DOT/FAA/TC-17/59

Federal Aviation Administration
William J. Hughes Technical Center
Aviation Research Division
Atlantic City International Airport
New Jersey 08405

Initial Investigations Into Alternate Certification Approaches Using Run-Time Assurance for Small Aircraft Autopilots

February 2019

Final Report

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof. The U.S. Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report. The findings and conclusions in this report are those of the author(s) and do not necessarily represent the views of the funding agency. This document does not constitute FAA policy. Consult the FAA sponsoring organization listed on the Technical Documentation page as to its use.

This report is available at the Federal Aviation Administration William J. Hughes Technical Center's Full-Text Technical Reports page: actlibrary.tc.faa.gov in Adobe Acrobat portable document format (PDF).

Technical Report Documentation Page

1. Report No. DOT/FAA/TC-17/59	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle INITIAL INVESTIGATIONS INTO ALTERNATE CERTIFICATION APPROACHES USING RUN-TIME ASSURANCE FOR SMALL AIRCRAFT AUTOPILOTS	5. Report Date February 2019 6. Performing Organization Code
7. Author(s) Mark A. Skoog, Loyd R. Hook IV	8. Performing Organization Report No.
9. Performing Organization Name and Address National Aeronautics and Space Administration Armstrong Flight Research Center Mailstop 4830C 4800 Lilly Dr. Edwards, CA 93523-0273	10. Work Unit No. (TRAIS) 11. Contract or Grant No.
12. Sponsoring Agency Name and Address Dave Sizoo FAA Central Regional Office 901 Locust St Kansas City, MO 64106	13. Type of Report and Period Covered Final Report 14. Sponsoring Agency Code AIR-714

15. Supplementary Notes

The FAA William J. Hughes Technical Center Aviation Research Division COR was Robert McGuire.

16. Abstract

This report details initial theoretical and experimental development of this concept, which is called run-time assurance or RTA, on a small aircraft autopilot. It begins with a more detailed look at the motivations for this work and the background of the aircraft and system certification process. The report continues by introducing an architecture based on RTA called Outer Loop Integrity Verifier (OLIV), which is meant to allow application of the RTA concept to small aircraft autopilots. Initial experimentation with OLIV on a small unmanned aircraft vehicle (UAV) testbed produced important lessons learned, which are also provided. Finally, two case studies, which delve deeper into the details of developing the OLIV architecture, are included. The first factors in pilot reaction time when determining the boundary of safe and recoverable operation of the autopilot, and the second explores practical considerations for testing an RTA system on a general aviation aircraft.

17. Key Words Run-time assurance, Small aircraft, Envelope protection, Auto-pilot	18. Distribution Statement This document is available to the U.S. public through the National Technical Information Service (NTIS), Springfield, Virginia 22161. This document is also available from the Federal Aviation Administration William J. Hughes Technical Center at actlibrary.tc.faa.gov.

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 38	22. Price

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AAG	Adaptive Aerospace Group
AC	Advisory Circular
ADAHRS	Air Data Attitude and Heading Reference System
AFRL	Air Force Research Laboratory
AIM	Autopilot integrity monitor
Auto FLS	Automatic forced landing system(s)
Auto GCAS	Ground collision avoidance system(s)
BAI	Barron Associates Incorporated
CFIT	Controlled flight into terrain
CFR	Code of Federal Regulations
GA	General aviation
GPS	Global Positioning System
IFR	Instrument flight rules
LaRC	NASA Langley Research Center
LOC	Loss of control
OLIV	Outer loop integrity verifier
PFD	Primary Flight Display
RTA	Run-time assurance

EXECUTIVE SUMMARY

Over the past decade, the FAA has recognized that the emphasis for airplane-certification standards has shifted away from small aircraft in favor of larger aircraft. This has led to much higher costs for new small airplanes, especially general aviation (GA) airplanes, and an overall reduction in the number of new models available. The effect of this trend is that the average age of GA airplanes is nearly 40 years, and to a large degree, new technologies have not been adopted into these older aircraft. These facts have led the FAA and the small-aircraft community to seek alternate methods of certification to reverse these trends.

