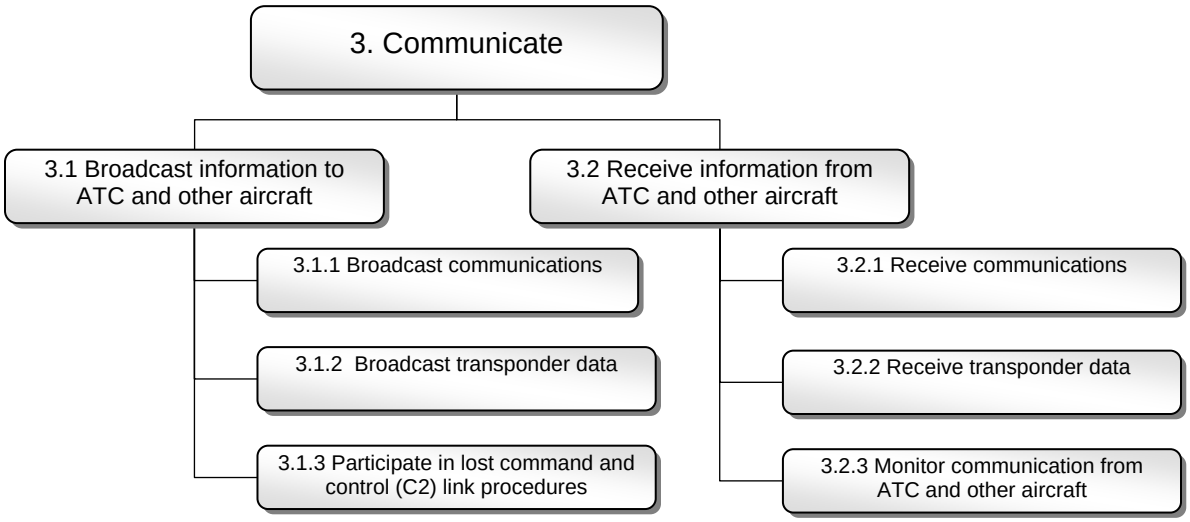


Figure 9. Mitigate Functions

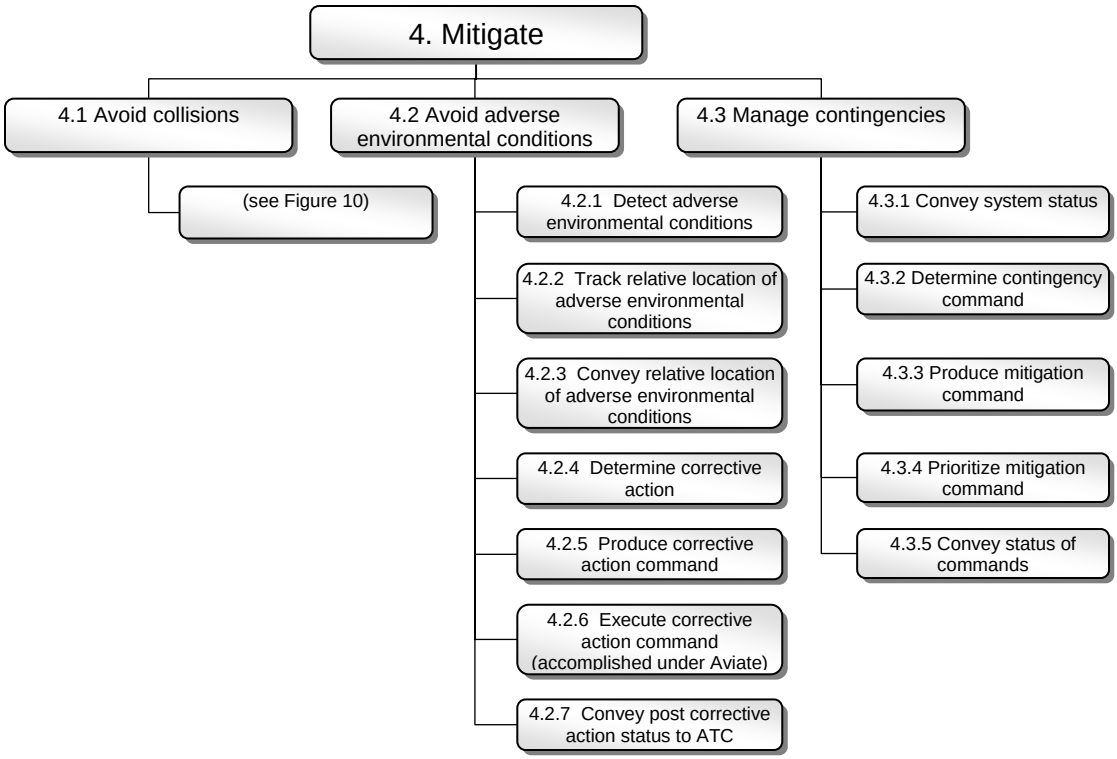
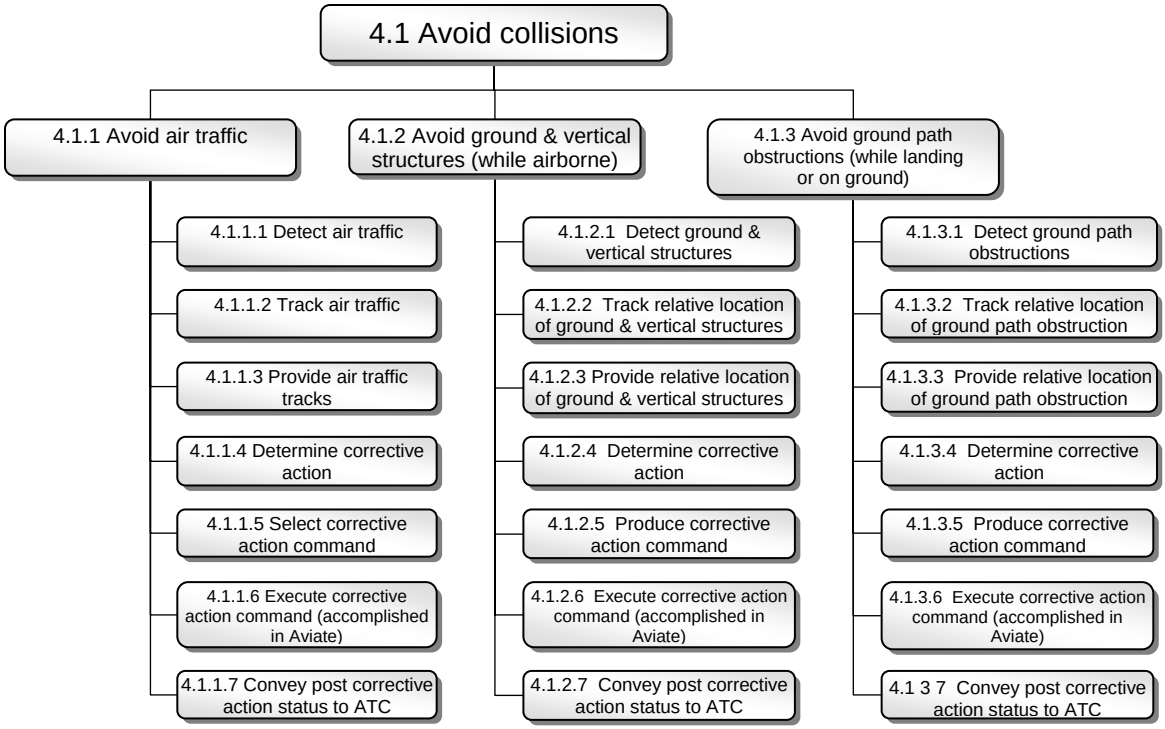


Figure 10. Avoid Collisions



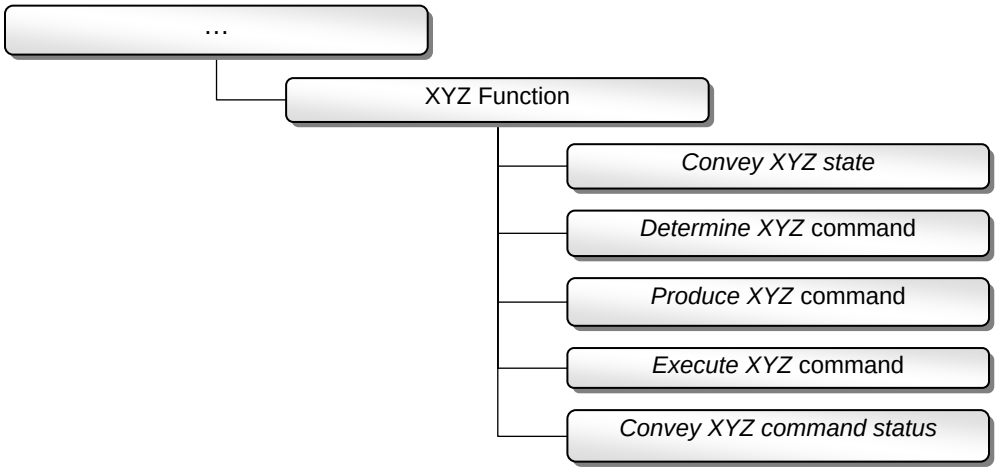
One important point about functions in these categories is that they often rely on the existence of other functions in other categories. For instance, the functions within Navigate perform tasks such as finding the next waypoint and determining guidance commands. However, the actual moving of control surfaces and changing propulsion settings to reach that waypoint are handled by the functions within Aviate. In a similar way, the Mitigate function relies on functions within Communicate, Navigate, and Aviate. As an example, handling contingencies may require communication to alert ATC, navigation to fly to a contingency waypoint, and aviation to move control surfaces.

5.3.1 Low-level Function Template

In the early stages of developing the decomposition, a definite pattern emerged. This pattern, included five basic actions related to a given function, which may be executed sequentially or concurrently (or some combination thereof). To help provide consistency in terminology, a template for those actions or low-level functions was developed, as shown in Figure 11.

The first action is to *convey* any *state* that is relevant to the function. This action includes all aspects of conveying the state: sensing, communicating, and displaying. Originally, we used the term "display;" which is common in function lists for manned aircraft. This term was rejected, however, because it could imply a design decision that the information is to be visually presented to the operator. Because we cannot assume that all unmanned aircraft will present the information to the operator (visually or otherwise), a more generic term was chosen: convey. For example, conveying the state of a navigation function would involve sensing and communicating information about latitude, longitude, and altitude (and perhaps other quantities).

Figure 11. Low-level Function Template



The *determine* function means gathering and selecting the appropriate high level command. For instance, the determine command may involve gathering flight plan information for a navigation command.

The *produce* function involves the translation of a strategic goal into a tactical command. One example is the behavior of a traditional flight control system: high-level attitude commands are translated into low-level flight control surface commands.

