Analysis of Unmanned Aerial Vehicles Concept of Operations in ITS Applications

Final Report

Prepared by:

Demoz Gebre-Egziabher
Zhiqiang Xing

Department of Aerospace Engineering & Mechanics
University of Minnesota

CTS 11-06

Technical Report Documentation Page

1. Report No. CTS 11-06	2.	3. Recipients Accession No.	
4. Title and Subtitle Analysis of Unmanned Aerial Vehicles Concept of Operations in ITS Applications		5. Report Date March 2011 6.	
7. Author(s) Demoz Gebre-Egziabher, Zhiqiang Xing		8. Performing Organization Report No.	
9. Performing Organization Name and Address Department of Aerospace Engineering and Mechanics University of Minnesota 110 Union Street, SE Minneapolis, MN 55455		10. Project/Task/Work Unit No. 11. Contract (C) or Grant (G) No. CTS Project #2008023	
12. Sponsoring Organization Name and Address Intelligent Transportation Systems Institute Center for Transportation Studies University of Minnesota 200 Transportation and Safety Building 511 Washington Ave. SE Minneapolis, MN 55455		13. Type of Report and Period Covered Final Report 14. Sponsoring Agency Code	
15. Supplementary Notes http://www.its.umn.edu/Publications/ResearchReports/			

16. Abstract (Limit: 250 words)

The work described in this report is about developing a framework for the design of concept of operations (CONOP), which use small uninhabited aerial systems (SUAS) to support of intelligent transportation system (ITS) application of highway and transportation infrastructure monitoring. In these envisioned applications, these vehicles will be used for tasks such as remote collection of traffic data or inspection of roads and bridges. As such, a risk that has to be managed for these applications is that of vehicle-infrastructure collision. Various solutions to ensure safe separation between the unmanned aerial vehicle (UAV) and the object being inspected have been proposed. However, most, if not all, of these solutions rely on a multi-sensor approach, which combines digital maps of the infrastructure being inspected with an integrated GPS/Inertial navigator. While ``turn key'' solutions for such multi-sensor systems exist, the performance specifications provided by their manufactures does not provide sufficient information to allow precisely quantifying or bounding the collision risk. Furthermore, size, weight and power (or SWAP) constraints posed by these small aerial vehicles limits the use of redundant hardware and/or software as a risk mitigation strategy. The purpose of the work reported here was to develop a framework for the design of CONOPs, which take these SUAS limitations into account. The method outlined shows, in part, how these vehicle/infrastructure collision risks can be estimated or conservatively bounded.

17. Document Analysis/Descriptors Unmanned aerial vehicle, National airspace, Airspace (Law), Integrated navigation, Navigation aid, Risk mitigation, Risk quantification, Risk management, Risk assessment, DRONE aircraft		18. Availability Statement No restrictions. Document available from: National Technical Information Services, Alexandria, Virginia 22312	
19. Security Class (this report) Unclassified	20. Security Class (this page) Unclassified	21. No. of Pages 43	22. Price

Analysis of Unmanned Aerial Vehicles Concept of Operations in ITS Applications

Final Report

Prepared by:

Demoz Gebre-Egziabher
Zhiqiang Xing

Department of Aerospace Engineering & Mechanics
University of Minnesota

March 2011

Published by:

Intelligent Transportation Systems Institute
Center for Transportation Studies
University of Minnesota
200 Transportation and Safety Building
511 Washington Ave SE
Minneapolis, Minnesota 55455

ACKNOWLEDGEMENTS

The authors wish to acknowledge those who made this research possible. The study was funded by the Intelligent Transportation Systems (ITS) Institute, a program of the University of Minnesota's Center for Transportation Studies (CTS). Financial support was provided by the United States Department of Transportation's Research and Innovative Technologies Administration (RITA).

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The work described in this report is about developing a framework for the design of a concept of operation (CONOP), which uses small uninhabited aerial systems (SUAS) to support of intelligent transportation system (ITS) application of highway and transportation infrastructure monitoring. In these envisioned applications, these vehicles will be used for tasks such as remote collection of traffic data or inspection of roads and bridges. As such, a risk that has to be managed for these applications is that of vehicle-infrastructure collision.

Various solutions to ensure safe separation between the unmanned aerial vehicle (UAV) and the object being inspected have been proposed. However, most, if not all, of these solutions rely on a multi-sensor approach, which combines digital maps of the infrastructure being inspected with an integrated GPS/Inertial navigator. While "turn key" solutions for such multi-sensor systems exist, the performance specifications provided by their manufactures does not provide sufficient information to allow precisely quantifying or bounding the collision risk. Furthermore, size, weight and power (or SWAP) constraints posed by these small aerial vehicles limits the use of redundant hardware and/or software as a risk mitigation strategy.

The purpose of the work reported here was to develop a framework for the design of CONOPs, which take these SUAS limitations into account. The method outlined shows, in part, how these vehicle/infrastructure risks can be estimated or conservatively bounded. As is shown, estimating this risk or placing conservative bounds, at a minimum, depends on the knowledge of the following: CONOP design requirements and the architecture of the multi-sensor system. That is, the collision risk cannot be determined independently of the CONOP or the sensor integration strategy. Using a simple integrated GPS-dead reckoning system such as one found on some off-the-shelf autopilots, the approach for placing conservative bounds is demonstrated.

CHAPTER 1

INTRODUCTION

The work described in this report examines issues associated with the design of concepts of operation or for small unmanned aerial systems (SUAS). The term UAS as used in this report is taken to mean a system consisting of an unmanned aerial vehicle (UAV) and associated support systems including a ground station and data link. The focus here is on SUAS operations to support envisioned Intelligent Transportation Systems (ITS) applications. In these applications UAVs are used as mobile sensor platforms which can be used to remotely gather traffic data; inspect highway and transportation infrastructure; or as nodes for *ad hoc* communication networks during emergencies [1, 2, 3].

UAVs span a wide range in size and complexity, where some of the largest ones such as the Global Hawk, Predator or Reaper, weigh several thousand pounds and are large enough to require the use of an airport for launch and recovery operations. For the ITS applications considered here, the UAVs in question are small and in the 5-to-10-lb weight range. We will refer to these vehicles as as small UAV or SUAV hereafter. SUAVs are small enough to fit in the trunk of a car for easy transportation. Therefore, they do not require large infrastructure for launch and recovery operations. They fall in the the so-called "Class I" category of UAVs as defined in [4].

In general, the concern associated with using Class I UAVs in the various applications noted above is with the potential for collisions. The collision threat can be divided into two categories: collision with other airplanes operating in the NAS and collision with infrastructure. The consequences of a collision between a small UAV and a person-carrying aircraft can be loss of life, property or both. As such, developing solutions to mitigate this threat have been the subject of intense research and development activities for some time. A significant amount of work in this area goes under the moniker of "sense and avoid" technologies and has focused on developing solutions (hardware, software and procedural) to enable UAVs to "see" other aircraft and navigate clear of them.

In the ITS-related UAV missions considered here, the potential of collisions with infrastructure is more of a concern. This is because the Class I UAVs envisioned for these operation will be operated in and around highway infrastructure (roads, buildings, bridges, etc). While a collision with infrastructure can cause property damage, it can also lead to personal injury if a disabled UAV lands on persons or fast-traveling vehicles below. It is because of this that it can be argued that collision with infrastructure can be more of an important concern for Class I UAVs used in ITS application. This is because such operations are more than likely going to occur in areas that are not close to airports or areas where there is a sizable level of aircraft traffic.

The term concept of operations (or CONOPs for short) is taken to mean a description of the mission and operational procedure used when implementing a UAS in ITS applications. For example, the CONOPs for using a UAS for inspection of transportation infrastructure would describe the procedure

from launch to recovery. Based on such a description, performance requirements for the UAS can be specified. These requirements would include items such as the vehicle's endurance (in time); the capability and range of the datalink used by the aerial vehicle and its ground station; and weather limitations (ceilings, wind speeds, etc.) during operation. A procedure for identifying and quantifying the potential risk for collision with infrastructure and how this is related to concepts of operation for these missions was the focus of the work reported here.

1.1. SMALL UAV SYSTEMS

The severe size, weight and power (SWAP) constraints, as well as cost issues associated with Class I UAVs, result in a tight connection between the onboard systems and the collision risk. The objective, in part, of the work reported here was to elucidate this connection and show that *for a given level of risk, the procedures for carrying out the CONOP cannot be viewed independently from the systems used to navigate, guide and control the aerial vehicle. The procedures will be shaped by the capabilities and limitation of the onboard systems*. Understanding this will require a overview of the airframe, propulsion and sensing solution available today for SUAVs.

Currently, there are several off-the-shelf UAS that are purportedly "turn key" solutions for many potential CONOPS including those specifically for ITS applications. These off-the-shelf solutions consist of a UAV, avionics and associated ground support systems. Less complete kits are also available where the user can customize various aspects of the UAVs. One of the areas where this is particularly true is in the area of onboard avionics used for navigation, guidance and control. In this regard, a user can select one of many avionics suites and adapt them to the particular aerial vehicle.

While the availability of various solutions for either the complete UAS or its onboard avionics suites can be viewed as a positive in that it provides for a level of flexibility. It also presents a challenge for those wishing to quantify the collision risk associated with their operation. That is, how does one go about to prove that these vehicles are safe to operate? This becomes particularly challenging when one examines the performance specification of many of the off-the-shelf components. If one considers navigation, guidance and control systems, there is very little in their vendor-supplied performance specification that will allow one to assess the risk associated with operating these systems. For example, the performance navigation suites are characterized in terms of accuracy. While useful, accuracy does not give all the information needed to quantify risk.

In view of this, the work described in this report was aimed at showing that there is a clear connections between CONOP requirements and a small UAS fielded to support this CONOP. Unlike using larger and perhaps manned aircraft where a particular aerial platform can support various CONOPs, the performance, cost and size limitations of small aerial vehicles and associated sytems must be specifically accounted for if they are to be used safely and cost effectively. The work described shows what this link between UAS and CONOP looks like. In more concrete terms, it is about developing and demonstrating a systematic approach for evaluating whether navigation and guidance systems envisioned for use in small, hand-launched aerial vehicles in ITS applications (remotely monitoring of vehicle states and other useful traffic management parameters) meets safety requirements established by regulation. The methodology proposed involves identifying hazards associated with the concept of operation and quantifying the likelihood of their occurrence. For hazards where the likelihood of occurrence is judged to be too large, risk mitigation strategies must be proposed.

1.2. MOTIVATION

Aerial sensor platforms, ranging from expensive remote sensing satellites to the smallest UAS, are complex systems. Their design and operation relies on the interaction of various systems. For vehicles larger than small UAS, these various systems can be designed and analyzed separately. If they are found to be lacking in reliability for a certain mission, they can be redesigned without affecting the other systems or operations. Furthermore, hardware redundancies can be used to boost reliability.

For small UAS, this approach, which views the onboard sensors and systems as distinct from the vehicle and its operation, will be inefficient if not ineffective when it comes to minimizing risk. This is because at the size of SUAS, sensor payload dimensions and weight are a significant fraction of the overall vehicle dimension and weight, respectively. Integration of miniature systems and sensors into an already existing miniature vehicle, therefore, will be physically difficult and will also exact an unnecessary weight penalty. This is, of course, assuming that compact, off-the-shelf sensors that can be integrated into a miniature vehicle exist.

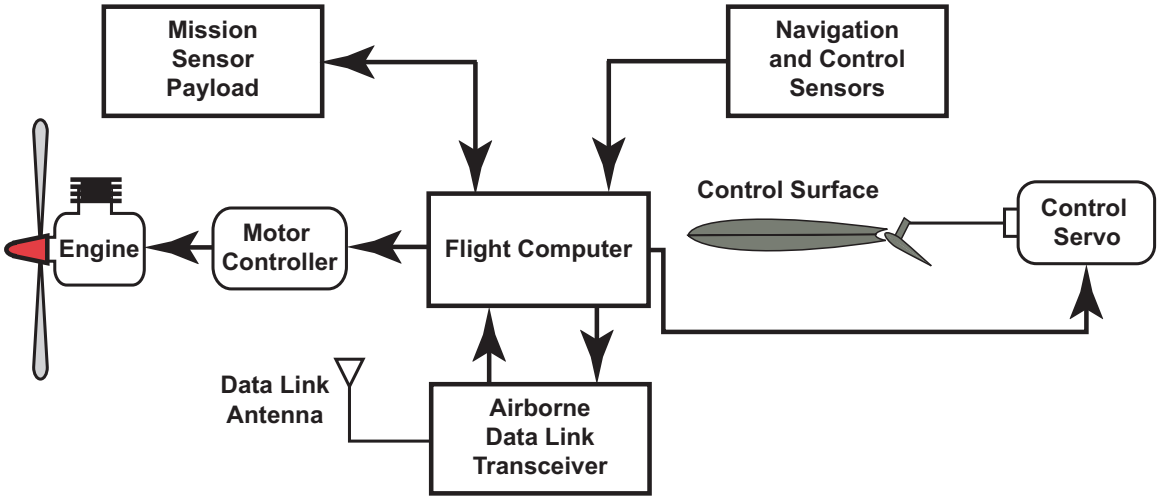

Figure 1.1: SUAV Physical Block Diagram of Airborne Sub-Systems

Figure 1.1 shows the basic systems found on a typical UAS aimed at the types of ITS operations discussed in [2]. Because of size, weight and power constraints, the systems shown in Figure 1.1 are used in a "single thread" fashion with very little hardware redundancies. Therefore, when it comes to risk mitigation or quantification, one has to rely on the flawless functioning of the various systems and their interaction with each other. Except for the mission sensor payload, a failure in any one of the systems shown in Figure 1.1 is a potential collision risk. Therefore, any CONOP design will have to take the connection between collision risk and onboard systems into account. For those risks that cannot be mitigated by hardware approaches, the CONOP procedures must be designed to ensure that their failure does not lead to scenarios with unacceptable consequences.

1.3. PROBLEM STATEMENT & SOLUTION

In view of the discussion above, the objective of the research work described in this report was to explore the issues and develop a framework or methodology that can be used to assess whether a

proposed CONOP relying on UAS meets safety requirements established by regulation. Thus, on a practical level, the work will involve identifying the risks of UAS operations in these ITS applications and assessing the likelihood of their occurrence. It will connect the CONOP procedures to the risks identified and show how CONOP redesign can be used to mitigate risk. Thus, hardware or engineering solutions to mitigate these risks was considered to be beyond the scope of this work.

1.4. PRIOR WORK & CONTRIBUTIONS

There has been a considerable effort focused on identifying operational concepts which use UAVs in ITS applications [3], but the effort focused on developing systematic methods for quantifying risks or dealing with certification issues is lagging. The analysis of risk associated with these operations has been more in the area of developing and evaluating methods for preventing collisions between UAVs and other manned aircraft.