The certification process has successfully produced extremely reliable systems for many decades. In fact, software systems, which add relatively heavy certification requirements to aircraft, have been found to be a factor in an exceedingly small number of airplane accidents. However, reliability is not the same as safety, especially for GA airplanes. Safety statistics show that one is 11 times more likely to be killed while traveling in a GA airplane than when making the same trip in an automobile, or more than 1100 times more likely to be killed in a GA airplane than when making the trip in a commercial aircraft. This is true despite the fact that there are aircraft safety systems that could provide a dramatic positive effect on these statistics. Even relatively simple wing-leveler autopilots retrofit onto older aircraft may decrease loss of control (LOC) accidents, the most frequent cause of GA mishaps, by as much as 50%. Other safety systems, such as automatic ground collision avoidance systems, LOC avoidance systems, and automatic forced-landing systems, could prevent accidents at an even larger rate. However, these systems require an autopilot to actuate their safety decisions.

For these reasons, the FAA began working with NASA to develop alternate certification strategies for autopilots and automatic safety systems. This collaboration led to the development of concepts to reduce the certification burden and potentially provide the means to make these systems available in GA aircraft at a fraction of the current cost. One particular concept that has gained significant traction addresses the longstanding certification requirement of exhaustively verifying a flight-critical system, such as an autopilot, prior to fielding. This new concept allows for assurance of safety at run time and therefore allows for a potential system failure but puts other systems and procedures in place so the overall effect of the failure allows the continued safe flight and landing of the airplane. Although this change may seem small, if developed correctly, it could have a dramatic impact on the cost and availability of new technologies on small aircraft, leading to an important increase in overall safety.

This report details initial theoretical and experimental development of this concept, which is called run-time assurance (RTA), on a small aircraft autopilot. It begins with a more detailed look at the motivations for this work and the background of the aircraft and system certification process. The report continues by introducing outer loop integrity verifier (OLIV), an architecture based on RTA that is meant to allow application of the RTA concept to small aircraft autopilots. Initial experimentation with OLIV on a small unmanned aerial vehicle (UAV) test bed produced important lessons, which are also provided. Two case studies, which delve deeper into the details of developing the OLIV architecture, are also included: the first factors in pilot reaction time when determining the boundary of safe and recoverable operation of the autopilot, and the second explores practical considerations for testing an RTA system on a GA aircraft.

1. INTRODUCTION

The FAA has been interested in alternate certification strategies for small airplanes for several years. It recognizes that new technologies are available that could significantly increase safety. However, many of these technologies are not implemented or certified due to several barriers, including the certification burden of regulations intended for larger aircraft with a higher expectation for safety. The Small Aircraft Revitalization Act (SARA) of 2013 provides a framework to consider new certification options. Of primary importance is reducing the certification burden for systems which will improve overall aircraft safety, which is consistent with the core purpose of the certification process.

The most frequent causes of fatal accidents affecting small aircraft are loss of control (LOC), controlled flight into terrain (CFIT), and component failure involving the power plant (General Aviation Joint Steering Committee [GAJSC] Loss of Control Work Group, 2012) [1]. Of particular interest is LOC, which accounts for more than 40% of the total fatal accidents. In many instances, LOC and CFIT statistics (because of spatial disorientation or pilot distraction) could be significantly improved with the addition of very simple autopilots, such as a wing leveler. There are other automatic aircraft systems that would improve accident rates in many other categories. For instance, an automatic LOC prevention and recovery system could have a dramatic impact on the safety of small aircraft. This would also be true for an automatic ground collision avoidance system (Auto GCAS) or an automatic forced landing system (Auto FLS). These technologies would all require an integrated autopilot to provide decision actuation to achieve the safety enhancements. These facts have led researchers and regulators to conclude that inclusion of an integrated autopilot into small aircraft would provide or facilitate a significant increase in safety for this type of airplane. However, the majority of small airplanes do not have autopilots. This is due to, in large part, the average age (nearly 40 years) of small airplanes, and the cost and certification challenges of developing autopilots for these older airplanes.