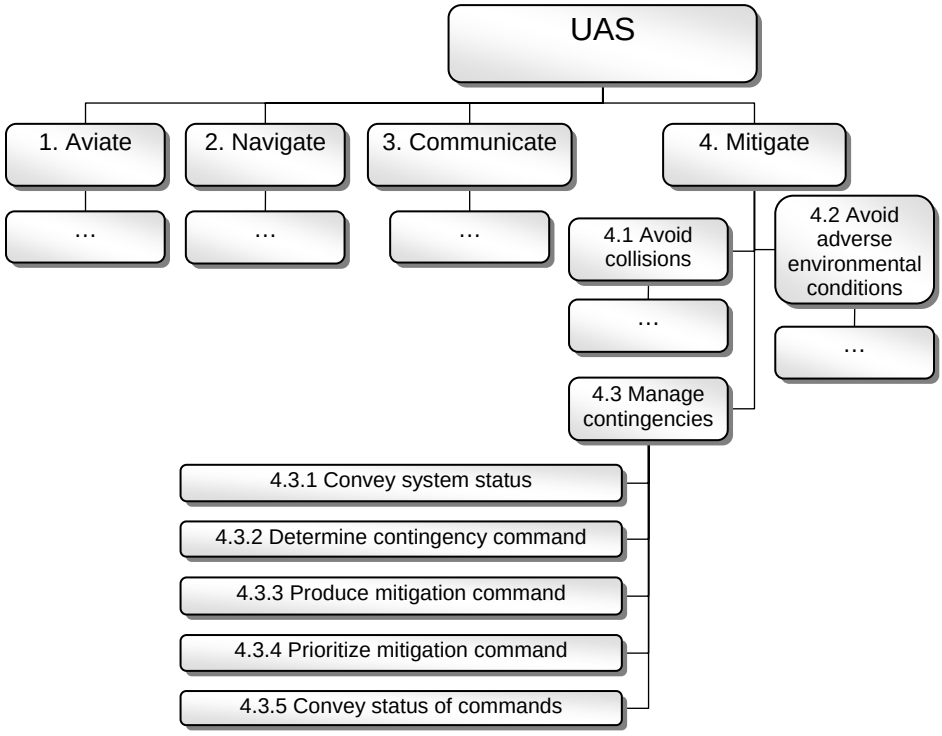
The *execute* function refers to physically maneuvering the vehicle in some way. All execute functions are listed in the Aviate category.

The final function in the template is to *convey* the *command status*. This function is intended to address the difference between command and execution; that is, what is commanded and what is executed may be different. The command status informs the operator or perhaps some diagnostic system about what was commanded and the actual effect of the commanded action.

5.3.2 An Example of Low-level Functions

To demonstrate how the template was used, consider function 4.3 Manage Contingencies, as shown in figure 12. In this example, no decision has been made about where (control station or vehicle) or who (operator or automation) manages contingencies.

Figure 12. Manage Contingencies



Convey the system status (function 4.3.1) means gathering information about the state of the UAS related to contingencies, such as the communication status. Determine the contingency command (function 4.3.2) means analyzing the system to determine what contingencies have occurred. Because there may be multiple failures, determining what is actually wrong with the UAS may not be trivial. Producing a mitigation command (function 4.3.3) means deciding which actions should be taken to respond to the current contingencies. Prioritize the mitigation commands (function 4.3.4) attempts to reconcile that sometimes one event will cause multiple contingencies. Some of these contingencies may be very important and need to be dealt with right away, whereas other contingencies can be dealt with later. Finally conveying the status of the mitigation commands (function 4.3.5) means that the operator (and perhaps automation) will want to know what mitigation actions have taken place. For instance, if the fire detectors are

going off and fire extinguishers have been deployed, then that could mean the fire is too extensive for the fire extinguishers to extinguish, that the fire detector sensor is faulty, or that the design of the fire detection system is faulty. There could be other explanations, as well. In any case, it is important that the operator knows that the fire extinguishers have been deployed so that time is not wasted attempting to deploy them again.

Notice that in this example, the execute function is not listed. This is because executing a mitigation command may require the resources of aviate, navigate, and communicate. In addition, a "prioritize" function was added which was not part of the functional template. For managing contingencies, the act of prioritizing contingency commands was considered a significant function whose failure could have safety consequences.

6 Functional Hazard Assessment Overview

The preliminary FHA discussed here and shown in the appendix is not, in any way, intended to represent a complete, validated FHA. Significant effort was put into correct and complete identification of potential UAS failure conditions and characterization of their severity, for single failure events in the enroute phase of flight only. Additional work remains to be done for other phases of flight and multiple failure events.

To understand the FHA, it is helpful to know some of the ground rules and assumptions used in the FHA process. Rule number one is "do no harm". The safety goal is to avoid any UAS-initiated decrease in the safety of the NAS. As a result, failure condition criticality is determined by its effect on people on the ground or in other aircraft. The latter case includes stress or injury to occupants of other aircraft as a result of an evasive maneuver. Damage to material assets is out-of-scope, unless it affects human safety.

The following assumptions were made in the development of the preliminary FHA. For the purposes of this study, the FHA shall:

- assume no specific architecture or design
- make no presumption about where a function resides
- consider the enroute flight phase only. Because of the Access 5 focus on high-altitude aircraft, the enroute phase of flight was assumed to be at flight level 430 or above, where air traffic control is responsible for separation.
- consider single failures only
- assume current air traffic control operations, procedures and technologies (that is, concepts such as "free flight", 4-D trajectory, or fully data-linked, autonomous concepts of operation are not considered)
- use the FHA table format from SAE ARP 4761, with minor variations, as described in section 4.1
- consider failure condition classifications as described in section 4.2

6.1 Assignment of Failure Condition Severities

A significant step in the FHA process is assigning criticality or severity levels to each of the failure conditions that are defined for each function. The definitions for the failure condition severities are given in Section 3. Here we discuss how to interpret and apply those definitions for specific failure conditions. The operational consequence and corresponding severity is obvious

for some failure conditions, while others are controversial or difficult to classify. When controversy does arise, it is usually due to a couple of factors:

- natural tension between the desire to be conservative when it comes to safety, but on the other hand, not to be so conservative as to impose unreasonable requirements
- sensitivity of the outcome of a given failure condition to operational or environmental circumstances

A "catastrophic" assessment for a particular failure condition may appear to impose an onerous burden on product development, not only in terms of the hardware and software design and equipment costs, but also in the certification costs. This is due to the fact that the more severe a failure condition is, the less likely it must be proved to be. For example, some catastrophic failures are assigned a frequency of occurrence somewhere between 10^{-6} and 10^{-9} per flight hour[4], depending on aircraft category, whereas major failures are assigned in the 10^{-4} to 10^{-5} range. Reaching such levels for catastrophic failures has traditionally been very costly, and may even be prohibitive, especially for a small UAS manufacturer.

During and after the subsequent architecture development and system design phases, the manufacturer will have ample opportunity to address the concerns by various means. One option is to produce an architecture and a design that includes effective redundancy management and mitigation strategies. Based on this or other strategies, the supplier may petition the FAA to acknowledge lower levels of hazard categories in specific areas of concern, that is, from architectural mitigations for certain failure conditions formerly labeled as catastrophic.

For this study, we defined and documented a method for assigning a severity to any particular failure condition. This method was intended to help clarify why particular severity assignments were made, and also to facilitate consistency for assigning severities.

A worst-case, single-failure assessment strategy was used to assign a severity to each failure condition. Failure conditions that are not the worst case may be included to better describe system behavior in certain situations; however, the worst case was always captured. Only single failures were considered in the FHA due to time limitations on the project[5]. For this discussion, it is assumed that the function, flight phase, and failure condition have already been determined. The operational consequence and the severity classification are developed together, using the following steps.

Step 1. The first consideration is a creative process of imagining the operating conditions in which the failure occurs. The hazard severity definitions disallow the assumption of perfect conditions. Therefore, if the consequence is made worse by any of the following adverse operating conditions, a more severe classification should be given:

a. Flight crew is busy with another task.

b. Weather (visibility, winds, turbulence) conditions are bad.

c. Traffic conditions are heavy.

Recall that failures are not included in this list of adverse operating conditions. At this phase in the analysis, multiple failures were not considered.

[4] It is important to recognize that target reliability figures specific for UAS have not been developed. Determining reasonable estimates for such numbers requires extensive analysis beyond that given in this report. Ultimately, regulatory authorities will determine the final values.

[5] Multiple failure conditions should be considered in future phases of the analysis.

Step 2. The assessment proceeds by assessing the effects on three entities: the UAS itself, the flight crew of the UAS, and any people external to the UAS, as shown in table 4 in section 3. The specific evaluation of each of these effects is described in the three steps that follow; however, the evaluation is usually easier if the effects on flight crew and people external to the UAS are considered first. Because this is a worst case analysis, when the effects on one entity are determined, effects on other entities are only relevant if they have a more severe consequence.

Step 2a. The assessment on the UAS is performed in two dimensions: safety margins and operational capabilities. Safety margin refers to the gap between expected use and an unsafe condition. Safety margins are added to mitigate the normal uncertainties involved in aviation systems including: design, manufacture, flight crew abilities and training, sensor inaccuracies, etc. By definition, some safety margin can be lost, and the UAS will continue to be safe. Safety margins include separation standards between vehicles, between a vehicle and the ground, between a vehicle and weather, etc.

If a failure condition causes a complete loss of safety margins (normally involving a loss of the vehicle), then this condition is designated catastrophic. An example of this is if the UAS can no longer be controlled. If a failure condition has no effect on safety margins, then this condition is labeled "no effect." A significant reduction of safety margins means some condition where—absent other failures and all but the most extreme adverse operating conditions—it is reasonably expected that safe flight and landing can occur. Such a failure condition is labeled major. Even though a UAS which experiences one of these failures is expected to be safe, the safe use of the UAS may result in damage to the UAS. For instance, a vehicle may run off the end of the runway into a field and have the landing gear collapse. If the effect of the failure condition causes more than a significant reduction of safety margin, but does not cause a complete loss of safety margin, then this condition is designated hazardous. If a failure condition has more than no effect but less than a significant effect (as just described), then this failure condition is labeled minor.

Loss of operational capabilities is important to safety because as operational capabilities are lost, possible actions which can mitigate unsafe situations are eliminated. Therefore, if a failure condition causes loss of all operational capabilities—normally including loss of the vehicle—then this condition is designated catastrophic. If the failure condition causes no loss of operational capabilities, then this condition is labeled no effect. A significant loss of operational capabilities means that a failure condition causes cascading failures of only a few less critical functions such that, at most, one mitigating action is lost[6]. Such a failure condition is designated major. If the effect on the UAS of the failure condition causes more than a significant loss of operational capability, but does not cause a complete loss of operational capabilities, then this condition is designated hazardous. If a failure condition has more than no effect but less than a significant effect (as just described), then this failure condition is labeled minor.

[6] Communication with air traffic control is an example of one mitigating action.

Step 2b. Next, an assessment of the effects on the flight crew is performed. If the crew is no longer able to perform their assigned tasks (due to either incapacitation or death), then the event that caused this is catastrophic. Other effects on the flight crew are examined in two dimensions: physical effects and workload effects. In terms of physical effects on the flight crew, if any member of the flight crew sustains an injury that would normally require significant medical attention (for example, a broken leg), then this is considered physical distress and is designated hazardous. If any member of the flight crew sustains an injury that normally does not require medical attention (for example, scrapes and bruises), then this effect is considered physical discomfort and is designated major.

In terms of workload, if the expected result from a failure condition is that any member of the flight crew is unable to perform one of their important[7] tasks, then this condition is considered hazardous. If the failure condition requires any member of the flight crew to slightly increase their workload, then this failure condition is classified as minor. If the workload of any member of the flight crew is more than slightly impacted, but not impacted enough to preclude them from performing tasks, then this failure condition is designated major. When assessing workload, a flight crew of average training and ability is assumed. It is immaterial that the presence of a flight crew of exceptional ability or training would result in a less severe event.