Related to this project is the work done by the MIT Center for Air Transportation. The researchers at MIT have proposed and developed analysis techniques that allow safety evaluation and risk mitigation measures associated with operation of UAVs [5, 6]. The work in [5] and [6] provides a systematic method for assigning acceptable level of risk to UAV concept of operation. However, while the work in [5] and [6] provides general guidelines on how to perform such evaluations, it does not provide a way of "flowing down" those risks to the various components on board. This requires a UAV platform and operational concept-specific information.

The work described here uses UAVs and procedures developed as part of previous research to determine the platform and operational concept-specific details. While a complete analysis of the entire UAS was beyond the scope of this work, the methods developed for considering a subset of the systems (in this case, navigation and guidance systems) can be extended to other systems (e.g., control systems, data link, etc.). As noted above, we envision such a tool being used for establishing certification standards by federal and state agencies responsible for the safe operation of UAS. It will also be a useful tool for designers of UAS and associated systems because it can be used to map operational requirements (e.g., system reliability, required accuracy on vehicle location and velocity estimation, etc.) into hardware specifications. Operational procedure designers can also use it to determine the required operator equipment qualifications for a given concept of operation.

1.5. REPORT ORGANIZATION

The remainder of this report is organized as follows: In the Section 2 of the report we discuss collision risks and group the into two main groups. Then we outline a CONOP design procedure, which uses these identified risks as inputs. In Section 3, the method outlined in Section 2 is used to analyze and identify the risks in the highway infrastructure inspection CONOP discussed in [2]. In Section 4, one specific risk (navigation system error) is analyzed and it effect on CONOP design is explored. Section 5 provides concluding remarks.

CHAPTER 2

UAS MISSION RISKS

In the introduction we briefly stated that the term CONOP is taken to mean a complete description of the mission that a SUAS is to undertake. The CONOP will include a procedure for the mission to be carried out in support of accomplishing the task it is designed to do. The procedure will depend on what kind of capability (sensing, guidance, navigation and control) are available on the SUAV. They may also depend on safety considerations for the UAV as well as the population at large in and around the operations area. The procedure may include a list of initial conditions (e.g., weather minimums such as visibility, wind speeds, etc.), that must be present before the mission can be initiated. CONOP designs, therefore, must take into account a broad range of issues, some of which are technical. This is particularity true when we consider the issue of safety. This is because a CONOP design needs to consider risks as it answers the following question: Are the benefits that result from using SUAS in a particular ITS operation offset by the potential hazard resulting from a vehicle malfunction or collision? Answering this question involves defining what we mean by risk and establishing a threshold for acceptable risk. While quantifying risk may be, in part, an objective, technical problem, establishing a threshold of acceptable risk potentially involves some level of subjectivity.

A potential systematic approach that shows the objective and subjective aspects of CONOP design is outlined in Figure 2.1. We note that this is not meant to be the definitive CONOP design procedure but one possible approach that can be used.

2.1. CONOP DEFINITION

The design procedure starts with the "CONOP Definition" box at the far left of the the figure. In this definition process, the ITS operation that will be supported by using a SUAS is defined. This includes a clear articulation of the objectives of the operation and why SUAS should be used in lieu of other traditional approaches. This is the point in the design process where the potentially subjective task of establishing what is deemed *acceptable risk* must occur. We use the term "potentially subjective" because there are times when engineering judgement and prior experience must be used to set this threshold. However, a systematic and somewhat objective process such as those outlined in [5] and [6] can be used.

This step of the procedure will be examined in more detail later in this section, but for moment the key point to note is this: In addition to procedures for the operation, an output of this step in the design process is a number that captures (or a set of numbers that capture) what is considered an acceptable risk. We use the variable P_A for this number and it is defined as the probability that a hazardous situation will occur per operation of the SUAS in the ITS operation defined by this CONOP.

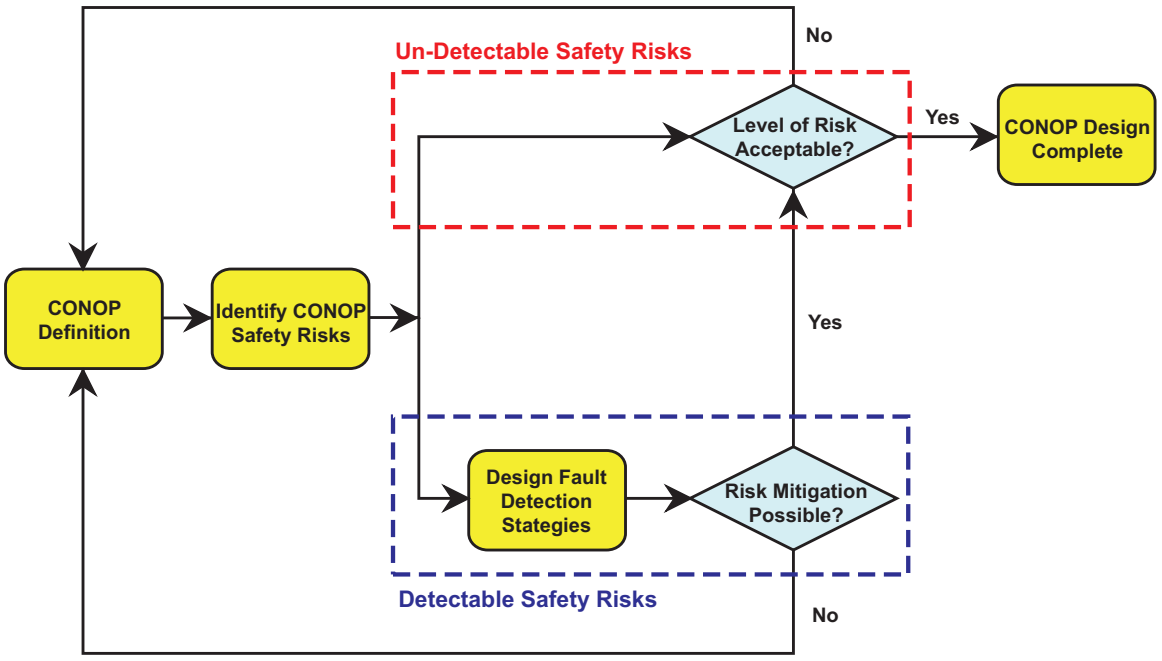

Figure 2.1: Flow Chart for Small UAS Concept of Operation (CONOP) Design Process

For example, $P_A = 1 \times 10^{-6}$ would mean that one hazardous mishap in 1,000,000 operations of this CONOP is considered to be an acceptable level of risk. Therefore, the designer of the CONOP must ensure that the actual risk posed by this CONOP or the probability of a hazardous mishap P_H is less than P_A.

2.2. IDENTIFY CONOP SAFETY RISKS

Calculating the hazard risk P_H requires identifying the conditions under which a hazardous situation can develop. The conditions that can lead to a hazardous situation are called *safety risks* in this report. This step of the design process requires generating a list of these conditions. Since one of the primary hazard in SUAS operations is the collision hazard (primary collisions with infrastructure or other aerial/ground vehicles or secondary collisions with ground vehicles or people below), this step is closely associated with identifying safety risks that can lead to collision hazards.

The conditions that can lead to a collision are varied and identifying them will require considering both causes that are part of SUAS, as well as environmental factors that are external to the vehicle. Examples of the former include control system hardware or software failures. Examples of the latter include the operational procedures that were developed in the "CONOP Design" step of the design process. A more specific example will help clarify this. For example, a hypothetical SUAV which we are considering in a CONOP design process may have a control system that can effectively reject gust disturbances that are less than 5 m/s in magnitude. If the SUAV is operating in close proximity to other vehicles or structures, encountering a gust of 5 m/s or greater may lead to a situation where the control system cannot avert a collision. Therefore, unexpected gusts of a magnitude greater than 5 m/s would be a condition external to the UAS that needs to be listed or identified in this step of the design process.

In addition to identifying the safety risks, this step of the design procedure also requires characterizing them. In this report we group the safety risks under two categories: detectable and undetectable safety risks. The way in which we deal with these two types of risks in the CONOP design processes can be very different. Therefore, the next step of the CONOP design process requires dealing with detectable and undetectable risks separately.

2.3. DETECTABLE RISKS

Detectable risks are associated with events that are apparent when they occur. If we consider the data link system used for communication between the ground control station and the SUAV as an example, a complete failure of this system will be readily apparent during operations. A clear indication of this, for example, would be a situation where the SUAV does not respond to commands from the ground station or data from it cannot be accessed by its operators. Such detectable failures can sometimes be dealt with by hardware/software redundancies or emergency procedures. In the most ideal case, these risks can be completely removed or dealt with once they are detected. In some instances, however, they cannot be completely removed and the best we can hope to do is mitigate their consequences.

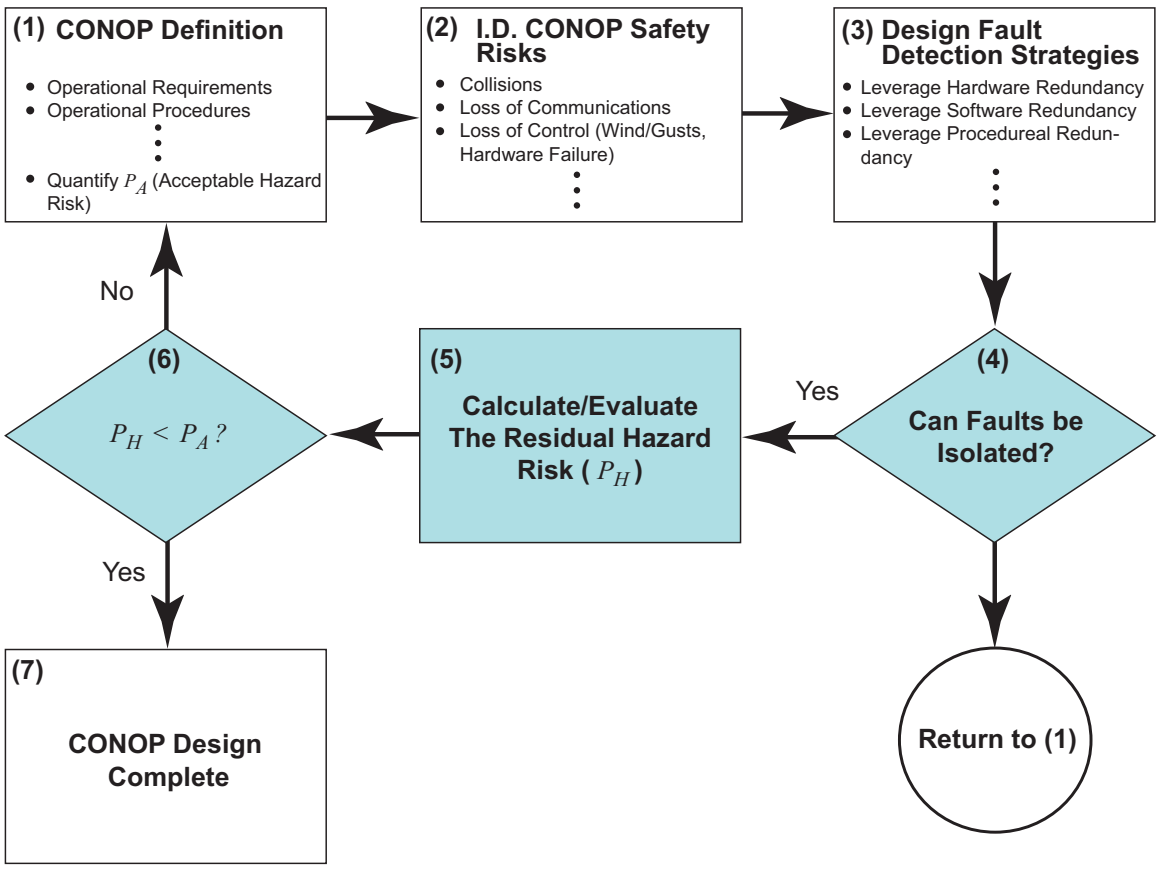

Figure 2.2: Flow Chart for Dealing with Detectable Safety Risks in CONOP Design

The lower path, proceeding from left to right, in Figure 2.1 shows how detectable risks are dealt

with in the proposed design procedure. Figure 2.2 is used to clarify how this is done. Figure 2.2 shows the path from the initial CONOP definition to the end assuming we are dealing with only detectable risks. After the each one of the detectable risks is identified (Step 2 in Figure 2.2), we proceed to next step where we attempt to design fault detection strategies. The fault detection strategies are designed to detect the onset of a risk that can lead to a hazardous situation. These fault detection strategies can leverage hardware redundances, software redundancies or procedural redundancies. For example, let us once again consider the data link system. If two independent data links are used, they can be compared to detect a malfunction in the communication link between the SUAV and the ground station. If three independent data link systems are used, they can detect and isolate a *single* malfunction. It is not difficult to imagine algorithms or procedures (such are interrogations at regular intervals) that can be used with a single- or multiple-data link architecture to detect communication failures. The key point here is that if one can devise a mechanism by which a hazard risk can be detected, then this mechanism becomes the fault detection strategy.

Once a strategy is designed, its efficacy has to be determined. In doing this, at least three performance metrics have to be quantified. First, the probability of a missed detection (P_{MD}) has to be quantified. This is the probability that the designed fault detection strategy will miss detecting an actual hazard risk. The second metric is the probability of a false alarm or P_{FA}. This is the probability that the fault detection strategy will detect and alarm a non-existent fault. This can be a hazard risk if the response to a detected fault (i.e., the fault mitigation strategy) is a procedure that possesses an inherent risk that is non-negligible. The third metric is the residual hazard risk or P_{H}. This is the conditional probability of a hazard given that one of the following has occurred: (1) a false alarm of a non-existent fault; (2) a missed detection of an actual fault has occurred; (3) a fault that cannot be completely removed has occurred and mitigating its consequence is the only possible strategy for dealing with its occurrence.

In summary, what Figure 2.2 shows is the following: If a detectable risk is identified, the efficacy of the detection strategy is assessed (as measured by P_{MD} and P_{FA}). If the efficacy of the detection strategy is not acceptable, the designer must return to the starting point and re-define the CONOP in such way as to remove the risk or make it detectable to an acceptable level. Once an effective detection strategy has been designed, its efficacy in removing the risk is assessed. This is characterized by the hazard probability or P_H. If hazard probability is less than the acceptable risk P_A, then the design of the CONOP relative to that risk is complete.