In response to this reality, the FAA is partnering with NASA, the University of Tulsa, and Air Force Research Laboratory (AFRL) to develop strategies to ease the certification burden for small aircraft autopilots and to lower the cost for their inclusion in both existing aircraft and newer, lower-cost aircraft. One particular strategy for accomplishing this is to transfer the authority and certification burden to a simpler, standardized system that would monitor an autopilot during operation and assure that it could not direct unintended or unsafe actions. This autopilot assurance system would observe both the input plane (aircraft state sensor inputs) and output plane (control commands) of the autopilot to determine if the aircraft is being directed into an unsafe or unrecoverable region of its state space. If this is the case, the assurance system would disable the autopilot and return full control to the pilot in command in a manner that mitigates LOC during the transition (See figure 1). At this early stage, run-assurance requires three components to be successful: a) having independent and partitioned monitors, b) having architecture that allows switching, and c) having a safe "plan b", whether it is the pilot, another system, or a parachute. Therefore, confidence in this method of alternate certification is high, but there remains a lot of work to be done before certification authorities have the data required to make decisions based on this alternate method of certification.

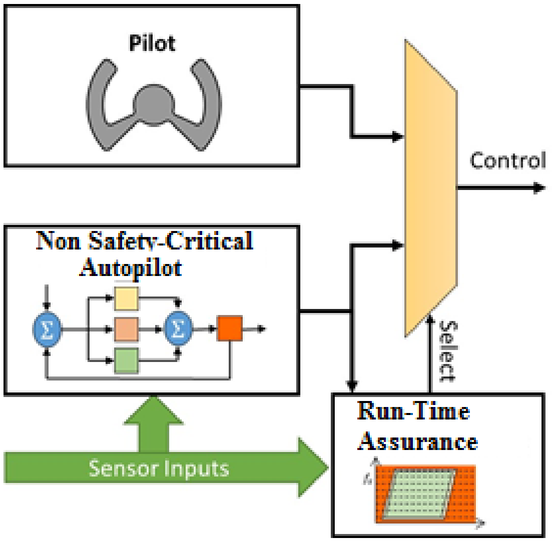


Figure 1. Autopilot monitor and control switch strategy which may relieve certification burden for an autopilot

1.1 MOTIVATIONS

1.1.1 Small Aircraft Safety Statistics

The heart of the issue SARA and the FAA are trying to address is the relatively poor safety record of general aviation (GA) travel compared to other common forms of transportation. In the 10-year period from 2001–2010, the average number of GA accidents was more than 1600 per year, with more than 300 of those causing at least one fatality [2] [2] (National Transportation Safety Board, 2013). There were more than 550 fatalities per year on average, or more than 1.5 fatalities per day. When adjusted for the number of GA flight hours during these years, and assuming a conservative average velocity of 100 mph and average occupancy of two persons per vehicle, the fatality rate per personal mile traveled was more than 11.6 fatalities per 100 million personal miles traveled (see figure 2). When comparing this rate to other common forms of transportation, the data reveal that GA pilots and occupants are more than 11 times more likely to be killed per mile traveled than traveling by car. This number increases to more than 1100 times more likely when compared to commercial air. Only when compared against travel in motorcycles, known to be one of the most dangerous forms of transportation, does GA have an advantage in safety, and this advantage is only by a factor of 2.5 [3, 4]. Whereas motorcycles and GA airtravel are and will continue to be societally acceptable, the goal is continuous improvement, not zero risk.

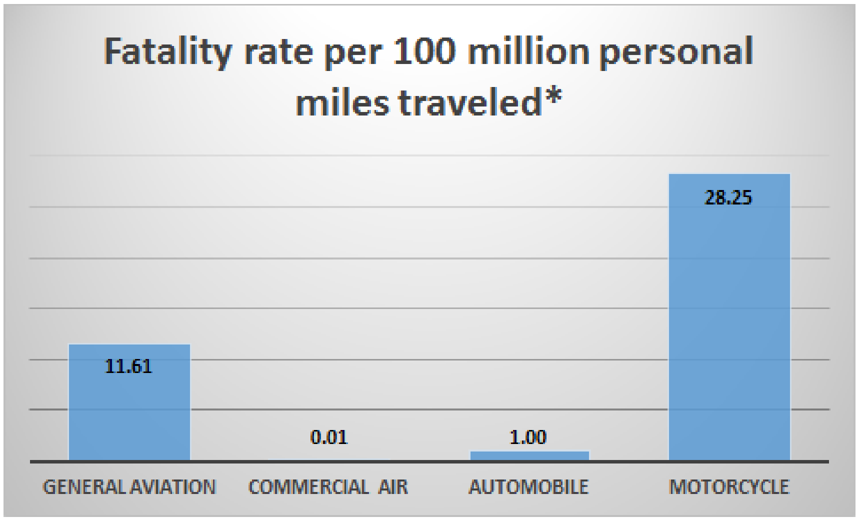


Figure 2. Comparing fatality rates in transportation categories per personal mile traveled [2,–4]