Step 2c. Finally, an assessment of the effects on anyone who is not a member of the flight crew is performed. This includes people on board other aircraft, people located at airports, and the public at large. If anyone is killed or severely injured (that is, requiring an extended hospital stay), then this failure condition is classified as catastrophic. If anyone sustains an injury that normally requires significant medical attention (for example, a broken leg), then this is considered physical distress and is designated hazardous. If anyone sustains an injury that does not normally require medical attention (for example, scrapes and bruises), then this effect is considered physical discomfort and is designated major.

Step 3. Because this is a worst-case analysis, the most severe consequence of these three effects is captured in the FHA.

Step 4. The hazard classification from Step 3 is compared to the classification of other failure conditions for this function. Is the classification uniform? Is it clear that more severe failure conditions have more severe operational consequences and therefore, more severe classifications?

Step 5. As an initial validation, the example FHA in appendices A and B of AC 23.1309-1C should be consulted to determine if a similar function and failure condition exists. If so, then the severity classification should be the same, or a clear reason should exist as to why the classification is different.

6.2 Example FHA Entries

The preliminary FHA to date is extensive, and is thus relegated to the appendix. In this section, several examples of FHA entries are discussed to illustrate how the FHA was done. In

[7] Not all required tasks are of equal importance or complexity.

each example, the record number for the FHA entry is given, along with the name of the function, specific failure condition under consideration, assigned criticality level, phase of flight, and remarks as appropriate. These examples are chosen from the functions 1.1 Control Flight Path (under 1. Aviate), and 4.1 Avoid Collisions and 4.3 Manage Contingencies (under 4. Mitigate). Several possible failure conditions are described for each function. The examples are taken directly from the FHA in the appendix.

6.2.1 Example from the "Execute Flight Path Command" Function

The first example is based on function 1.1.4 Execute Flight Path (FP) Command, under Aviate. This function involves using the flight path command to change the physical state of the vehicle. Tables 5 presents two entries in the FHA for this function.

Table 5. FHA Example: Execute Flight Path Command

Number	Function	Flight Phase	Failure Condition	Operational Consequence	Classification	Remark
1.1.4.a	Execute FP command	enroute	Loss of function with soft landing flight termination function	Vehicle will not be controllable; landing will be somewhat controllable.	hazardous	Execution of a soft landing function assumes that people will not be killed or seriously injured.
1.1.4.b	Execute FP command	enroute	Loss of function without soft landing flight termination function	Vehicle will not be controllable.	catastrophic	

In both of these failure modes, the vehicle is unable to execute a flight path command in the enroute phase of flight. This situation means the vehicle is uncontrollable. By Step 2a of section 6.1.1, a failure mode that results in an uncontrolled vehicle is designated catastrophic. In record number 1.1.4.a, the failure condition assumes the existence of some type of function that will "gently" end the flight. Because of this mitigating action, the hazard classification for this failure mode is lowered from catastrophic. This mode is designated hazardous because there has been a reduction in safety margins such that "safe flight and landing" cannot be reasonably assured.

6.2.2 Example from the "Detect Air Traffic" Function

The next example is based on the detect air traffic function, which is function 4.1.1.1 in the functional decomposition. This function is the first step in any "sense and avoid" function. Table 6 gives the FHA entry of three failure conditions for this function. Each of these failure modes has been assigned a hazard classification of "major."

One might imagine that if the UAS is unable to detect air traffic, then there is the possibility that collisions will result; and, therefore this failure mode should be designated catastrophic. However, in the enroute flight phase, the vehicle is in class A airspace where ATC has the main responsibility for separation. In this case, it is assumed that ATC is functioning normally, with situational awareness of the UAS and other air traffic. If the potential for conflict arises, it is assumed that ATC would vector the UAS or other aircraft as needed to mitigate the conflict. In this phase of flight, there is the reasonable expectation that safe flight and landing can still occur.

In other phases of flight, especially where there is reduced separation, a different severity classification may be justified.

Table 6. FHA Example: Detect Air Traffic

Number	Function	Flight Phase	Failure Condition	Operational Consequence	Classification	Remark
4.1.1.1.a	Detect air traffic	enroute	Total loss of function	Possibility of conflict with another aircraft. However, assumption of being in Class A airspace under IFR means that ATC will provide separation.	major	
4.1.1.1.b	Detect air traffic	enroute	Intruder is "detected" when none is there (false alarm)	Possibility of loss of control and/or conflict with another (real) aircraft. Could result in unnecessary avoidance maneuver that endangers another aircraft.	major	Hazard severity assigned per FAA practice for manned aircraft
4.1.1.1.c	Detect air traffic	enroute	Intruder is not detected when there is a real threat.	Possibility of conflict with another aircraft. If both aircraft are being tracked by service provider and time permits, ATC will attempt to warn one or both aircraft to avoid collision.	major	Hazard severity assigned per FAA practice for manned aircraft

6.2.3 Example from the "Determine Contingency Command" Function

This example is based on function 4.3.2 Determine Contingency Command, which is a sub-function of 4.3 Manage Contingencies. Table 7 shows two FHA entries of various failure conditions for this function.

Table 7. FHA Example: Determine Contingency Command

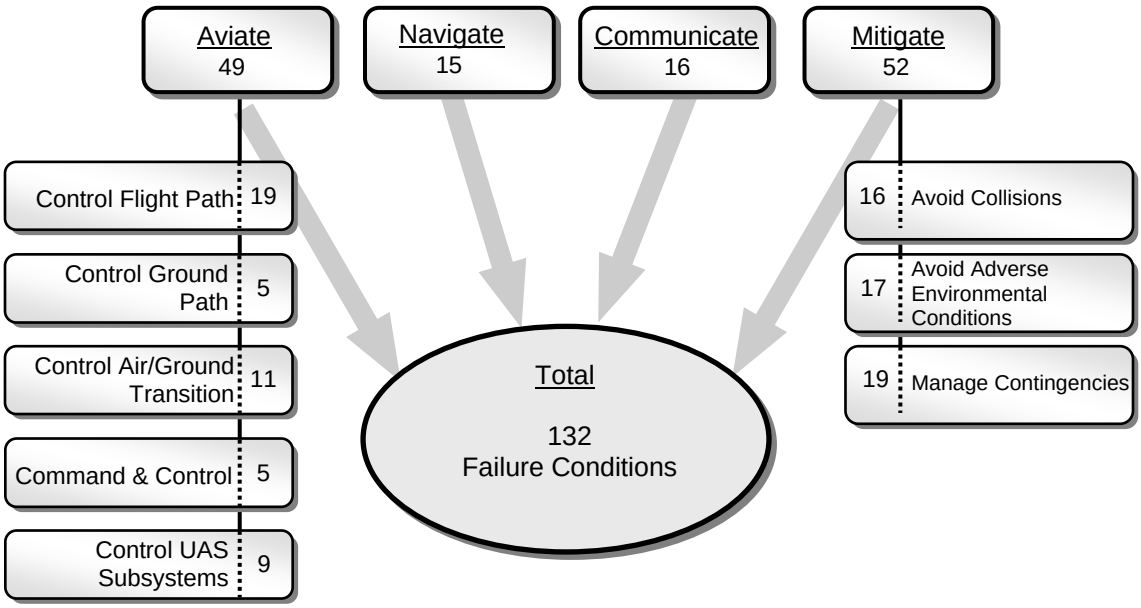
Number	Function	Flight Phase	Failure Condition	Operational Consequence	Classification	Remark
4.3.2.a	Determine contingency command	enroute	Loss or malfunction when C2 link is up.	Flight crew/UAS will not be able to initiate a contingency. Since C2 link is up, vehicle is still controllable. Significant loss of safety margin results.	major	Situations where this failure has more dire consequences involve other systems failing. These multiple-failure scenarios must be dealt with later.
4.3.2.b	Determine contingency command	enroute	Loss or malfunction when C2 link is down.	Flight crew/UAS will not be able to initiate a contingency. Since C2 link is down, the vehicle is uncommanded.	catastrophic	

These failure conditions are predicated on whether the command and control (C2) link is up or down. The reason for this distinction is that a transient loss of the C2 link is considered a normal part of operation of the vehicle and not a failure. For example, a banking turn may shield the antenna and cause the link to be temporarily lost. The manage contingencies function is normally only used when another failure has occurred. In many cases, the failure of this function in this functional group only becomes dangerous when it is being used; that is, when a failure in some other function has occurred. These circumstances would mean that multiple failures have occurred. Because this FHA only covers single failure conditions, the operational consequences listed in table 7 only reflect the failure to the determine contingency command without any other functional failures.

6.3 Summary Statistics

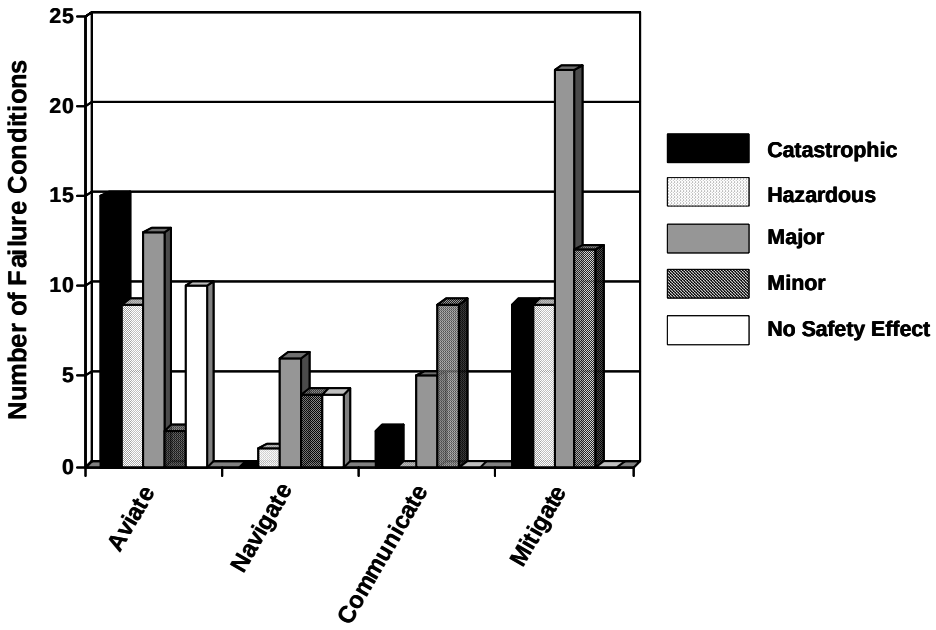
Even though the preliminary FHA does not cover multiple failures or all phases of flight, it is interesting to examine a few statistics. The functional decomposition shows 69 leaf nodes, which equates to 69 different functions to which the FHA process was applied. Figure 13 shows the total number of failure conditions by the four major categories in the functional decomposition.

Figure 13. Failure Condition Totals, by Functional Category



As shown in figure 13, the majority of potential failure conditions fall under the Aviate or Mitigate functions. Out of a total of 132 failure conditions described in the FHA, 49 of them are under Aviate and 52 of them are under Mitigate. The remaining failure conditions are almost evenly split between Navigate and Communicate. Figure 14 presents the same data, with detail regarding the number of failure conditions per each severity level.

Figure 14. Failure Condition Severities by Major Functional Category



As shown in figure 14, the majority of failure conditions with catastrophic and hazardous consequences are found in the Aviate and Mitigate functions. Catastrophic failure conditions are less prominent in Navigate and Communicate. It is important at this stage to keep in mind that only single failures have been considered in the FHA. The ratios for the various severity levels may change as multiple failure events and other phases of flight are considered.