It should be noted that, the discussion above applied to a single, detectable risk. The methodology outlined in Figure 2.1 requires that a similar evaluation be carried out for all risks identified in the "Identify CONOP Safety Risks" phase of the design process.

2.4. UNDETECTABLE RISKS

Risks that are not detectable fall into two categories. The first ones are those risks that are not apparent when they occur. Examples include some time-varying navigation sensor or software errors. The characteristic of these errors is that they are very small and undetectable by fault detection mechanisms. Their consequence, however, grows with time and can be catastrophic. Ones in the second category are those that are always present but the probability they will lead to a hazardous situations is shown to be less than P_A. Examples of these types of risk are those caused by stationary and non-stationary stochastic sensor errors. Non-stationary sensor errors are of a particular concern here because a large number of low-cost sensors aimed at SUAS applications tend to exhibit such output

errors. Practical algorithms (i.e., can be implemented in real time on computers suitable for small SUAV) to quantify or deal with such risks are, at best, *ad hoc* or non-existent. Part of the objective of the work reported here was to develop a means for dealing with such risks and the case study presented at the end of this report will discuss this in some detail.

2.5. CALCULATING THE HAZARD RISK P_H

Normally, the hazard risk P_H is a very small number and this makes calculating it accurately challenging. This is especially true if P_H is variable during the flight of a SUAS. A safety risk which changes in real time must monitored in real time. This can be a very challenging task and the point of the brief discussion that follows highlights this point. It is given here to help put Figures 2.1 and 2.2 in context, as well as motivate one of the contributions of this work that will be examined in some detail the last section of this report.

The CONOP design methodology outlined in Figure 2.1 (and detailed in Figure 2.2 for detectable safety risks) requires quantifying the acceptable risk threshold (P_A) and then *demonstrating* or *proving* that the risk posed by the SUAS operation (P_H) is below this threshold. In the work here, *demonstrating* is taken to mean using experiments, leveraging knowledge from other similar operational systems, using engineering judgement, or a combination of all three to show that $P_H < P_A$. When P_A is a very small number (say, on order of one in a million) then demonstrating via experiments becomes a nearly impossible task. This is because it is impractical to collect sufficiently large data sets to construct a statistically meaningful estimate of P_H. In this case the option that must be pursued is that of *proving*.

In this report *proving* is taken to mean using analytical means to show that $P_H < P_A$. It can be in one of two ways: calculating P_H or overbounding P_H. Calculating P_H can be problematic because it is normally a small number and estimates of it can be very sensitive to inaccuracies in initial conditions and other calculation inputs. Furthermore, in many instances P_H is not a static variable but changes from moment to moment during the operation of a SUAV. In these instances, it must be calculated and monitored in real time. When P_H is small, these calculations can be computationally intensive to the point where they are impractical to implement on processors satisfying the size, weight and power (SWAP) constraints of a SUAV. The overbounding approach circumvents these two issues by generating a computationally tractable (i.e., can be generated in real time on a small processor meeting the SWAP constraints for a SUAV), yet conservative estimate of P_H denoted $\bar{P}_H$. This conservative estimate $\bar{P}_H$ is called an overbound of P_H and it is greater than P_H but less than P_A. The last section of this report deals with generating overbounds for navigation system risks used in SUAS.

2.6. RISK ALLOCATION

The magnitude of P_H is small for the following two reasons: (1) the acceptable risk threshold P_A is small and (2) the concept of *risk allocation*. The reason behind the first item is obvious: If the risk posed by the operation of SUAS is not small, its use will not be adopted. The second reason for *risk allocation*, requires some explaining. The acceptable risk P_A can be in the range of 10^{-9} to 10^{-4} depending on the operation being envisioned, the SUAV being used, and final customers of the SUAS's services. Even though a P_A of 10^{-4} cannot be considered small, the individual hazard risk P_H values may be very small indeed. They can potentially be an order of magnitude or two less than P_A. This is because the *overall* system safety risk is a function of various *individual* safety risks. That is, the total

risk has to be allocated among the various potential safety risks.

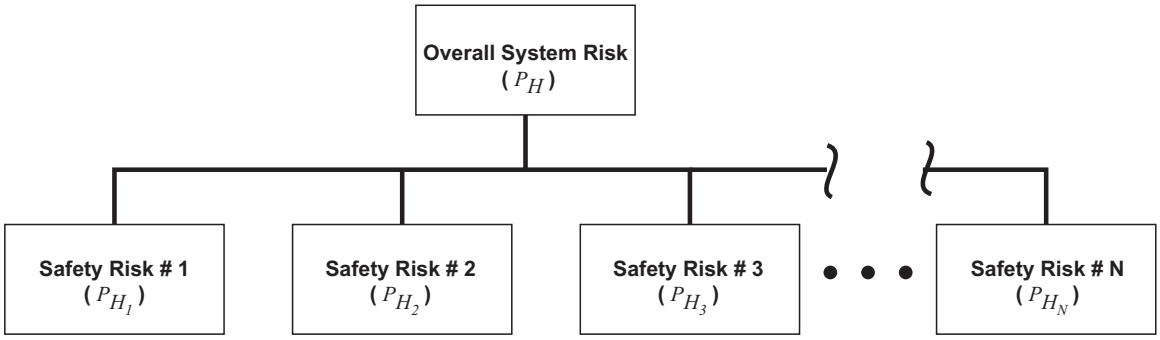

Figure 2.3: Risk Allocation for Overall CONOP

The concept of risk allocation is depicted schematically in Figure 2.3. Since a SUAS is a system of systems, the overall risk of a hazard depends on the risk posed by the constituent systems. Some of the constituent systems are more complex than others so the risk is not uniform across systems. Furthermore, the failure of some system is more critical than that of other systems. For example, failure of control systems is an event that renders a SUAV uncontrollable and, hence more serious than a fault of a dedicated payload communication link (i.e., a separate link than the one used for control of the SUAV). This is why the overall safety risk has to be allocated or spread across the various systems that make up the SUAS. The allocation must take into account the severity of a failure in a given system with the more critical system receiving more stringent allocation. In Figure 2.3, P_{H_i} is the i^{th} system's safety risk. If the individual safety risks are independent, then each individual P_{H_i} may be larger than P_A. In general, however, this is not the case and risk allocation can lead to P_H for the individual safety risks being smaller than the overall system safety risk.

CHAPTER 3

MISSION DESIGN

In what follows we will use the ITS application of SUAS described in [2] and go through some of the steps of the CONOP design process outlined in Figure 2.1. This is not meant to be a complete CONOP design exercise but an exercise in highlighting key points discussed above. More specifically, we will first present a high level discussion of the CONOP. Then we will identify a pair of detectable and undetectable risks (four safety risks in total). Then we will show how some of these risks can be dealt with by modifying the CONOP procedures, hardware, software, or both. The goal is to show how detectable and undetectable safety risks affect CONOP design. It is also how to show the redesign of the CONOP can be used to mitigate these risks.

In the CONOP discussed in [2], a SUAV will be equipped with a camera that can be used to capture video or still images. The SUAV can then be flown in the vicinity of bridges, dams, buildings, etc., and capture images that can be relayed back to some base station for inspection. It can also be used to monitor traffic flow in areas where sensors are sparse (remote areas like rural Minnesota) or normally installed sensors are off-line (due to maintenance or an emergency such as the aftermath of the I-35 bridge collapse near downtown Minneapolis in August 2007). The SUAV will be operating in a *tactical* mode, in that it will not be traversing large distances from its point of launch to its operational area. This implies that collision with infrastructure (and associated secondary collisions with persons or vehicles on the ground) is more of a safety risk than collision with other aircraft. Thus, this collision should be the focus of the safety risk and risk mitigation associated with the analysis

The discussion presented here in relation to these risks will not involve calculating P_H. This will be saved for the last section of thus report where we present a detailed analysis of how overbounding is used to deal with safety risks that have to be estimated in real time but are hard to compute precisely. One of the undetectable safety risks we are going to consider is a collision risk posed by navigation system error. It is this risk that we will deal with in detail in the next section of this report.

3.1. CONOP DEFINITION

Figure 3.1 depicts the operation envisioned by this CONOP. The figure depicts a SUAV operating close to a bridge. The SUAV used will be in the Class I category as defined in [4] which implies that it can be transported to the area of operation in the trunk most any vehicle. Thus, this represents a tactical SUAV operation as defined in [2] and the major safety risk that needs to be considered are primary collisions with infrastructure or secondary collisions with objects below.

If the weather and visibility conditions are suitable to support the operation, then the operation can be launched. Just how to determine the acceptable weather and visibility conditions will become

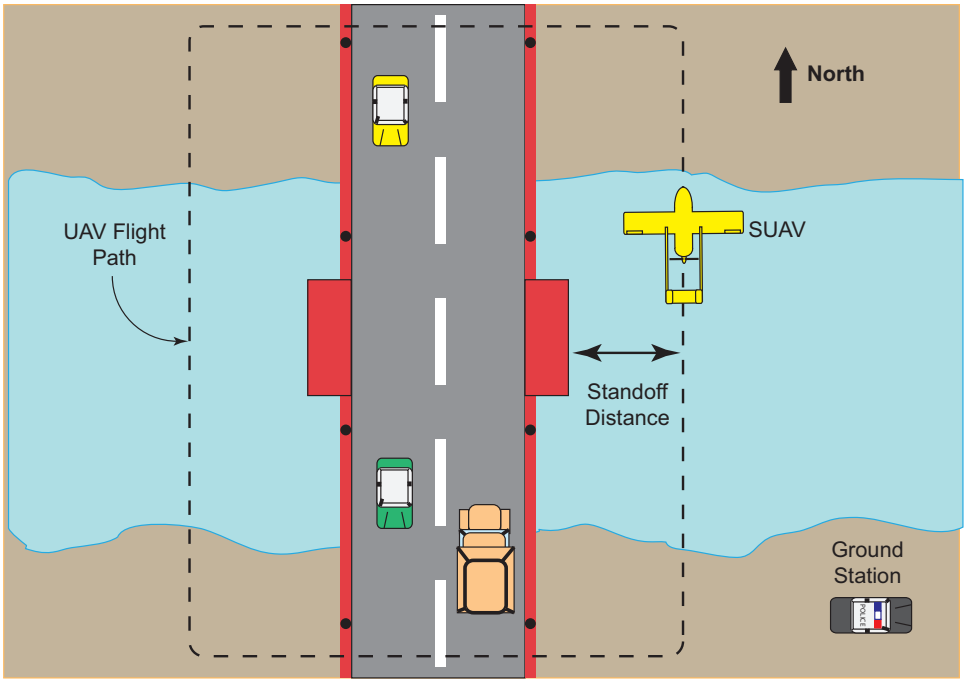

Figure 3.1: Infrastructure Inspection Using a SUAS (Figure NOT to Scale)

apparent when we examine safety risks below. Figure 3.2 is a functional block diagram of the systems (airborne and ground) that are required to support the CONOP described next. It depicts the information flow between the various systems of the SUAS. It is *not* a depiction of the actual architecture of the onboard system. A schematic of the systems on the airborne side were shown earlier in Figure 1.1. The connection between these two figures is that all the airborne systems blocks shown in Figure 3.2 (with the exception of the data link radios and the navigation and control sensors) are algorithms that reside in the flight computer shown in Figure 1.1. From a CONOP design and analysis point of view, it more useful to deal with the functional block diagram than the actual, physical block diagram.

The operation commences by setting up the ground station that, ideally, will be nothing more than a laptop computer with a data link radio. An inspection of the vehicle (airframe, power plant and avionics) is performed to ensure that the vehicle is in an airworthy state. An operational check of the data link between the ground and air vehicle is also performed. If the operation is in response to a pre-planned infrastructure inspection, then an operation plan (equivalent to test point during flight tests) should have been prepared in advance. This plan should be reviewed to ensure that it is consistent with the prevailing weather and other operational constraints. For example, if there is an area over which flying a SUAS is not allowed (e.g., an outdoor gathering, proximity to certain structures, etc.) this must be taken into account with the operation plan. All of these pre-launch activities constitute the CONOP initial conditions that must be satisfied before the launch of the aerial vehicle.

Once the vehicle is launched, it commences operating per the operation plan and procedures unless the operation is in response to an emergency (in which case there may be standard operating procedure but no specific operation plan). For example, the operational plan may require flying a “race track” pattern as shown in Figure 3.1. The operational plan (or procedure) will include items such as of how close the vehicle must be (or how far away it needs to stay) from the structure being inspected. These

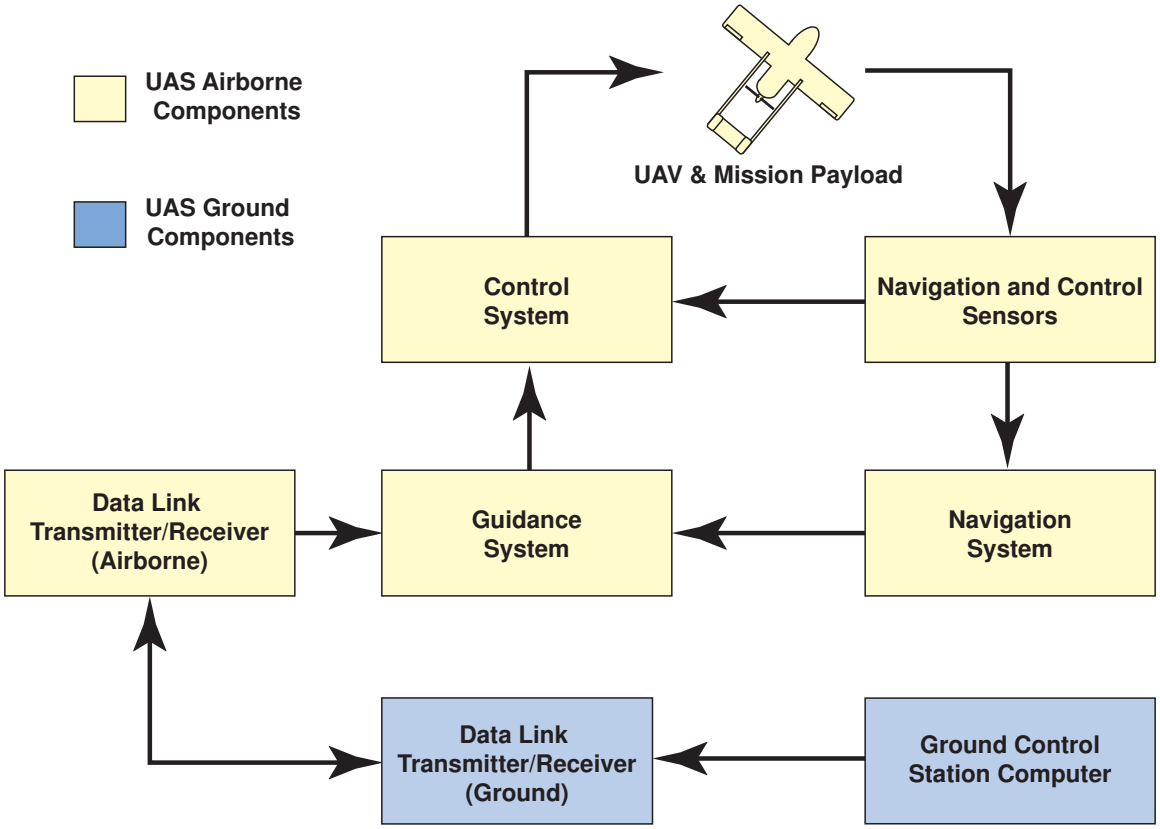

Figure 3.2: SUAS Functional Block Diagram of Constituent Sub-Systems

are determined by mission payload requirements (camera resolution, for example) and control system performance. This "standoff" distance is an operational requirement. This operational requirement, in turn, is considered acceptable or not depending on the SUAS system capabilities. While it is easy to understand how camera requirements play into this standoff distance requirement, it is not clear how control system requirements play into this. This will become apparent when we identify risks and design mitigation strategies for them next.