Of these fatal accidents, more than 60% can be attributed to three specific causes: LOC, CFIT, and component failure of the power plant [1]. Of these three major causes, LOC is the cause of more than 40% of the total fatal mishaps in GA (see figure 3). Therefore, targeting solutions to these three major causes, with special emphasis on LOC, would provide the largest contributions to increases in safety for GA aircraft.

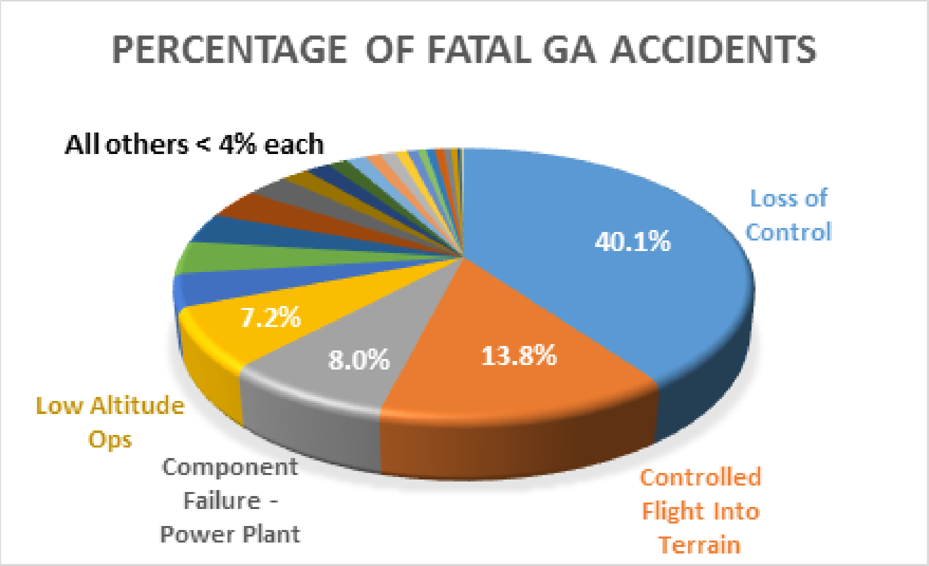


Figure 3. Categorization of fatal GA accidents from the GAJSC [1]

1.1.2 Effect of Autopilots on GA Safety

Fortunately, automated systems are currently available that can have a major impact on fatality statistics from these three major causes. Of immediate interest, LOC and CFIT accidents caused by poor situational awareness produced by environmental, geographical, or time-of-day factors could be significantly reduced by a simple altitude-hold/heading-hold autopilot system. This is stated more specifically by the FAA General Aviation Joint Steering Committee's (GAJSC) findings that "LOC accidents at night and in IMC would drop by 50 percent simply by installing autopilots in the more than 100,000 instrument flight rules (IFR) capable GA airplanes [1]." However, increases in safety produced by autopilot inclusion are not limited to this class of accident.

Other automated safety systems are available that would provide a significant increase in safety for other accident categories. For instance, Auto GCAS have been developed and are being deployed on United States Air Force (USAF) F-16s (see figure 4). These Auto GCAS may have the ability to reduce CFIT accidents by as much as 98% in military fighter aircraft [5]. Development of an Auto GCAS for GA aircraft is underway with the hope that similar reductions can be achieved. In addition, systems to automatically avoid or recover from LOC are being developed, which, when applied to the GA regime, would have a dramatic impact in safety for all types of LOC situations. Even power plant failure could be significantly reduced with the inclusion Auto FLS [6, 7]. These Auto FLS are currently under development for commercial and GA category aircraft.

Each of these automatic safety systems could dramatically influence the safety statistics of GA aircraft in the future, but they all rely on an integrated autopilot to actuate their automated decisions. Therefore, not only would the inclusion of a low-cost autopilot in a large number of GA aircraft immediately provide substantial increases in safety and decreases in fatal accident rates, but it would also allow for more advanced automatic systems to be integrated providing further safety enhancement.