In this assessment, twenty-six potentially catastrophic failure conditions were identified, considering only single failures in the enroute phase of flight. An interesting observation to make at this point is how the number of catastrophic failure conditions for a generic UAS compares with those numbers assumed for commercial transport (Part 25) aircraft and for general aviation (Part 23) aircraft. According to AC 23.1309-1C, there are ten catastrophic failure conditions assumed for a general aviation aircraft (covering single and multiple failures over all phases of flight); and there are 100 catastrophic failure conditions assumed for a commercial transport aircraft according to AC 25.1309-1A. While recognizing that these are broad generalizations, preliminary indications are that the number of potential catastrophic failure conditions for a generic UAS will be greater than the number for general aviation aircraft. How close the estimate will be to commercial transport aircraft depends on further assessment of failure conditions in all phases of flight.

7 Electromagnetic Considerations

As discussed in Section 2, FAR Parts 23.1309 and 25.1309 specify that equipment, systems and installations must be designed to ensure that they perform their intended functions under any foreseeable operating condition. In particular, because unmanned aircraft do not have an on-board pilot, they will necessarily rely on electronic components for safe operation. Therefore,

foreseeable operating conditions must include the electromagnetic effects on safety-relevant electronic components. In particular, FAR 23.1309 subpart (e) states

> In showing compliance with this section with regard to the electrical power system and to equipment design and installation, critical environmental and atmospheric conditions, including radio frequency energy and the effects (both direct and indirect) of lightning strikes, must be considered.

This statement formalizes the regulation in which electromagnetic effects, including high intensity radiated electromagnetic fields (HIRF) must be considered and appropriate guidelines must be followed. Due to the high altitude flight profile of some unmanned aircraft, consideration should also be made for single event upset (SEU) effects. The following subsections provide a brief discussion of issues relevant to HIRF and SEU for a UAS.

7.1 HIRF Considerations

High intensity radiated electromagnetic fields are created by transmissions from high-power radio emitters such as radio and television broadcast stations, radars, and satellite uplink transmitters. The emitters may be ground-based, ship-borne, or airborne. Although these transmissions can have serious effects on electronic equipment, engineering and design methods to protect against HIRF effects are well documented and understood. Shielding cables and bulkhead connectors from spurious electromagnetic emissions is a common practice. Metal enclosures surrounding electronic circuits (e.g., Faraday cages) usually provide sufficient protection against HIRF.

The FAA requires testing of aircraft electronic systems, in accordance with the procedures outlined in RTCA DO-160E, *Environmental Conditions and Test Procedures for Airborne Equipment,* (ref. 20) to guard against possible interruptions, erroneous operation, or loss of function due to HIRF exposure. A UAS flying similar mission profiles to fixed wing, manned aircraft will be exposed to the same HIRF environment and therefore should be tested to the same standards. UAS mission profiles that include long loiter times may increase the duration of exposure to HIRF; however, current FAA guidelines do not consider exposure time as part of the certification process. UAS mission profiles that require flight close to the earth, more closely matching the rotorcraft flight profiles, should be tested to the rotorcraft standards of DO-160E. Very low altitude flying aircraft may encounter an even harsher HIRF environment than typical rotorcraft missions and thus may require more stringent guidelines. Electronic payloads operating aboard UAS platforms that can interfere with critical systems may also need to comply with FAA radio frequency emission and susceptibility guidelines outlined in section 21 of the DO-160E document.

7.2 Single Event Upset Considerations

Single event upset phenomena are the result of cosmic ray interactions with the atmosphere, and occur more frequently at higher altitudes. These interactions can produce a number of decay products, including atmospheric neutrons that can intercept and corrupt the operation of semiconductor devices. A particle that strikes a processor at just the wrong place and time can cause it to latch-up. The most critical SEU sensitivities in modern aircraft systems occur with memory devices.

SEU is of particular concern for unmanned aircraft that fly high altitude and long endurance missions (ref. 21, 22). High altitude aircraft would be expected to encounter more frequent SEU than aircraft flying at lower altitudes. Long mission times increase exposure to SEU, as well. Finally, because there is no on-board pilot, a UAS relies on electronic components for safety

critical functions and these electronic components have grown more susceptible to SEU as integrated circuit geometries have decreased. Therefore, the design of high altitude or long-endurance aircraft must account for SEU effects to achieve acceptably safe and reliable UAS operations.

Approaches exist for mitigating HIRF and SEU effects, including shielding, fault tolerant architectures, and error detection and correcting schemes. The eventual development of "1309" regulations for unmanned aircraft will clearly need to address HIRF and SEU effects as part of the expected operating environment. Further research may be required to establish the analysis and testing methods for electronic systems, beyond those already prescribed in DO-160E, necessary to assure safe operation of a UAS in adverse environments.

8 Summary

In recent testimony before Congress, Nicholas Sabatini, FAA Associate Administrator for Aviation Safety stated that the "development and use of unmanned aircraft (UAs) is the next great step forward in the evolution of aviation." (ref. 13) This step, however, involves overcoming significant challenges with respect to developing the technology and regulatory infrastructure necessary for integrating unmanned aircraft safely into the NAS. A notable challenge for the regulatory infrastructure involves defining safety and reliability requirements necessary for providing assurance that a UAS poses no greater risk to persons or property in the air or on the ground than that presented by conventional aircraft.

This report discusses some of the basic considerations necessary for setting requirements for UASs consistent with those in current FAR paragraphs "1309". These considerations include definitions of hazards and their classification for unmanned aircraft. New definitions for the five standard hazard classes (catastrophic, hazardous, major, minor, and no effect) were proposed, with rationale given for deviation from existing definitions. In particular, the definition of "catastrophic" was modified to deal with concerns about loss of control situations.

The proposed definitions for hazard classification were applied in a preliminary functional hazard assessment of a generic UAS. The preliminary FHA identified failure conditions for a generic UAS model, for single failure events occurring in the enroute phase of flight. Much of the purpose of conducting the preliminary FHA was to help explore potential hazards unique to unmanned aircraft and how those hazards could be classified.

The revised hazard definitions and preliminary FHA are intended only as very initial steps in thinking about regulating the hazards that a UAS will pose to the NAS. Further exploration is necessary to better understand potential UAS failures and their effects on remote flight crews and communications, as well as the effect on the air traffic management system. Understanding these effects is essential to establishing a truly reasonable basis for setting reliability and safety standards for unmanned aircraft.

9 References

1. Pearson, Lee: *Developing the Flying Bomb*. http://www.history.navy.mil/download/ww1-10.pdf, pp. 70-73, Accessed May 12, 2006.
2. DeGaspari, John: *look, Ma, no pilot!* Mechanical Engineering, November 2003, http://www.memagazine.org/backissues/nov03/features/lookma/lookma.html, Accessed July 12, 2006.
3. Office of the Secretary of Defense, *Unmanned Aircraft Systems Roadmap, 2005-2030*. August 2005.

4. Haddon, D. R., Whittaker, C. J.: *Aircraft Airworthiness Certification Standards for Civil UAVs*. Civil Aviation Authority, UK, August 2002.

5. Code of Federal Regulations, Title 14, Aeronautics and Space, Chapter I, Federal Aviation Administration, Department of Transportation.

6. Federal Aviation Administration, Advisory Circular AC 23.1309-1C, *Equipment, Systems, and Installations in Part 23 Airplanes*. March, 12, 1999.

7. DeWalt, Michael P.: *Design Assurance Levels in Experimental Airworthiness Certificates for UASs*. (unpublished) white paper from Certification Services, Inc, December 30, 2005.

8. Federal Aviation Administration, Draft Advisory Circular/Advisory Material Joint AC 25.1309-1B, *System Design and Analysis*. June 10, 2002, (to be published).

9. Office of the Secretary of Defense, *Unmanned Aerial Vehicle Reliability Study*. February 2003.

10. Federal Aviation Administration, *FAA System Safety Handbook*. December 30, 2000, http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/media/chap1_1200.PDF. Accessed May 12, 2006.

11. Federal Aviation Administration, Advisory Circular AC 25.1309-1A, *System Design and Analysis*. June 21, 1988.

12. McGraw, J. W.: Unmanned Aircraft Systems Operations in the U.S. National Airspace System–Interim Operational Approval Guidance. AFS-400 UAS Policy 05-01, Dept. of Transportation, Federal Aviation Administration, Washington, DC, September 2005.

13. Statement of Nicholas A. Sabatini, Associate Administrator for Aviation Safety, Before the House Committee on Transportation and Infrastructure, Subcommittee on Aviation on Unmanned Aircraft Activities, March 29, 2006.

14. CNS ATM Technology Evolution Workgroup: Developing Guidance Material for ANSPs on UAS (Unmanned Aerial Systems). *UVS International – News Flash*, February 18, 2006, pp. 14-18.

15. RTCA, DO-264: *Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications*. Issued 12-14-00.

16. Society of Automotive Engineers, International SAE ARP 4761, *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*, 1996-12.

17. Access 5 Systems Engineering and Integration Team, *Functional Requirements Document For HALE UAS Operations in the NAS Step 1*, Version 2, September 2005, (unpublished).

18. Access 5 Systems Engineering and Integration Team, *Access 5 HALE ROA Concept of Operations*, rev 4, 30 September 2003 (unpublished).

19. Society of Automotive Engineers, International. SAE ARP 4754, *Certification Considerations for Highly-Integrated or Complex Aircraft Systems*, 1996-11.

20. RTCA, DO-160E: *Environmental Conditions and Test Procedures for Airborne Equipment*, Issued December 9, 2004.

21. Taber, A. and Normand, E.: Single Event Upset in Avionics, *IEEE Transactions on Nuclear Science*, vol. 40, no. 2, April 1993, pp. 120-126.

22. Edwards, Robert; Dyer, Clive; and Normand, Eugene: Technical Standard for Atmospheric Radiation Single Event Effects, (SEE) on Avionics Electronics, *2004 IEEE Radiation Effects Data Workshop*, 22 July 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

Appendix: UAS Preliminary Functional Hazard Assessment

This appendix contains a preliminary functional hazard assessment of a generic UAS. It is recognized that there is considerable variation among unmanned aircraft platforms. For this study, a core set of functions that most aircraft, including UASs, will need to operate routinely and safely within the NAS were identified. The core set of functions is based on fundamental tenets of piloting; namely, to fly the plane (*aviate*), fly it in the right direction (*navigate*), and, finally, to state your condition or intentions to other people (*communicate*). For the generic UAS model, a fourth fundamental function was added: *mitigate hazards*. This function is intended to capture those actions necessary to (1) stay clear of hazards, including other air traffic, flight or ground path obstructions, and adverse weather conditions, and (2) manage contingency situations that may arise.

The FHA consists of a listing of the functions specified in the functional decomposition discussed in section 5 of the report, identification of potential failure conditions and their operational consequences in the enroute phase of flight, and a hazard classification for each failure condition.

Record Number	**Function**	**Flight Phase**	**Failure Conditions**	**Operational Consequences (effect of failure on UAS)**	**Hazard Classification (Criticality)**	**Remarks**
1.0	Aviate					
1.1	Control Flight Path (FP)					This function involves controlling the vehicle while in the air.
1.1.1	Convey FP state					Because of the periodic nature of this information, there cannot be an undetected loss of this function.
1.1.1.a	Convey FP state	enroute	Detected loss of function	Without basic information such as attitude continued safe flight cannot be assumed. Flight termination should be initiated. Effectiveness of flight termination systems, may be compromised without FP state information.	hazardous	A similar failure in the AC 23.1309 example is classified as catastrophic, because of the unmanned nature of UAS, this classification has been lowered.