3.2. Identifying Safety Risks

While a long list of potential safety risks for this CONOP can be compiled, as noted above we will only consider a subset of them consisting of two detectable and two undetectable risks. The two detectable risks we will focus on are data link system failure and engine failure. The undetectable risks we will consider are control system lack of authority and navigation system stochastic errors.

3.2.1. Safety Risk #1: Data Link Failure

The data link system's purpose is relay information from the ground station up to the SUAV an vice versa. The information relayed up to the SUAV can be instructions for changes in ground paths to be followed, altitudes changes, speed changes, turning on or off the mission payload, and mission termi-

nation instructions. The information relayed down may be a real time streaming of images (or video) from the onboard camera or telemetry of the status of the various sub-systems. From a safety risk point of view, the data link provides a way to change the mission of the SUAV in real time to adapt to changing environmental conditions. For example, new collision threats can be identified and relayed up to the SUAV flight computer. Another important safety function of the data link is to provide a means by which the SUAV's flight can be terminated in the event of an anomalous condition. That is, if the SUAV is operating in a way which is deemed to be unsafe (due to sensor or a sub-system malfunction, for example) the flight can be terminated. In this instance the SUAV can be commanded to return and land or, if the malfunction is too severe, execute a safe termination procedure pre-programmed prior to the flight (e.g., deploy a parachute, ditch into an open area, etc.).

Failure Modes & Detection: The data links can fail in several ways that pose a safety risk, of which two are described next. First, the data link can fail in a manner where data being transmitted from the ground station to the SUAV (and vice versa) is corrupted or contains errors. We will call this a "soft" failure. The second failure potential is a "hard" failure where the data link ceases to transmit or receiver messages. One can create a list of credible reasons that can cause both soft and hard failures of the data link. Regardless of their cause, most soft and hard failures of the data link are detectable. Simple procedural methods or built-in periodic checks can be used to determine whether a failure of the data link has occurred. For example, the ground station can initiate periodic, variable messages transmissions have to be echoed by the the SUAV (or vice a versa).

Mitigation Strategy: While it is possible to mitigate this safety risk by redundant hardware, that requires modifying the SUAS systems from those that we started with during the design of the CONOP (Figure 3.2). A mitigation strategy that does not require changing hardware may involve building into the guidance and control strategy of the vehicle a "no data link" termination procedure. This procedure would be initiated (automatically by the aerial vehicle) in the event that a data link failure occurs. This procedure would consist of flying to a pre-determined safe spot and landing or ditching the airplane.

Residual Safety Risk: The question that the CONOP designer must now answer is, what is the residual safety risk of these failure modes with their associated detection and mitigation strategies (i.e., step 5 in Figure 2.2)? That is, what is $P_H|_{\text{Data Link}}$? This will require characterizing the data link and the environment in which it is expected be used (as defined by the CONOP) and generate a statistic for reliability or a probability of failure P_F of the data link system. How this can be determined is beyond the scope of the discussion here and we will assume the CONOP designer knows P_F for the data link system in use. Given P_F, three potential scenarios must be considered.

1. Procedural methods or built-in periodic checks can detect a faulty data link system with 100% reliability ($P_{MD} = 0$) and with no false alarms ($P_{FA} = 0$).

2. Missed detection probability $P_{MD} \neq 0$ but false alarm rate $P_{FA} = 0$.

3. Missed detection probability $P_{MD} \neq 0$ and false alarm rate $P_{FA} \neq 0$.

Estimating realistic or accurate values for P_{MD} and $P_{FA} = 0$ are also beyond the scope of the discussion here. Assuming that accurate estimates for them are available, then the key question remaining is the following: What is the likelihood of a collision of SUAS as it starts executing the maneuvers associated with the "no data link" procedure? If we can determine this likelihood or probability (let us

call it P_C where "C" is for collision), the the residual hazard P_H will be a function of P_C, P_F, P_{MD} and P_{FA} or mathematically:

$$P_H|_{\text{Data Link}} = f(P_C, P_F, P_{MD}, P_{FA}) \tag{3.1}$$

The collision hazard, in turn, will be a function of the guidance, navigation and control algorithms and systems on the small SUAV. Calculating or estimating the contribution of the navigation system to P_C and P_F is what will be treated in some detail at the end of this report.

3.2.2. SAFETY RISK #2: ENGINE FAILURE

The engines on SUAVs (sometimes referred to as the power plant or motor) provide thrust required for flight. The thrust generated by the engines allows the SUAV to maintain a constant altitude or climb. Without the engine, SUAVs are gliders and cannot fly at a constant altitude or climb. The engines are either electric or gas (or glow) powered and in most instances they turn a propeller that generates thrust. Therefore, unless noted specifically, when we use the term "engine," it is taken to mean the combination engine/propller system.

Failure Modes & Detection: Engine failure is another detectable safety risk in that there is usually a very clear indication that an engine has failed and is not providing propulsive thrust to the SUAV. When this happens, the SUAV can neither climb nor maintain a constant altitude and will start a gliding descent. In this instance the safety risk present is that of a collision potential with buildings, persons or vehicles. A particular concern in urban operations would be a gliding descent into a vehicle on a highway that is moving at high speeds. It should be noted that there can be engine failure modes in which the engine does not completely cease to function but continues to generate partial power. In this case the ability of the SUAS to climb or maintain constant altitude may not be completely compromised. However, the actual performance of the SUAV will be different from the performance around which the CONOP was designed. This and other similar failure modes are more in the category of *control system lack of authority*, which will be dealt with later. There are several ways in which a failed engine can be detected. In the case of an electric motor current flow to the engine can be monitored. The difference between the actual current draw and the known current draw from a given power setting can be used to determined a failed engine. Another way to determine the engine failure is to monitor the aircraft performance (in terms of speed, altitude, attitiude/orientation) and see if it is different from what is expected from a given power setting. This requires knowledge of the SUAVs dynamics in the form of a kinetic model of the vehicle.

Mitigation Strategy: There are two (of many) mitigation strategies that can be considered for this failure. One strategy would be similar to the "no data link" termination procedure discussed above in that it will initiate a series of maneuvers that will guide the gliding SUAV to a safe landing spot after an engine failure. This procedure would be initiated automatically by the aerial vehicle when an engine failure has been detected. Ensuring that the procedure can be executing safely will require constant monitoring of the aircraft's state to ensure that it is always in a position where it can glide to safety. This will affect the CONOP design by requiring specific trajectories (ones which ensure the ability of safe gliding). This is an example where a fault detection or mitigation strategy required a redefinition or refinement of a CONOP ("feedback" path in the design procedure of Figures 2.1 and 2.2).

Another mitigation strategy can involve modifying the trajectories flown during the operation. For example, if we are inspecting bridges and their associated highways as depicted in Figure 3.1, an engine failure can lead to a collision between the gliding SUAV and traffic on the bridge. This can be avoided by operating the SUAV as shown in Figure 3.3. In this instance, an engine failure results in a gliding path that leads into the river thereby minimizing the collision risk with cars. Of course, the potential for collision with boating traffic on the water has to be evaluated. Equally important is the impact on the objective of the CONOP resulting from this modified procedure. If the quality of inspections provided by the modified flight paths is not acceptable, a compromise needs to be found. Alternately, a new SUAV that features some form of a recovery system (a controllable parachute, for example) may have to be considered. In any event, the risk of collision that results from the recovery will have to be considered in the next step of the risk assessment.

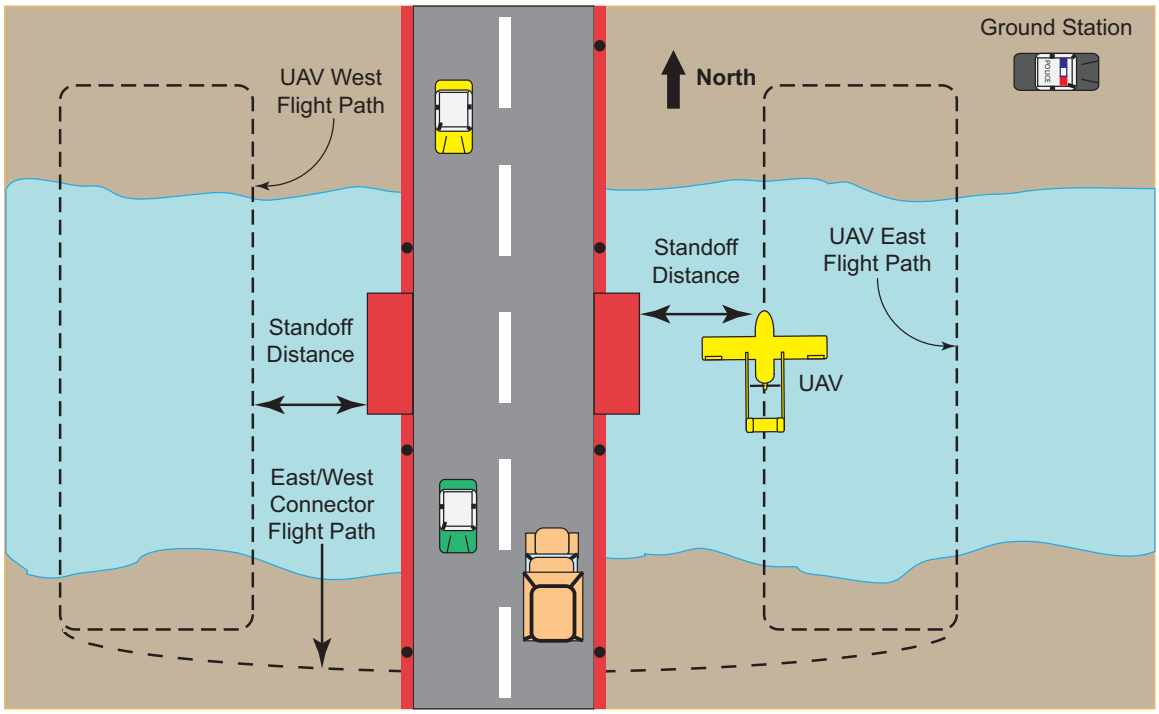

Figure 3.3: Engine Failure Mitigation Strategy Requiring CONOP Procedure Changes. This is essentially a modification of the trajectories depicted in Figure 3.1.

Residual Safety Risk: Once again, the question that the CONOP designer must now answer is this: What is the residual safety risk of the various engine failure modes with their associated detection and mitigation strategies or $P_H|_{\text{Engine Failure}}$? The steps that have to be taken to determine this are identical to what was done above for the data link failure and, thus, we will not repeat it here. In summary, there are several methods by which one can detect the failure of an engine on a small SUAV. Like any other fault detection scheme (including the ones discussed above), there is a finite (even though it may be small) probability that these methods may fail to detect an actual engine failure (i.e., $P_{MD} \neq 0$). There is also the potential that they may flag an engine as failed when in fact it is operational (i.e., $P_{FA} \neq 0$). These in conjunction with the prior engine failure probability P_F and collision probability during the recovery process P_C will help establish $P_H|_{\text{Engine Failure}}$.

3.2.3. SAFETY RISK #3: CONTROL SYSTEM LACK OF AUTHORITY

As noted earlier, the purpose of the control system is to ensure that the SUAV follows remains in controlled flight and follows the trajectory and guidance instruction given by the operators on the ground. It has a direct bearing on the procedures of the CONOP that can be seen by examining Figure 3.1. For example, it has a bearing on how close the vehicle must be (or how far away it needs to stay) from the infrastructure being inspected. This "standoff" distance is an operational requirement that will be spelled out in the procedures for the CONOP. This operational requirement, in turn, is considered acceptable or not depending on the SUAV system capabilities. While it is easy to see how mission payload (or camera) requirements play into this standoff distance requirement, it may not clear to see how control system requirements play into this. This will become apparent when we consider failure modes of the control system next.

Failure Modes & Detection: "Hard" failures of the control system are detectable just as data link or engine failures discussed above are detectable. However, there are "soft" failures that are not. These are cases where the control system is functioning nominally but the environment in which it is operating is beyond its capabilities. We can see this if we examine Figure 3.1 once again. The control systems must be able to keep the aerial vehicle at this standoff distance. If a disturbance (a gust of wind, for example) upsets the aerial vehicle and pushes it toward the building, the control system must respond quickly to move the airplane back to the standoff distance. The available control authority and bandwidth, therefore, play an important role in defining the concept of operation. That is, if a control system cannot be found that meets the SWAP requirements for the vehicle on hand while simultaneously satisfying the performance requirements of being able to maintain a given standoff distance, then the CONOP cannot be carried out. In this instance a new vehicle, a new CONOP, or both must be devised. This is an undetectable failure because it is not a failure of the control system *per se*. It is the result of the control system being forced to operate in a condition that is beyond its capability. It is a failure of *lack of authority* on part of the control system that cannot be detected by monitoring the control system itself.

Mitigation Strategy: A mitigation strategy which will require refining procedure of the CONOP involves establishing initial conditions based on weather reports. If the reported weather conditions favor the presence of gusts greater than the the authority of the control system, then operations should not be initiated. While other mitigation strategies can be devised, this one will be sufficient for what we are attempting to demonstrate here; we want to examine the issues associated with undetectable safety risks.