Figure 4. USAF F-16 with integrated Auto GCAS

Because a failure in an autopilot could lead to catastrophic consequences for an aircraft, the hardware and software used to implement the autopilot must be certified to the highest standard. This means several strict requirements for the development, verification, and validation of these components. In addition, because most older aircraft were designed and certified without autopilots, the parts of the aircraft that could be touched by the autopilot installation would need to be recertified. These factors have led to an absence of low-cost autopilots on a majority of older aircraft. This is important when one considers that the average age of the GA fleet is nearly 40 years and increases every year [8].

Available autopilots are relatively expensive to purchase, install, and certify. For example, a simple two-axis, rate-based autopilot (which was state of the art 15 years ago) costs $20,000–$25,000 to install on a Cessna C-182. This high cost means that sometimes the hull value of the aircraft is less than the installed autopilot. Modern attitude-based autopilots are even more expensive and harder to justify on older retrofit aircraft.

1.2 BACKGROUND

1.2.1 Current Certification Approaches

Title 14 of the Code of Federal Regulations (CFR) defines rules governing all aviation activities in the United States. In particular, the FAA regulates aircraft through Chapter 1, Subchapter C (Parts 21-49) of the Title 14 CFR. Specifically relevant to this report, aircraft airworthiness standards relating to the normal, utility, acrobatic, and commuter categories of airplanes are contained in Title 14 CFR Part 23. Part 23 aircraft are less than 19,000 lb and have fewer than 19 passenger seats. The normal, acrobatic, and utility categories, which encompass the large majority of the GA fleet, are required to be less than 12,500 lb with no more than nine passenger seats. Advisory Circulars (ACs) are also published by the FAA to provide guidance for compliance of the CFRs and often overlap between each other. AC 23.1309-1E is particularly relevant and provides guidance suggesting the use of RTCA DO-178C and DO-254A as acceptable methods of compliance when developing software/hardware systems.

DO-178 [9] is the primary means to satisfy FAA airworthiness requirements for software to be used in airborne systems. It provides a description of what the FAA sees as high-integrity processes that will produce software that provides its desired function [10]. As a part of this process, verification and validation of the software must assure the system is correct for a multitude of system inputs. For flight-critical systems, such as an autopilot, rather exhaustive modified condition/decision coverage testing coverage is required [11]. Although this requirement and many others have been largely successful at producing reliable flight-critical systems, they significantly affect the amount of effort expended to verify software correctness and add to the final cost of the system. Work by Goldberg and Horvath [12] cites up to 50% of avionics software budgets going to validation and verification. Such expenditures have traditionally been necessary for avionics technology to be certified. However, work is underway in the FAA to update certification methodologies to accommodate alternative certification strategies [13].

1.2.2 Alternate Assurance Approaches

The difference between reliability and safety has been recognized by the FAA and has led to efforts to foster alternative methods of certification aside from DO-178. One method to reduce the testing and certification burden is to verify the flight critical code at run-time instead of exhaustively verifying prior to run-time. This method is called run-time assurance (RTA). In general, an RTA framework has at least three different major components: an advanced controller, a recovery controller, and a monitor and switch.

The “advanced” controller is a controller with additional or improved functionality as compared to the baseline controller. The “recovery” controller, however, must be reliable to the point that its correct operation can be assumed in a pre-defined region of the aircraft state space. The “monitor and switch” is meant to operate by monitoring the aircraft or system state for potential safety risks and switch control of the system to the recovery controller if pre-defined bounds are broken. The concept provides the ability to remove the burden of safety from the advanced controller and certify it to a less-than-flight-critical level. A more thorough treatment of RTA will be found in the next section.