1.1.1.b	Convey FP state	enroute	Displays "freeze" with old information	Flight crew/UAS does not know FP state. It is expected that the flight crew will recognize that the vehicle is not performing correctly soon and will initiate a flight termination. Effectiveness of flight termination systems, may be compromised without FP state information.	hazardous	A similar failure in the AC 23.1309 example is classified as catastrophic, because of the unmanned nature of UAS, this classification has been lowered.
1.1.1.c	Convey FP state	enroute	Incorrect information	Flight crew/UAS does not know FP state. The flight crew may or may not recognize that the vehicle is not performing correctly: flight termination may or may not be initiated.	catastrophic	
1.1.2	Determine guidance command					
1.1.2.a	Determine guidance command	enroute	Detected loss of function, with alternate means to change FP state	Flight crew/UAS not able to use guidance commands to change FP state.	minor	
1.1.2.b	Determine guidance command	enroute	Undetected loss of function, with alternate means to change FP state	Flight crew/UAS is trying to control FP state, but this is ineffective. By function 1.1.5, the UAS/flight crew will recognize that guidance commands are ineffective then use other means to control FP state.	major	
1.1.2.c	Determine guidance command	enroute	Incorrect command determined, with alternate means to change FP state	Flight crew/UAS is trying to control FP state, but this is ineffective. By function 1.1.5, the UAS/flight crew will recognize that guidance commands are ineffective then use other means to control FP state.	major	
1.1.2.d	Determine guidance command	enroute	Loss of function, without alternate means to change FP state, with "soft landing" flight termination function	Flight crew/UAS not able to change FP state. Vehicle is uncontrollable. "Soft landing" flight termination function is used.	hazardous	Execution of a soft landing function assumes that people will not be killed or seriously injured.

1.1.2.e	Determine guidance command	enroute	Loss of function, without alternate means to change FP state, without "soft landing" flight termination function	Flight crew/UAS not able to change FP state. Vehicle is uncontrollable.	catastrophic	
1.1.3	Produce FP command					
1.1.3.a	Produce FP command	enroute	Detected loss of function, with "soft landing" flight termination function	Loss of ability to translate high-level direction to specific vehicle actions. "soft landing" flight termination is executed.	hazardous	Execution of a soft landing function assumes that people will not be killed or seriously injured.
1.1.3.b	Produce FP command	enroute	Detected loss of function, without "soft landing" flight termination function	Loss of ability to translate high-level direction to specific vehicle actions. Vehicle is uncontrollable. It may be possible to predict where the vehicle will land and get people and property out of the way.	catastrophic	
1.1.3.c	Produce FP command	enroute	Undetected loss of function or incorrect operation	Loss of ability to translate high-level direction to specific vehicle actions. Vehicle is uncontrollable.	catastrophic	
1.1.4	Execute FP command					
1.1.4.a	Execute FP command	enroute	Loss of function with soft landing flight termination function	Vehicle will not be controllable; landing will be somewhat controllable.	hazardous	Execution of a soft landing function assumes that people will not be killed or seriously injured.
1.1.4.b	Execute FP command	enroute	Loss of function without soft landing flight termination function	Vehicle will not be controllable.	catastrophic	
1.1.4.c	Execute FP command	enroute	Primary surfaces respond slowly	Vehicle will respond slowly. May create "pilot induced oscillation."	hazardous	

1.1.4.d	Execute FP command	enroute	Primary surfaces do not have full authority.	Vehicle will not be able to take actions within its normal performance envelope.	major	
1.1.4.e	Execute FP command	enroute	Detected loss of propulsion	Vehicle can no longer maintain altitude.	hazardous	Assumes critical systems (control surfaces, avionics, etc.) have an alternate power source.
1.1.4.f	Execute FP command	enroute	Undetected loss of propulsion	Vehicle can no longer maintain altitude. This should be detectable fairly soon.	hazardous	Assumes critical systems (control surfaces, avionics, etc.) have an alternate power source.
1.1.5	Convey FP command status					
1.1.5.a	Convey FP command status	enroute	Detected loss of function	Flight crew/UAS will not know what the vehicle is attempting to do. No mitigating actions are lost.	minor	
1.1.5.b	Convey FP command status	enroute	Incorrect command status conveyed	Flight crew/UAS will not know what the vehicle is attempting to do. Flight crew may take action on this bad information. Flight crew's response will be delayed because of lack of knowledge of status of UAS.	major	
1.2	Control ground path (GP)					
1.2.1	Convey GP state					
1.2.1.a	Convey GP state	enroute	Any malfunction	none	no effect	
1.2.2	Determine ground intent					
1.2.2.a	Determine ground intent	enroute	Any malfunction	none	no effect	
1.2.3	Produce GP command					
1.2.3.a	Produce GP command	enroute	Any malfunction	none	no effect	
1.2.4	Execute GP Command					

1.2.4.a	Execute GP Command	enroute	Any malfunction	none	no effect	
1.2.5	Convey GP command status					
1.2.5.a	Convey GP command status	enroute	Any malfunction	none	no effect	
1.3	Control air/ground transition (AGT)					The only AGT function used in the enroute flight phase is flight termination.
1.3.1	Convey AGT state					AGT state includes height above terrain, weight on wheels, etc. Because of the periodic nature of this information, there cannot be an undetected loss of this function.
1.3.1.a	Convey AGT state	enroute	Any malfunction	none	no effect	
1.3.2	Determine AGT intent					
1.3.2.a	Determine AGT intent	enroute	Any malfunction	None. Assumes mitigation of function being "off" in this flight phase	no effect	
1.3.3	Produce AGT command					
1.3.3.a	Produce AGT command	enroute	Any malfunction	None. Assumes mitigation of function being "off" in this flight phase	no effect	
1.3.4	Execute AGT Command					
1.3.4.a	Execute AGT Command	enroute	Inadvertent deployment of flaps/slats	Vehicle makes large altitude diversions.	major	Structural problems should be considered for a specific UAS.
1.3.4.b	Execute AGT Command	enroute	Inadvertent deployment of thrust reversers	Major structural and propulsion system failures	catastrophic	This failure mode is irrelevant if a UAS does not have retractable thrust reversers.

1.3.4.c	Execute AGT Command	enroute	Inadvertent landing gear deployment	Vehicle's performance changes significantly	major	Structural problems should be considered for a specific UAS. If a UAS does not have retractable landing gear, then this failure mode is irrelevant.
1.3.4.d	Execute AGT Command	enroute	Detected loss of flight termination function	Vehicle is not able to terminate flight in contingency or emergency situations. This is the loss of a single mitigating action.	major	A flight termination function is not necessarily a parachute or a "destructive" system.
1.3.4.e	Execute AGT Command	enroute	Undetected loss of flight termination function	Vehicle is not able to terminate flight in contingency or emergency situations. This is the loss of a mitigating action. Flight crew's reaction to adverse events is impacted due to lack of knowledge of the state of this function.	hazardous	This condition is more severe then the detected loss since the flight crew does not know of the loss. A flight termination function is not necessarily a parachute or a "destructive" system.
1.3.4.f	Execute AGT Command	enroute	Inadvertent deployment of flight termination function	Vehicle goes through emergency actions when none is warranted.	major	The assessment of this function is highly dependent on the characteristics of the specific UAS and its flight termination system. A "return to base" command may involve a significant loss of safety margin. A flight termination function is not necessarily a parachute or a "destructive" system.

1.3.5	Convey AGT command status					
1.3.5.a	Convey AGT command status	enroute	Misleading status of flight termination command	Flight crew/UAS is unaware that flight termination system has been deployed. Flight crew/UAS will not immediately alert ATC of situation. However, fairly soon because of the behavior of the vehicle will be known to the flight crew and ATC.	major	
1.3.5.b	Convey AGT command status	enroute	Any malfunction other than loss of status of flight termination command.	None	no effect	
1.4	Command & Control between control station and UAS					
1.4.1	Maintain Command and Control during all phases of flight					
1.4.1.a	Maintain Command and Control during all phases of flight	enroute	Total loss of C2 data link function.	UAS may make an unpredictable maneuver resulting in uncontrolled crash possibly causing injury and/or death.	catastrophic	There are many levels of Autonomy that can be deployed in case of Command and Control loss. As an example some UASs are guided to a specific waypoint location and fly a pattern waiting for new commands. Some even have autonomous return home capability. These are all mitigating factors to be used in a lower level FHA.
1.4.1.b	Maintain Command and Control during all phases of flight	enroute	Slow response of C2 data link function	Significant reduction in safety margin and increase in pilot workload.	major	

1.4.1.c	Maintain Command and Control during all phases of flight	enroute	Degraded C2 data link function resulting in incorrect signal	UAS may make an unpredictable maneuver resulting in uncontrolled crash possibly causing injury and/or death.	catastrophic	
1.4.2	Prevent unauthorized access to Command and Control					
1.4.2.a	Prevent unauthorized access to Command and Control	enroute	Unauthorized access of C2 data	UAS may make an unpredictable maneuver resulting in uncontrolled crash possibly causing injury and/or death.	catastrophic	
1.4.3	Prioritize Command & Control data					
1.4.3.a	Prioritize Command & Control data	enroute	Loss of prioritization function undetected	UAS may make an unpredictable maneuver resulting in uncontrolled crash possibly causing injury and/or death.	catastrophic	
1.5	Control UAS subsystems					
1.5.1	Control power subsystems(hydraulic/electrical)	enroute				The Power Subsystems are defined as the components that generate and distribute the power such as the electrical generator/distribution, hydraulic pumps/manifolds/valves, but not the end item components that move the UAS AV such as propulsion, and flight controls. The functions of the end item components are covered under other nodes within Aviate.