Residual Safety Risk: Since this is an undetectable fault, safety risk, $P_{MD} = P_{FA} = 0$. That is, we cannot detect these faults so we do not design fault detection or mitigation strategies. Instead, we assess the residual safety risk based on how well the procedural mitigation strategy guarantees the control system will not be overwhelmed by a gust. For example, if we designate the threshold gust velocity above which the control system lacks authority as $V_{\text{Max Gust}}$, then $P_H|_{\text{Control Authority}}$ is related to the likelihood that during a given operation, gust velocities greater than $V_{\text{Max Gust}}$ will be encountered. More precisely, the residual hazard is related to the probability that gust velocities will exceed $V_{\text{Max Gust}}$ on a day when forecasts predict they will be no greater than V_{Gust}. This is a difficult probability to quantify especially, when operating in and around buildings, bridges and other structures. This is

because these structures can have very strong local effects on the nature of gusts.

3.2.4. Safety Risk #4: Navigation System Stochastic Errors

Navigation systems are part of the "eyes and ears" of autonomous UAVs as they tell the vehicle where it is in relation to the world around it. As such, they have a direct bearing on the collision risk. An undetectable safely risk presented by these systems is the situation where the navigation errors during operation of the SUAV become larger than expected, but there is no indication of this. This safety risk is the direct result of navigation sensor errors being stochastic in nature. This is particularly true of inexpensive sensors aimed at the guidance, navigation and control of SUAVs. We will examine this in some detail for the remainder of this report.

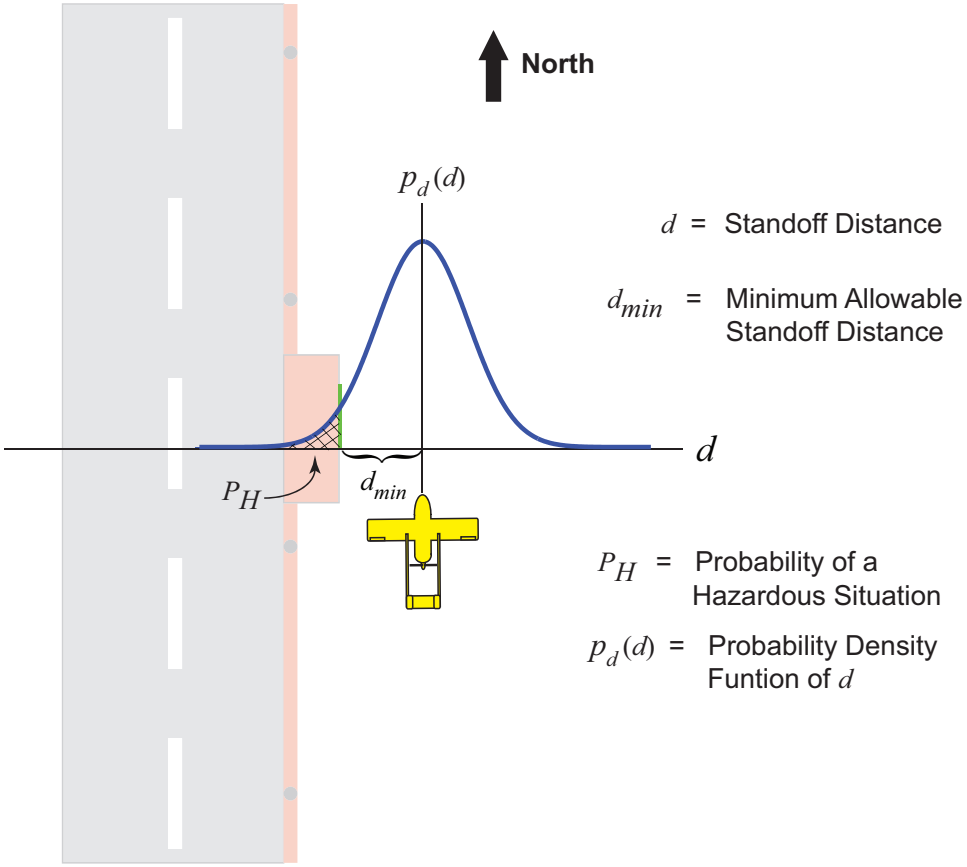

Figure 3.4: Risk Due to Navigation System Stochastic Errors

Failure Modes & Detection: To understand what this safety risk is and why it is undetectable, let us consider Figure 3.4, which is a modified form of Figure 3.1. The control system bases its control action on information coming from, in part, the navigation system. The navigation system, in conjunction with the onboard maps of the building or infrastructure being inspected are used to determine whether the aerial vehicle is positioning at the appropriate standoff distance. Knowledge of the infrastructure being inspected is important because, as shown in Figure 3.1, the standoff distance is defined by the position of the vehicle and closest point on the infrastructure being inspected. So not only must we

know the position coordinates of the vehicle at any point, but we must know the position coordinates of the closest point on the building as well. In Figure 3.4 the navigation output error distribution is shown along with the standoff distance. Note that what is shown is the navigation system output errors that can be expected in normal or non-faulted operation. That is, assuming the standoff distance estimation errors are Gaussian distributed, the likelihood of errors that are large enough to result in a collision would be equal to the area of the red shaded region in Figure 3.4. That is, it is possible to have the navigation system generate an estimate of the SUAV's actual standoff distance at some point during an operation that is erroneous. The errors can be such that the SUAV is actually located closer to than infrastructure than d_{Max}. In this instance, the control system will not react to correct the position of the vehicle because it "thinks" that the vehicle is actually at the standoff distance or further. Thus, the overall system is in an unsafe state while there is no indication of this unsafe condition. This is sometimes referred to as the *fault-free integrity*. That is, we define the fault-free integrity to be equal to the likelihood of the vehicle being in an unsafe state while all systems are operating normally such that fault detection and mitigation mechanisms have not been activated.

Mitigation Strategy: Once again, since this is a undetectable safety risk, a mitigation strategy *per se* cannot be designed. Performing a cost-benefit analysis is required to quantify how much risk is tolerable. This is part of the iterative process of designing a CONOP. For example, if it is judged that a hazardous situation such as the one described above is acceptable in one out of one million operations of the SUAS, then the integrity risk is said to be at 10^{-6} and the standoff distance has to be designed accordingly. If a smaller standoff distance is required, newer and more accurate navigation sensors or a better and higher-quality mission sensor payload (camera) must be used.

Residual Safety Risk: Like the previous undetectable risk, $P_{MA} = P_{FA} = 0$. That is, we cannot detect these faults so we do not design fault detection or mitigation strategies. Instead, we assess the residual safety risk by performing what is known as *an integrity risk assessment*. This is nothing more than defining d_{min} and then determining the associated P_H. If P_H is found to be greater than P_A (the acceptable risk threshold), the CONOP must be redefined/refined with a new d_{min}. The next section of the report explores this issue in detail.

(Intentionally Left Blank)

CHAPTER 4

MISSION RISK ANALYSIS

This section provides an example of how risk due to undetectable navigation system errors can be quantified or overbounded. We choose to focus on this risk for the following two reasons. First, these systems are, to a large extent, the only inexpensive "eyes and ears" suitable for small aerial vehicle. Their proper functioning is key to safe operations of a UAS. The second reason is because there are many "turn key" or off-the-shelf navigation solutions proposed for SUAS operations. When examining the performance specification sheets for these devices, it is not clear that they take into account the type of risk assessments needed in liability and safety critical operations of SUAS. More specifically, usually the performance metric used to sell these devices is accuracy. Accuracy is defined as the magnitude of the 95% (or approximately 2-σ) of the navigation errors [7]. This is not a sufficient indicator of the collision risk presented by these systems. It is our hope that this analysis will show that there is more that needs to be taken into account when assessing the risk associated with operations of SUAS which rely on off-the-shelf navigation solutions.

4.1. PRECISE RISK ESTIMATION VS. OVERBOUNDING

As noted earlier, SUAS operations in ITS application are what are considered safety of life or liability critical applications. Minimizing the exposure to undetectable safety risks is an integral part of designing these types of systems. In more concrete terms, this means ensuring that $P_H < P_A$. In the area of design and operation of navigation systems when this conditions is satisfied the system is said to possess *integrity* [8, 9, 10].

Since we are interested in quantifying integrity let us re-examine Figure 3.4. An initial CONOP design will define P_A (the maximum tolerable collision risk). It will also specify a desired minimum standoff distance d_{min}. The latter requirement will most likely be the result of the mission payload's (the camera's) capability. The integrity analysis will determine whether the actual collision hazard P_H (monitored in real time) is indeed less than P_A. Note that no system failures have been assumed and, thus, this is an undetectable safety risk. It is sometimes called the potential for hazardously misleading information (HMI).

In terms of Figure 3.4, the state of interest is d and it is estimated in real time by fusing the outputs y_i (where $i = 1, 2, \ldots, N$) of many sensors. A typical navigation system architecture is shown in Figure 4.1 and the y_i in the above sentence refers to the output of the sensors shown on the left side of the figure. The safety risk P_H is equal to the shaded area under the probability density function for d

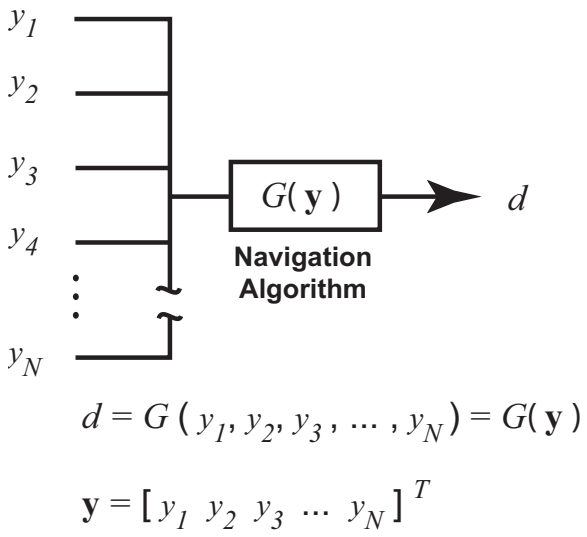

Figure 4.1: Generic Block Diagram of an Integrated Navigation System

in Figure 3.4 and is equal to:

$$P_H = P\{d < -d_{\min}\} = \int_{-\infty}^{-d} p_d(\xi) d\xi, \tag{4.1}$$

where the notation $P\{\bullet\}$ is used to denote "the probability of" the event defined by the expression between the braces. The uncertainty in the standoff distance d (or any other navigation state that is important to the risk analysis) results from errors and uncertainties in the inputs. As was shown in some detail in [11]-[13], the outputs of sensors that are suitable for use in SUAS tend to have outputs that are corrupted by stochastic noise. Thus the probability density function of the standoff distance errors p_d will be a function of the probability density of the input sensor errors p_{y_i}. Once we know p_{y_i} and the algorithms used in the navigation system (which are represented by the function $G(y)$ in Figure 4.1), then we can determine p_d. If p_d is known, we can calculate the collision risk P_H by evaluating Equation 4.1 above. While this can be done in principle, in practice it is difficult if not impossible to do. The difficulty in evaluating the collision risk P_H in practice stems from the following two issues identified in [11] and [13]: (1) non-linearities in $G(\mathbf{y})$ and (2) uncertainties in p_{y_i} to which the estimate of P_H is very sensitive.

Evaluating P_H involves propagation of probability densities through non-linear functions. This is generally a computationally intensive process. If P_H could be evaluated once off-line prior to a SUAS operation then this would not be a problem. However, non-linearity of $G(\mathbf{y})$ implies that P_H is time varying and, therefore, needs to be evaluated continually during a SUAS's operation. This computation can put burden on the resources of the types of small computer that would be found in a SUAV. Simply inflating P_H to cover all possibilities that would be encountered in flight is not always practical in that it may result in a CONOP that is useless.

The non-linearity found in some navigation algorithms is somewhat mild and the assumption of linearity can be made. A case in point is GPS-based navigation (as well as other Global Navigation Satellite Systems or GNSS). While this may remove the computational burden associated with estimating P_H, there still remains the second issue which is the uncertainty in our knowledge of p_{y_i}. As

shown in [11] - [13], most navigation sensors suitable for SUAS applications have outputs corrupted by stochastic errors. In addition to being inexpensive, these are sensors that satisfy the size, weight and power or SWAP constraints imposed by SUAVs. Stochastic error models that are precise enough for an accurate determination of P_H are difficult to construct because they are variable from sensor to sensor. They can also be non-stationary.

Because of these challenges, we propose resorting to an approach where we replace actual error distributions p_{y_i} with conservative approximation called overbounds. This concept is demonstrated in Figure 4.2. The actual sensor error distributions and the resulting navigation solution error distributions are shown in blue. The red distributions are overbounds. Thus, by using a simple input overbound, which guarantees the output is overbounded, we can generate a conservative estimate of the risk at all times. The risk generated by overbounding is said to be conservative because it will be larger than the actual risk. That is, the overbounding approach will generate a risk estimate equal to $\bar{P}_H$ which is greater than the *actual* risk P_H.

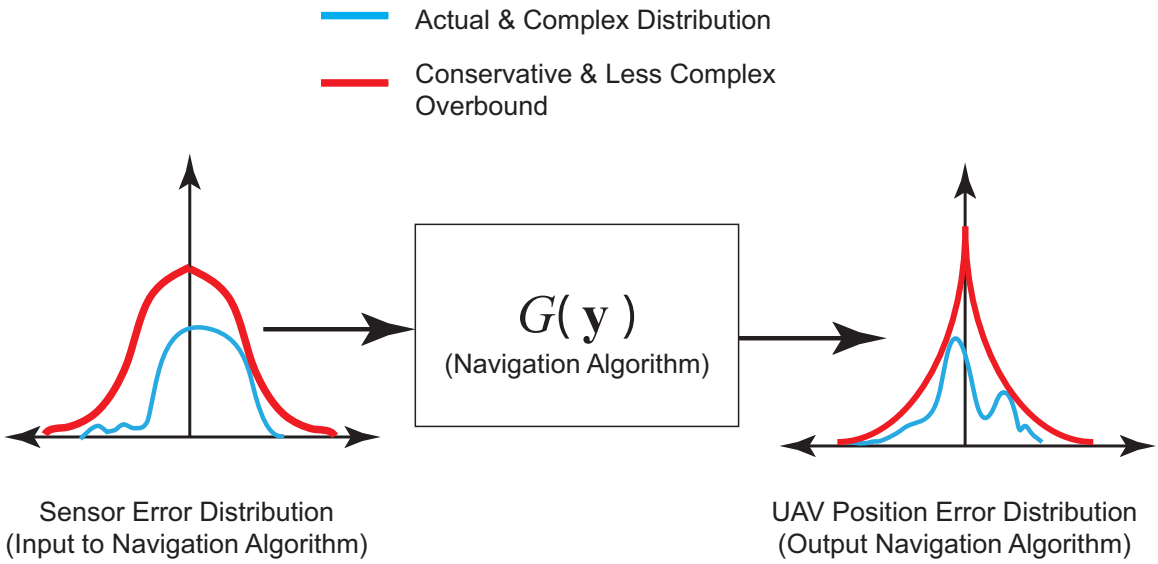

Figure 4.2: Graphical Depiction of the Overbounding Concept

The theoretical underpinnings for overbounding, as well as the derivation of an overbounding Kalman Filter that was developed specifically for the work reported here, are discussed in [13]. It is based on the seminal work on overbounding given in [8], while a representative (to the work discussed but not complete) list of works documenting applications and extensions of overbounding are found in [9], [10] and [13]. In what follows we will consider a generic SUAV navigation system architecture and examine how it relates to the collision risk of the CONOP being considered here.