2. RTA

2.1 GENERAL

RTA can be defined as a structured argument supported by evidence, justifying that a system is acceptably safe and secure, not through reliance on offline tests or verification methods but through reliance on real-time monitoring, prediction, and failsafe recovery mechanisms [14]. As illustrated in figure 5, an RTA system used for alternate certification consists of at least three components: the untrusted (or lesser certified) component, a run-time monitor or flight executive, and one or more recovery systems. The untrusted component contains functional subcomponents, which may not be sufficiently reliable or verified according to current development or certification standards. There may be multiple reasons for having such components in a system. Under normal conditions, they can provide improved performance or operational efficiency for the system or enhance the user experience. In the case of a GA aircraft, a low-cost autopilot could be considered the untrusted component. The core idea in RTA that enables the use of such components in a system is the presence of a safe fallback mechanism that 1) reliably detects potential problems (the monitor or flight executive), and 2) invokes a recovery mechanism that can ensure safe operation of the system, possibly with reduced capabilities and performance. It is assumed that the RTA monitor and recovery systems are certified at the highest criticality level required for the total system to operate. For example, consider an RTA-protected subsystem with a potential failure mode that has been determined to be highest risk, endangering human life or significant cost. This risk level would translate to the highest criticality level (referred to as Level A critical for civil aviation). For the RTA protected system, the corresponding processes, design approaches, and verification methods prescribed for Level A critical software and hardware must apply to the run-time monitor, switch, and recovery system.

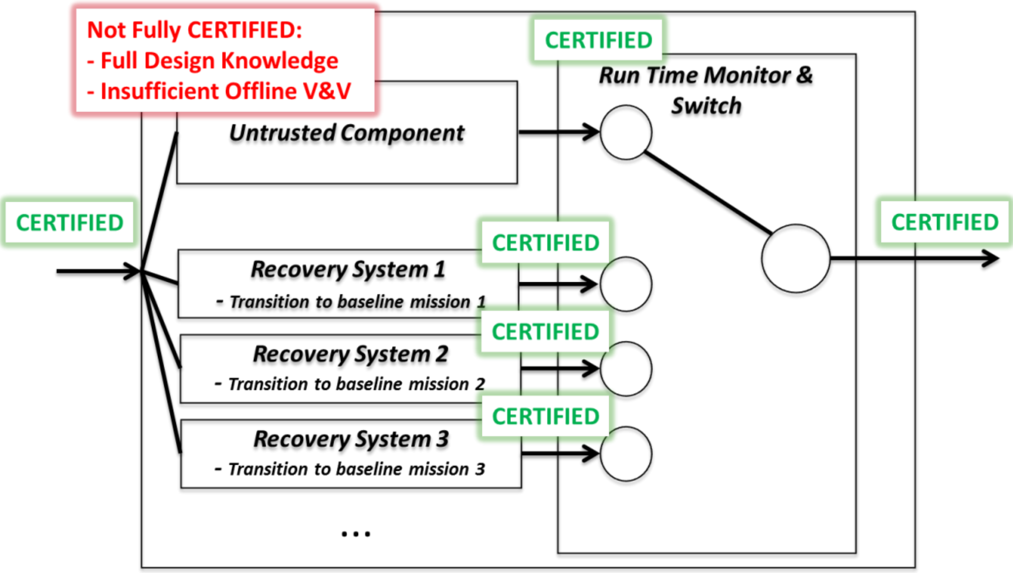


Figure 5. Generic run-time assurance architecture

The key advantage to a RTA approach is that lower cost autopilot systems can be employed without expensive certification, allowing only the behaviors that are protected by certified monitors and recovery systems. On the surface, allowing a system to function without exhaustive testing or analysis may seem concerning. However, that assumes current software systems are exhaustively tested and are without errors or defects, which is not the case. Rather, software is run through a series of quality steps, checklists, and verification practices that increase the implicit confidence of that code. It is our claim that the functional capability that has been tested, examined, and proven safe in a particular context can be argued as safe even if the underlying software has not been created using a design-assurance process. Within this paradigm, a design approach called assume-guarantee reasoning might provide the offline design considerations and formalisms necessary for articulating the allowable and certifiable behaviors of an advanced system by constraining behaviors to only what is safe or recoverable.

In 2013, AFRL started a Phase III Small Business project with Barron Associates Incorporated (BAI) to develop a RTA framework for untrusted flight-critical software within any control layer from mission planning to trajectory planning to inner loop control. The following are some design considerations that were noted within the program that may be applicable to a RTA-based certification paradigm for a low-cost GA autopilot system:

- The controller need not be a total black box. The complete certification case is better suited with at least some evidence the controller is capable within a portion of the flight envelope under specific assumed operating conditions (i.e., assuming the GA autopilot is being fed reliable inertial and guidance inputs). Under these defined assumptions, the autopilot must be designed with an RTA mechanism in mind, or the autopilot code must be instrumented to provide insight into the reasoning behind the calculations being made in real time.