1.5.1.a	Control power subsystems(hydraulic/electrical)	enroute	Total loss of function	Loss of the power subsystem may result in loss of control of the UAS AV and possible out of control landing.	catastrophic	
1.5.1.b	Control power subsystems(hydraulic/electrical)	enroute	Misleading command	Misleading information to/from the power subsystem may result in loss of control of the UAS AV and possible out of control landing.	catastrophic	
1.5.2	Control fire suppression system	enroute	All failure conditions	The fire suppression system is a back-up system that is only required when a primary system has failed. Loss of this system is a significant loss of safety margin, but doesn't affect the operation of the UAS (Air Vehicle or Control Station)	major	If the loss of function is detected, the UAS AV operator can abort the mission and make a control landing at base of operation or an alternate site. Even if the loss of state is undetected or misleading and the mission continues, loss of safety margin increases but not enough to change hazard category.
1.5.3	Control center of gravity					
1.5.3.a	Control center of gravity	enroute	Total loss of control of center of gravity	Loss of ability to control center of gravity function may result in the UAS being operated outside its envelope and/or result in the operators inability to control the UAS. These conditions can result in an out of control landing.	catastrophic	
1.5.3.b	Control center of gravity	enroute	Degraded control of center of gravity	A significant increase in the pilot workload to maintain controlled flight of the UAS and a significant reduction in safety	major	Assumed there is enough control to abort mission and return UAS to a safe landing

1.5.4	Control environment inside the UAS	enroute				
1.5.4.a	Control environment inside the UAS	enroute	Total loss of function	Loss of ability to control environment inside the UAS may cause consuming function to take the wrong action resulting in the UAS AV to be operated outside its envelope and/or result in the operators inability to control the UAS AV. These conditions can result in an out of control landing.	catastrophic	
1.5.4.b	Control environment inside the UAS	enroute	Misleading command	misleading information may cause consuming function to take the wrong action resulting in the UAS AV to be operated outside its envelope and/or result in the operators inability to control the UAS AV. These conditions can result in an out of control landing.	catastrophic	
1.5.4.c	Control environment inside the UAS	enroute	Degraded control	A large increase in the pilot workload to maintain controlled flight of the UAS and a large reduction in safety	major	Assumes the degradation is known and slow enough to allow a mission abort and controlled landing
1.5.5	Monitor and record UAS state data	enroute	All failure conditions	UAS would not be able to reproduce state data in case of incident/mishap.	no effect	This system is only in place to record data in case there is a crash or mishap so there is no effect on the UAS during normal operations. However, there is the possibility of design assurance levels being placed on this system, such as Level B software requirements.
2.0	Navigate					

2.1	Convey navigation state					Navigation state information is updated periodically. Because of this, undetected loss of this function is not a reasonable failure mode.
2.1.a	Convey navigation state	enroute	Total loss of function (detected)	The UAS loses awareness of AV location and environmental conditions affecting its intended flight path. Pilot/operator will have to rely on ATC for tactical guidance. Workloads of ATC and UAS pilot/operator are increased, thus reducing safety margins.	major	
2.1.b	Convey navigation state	enroute	Total loss of function (undetected)		no effect	Not a reasonable failure mode. Row retained to avoid renumbering.

2.1.c	Convey navigation state	enroute	Incorrect navigation state is conveyed	The UAS is mislead about the current navigational state. In the worst case, there is a possibility of conflict with other air traffic. At best, ATC will notice flight plan deviation or other anomaly, and will provide tactical guidance. Workloads of ATC and UAS pilot/operator are increased, thus reducing safety margins. Potential mid-air collision resulting from use of misleading navigational information. The most pressing concern is a potential loss of vertical separation due to misleading altitude. Not recognizing that the navigational state is misleading will likely result in more than a significant increase in crew/ATC workload, and more than a significant decrease in safety margin.	hazardous	This classification is more severe than the corresponding function in AC 23.1309-1C. There, a comment indicates that routine eye scan mitigates loss of navigational information. For a UAS, we do not have the potential mitigating effects of an eye scan, so the severity level is higher. In the enroute phase, the most serious type of misleading information is altitude, as this could readily lead to potential conflict with other aircraft. When this FHA is expanded to consider other flight phases, misleading navigational state could also contribute to CFIT accidents. These may elevate the severity to catastrophic.
2.2	Determine navigation intent					
2.2.1	Determine flight plan					

2.2.1.a	Determine flight plan	enroute	Total loss of function (detected)	Mission will be delayed until flight-planning capability can be restored.	no effect	This presumes that this function refers only to the pre-flight phase of flight planning. Consequences of the loss of flight planning during the mission may be more severe.
2.2.1.b	Determine flight plan	enroute	Total loss of function (undetected)	Not a meaningful failure mode.	no effect	
2.2.1.c	Determine flight plan	enroute	Incorrect flight plan is determined	Potential conflict with other aircraft, adverse environmental conditions, terrain or obstacles. Monitoring by ATC will provide safety backup if anomalies in flight path are noticed in time. This constitutes a significant reduction in safety margins and significant increase in crew/ATC workload.	major	Consequences could be more severe in a high-traffic density environment.
2.2.2	Determine next waypoint					
2.2.2.a	Determine next waypoint	enroute	Total loss of function (detected)	UAS unable to continue on desired flight path. Will have to work with ATC to plan next portion of flight. Will increase workloads of pilot-operator and ATC. May require mission abort.	minor	
2.2.2.b	Determine next waypoint	enroute	Total loss of function (undetected)	Not a meaningful failure mode.	no effect	

2.2.2.c	Determine next waypoint	enroute	Next way point is incorrectly determined	Potential conflict with other aircraft or adverse environmental conditions. Monitoring by ATC will provide safety backup if anomalies in flight path are noticed in time. This constitutes a significant reduction in safety margins and significant increase in crew/ATC workload.	major	Consequences could be more severe in a high-traffic density environment.
2.2.3	Determine long-term required separation					
2.2.3.a	Determine long-term required separation	enroute	Total loss of function (detected)	UAS pilot/operator will follow ATC clearances to maintain required separations from other aircraft.	no effect	If ATC is the sole means of providing separation requirement information, then this failure implies a loss of contact with ATC, which is a much more serious situation.
2.2.3.b	Determine long-term required separation	enroute	Total loss of function (undetected)	Not a meaningful failure mode.		
2.2.3.c	Determine long-term required separation	enroute	Incorrect long-term required separation is determined	Potential for conflict with other traffic. However, ATC will be monitoring situation and providing clearances to avoid separation violations.	minor	Consequences depend upon the source of the information. Obviously, if it was provided by ATC to begin with, this may pose a much more serious problem.
2.2.4	Determine right-of-way rules					

2.2.4.a	Determine right-of-way rules	enroute	Total loss of function (detected)	UAS pilot/operator will consult with ATC as needed.	no effect	If ATC is the sole means of providing right-of-way rules information, then this failure implies a loss of contact with ATC, which is a much more serious situation.
2.2.4.b	Determine right-of-way rules	enroute	Total loss of function (undetected)	Not a meaningful failure mode.		
2.2.4.c	Determine right-of-way rules	enroute	Incorrect right-of-way rules are determined	Potential for conflict with other traffic. However, ATC will be monitoring situation and providing clearances to avoid separation violations. This constitutes a significant reduction in safety margins and significant increase in crew/ATC workload.	major	Consequences depend upon the source of the information. Obviously, if it was provided by ATC to begin with, this may pose a much more serious problem.
2.3	Produce navigation command					
2.3.a	Produce navigation command	enroute	Total loss of function (detected)	UAS unable to continue on desired flight path. Will have to work with ATC to plan next portion of flight. Will increase workloads of pilot-operator and ATC. May require mission abort.	minor	
2.3.b	Produce navigation command	enroute	Total loss of function (undetected)	UAS AV may continue on current flight path when it should be changing path. Potential conflict with other aircraft or adverse environmental conditions. Monitoring by ATC will provide safety backup if anomalies in flight path are noticed in time.	no effect	

2.3.c	Produce navigation command	enroute	Incorrect navigation command is produced	Potential conflict with other aircraft or adverse environmental conditions. Monitoring by ATC will provide safety backup if anomalies in flight path are noticed in time. This constitutes a significant reduction in safety margins and significant increase in crew/ATC workload.	major	Consequences could be more severe in a high-traffic density environment.
2.4	Determine navigation command status					
2.4.a	Determine navigation command status	enroute	Total loss of function (detected)	UAS pilot/operator will consult with ATC as needed. Will increase pilot/operator and ATC workload.	minor	
2.4.b	Determine navigation command status	enroute	Total loss of function (undetected)	Not a meaningful failure mode.	no effect	Presumes that pilot/operator will be expecting status and will notice a missing status, even if there is no alert.
2.4.c	Determine navigation command status	enroute	Navigation command status is incorrectly determined	UAS AV may be maneuvered into danger as a result of misunderstood navigational status. Potential conflict with other aircraft or adverse environmental conditions. Monitoring by ATC will provide safety backup if anomalies in flight path are noticed in time. This constitutes a significant reduction in safety margins and significant increase in crew/ATC workload.	major	
3.0	Communicate					

3.1	Broadcast information to ATC and other aircraft					Unless otherwise noted, communicate refers to voice.
3.1.1	Broadcast communications					
3.1.1.a	Broadcast communications	enroute	Total loss of communications function detected	The aircraft detects the loss of Voice Communication, may not end the mission and return to base if alternate ATC communication link exists.	minor	Assumption is that Communicate refers only to voice transfer, and that command and control data link remains operable. Pilot has alternate means of communication, via land line
3.1.1.b	Broadcast communications	enroute	Loss of communications function undetected	No response is received when communication is attempted using the UA systems. Alternate communication system, such as land line can be utilized.	major	Assumption is that Communicate refers only to voice transfer, and that command and control data link remains operable. Latency in determining loss of voice communication poses an additional hazard because ATC or other air traffic instructions will not be received.
3.1.1.c	Broadcast communications	enroute	Degraded communications function	All Communication being sent is not received by intended receiver. Alternate communication system, such as land line can be utilized.	major	Assumption is that Communicate refers only to voice transfer, and that command and control data link remains operable. Includes dropped words, garbled information.

3.1.2	Broadcast transponder data					
3.1.2.a	Broadcast transponder data	enroute	Total loss of function detected	Since the loss of capability is detected, UAS pilot/operator can turn to ATC for assistance to convey range, bearing and altitude.	major	Mitigation by the service provider assumes that UAS is not entirely dependent on ATC for collision avoidance and has some method of detect and avoid. ATC has primary and secondary radar. Transponder picked up by secondary. ATC will know that UAS transponder function has been lost.
3.1.2.b	Broadcast transponder data	enroute	Loss of function undetected	If both aircraft are being tracked by service provider, and time permits, ATC will attempt to warn one or both aircraft to avoid collision.	major	Primary radar still available
3.1.2.c	Broadcast transponder data	enroute	Misleading/degraded function	Incorrect data being sent to other aircraft may cause possible conflict with other aircraft. ATC is unable to direct safe separation.	catastrophic	
3.1.3	Participate in lost C2 link procedures			This assumes a double function failure has occurred.		
3.1.3.a	Participate in lost C2 link procedures	enroute	Total loss of function	Since the loss of capability is detected, UAS pilot/operator can turn to ATC for assistance by alternate method (land line).	major	Mitigation by the service provider assumes that UAS is not entirely dependent on ATC for collision avoidance.
3.2	Receive info from ATC and other aircraft	enroute				

3.2.1	Receive communications					
3.2.1.a	Receive communications	enroute	Total loss of communications function detected	The aircraft detects the loss of voice communication, may not end the mission and return to base if alternate ATC communication link exists.	minor	Assumption is that Communicate refers only to voice transfer, and that command and control data link remains operable. Pilot has alternate means of communication, via land line
3.2.1.b	Receive communications	enroute	Loss of communications function undetected	No response is received when communication is attempted using the UA systems. Alternate communication system, such as land line can be utilized.	minor	Assumption is that Communicate refers only to voice transfer, and that command and control data link remains operable. Latency in determining loss of voice communication poses an additional hazard because ATC or other air traffic instructions will not be received .
3.2.1.c	Receive communications	enroute	Degraded communications function detected	All communication being sent is not received by intended receiver. Alternate communication system, such as land line can be utilized.	minor	Assumption is that Communicate refers only to voice transfer, and that command and control data link remains operable. Includes dropped words, garbled information,
3.2.2	Receive transponder data					