4.2. SUAV Navigation Systems

Navigation systems used in small aerial vehicles are going to be integrated navigation systems. That is, they combine the information from many sensors in real time to generate an optimal estimate of the vehicle's position and attitude (orientation). Schematically, this is shown in Figure 4.3. While differentially corrected GPS or other GNSS is the core sensor for such applications, GPS/GNSS have

limitations that have been well documented in the literature. In particular, errors such as multipath can be very problematic in such applications. Therefore, a fusion of inertial, vision-based, acoustic, GNSS, etc. sensors must be used. The important point of this is that the accuracy and reliability of the navigation solution is going to be determined by the sensor integration or fusion algorithms used and the quality of the sensors integrated. Mapping the sensor performance (especially error characteristics) to the position solution is, therefore, crucial to the realization of UAS CONOP.

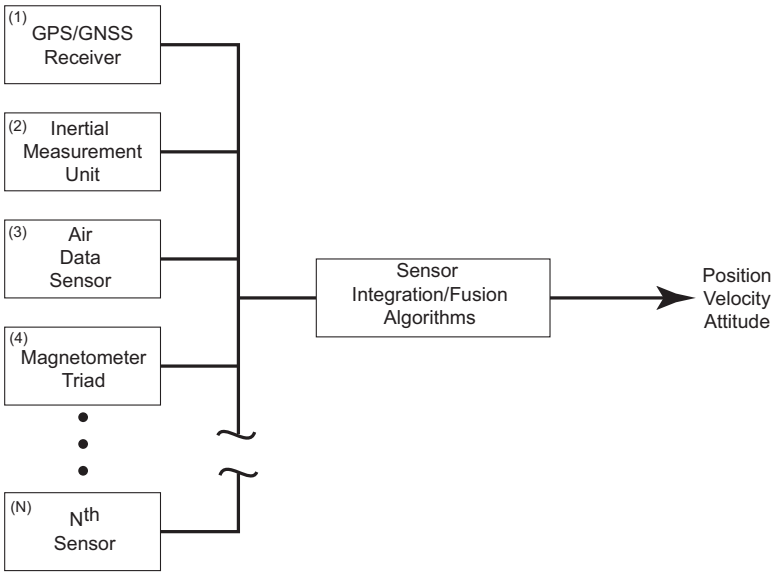

Figure 4.3: Typical, Low Cost Multi-Sensor or Integrated Navigation System

Most low-cost, integrated navigation systems that satisfy the SWAP constraints for SUAVs fuse the navigation solution from a dead reckoning system with GPS/GNSS. The dead reckoning systems used are either an inertial navigation systems (INS) [15] or an airspeed/AHRS [16, 17]. The mechanics of this integration are discussed some detail in [14] and [15] and will not be covered here. The important point for the discussion here is to note that the dead reckoning systems provide a navigation solution when the GPS/GNSS solution is not reliable or unavailable. In addition, the dead reckoning systems provide an attitude solution (orientation), which is required for autonomous control of SUAVs. The dead reckoning system alone (especially those satisfying the SWAP constraints for SUAVs) cannot provide an accurate solution for extended periods of time. Therefore, the dead reckoning errors have to be periodically "reset" using GPS/GNSS updates. In the previous sentence, the word "reset" is in quotes because in practice the periodic GPS/GNSS updates do more than a simple reset or zeroing-out of errors. The details of what occurs with these updates and the mechanics of how it is accomplished are beyond the scope of this report. The interested reader can find more details about this in [15], [14] and [18].

4.3. NAVIGATION SYSTEM OPERATION

Given the basic architecture of a low-cost integrated navigation system shown in Figure 4.3 and the associated discussion above, we can now start assessing the collision risk associated with the CONOP we are designing. Focusing on Figure 3.3, let us consider only the east part of the the flight pattern.

Figure 4.4 shows how a well-designed navigation system will use the information from its sub-systems to generate a navigation solution when flying this pattern.

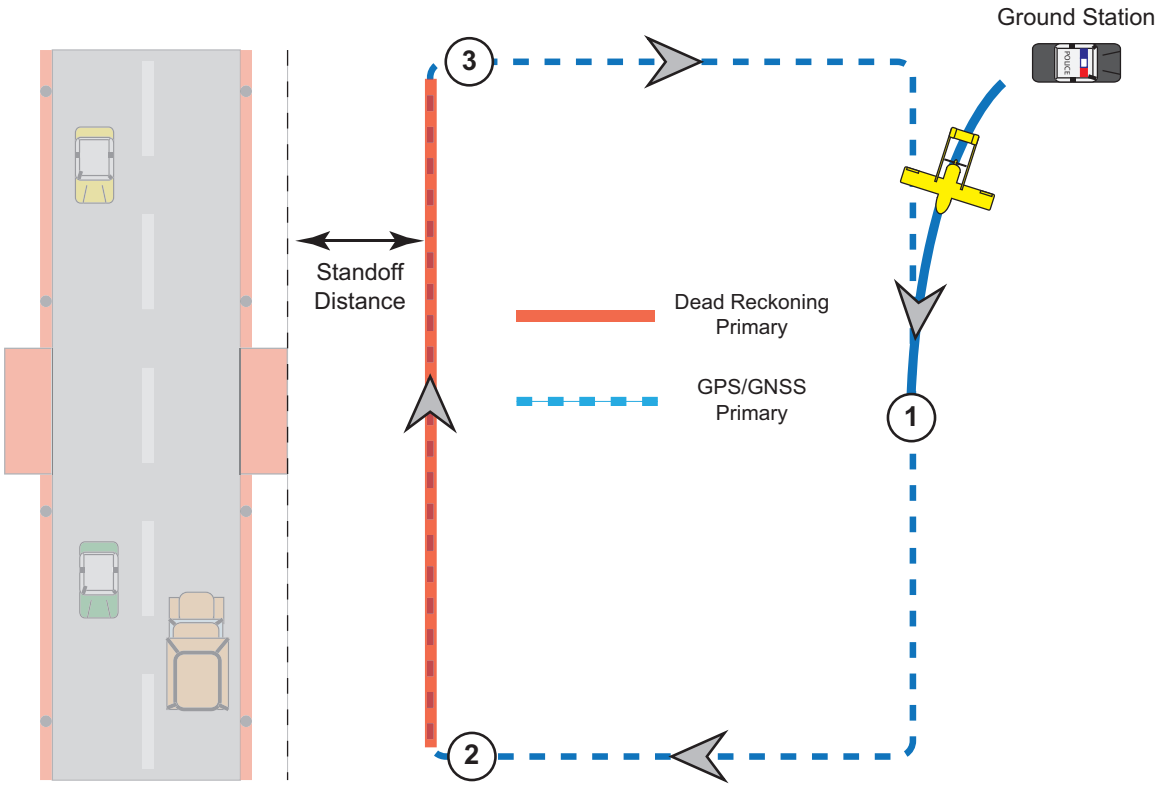

Figure 4.4: Navigation Sub-System Scheduling for Infrastructure Inspection CONOP

The SUAV enters the inspection pattern at Point 1. From Point 1 to Point 2 the navigation system is relying on GPS/GNSS for navigation. In parallel, the sensor integration or fusion algorithms are preparing the dead reckoning system to work in a stand-alone fashion along the route between Point 2 and Point 3 if needed. We say "if needed" because given that GPS/GNSS in a differential mode can provide accuracies on the order of centimeters, it is the navigation sensor of choice in most applications. However, the accuracy of GPS/GNSS is degraded when a receiver's antenna is in close proximity to (less than 300 m away from) a surface that can reflect the signals from the satellite. Thus, if it is judged that the GPS/GNSS accuracy is not sufficient (or the signals are not available altogether), the dead reckoning solution will be used.

4.4. Quantifying/Bounding the Collision Risk

In what follows we consider only the collision risk due to the navigation system and not that of errors in our knowledge of the infrastructure geometry. Recall that the navigation system, in conjunction with the onboard maps of the building or infrastructure being inspected are used to determine whether the aerial vehicle is positioned at the appropriate standoff distance. Knowledge of the infrastructure being inspected is important because, as shown in Figure 4.4, the standoff distance is defined by the position of the vehicle and the closest point on the infrastructure being inspected. So not only must

we know the position coordinates of the vehicle at any moment, but we must know the position coordinates of the closest point on the building as well. We are going to assume our knowledge of the infrastructure location/geometry is perfect.

4.4.1. BOUNDING P_H DUE TO GPS/GNSS ERRORS

In view of Figure 4.4, clearly GPS/GNSS will be the primary means of navigation along the route denoted by the blue broken lines. We will refer to this path as the downwind leg. If multipath is not present or severe along the route denoted by the solid red line on Figure 4.4, then GPS can be used there as well. We will refer to this path as the upwind leg. The infrastructure collision risk is clearly less on the downwind leg than it is on the upwind leg. Without loss of generality, therefore, we can consider analysis of the collision risk on the upwind leg as a conservative upper bound of the risk.

For completeness, however, we mention how the collision risk would be analyzed for a GPS/GNSS-only navigation system. Details on how this is done can be found in representative papers such as [8], [9] and [19]. In essence, it reduces to identifying the largest possible measurement error that can be expected from GPS/GNSS in the vicinity of the bridge. This error can be inflated by an appropriate amount and used in navigation error prediction calculations (i.e., the covariance matrix computation as described in [7] or [20]). This calculation yields $\bar{P}_H$ and the inflation factor is adjusted to obtain a desired risk margin relative to P_A.

4.4.2. BOUNDING P_H DUE TO DEAD RECKONING ERRORS

Similar to what was done for GPS/GNSS, we can generate an overbound for the dead reckoning solution along the upwind leg. Unlike the overbounding of GPS, however, prior work in overbounding dead reckoning errors is limited. In support of this work an overbounding Kalman Filter was developed for a airspeed/AHRS dead reckoning solution and is discussed in detail in [13].

Figure 4.5 *qualitatively* shows how the collision risk changes with time on the upwind leg. The probability density function (pdf) for the overbound on the standoff distance error d is shown at three points along the upwind trajectory. We use overbounds because they can be Gaussian and, thus, easier to deal with than other general distributions. The part of the pdf that intersects the bridge (or other infrastructure) represents the upper bound on the collision risk $\bar{P}_H$. We see that as time progresses, the collision risk grows. This is shown in Figure 4.5 as a widening of the pdf as we move from Point A to Point C. The collision risk will be highest at Point C. If it found that $\bar{P}_H$ is greater than P_A at this point, then the CONOP must be revised to ensure that $\bar{P}_H$ is reduced to below the threshold of acceptable risk. This can be done in one of many ways. For example, we can increase the minimum standoff distance required such that $\bar{P}_H$ is less than P_A along the entire upwind leg. Alternately, we can dynamically change the upwind leg pattern as shown in Pattern 1 of Figure 4.6. An alternative pattern is shown as Pattern 2 in Figure 4.6.

A *quantitative* feel for how this is done can be obtained by considering the following specific simulation example. A SUAV is performing infrastructure inspection using a flight profile similar to that of Pattern 1 of Figure 4.6. The upwind leg is being flown at a constant speed of 17 m/s. The onboard dead reckoning system uses air speed measurements V resolved into north and east components using heading estimates from an attitude heading reference system (AHRS) as follows:

$$v_N = v\cos\psi + \delta v_N \tag{4.2}$$

$$v_E = v\sin\psi + \delta v_E \tag{4.3}$$

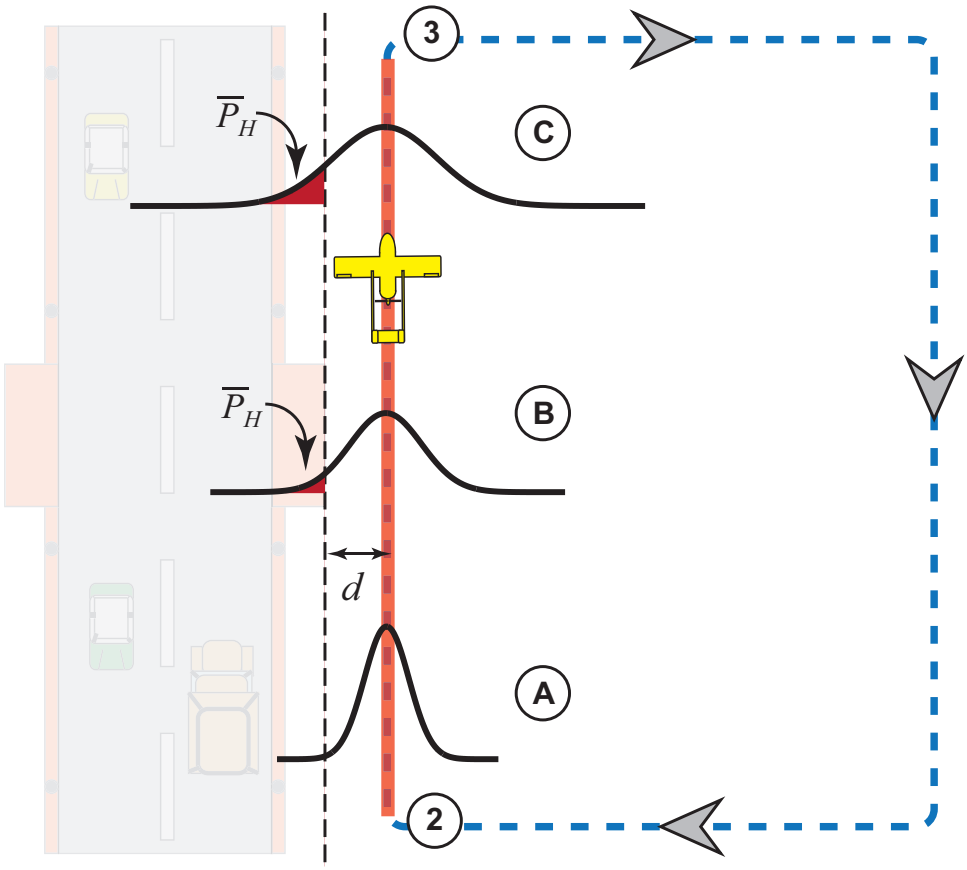

Figure 4.5: Time Growth of Upper Bound on the Collision Risk or $\bar{P}_H$

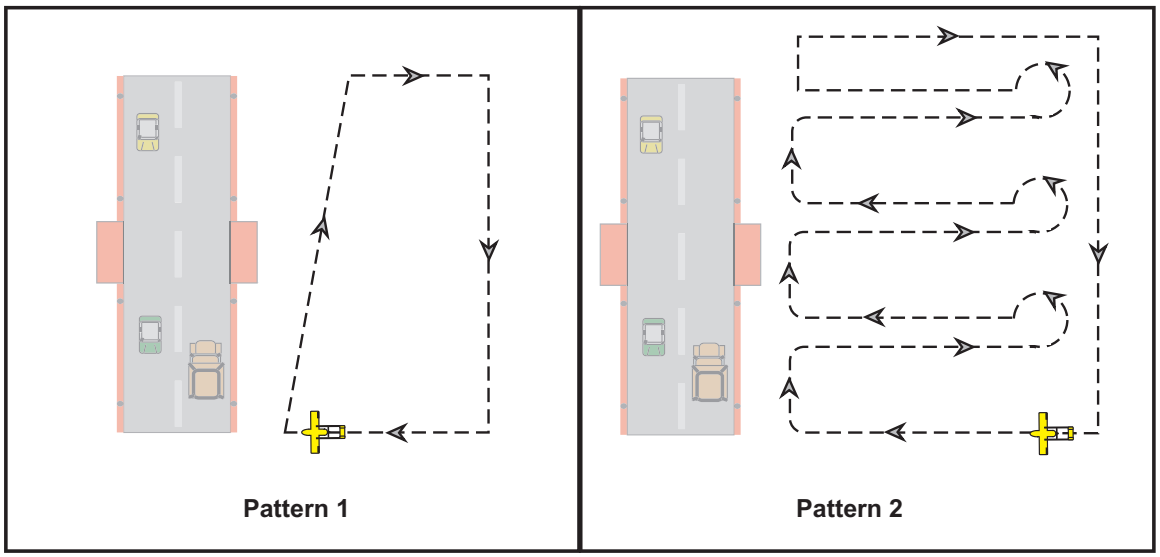

Figure 4.6: Alternative Inspection Flight Patterns to Always Ensure that $\bar{P}_H < P_A$

Table 4.1: Sensor Error Statistics

Sensor	Output	pdf	Error
AHRS	Attitude/Heading	Gaussian	3° to 8°
Air Data	Airspeed	Gaussian	5 m/s

where δv_N and δv_E are the north and south components of wind speed. We will assume that the wind is known precisely or has been estimated using an observer akin to the one described in [16]. Thus, we will set $\delta v_N = \delta v_E = 0$. The AHRS is mechanized using one of many available algorithms such as those described in [21, 22, 23, 24]. While it is not important how the AHRS is mechanized, we assume that the algorithm generates an estimate of the attitude accuracy with output errors characterized by a variance σ_ψ^2. Similarly, the airspeed measurement errors have been characterized by a variance σ_v^2. From v_N and v_E, we can estimate the north and east position coordinates by integrating the following differential equations:

$$\dot{p}_N = v_N \tag{4.4}$$

$$\dot{p}_E = v_E \tag{4.5}$$

If we establish a local coordinate frame with origin O as shown in Figure 4.7, then p_E is the standoff distance. The navigation system's estimate of the standoff distance is $\hat{p}_E$ and errors in its estimate are related to P_H (or alternately $\hat{P}_H$).

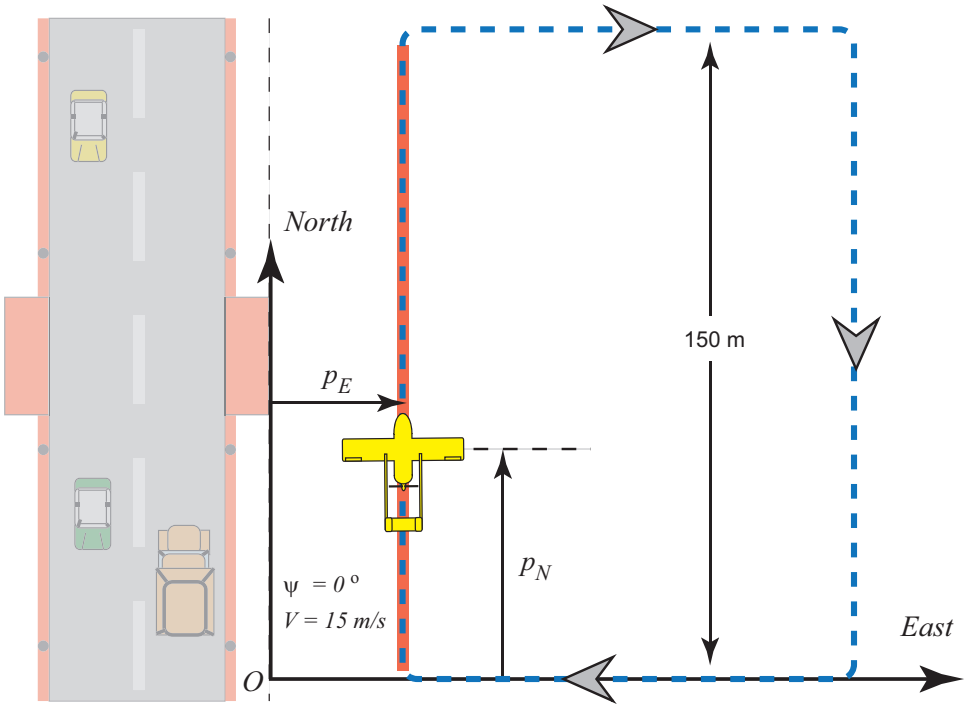

Figure 4.7: Quantifying the Collision Risk for the Infrastructure Inspection CONOP

Figure 4.8 shows the results of a Monte Carlo simulation for CONOP where the standoff distance is set at 5 m. What is shown in the figure is the spread of the north and east position estimate as the

SUAS travel along the length of the bridge at a standoff distance of 5 m. The SUAS's navigation system would compute a position solution at $t = 5$, 10 and 15 seconds which would correspond to the "+" marker. The blue dots represent possible *actual* position coordinates of the SUAS. Since the navigation sensor errors are stochastic, each blue dot is a possible position solution when the navigation system is operating nominally. What is apparent is that the collision risk is non-zero and becomes larger and larger as the SUAS travels farther along the upwind path.

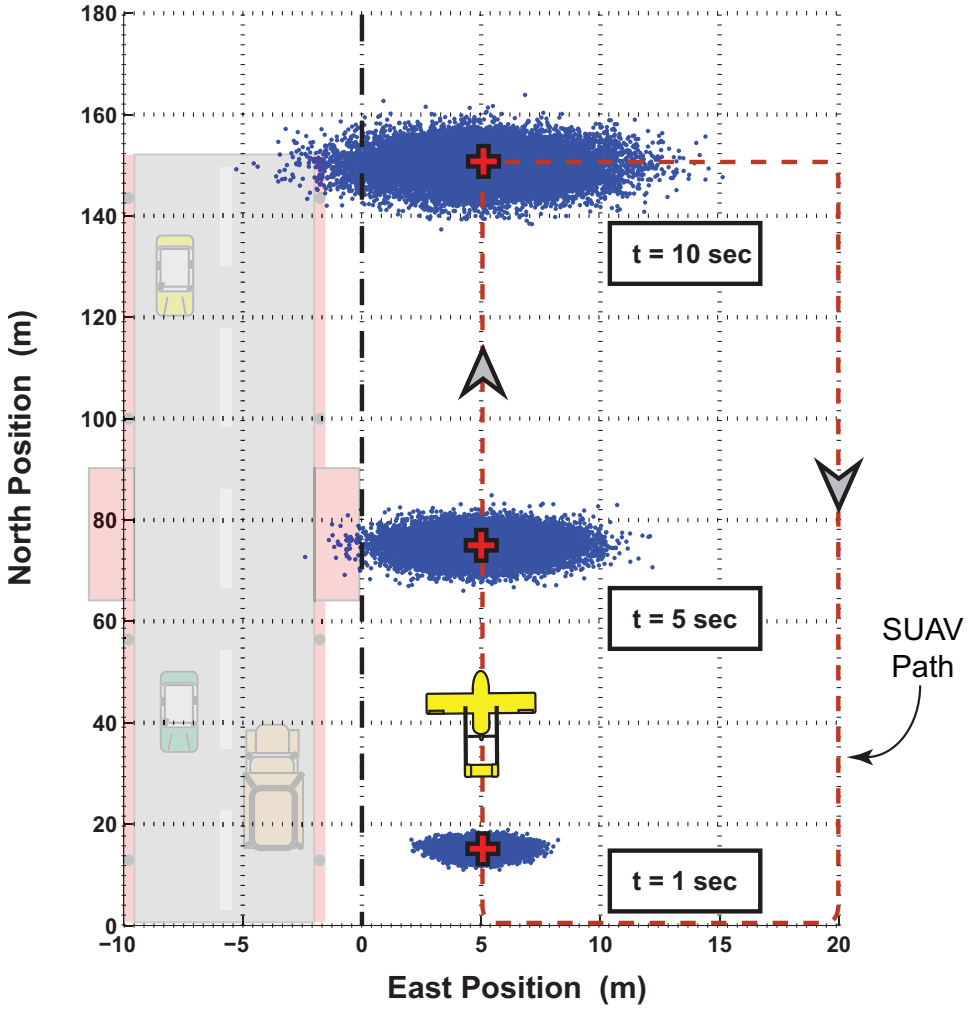

Figure 4.8: Visualization of the Effect of Navigation Error on Collision Risk. Heading Error $= 3°$. Airspeed Error $= 1$ m/s

While Figure 4.8 gives an intuitive feel for the relation between navigation error and risk, it does not allows us to precisely quantify the risk of collision P_H. To do that we need to extract information about the navigation error statistics from the sensor integration algorithm. The details for doing this are discussed in [13], as well as in many excellent texts on integrated navigation systems such as [15] and [18]. For the discussion here we note that many low-cost, off-the-shelf navigation systems use, at best, an Extended Kalman Filter and in some instances an *ad hoc* sensor integration algorithm. Assuming an Extended Kalman Filter is used, the navigation system will generate an estimate of the navigation system errors. The errors will be assumed to be Gaussian and, thus, only the first and second order

moments (mean and variance) of the error distribution are required to *completely* characterize it. Thus, the performance metrics reported by off-the-shelf navigation systems will be the mean (in this case the estimate of p_N and p_E) and the covariance of the error (σ_{p_N}, σ_{p_E} and $\sigma_{p_N p_E}$).

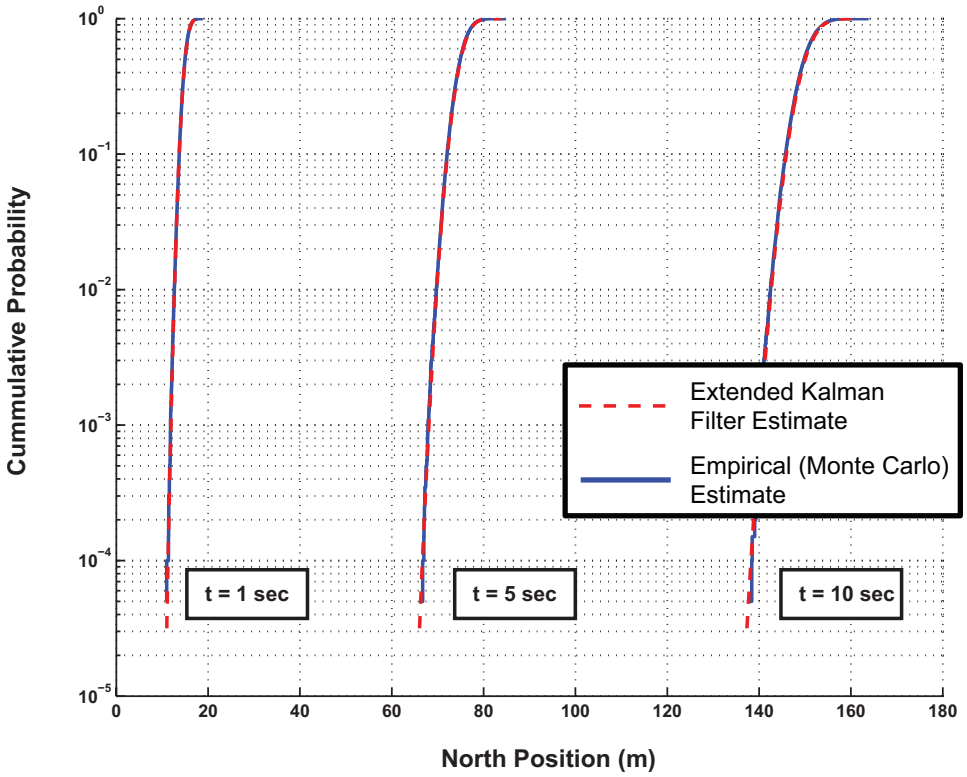

Figure 4.9: Cumulative Density for North Position. Standoff Distance $d = 5$ m. Heading Error $= 3°$. Airspeed Error $= 1$ m/s

Figures 4.9 and 4.10 show the cumulative density function for the errors in the north and east direction, respectively. The blue traces represent the estimate generated by an Extended Kalman Filter. The red traces represent an empirical estimate of the actual distribution based on Monte Carlo simulation. Since the Extended Kalman Filter (or *ad hoc* estimators) will more than likely linearize the underlying navigation equations, their description of the errors will be an approximation. When it comes to risk quantification this can have an important bearing because linearization tends to affect the tails of distributions. This is the part of the error description that is required to characterize P_H. This will become important when we examine what happens when sensor errors get larger.

With respect to Figures 4.9 and 4.10, the key point here is to note that the collision risk ($P\{p_E < 0\}$) one second into the upwind leg is $P_H = 3 \times 10^{-5}$ and increases to $P_H = 1 \times 10^{-3}$ four seconds later. At then end of the upwind leg or five seconds later the collision risk is at $P_H = 2.5 \times 10^{-2}$. Thus, unless P_A (the acceptable hazard risk) is greater than 2.5×10^{-2} (which is very unlikely) then the CONOP where the SUAV flies parallel to the infrastructure at a five meter standoff distance is not possible. The CONOP must be redesigned by increasing the standoff distance, modifying the flight path akin to what was shown in Figure 3.3 or a combination of both.