3.2.2.a	Receive transponder data	enroute	Total loss of function detected	Since the loss of capability is detected, UAS pilot/operator can turn to ATC for assistance.	minor	Mitigation by the service provider assumes that UAS is not entirely dependent on ATC for collision avoidance and has some method of detect and avoid. ATC has primary and secondary radar. Transponder picked up by secondary. ATC will know that UAS transponder function has been lost.
3.2.2.b	Receive transponder data	enroute	Loss of function undetected	If both aircraft are being tracked by service provider, and time permits, ATC will attempt to warn one or both aircraft to avoid collision.	minor	Assignment of "Minor" is based on the presumption that ATC is monitoring the situation. Primary radar still available
3.2.2.c	Receive transponder data	enroute	Misleading function	Incorrect data being sent to other aircraft my cause conflict with other aircraft. Incorrect data could also result in unnecessary avoidance maneuver that endangers another aircraft.	catastrophic	
3.2.3	Monitor communication from ATC and other aircraft					
3.2.3.a	Monitor communication from ATC and other aircraft	enroute	Total loss of function detected	The pilot detects the loss of voice communication, may not end the mission and return to base if alternate ATC communication link exists.	minor	Assumption is that Communicate refers only to voice transfer, and that command and control data link remains operable. Pilot has alternate means of communication, via land line

3.2.3.b	Monitor communication from ATC and other aircraft	enroute	Loss of function undetected	The pilot does not receive voice traffic from other air traffic or ATC. Alternate communication system, such as land line can be utilized.	minor	Assumption is that Communicate refers only to voice transfer, and that command and control data link remains operable. Latency in determining loss of voice communication poses an additional hazard because ATC or other air traffic instructions will not be received .
3.2.3.c	Monitor communication from ATC and other aircraft	enroute	Degraded function detected	All communication being sent is not received by intended receiver. Alternate communication system, such as land line can be utilized.	minor	Assumption is that Communicate refers only to voice transfer, and that command and control data link remains operable. Includes dropped words, garbled information, Latency in determining that voice communication has been degraded poses an additional hazard because ATC or other air traffic instructions will not be received .
4.0	Mitigate					
4.1	Avoid collisions					

4.1.1	Avoid air traffic					The function here should really be "Avoid Collisions", and further elaboration is unnecessary at this level. The "Detect", "Track", "Determine", "Select", "Execute", and "Convey Status" sub-functions impose a particular implementation. However, we decided to assume this structure in order to explore some issues of interest in conflict and collision avoidance.
4.1.1.1	Detect air traffic					
4.1.1.1.a	Detect air traffic	enroute	Total loss of function	Possibility of conflict with another aircraft. However, assumption of being in Class A airspace under IFR means that ATC will provide separation.	major	
4.1.1.1.b	Detect air traffic	enroute	Intruder is "detected" when none is there (false alarm)	Possibility of loss of control and/or conflict with another (real) aircraft. Could result in unnecessary avoidance maneuver that endangers another aircraft.	major	Hazard severity assigned per FAA practice for manned aircraft
4.1.1.1.c	Detect air traffic	enroute	Intruder is not detected when there is a real threat.	Possibility of conflict with another aircraft. If both aircraft are being tracked by service provider, and time permits, ATC will attempt to warn one or both aircraft to avoid collision.	major	Hazard severity assigned per FAA practice for manned aircraft
4.1.1.2	Track air traffic					

4.1.1.2.a	Track air traffic	enroute	Total loss of function	Possibility of conflict with another aircraft. However, assumption of being in Class A airspace under IFR means that ATC will provide separation.	major	
4.1.1.2.b	Track air traffic	enroute	Air traffic not on a collision course is incorrectly tracked as a threat to ownship.	Possibility of loss of control and/or conflict with another (real) aircraft. Could result in unnecessary avoidance maneuver that endangers another aircraft.	major	Hazard severity assigned per FAA practice for manned aircraft
4.1.1.2.c	Track air traffic	enroute	Air traffic on a collision course is incorrectly tracked as a non-threat to ownship.	Possibility of conflict with another aircraft. If both aircraft are being tracked by service provider, and time permits, ATC will attempt to warn one or both aircraft to avoid collision.	major	Hazard severity assigned per FAA practice for manned aircraft
4.1.1.3	Provide air traffic tracks					
4.1.1.3.a	Provide air traffic tracks	enroute	Total loss of function	Possibility of conflict with another aircraft. However, assumption of being in Class A airspace under IFR means that ATC will provide separation.	major	
4.1.1.3.b	Provide air traffic tracks	enroute	Relative location of air traffic on a collision course is incorrectly conveyed not to be a threat to ownship.	Possibility of conflict with another aircraft. If both aircraft are being tracked by service provider, and time permits, ATC will attempt to warn one or both aircraft to avoid collision.	major	Hazard severity assigned per FAA practice for manned aircraft
4.1.1.4	Determine corrective action					
4.1.1.4.a	Determine corrective action	enroute	Total loss of function	Possibility of conflict with another aircraft. However, assumption of being in Class A airspace under IFR means that ATC will provide separation.	major	

4.1.1.4.b	Determine corrective action	enroute	Relative location of air traffic not on a collision course is incorrectly conveyed to be a threat to ownship.	Possibility of loss of control and/or conflict with another (real) aircraft. Could result in unnecessary avoidance maneuver that endangers another aircraft.	major	Hazard severity assigned per FAA practice for manned aircraft
4.1.1.4.c	Determine corrective action	enroute	Relative location of air traffic on a collision course is incorrectly conveyed not to be a threat to ownship.	Possibility of conflict with another aircraft. If both aircraft are being tracked by service provider, and time permits, ATC will attempt to warn one or both aircraft to avoid collision.	major	Hazard severity assigned per FAA practice for manned aircraft
4.1.1.5	Select corrective action command					
4.1.1.5.a	Select corrective action command	enroute	Total loss of function	Possibility of conflict with another aircraft. However, assumption of being in Class A airspace under IFR means that ATC will provide separation.	major	
4.1.1.5.b	Select corrective action command	enroute	Unnecessary corrective action command produced.	Possibility of loss of control and/or conflict with another (real) aircraft. Could result in unnecessary avoidance maneuver that endangers another aircraft.	major	Hazard severity assigned per FAA practice for manned aircraft
4.1.1.5.c	Select corrective action command	enroute	Necessary corrective action command not produced.	Possibility of conflict with another aircraft. If both aircraft are being tracked by service provider, and time permits, ATC will attempt to warn one or both aircraft to avoid collision.	major	Hazard severity assigned per FAA practice for manned aircraft

4.1.1.6	Execute corrective action command (accomplished under Aviate)					Covered under Aviate function
4.1.1.7	Convey Post Corrective Action Status to ATC					Not yet clear if this function is relevant since it the effects are not directly caused by the UAS.
4.1.1.7.a	Convey Post Corrective Action Status to ATC	enroute	Total loss of function	ATC will be expecting a status update, and will consult radar displays and continue to attempt to reach UAS pilot/operator for outcome.	minor	Assumes ATC can deduce situation based on radar display.
4.1.1.7.b	Convey Post Corrective Action Status to ATC	enroute	Corrective action status information is misleading.	Will create different situational perceptions between pilot/operator and ATC. Increased workload for ATC and pilot/operator.	major	Confusion may result in an incorrect and potentially hazardous reaction.
4.1.2	Avoid Ground and Vertical Structures (while airborne)	enroute				While airborne -- implies a 2nd failure condition for this (enroute) phase of flight. To be considered in subsequent analysis.
4.1.3	Avoid ground path obstructions (while landing or on ground)	enroute				No hazards for enroute phase

4.2	Avoid adverse environmental conditions					The function here should really be "Provide Adverse Environmental Information", and further elaboration is unnecessary at this level. The "Detect", "Track", "Provide", "Determine", "Produce", "Execute", and "Convey Status" sub-functions impose a particular implementation. However, we decided to assume this structure in order to explore some issues of interest in avoiding adverse environmental conditions. Also, we admit that some of these functions don't even make sense in certain situations -- for example, what does it mean to "Track" an icing condition?
4.2.1	Detect adverse environmental conditions					

4.2.1.a	Detect adverse environmental conditions	enroute	Total loss of function	Could lead to loss of control of UAS AV or operation of the UAS AV outside of performance envelope. Possibility of conflict with another aircraft or encounter with ground or ground structures. If possible, ATC will provide instructions to UAS operator in order to mitigate effects of failure.	hazardous	
4.2.1.b	Detect adverse environmental conditions	enroute	Adverse environmental conditions does not exist but is "detected"	In best case, alternate weather source may provide UAS with correct weather information. In worst case, UAS AV will maneuver to avoid non-existent environmental conditions.	minor	Best case assumes there is a backup weather information source. In worst case, consequences could be more severe in a high-density traffic environment.
4.2.1.c	Detect adverse environmental conditions	enroute	Adverse environmental conditions exists but is not detected	Could lead to loss of control of UAS AV or operation of the UAS AV outside of performance envelope. Possibility of conflict with another aircraft or encounter with ground or ground structures. If a problem is noticed by ATC in time, ATC will attempt to provide instructions to UAS operator in order to mitigate effects of failure.	catastrophic	Assumes that ATC-UAS pilot loop cannot be closed fast enough to prevent loss of control.

4.2.2	Track relative location of adverse environmental conditions					This function must be interpreted broadly. For example, "tracking" icing conditions is different than tracking a storm cell. Icing conditions cannot be seen literally, only inferred from other weather data. (However, ice on the wing can be seen in some situations -- does that count?)
4.2.2.a	Track relative location of adverse environmental conditions	enroute	Total loss of function	Could lead to loss of control of UAS AV or operation of the UAS AV outside of performance envelope. Possibility of conflict with another aircraft or encounter with ground or ground structures. If possible, ATC will provide instructions to UAS operator in order to mitigate effects of failure.	hazardous	
4.2.2.b	Track relative location of adverse environmental conditions	enroute	Adverse environmental conditions are "tracked" as a threat when none exist.	In best case, alternate weather source may provide UAS with correct weather information. In worst case, UAS AV will maneuver to avoid non-existent weather conditions.	minor	Best case assumes there is a backup weather information source. In worst case, consequences could be more severe in a high-density traffic environment.

4.2.2.c	Track relative location of adverse environmental conditions	enroute	Adverse environmental conditions are not tracked as a threat.	Could lead to loss of control of UAS AV or operation of the UAS AV outside of performance envelope. Possibility of conflict with another aircraft or encounter with ground or ground structures. If a problem is noticed by ATC in time, ATC will attempt to provide instructions to UAS operator in order to mitigate effects of failure.	catastrophic	Assumes that ATC-UAS pilot loop cannot be closed fast enough to prevent loss of control.
4.2.3	Convey relative location of adverse environmental conditions					
4.2.3.a	Convey relative location of adverse environmental conditions	enroute	Total loss of ability to convey relative location of adverse environmental conditions	Could lead to loss of control of UAS AV or operation of the UAS AV outside of performance envelope. Possibility of conflict with another aircraft or encounter with ground or ground structures. If possible, ATC will provide instructions to UAS operator in order to mitigate effects of failure.	hazardous	
4.2.3.b	Convey relative location of adverse environmental conditions	enroute	Adverse environmental conditions conveyed as a threat when in fact none exist.	In best case, alternate weather source may provide UAS with correct weather information. In worst case, UAS AV will maneuver to avoid non-existent environmental conditions.	minor	Best case assumes there is a backup weather information source. In worst case, consequences could be more severe in a high-density traffic environment.

4.2.3.c	Convey relative location of adverse environmental conditions	enroute	Adverse environmental conditions not conveyed.	Could lead to loss of control of UAS AV or operation of the UAS AV outside of performance envelope. Possibility of conflict with another aircraft or encounter with ground or ground structures. If a problem is noticed by ATC in time, ATC will attempt to provide instructions to UAS operator in order to mitigate effects of failure.	catastrophic	Assumes that ATC-UAS pilot loop cannot be closed fast enough to prevent loss of control.
4.2.4	Determine corrective action					
4.2.4.a	Determine corrective action	enroute	Total loss of ability to assess adverse environmental conditions threat	Could lead to loss of control of UAS AV or operation of the UAS AV outside of performance envelope. Possibility of conflict with another aircraft or encounter with ground or ground structures. If possible, ATC will provide instructions to UAS operator in order to mitigate effects of failure.	hazardous	
4.2.4.c	Determine corrective action	enroute	Adverse environmental conditions assessed as a threat when in fact none exist.	In best case, alternate weather source may provide UAS with correct weather information. In worst case, UAS AV will maneuver to avoid non-existent environmental conditions.	minor	Best case assumes there is a backup weather information source. In worst case, consequences could be more severe in a high-density traffic environment.
4.2.4.d	Determine corrective action	enroute	Adverse environmental conditions not assessed as a threat.	Could lead to loss of control of UAS AV or operation of the UAS AV outside of performance envelope. Possibility of conflict with another aircraft or encounter with ground or ground structures. If a problem is noticed by ATC in time, ATC will attempt to provide instructions to UAS operator in order to mitigate effects of failure.	catastrophic	Assumes that ATC-UAS pilot loop cannot be closed fast enough to prevent loss of control.

4.2.5	Produce corrective action command					
4.2.5.a	Produce corrective action command	enroute	Total loss of ability to produce corrective action command	Could lead to loss of control of UAS AV or operation of the UAS AV outside of performance envelope. Possibility of conflict with another aircraft or encounter with ground or ground structures. If possible, ATC will provide instructions to UAS operator in order to mitigate effects of failure.	hazardous	Mitigation by the service provider assumes that UAS is not entirely dependent on ATC for avoidance of avoid adverse environmental condition.
4.2.5.b	Produce corrective action command	enroute	Unnecessary corrective action produced.	In best case, alternate weather source may provide UAS with correct weather information. In worst case, UAS AV will maneuver to avoid non-existent environmental conditions.	minor	Best case assumes there is a backup weather information source. In worst case, consequences could be more severe in a high-density traffic environment.
4.2.5.c	Produce corrective action command	enroute	Necessary corrective action not produced.	Could lead to loss of control of UAS AV or operation of the UAS AV outside of performance envelope. Possibility of conflict with another aircraft or encounter with ground or ground structures. If a problem is noticed by ATC in time, ATC will attempt to provide instructions to UAS operator in order to mitigate effects of failure.	catastrophic	Assumes that ATC-UAS pilot loop cannot be closed fast enough to prevent loss of control.
4.2.6	Execute corrective action command (accomplished under Aviate)					Covered under Aviate function
4.2.7	Convey post corrective action status to ATC					Not yet clear if this function is relevant since it the effects are not directly caused by the UAS.

4.2.7.a	Convey post corrective action status to ATC	enroute	Total loss of function	ATC will be expecting a status update, and will consult radar displays and continue to attempt to reach UAS pilot/operator for outcome.	minor	Assumes ATC can deduce situation based on radar display.
4.2.7.b	Convey post corrective action status to ATC	enroute	Corrective action status information is misleading.	Will create different situational perceptions between pilot/operator and ATC. Increased workload for ATC and pilot/operator.	major	Confusion may result in an incorrect and potentially hazardous reaction.
4.3	Manage contingencies					This function is a collection of many smaller functions. The smaller functions are not specifically defined since these functions would be very dependant on functions implemented in the vehicle. A reasonable case can be made that a specific mitigation function should be placed alongside of the function it is mitigating.
4.3.1	Convey system status					System status includes status of subsystems of the UAS: comm., command and control, propulsion, power, fire, etc. As in manned aircraft, we assume that loss of comm. between flight crew and ATC is always detectable by the flight crew and ATC.

4.3.1.a	Convey system status	enroute	Detected loss of function	Flight crew/UAS will recognize the system status is not available, but will not be able to respond to contingencies based on this non-information. Flight crew has a slightly increased workload.	minor	For this situation to get dangerous, another failure must occur. Expect operational constraints will dictate that the flight crew/UAS will abort the flight, but this can be done in a controlled manner.
4.3.1.b	Convey system status	enroute	Undetected loss of function for all but C2 system status	System status is not available, therefore no actions can be taken to respond to these contingencies. Significant loss of safety margin.	major	This hazard classification is not higher, because any dangerous scenario requires a multiple-failure condition. Absent other failures, continued safe flight and landing can occur.
4.3.1.c	Convey system status	enroute	Undetected loss of function for C2 system status	C2 system status is not available, therefore if C2 is lost also, then the vehicle cannot be controlled and no action (human or automation) can compensate.	catastrophic	A transient loss of C2 is considered a normal part of flight not a failure, therefore C2 could be lost and the loss of detection and this would NOT result in a two-failure scenario.
4.3.1.d	Convey system status	enroute	Degraded function - including no report from some systems, loss of precision, or late arrival of information.	Only part of the state of the UAS is available. Flight crew has a slightly increased workload.	minor	This hazard classification is not higher, because any dangerous scenario requires a multiple-failure condition. Note that undetected loss of C2 functions is covered in 4.3.1.c.

4.3.1.e	Convey system status	enroute	Reporting failure when there is none	Flight crew/UAS will believe the UAS is malfunctioning when in fact it is not. Flight crew/UAS may make a diversion based on this false information. Flight crew has a slightly increased workload.	minor	
4.3.1.f	Convey system status	enroute	Reporting no failure when there is one	TBD	TBD	This is a multiple-failure scenario, failure of system and failure of status. These multiple-failures must be examined in detail.
4.3.2	Determine contingency command					This is a flight crew or UAS initiated request for a contingency.
4.3.2.a	Determine contingency command	enroute	Loss or malfunction when C2 link is up.	Flight crew/UAS will not be able to initiate a contingency. Since C2 link is up, vehicle is still controllable. Significant loss of safety margin results.	major	Situations where this failure has more dire consequences involve other systems failing. These multiple-failure scenarios must be dealt with later.
4.3.2.b	Determine contingency command	enroute	Loss or malfunction when C2 link is down.	Flight crew/UAS will not be able to initiate a contingency. Since C2 link is down, then the vehicle is uncommanded.	catastrophic	
4.3.2.c	Determine contingency command	enroute	Degraded operation - delayed initiation of contingency when C2 link is up	Flight crew/UAS initiates contingency which takes significantly longer than normal. Expect there is a time buffer between initiation and hazardous situation. Loss of safety margin results.	major	

4.3.2.d	Determine contingency command	enroute	Degraded operation - delayed initiation of contingency when C2 link is down	Flight crew/UAS initiates contingency which takes significantly longer than normal. Expect there is a time buffer between initiation and the dangerous situation. Loss of safety margin results.	hazardous	
4.3.3	Produce mitigation command	enroute				
4.3.3.a	Produce mitigation command	enroute	Loss or malfunction when C2 link is up.	Flight crew/UAS will not be able to formulate a mitigation action. Since C2 link is up, vehicle is still controllable. Significant loss of safety margin results.	major	Situations where this failure has more dire consequences involve other systems failing. These multiple-failure scenarios must be dealt with later.
4.3.3.b	Produce mitigation command	enroute	Loss or malfunction when C2 link is down.	Flight crew/UAS will not be able to formulate a mitigation action. Since C2 link is down, then the vehicle is uncommanded.	catastrophic	
4.3.3.c	Produce mitigation command	enroute	Degraded operation - delayed initiation of contingency when C2 link is up	Flight crew/UAS formulates a mitigation action which takes significantly longer than normal. Expect there is a time buffer between initiation and hazardous situation. Loss of safety margin results.	minor	Situations where this failure has more dire consequences involve other systems failing. These multiple-failure scenarios must be dealt with later.
4.3.3.d	Produce mitigation command	enroute	Degraded operation - delayed initiation of contingency when C2 link is down	Flight crew/UAS formulates a mitigation action which takes significantly longer than normal. Expect there is a time buffer between initiation and hazardous situation. More than a significant loss of safety margin results.	hazardous	
4.3.4	Prioritize mitigation command	enroute				

4.3.4.a	Prioritize mitigation command	enroute	Any failure when C2 link is up.	The most important mitigation command will not be used and the flight crew/UAS know about this. Since C2 link is up, vehicle is still controllable. A significant loss of safety margin results.	major	The expectation is that all mitigation commands that have been produced will be executed, just in a different order from what is expected. If a mitigation command is never executed, then this is a failure of the "produce mitigation command" function. Situations where this failure has more dire consequences involve other systems failing. These multiple-failure scenarios must be dealt with later.
4.3.4.b	Prioritize mitigation command	enroute	Any failure when C2 link is down.	The most important mitigation command will not be used and the flight crew/UAS know about this. Since C2 link is down, then the vehicle is uncommanded.	catastrophic	
4.3.5	Convey status of commands	enroute				
4.3.5.a	Convey status of commands	enroute	Detected loss of function	System successfully formulates and executes a mitigation command, the flight crew/UAS does not know what happened, and is aware that they do no know. Small loss of safety margin, small increase in workload	minor	

4.3.5.b	Convey status of commands	enroute	Undetected loss of function	System successfully formulates and executes a mitigation command, the flight crew/UAS does not know what happened, and is unaware that they do no know. Flight crew/UAS may initiate more actions attempting to compensate for the perceived non-response to the mitigation command. More than a significant loss of safety margin. Flight crew will be focused on this event and may not be able to perform other required tasks.	hazardous	
4.3.5.c	Convey status of commands	enroute	Degraded operation - delayed or incomplete information about status of contingency/mitigation commands	System successfully formulates and executes a mitigation command, the flight crew/UAS only has a partial knowledge of what happened. Significant loss of safety margin, some increase in workload	major	
4.3.5.d	Convey status of commands	enroute	Malfunction/misleading operation	System successfully formulates and executes a mitigation command, the flight crew/UAS does not know what happened, and is unaware that they do no know. Flight crew/UAS may initiate more actions attempting to compensate for the perceived non-response to the mitigation command. More than a significant loss of safety margin. Flight crew will be focused on this event and may not be able to perform other required tasks.	hazardous	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01- 02 - 2007	Technical Memorandum	

4. TITLE AND SUBTITLE

Preliminary Considerations for Classifying Hazards of Unmanned Aircraft Systems

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Hayhurst, Kelly J.; Maddalon, Jeffrey M.; Miner, Paul S.; Szatkowski, George N.; Ulrey, Michael L.; DeWalt, Michael P.; and Spitzer, Cary R.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

457280.02.07.07

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

NASA Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER

L-19299

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)

NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

NASA/TM-2007-214539

12. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Category 01
Availability: NASA CASI (301) 621-0390

13. SUPPLEMENTARY NOTES

An electronic version can be found at http://ntrs.nasa.gov

14. ABSTRACT

The use of unmanned aircraft in national airspace has been characterized as the next great step forward in the evolution of civil aviation. To make routine and safe operation of these aircraft a reality, a number of technological and regulatory challenges must be overcome. This report discusses some of the regulatory challenges with respect to deriving safety and reliability requirements for unmanned aircraft. In particular, definitions of hazards and their classification are discussed and applied to a preliminary functional hazard assessment of a generic unmanned system.

15. SUBJECT TERMS

Reliability; Requirements engineering; Unmanned aircraft system

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
					19b. TELEPHONE NUMBER *(Include area code)*
U	U	U	UU	78	(301) 621-0390