Suppose the AHRS used in the navigation system has heading estimation errors that can be as large as $8°$. How would this impact the CONOP analysis? Examining Figure 4.11 and 4.12 provides

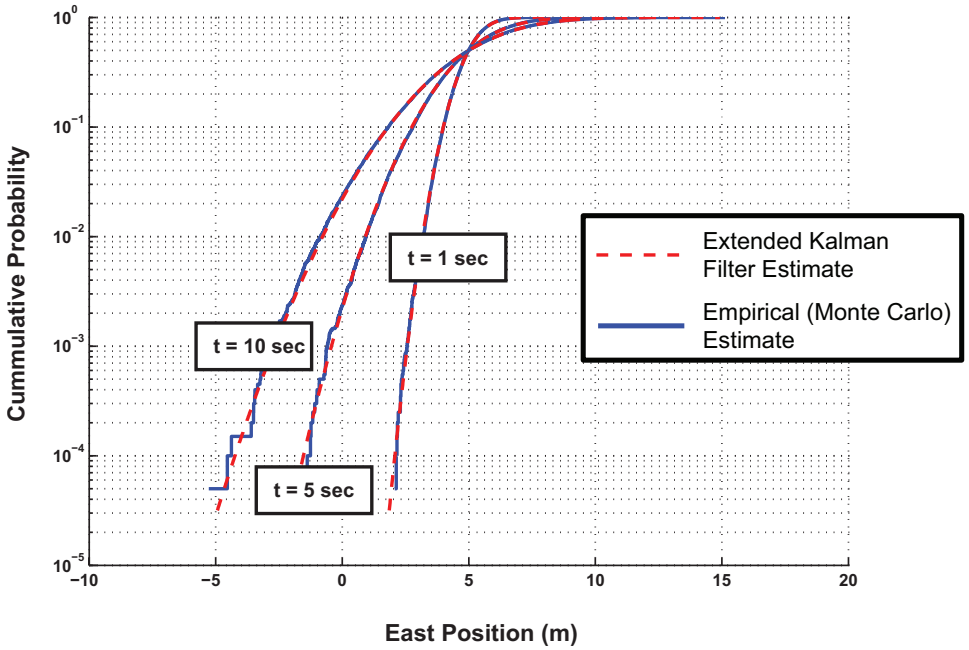

Figure 4.10: Cumulative Density for East Position (Standoff Distance d). Standoff Distance $d = 5$ m. Heading Error $= 3^\circ$. Airspeed Error $= 1$ m/s

an answer. As we would expect the collision risk becomes higher and once again the CONOP must be redesigned with a new standoff distance larger than 5 m. A more interesting point, however, is made by Figure 4.11. While the north position error is not related to the standoff distance directly, it has an impact on the collision risk because we must know our displacement relative to the structure being inspected to avoid a collision. Thus, an accurate estimate of both horizontal position coordinates is required.

What we note in this case is that the Extended Kalman Filter of the navigation system is providing a P_H estimate that is smaller than the true risk. It is being un-conservative. This is related to the issue of overbounding we discussed earlier. This is why the output of off-the-shelf navigation systems cannot be relied on for making collision risk assessments unless they have been analyzed specifically for this. In this case, an overbounding filter akin to the one developed in [13] must be used to provide a conservative bound on the collision risk $\bar{P}_H$.

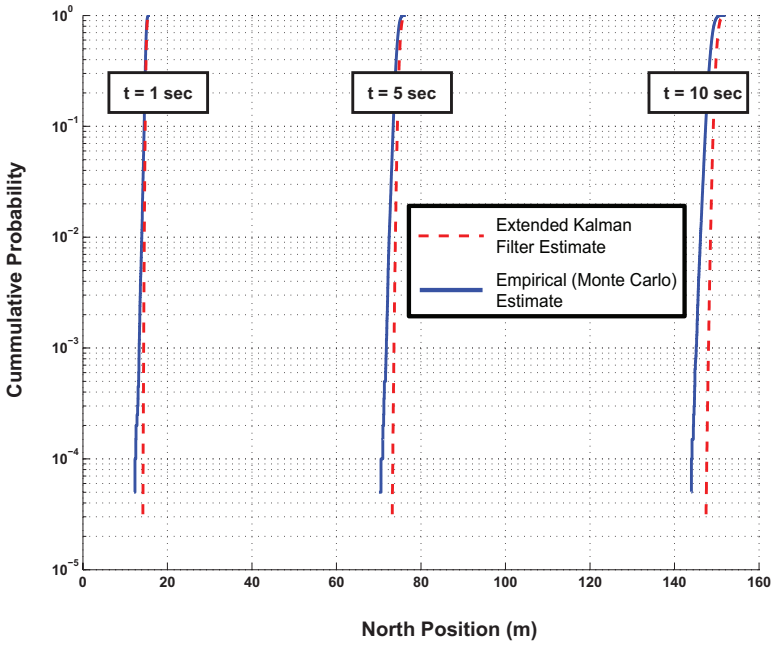

Figure 4.11: Cumulative Density for North Position. Standoff Distance $d = 5$ m. Heading Error $= 8°$. Airspeed Error $= 1$ m/s

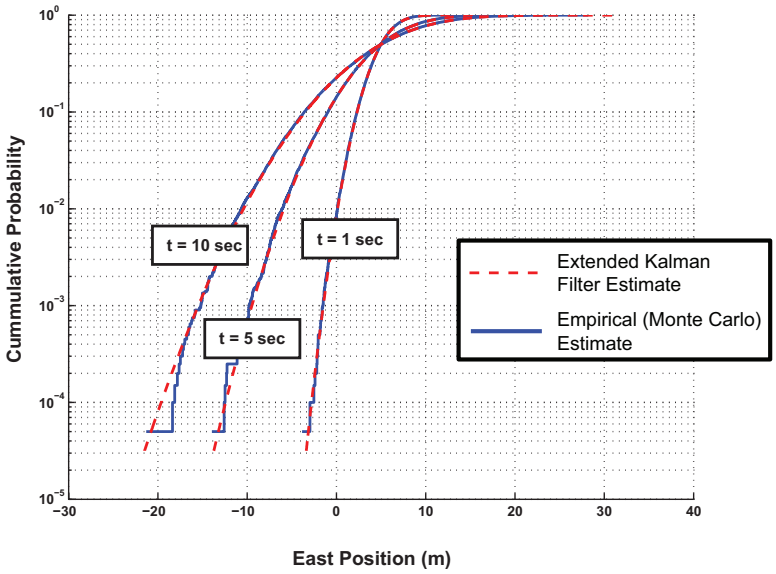

Figure 4.12: Cumulative Density for East Position (Standoff Distance d). Standoff Distance $d = 5$ m. Heading Error $= 8°$. Airspeed Error $= 1$ m/s

CHAPTER 5

SUMMARY & CONCLUSION

These days it is generally accepted that using miniature remotely operated aerial vehicles as sensing platforms will enhance data gathering for traffic management and infrastructure security. What is not clear, however, is whether use of these platforms in this application still represents an economical and practical solution to the problem when regulatory and certification issues related to safety are taken into account. Answering this question requires performing a detailed system analysis to precisely quantify the risk presented to the general public by the operation of these vehicles. The objective of the work was to develop a framework or methodology for performing this precise safety analysis. The framework developed shows that proving collision risks are small or bounded can be challenging.

The work described in this report outlines a method for designing CONOPs for small UASs when used in the envisioned ITS application of highway and transportation infrastructure monitoring. The procedure highlights the fact that SWAP constraints imposed by small UAS limit hardware redundancies. As such, there is a very close link between onboard systems, CONOPs, and risk. The onboard sensors and their performance affect the way the operating procedures must be carried out if collision risks are to be minimized or bounded at a known level.

Currently, some proposed CONOPs for UAS do not specifically take into account the aerial vehicle or its onboard sensor suite, which consists of avionics (i.e., navigation, guidance and control electronics) and mission sensor payloads. This approach provides some measure of flexibility because the vehicle can be used to support a variety of CONOPs. Similarly, the CONOPs can be realized using various aerial platforms. This approach to CONOP design, however, becomes inefficient, if not unusable, with small aerial vehicles because of the normally encountered SWAP constraints. This is because with these small vehicles the avionics and sensor payload dimensions and weight can represent a significant fraction of the overall vehicle dimension and weight. At the scale of such aerial vehicles, therefore, a dichotomy between CONOPs and vehicle along with sensors is somewhat artificial since the two cannot be viewed separately. This means that designing CONOPs will require a design methodology that formally accounts for aerial vehicle and sensor capability.

This last fact is perhaps the most important thing highlighted by this work: The tight interconnectedness of systems on small UAS requires that the internal workings of each system be known or the risk it presents be understood. Therefore, small UAS solutions based on off-the-shelf (or “turn key”) technologies can be considered acceptable only after a case-by-case evaluation of their use in a given CONOP or if they are designed to an overall accepted standard that takes risk into account.

REFERENCES

[1] M. Hickman, P. Mirchandani, A. Angel and D. Chandnani, *NCRST-F Year 1 Report. Project 3- Needs Assessment and Allocation of Imaging Resources For Transportation Planning and Management*, ATLAS Research Center, University of Arizona. Tucson, AZ, September 30, 2001.

[2] D. Gebre-Egziabher, *RPV/UAV Surveillance for Transportation Management and Security*, University of Minnesota Intelligent Transportation Systems Institute Report CTS 08-27, Minneapolis, MN, December 2008.

[3] "TIGER - Minnesota's Surface Transportation Security and Reliability Information System Model Deployment: Vol. one - Capabilities", proposal submitted to USDOT/FHA by Minnesota Department of Transportation and Partners, St. Paul, MN, September 13, 2002.

[4] Army UAS CoE Staff, *"Eyes of the Army": US Army Roadmap for Unmanned Aircraft Systems 2010 - 2035*, US Army UAS Center of Excellence (ATZD-CDI-Q), Fort Rucker, AL, 2010. pp. 12.

[5] R. E. Weibel and R. J. Hansman, "Safety Considerations for Operation of Different Classes of UAVs in the NAS," AIAA paper 2004-6244. *Proceedings of the Aviation Technology, Integration and Operation (ATIO) Forum*, Chicago, IL, September 2004.

[6] R. E. Weibel and R. J. Hansman, "An Integrated Approach to Evaluating Risk Mitigation Measures for UAV Operational Concepts in the NAS," AIAA paper 2005-6957. *Proceedings of InfotechAerospace Conference*. Arlington, VA, September, 2005.

[7] P. Misra and P. Enge, *Global Positioning System, Signals, Measurements, and Performance*, Ganga-Jamuna Press, Lincoln, MA, 2001.

[8] B. DeCleene, "Defining Pseudorange Integrity - Overbounding," *Proceedings of the Institute of Navigation's ION-GPS 2000*, Salt Lake City, UT, September 2000. pp. 1916-1924.

[9] S. Pullen, "Providing Integrity for Satellite Navigation: Lessons Learned (Thus Far) from the Financial Collapse of 2008-2009," *Proceedings of the 22nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2009)*, Savannah, GA, September 2009. pp. 1305-1316.

[10] Cosmen-Schortmann, J., Azaola-Saenz, M., Martinez-Olague, M.A., Toledo-Lopez, M., "Integrity in Urban and Road Environments and its use in Liability Critical Applications," *Proceedings of IEEE/ION PLANS 2008*, Monterey, CA, May 2008. pp. 972-983.

[11] Z. Xing and D. Gebre-Egziabher, "Modeling and Bounding Low Cost Inertial Sensor Errors," *Proceedings of IEEE/ION PLANS 2008*, Monterey, CA, May 2008. pp. 1122-1132.

[12] Z. Xing and D. Gebre-Egziabher, "Comparing Non-Linear Filters for Aided Inertial Navigators, "*Proceedings of the 2009 International Technical Meeting of The Institute of Navigation*, Anaheim, CA, January 26 - 28, 2009. pp. 1048 - 1053.

[13] Z. Xing, "Over-bounding Integrated INS/GNSS Output Errors," Ph.D. Dissertation, Department of Aerospace Engineering & Mechanics, University of Minnesota, Minneapolis, MN, October 2010.

[14] D. Gebre-Egziabher, M. Petovello and D. Bevly, "Integration of GNSS and INS," Chapter 6 (Part 1) and Chapter 7 (Part 2) in *GNSS Applicaitons and Methods*, Ed: Gleason and Gebre-Egziabher. Artech House Publisher, Boston, MA, 2009. pp. 149 – 190.

[15] P. D. Groves, "INS/GNSS Integration," *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*, Artech House, Boston, MA, 2008. pp. 363 - 406.

[16] D. Gebre-Egziabher, C. O. L. Boyce, J. D. Powell and P. K. Enge, "An Inexpensive DME-Aided Dead Reckoning Navigator," *Navigation*. Vol. 50, No. 4, 2004. pp. 247 - 263.

[17] H. Buell and L. Oleinik, "The AN/ASN-128B, An Integrated Doppler/GPS Navigation System for Helicopters," *Proceedings of the 54th Annual Meeting of the Institute of Navigation*, Denver, CO, June 1998. pp. 395-406.

[18] J. A. Farrell, *Aided Navigation: GPS with High Rate Sensors*, McGraw-Hill, New York, NY, 2008.

[19] J. Rife, S. Pullen, B. Pervan and P. Enge, "Paired Overbounding and Application to GPS Augmentation," *IEEE Position, Location and Navigation symposium 2004*, Monterey, CA, April 2004. pp. 439-446.

[20] S. Gleasson and D. Gebre-Egziabher, "GNSS Navigation: Estimating Position, Velocity, and Time," Chapter 3 in *GNSS Applicaitons and Methods*, Ed: Gleason and Gebre-Egziabher. Artech House Publisher, Boston, MA, 2009. pp. 55 – 86.

[21] R. Kornfeld, R. J. Hansman, R. J and J. Deyst, "Single Antenna GPS-Based Aircraft Attitude Determination," *Navigation: Journal of the Institute of Navigation*, Vol. 45, No. 1, 1998. pp. 51 – 60.

[22] R. Kornfeld, R. J. Hansman, J. Deyst, K. Amonlirdviman and E. Walker, "Applications of GPS Velocity Based Attitude Information," *AIAA Journal of Guidance, Control, and Dynamics*, Vol. 24, No. 5, 2001. pp. 998 – 1008.

[23] D. Gebre-Egziabher, and G. H. Elkaim, "MAV Attitude Determination by Vector Matching," *IEEE Transactions on Aerospace Electronic Systems*. Vol. 44, No. 3, 2008. pp. 1012- 1028.

[24] D. Gebre-Egziabher, R. C. Hayward and J. D. Powell, "Design of Multi-Sensor Attitude Determination Systems," *IEEE Transactions on Aerospace Electronic Systems*, Vol. 40, No. 2, 2004. pp. 627 -649.