- The RTA framework can be implemented using multiple recovery or failsafe mechanisms, which cover different areas of the operating envelope. Previous research limited the recovery controller to just one region of attraction (ROA) or region of recovery (ROR). This constraint made it difficult to justify a performance gain out of the advanced controller (or non-safety critical autopilot) since the performance was limited to one recovery system that was fully certified using conventional standards. A better approach would be to allow the untrusted code to operate under specific, tested conditions only if specific recovery mechanisms were in place to take over if the autopilot failed.
- For the GA aircraft, if the autopilot fails during operation, the predominant recovery controller may be the pilot. However, much care has to be taken to ensure that either the pilot is capable of recovering the aircraft at the point of autopilot failure or that alternate means of recovery are in place, such as a deployable parachute system.
- Each recovery region must have defined zones or safety regions that ensure proper timing for switching and recovery. BAI has defined these zones based on aircraft capability, ensuring that within the given time interval, the flight executive or RTA monitor has enough time to engage a recovery controller before the next time interval.

2.2 GA AUTOPILOTS AND OUTER LOOP INTEGRITY VERIFIER

The simplest near-term implementation of an RTA system that could provide benefit for GA aircraft would be a commercial off-the-shelf-type non-safety-critical autopilot monitored by a configurable and certified RTA system. The “recovery” controller (See figure 5) for this implementation would be the human pilot in command, who is always allowed to control the aircraft as a result of the pilot-training process. So, in essence, the human pilot would be the certified backup to the uncertified autopilot. For the remainder of this paper, this setup is referred to as the outer loop integrity verifier (OLIV). OLIV contains the three usual pieces of a RTA system in a form that has been described and can also be seen as a “Non-Critical Autopilot-Run-time Assured-with Manual Pilot Recovery” System (NCA-RTA-MPR). The concept for OLIV is shown in figure 6.

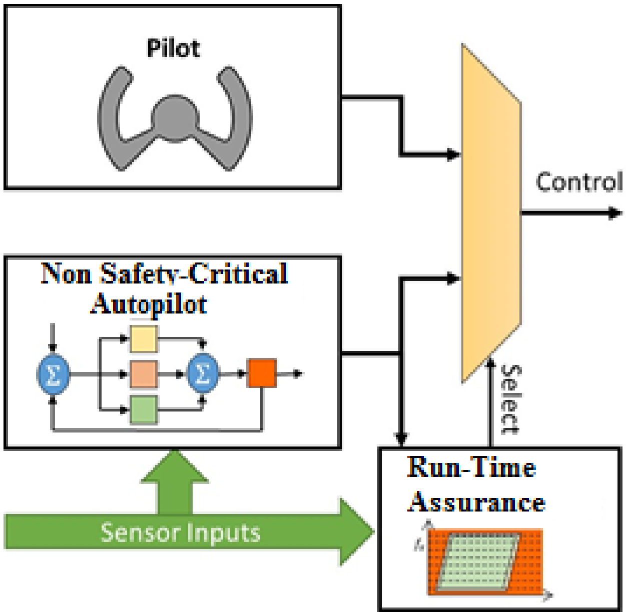


Figure 6. OLIV concept for GA aircraft (non-critical autopilot—run-time assured—with manual pilot recovery)

2.2.1 OLIV Preliminary Experimentation

As a part of this work, experimentation and implementation of the OLIV concept has started to be applied at the NASA Armstrong Flight Research Center. Initial testing on small unmanned aircraft has already provided limited but successful results and proved the feasibility of testing both in simulation and in flight on a small scale (see figure 7). For these initial tests, a small unmanned aerial vehicle (UAV) autopilot was given intentionally unreliable position data. When the data source predictably failed, the vehicle would be sent into an out-of-control situation. An RTA monitor was established that looked at the change in this position data from frame to frame. When the monitor tripped pre-set values (limits), which indicated it was likely that the position solution was invalid, control was immediately switched from autopilot control to a backup controller (in this case, the human pilot).

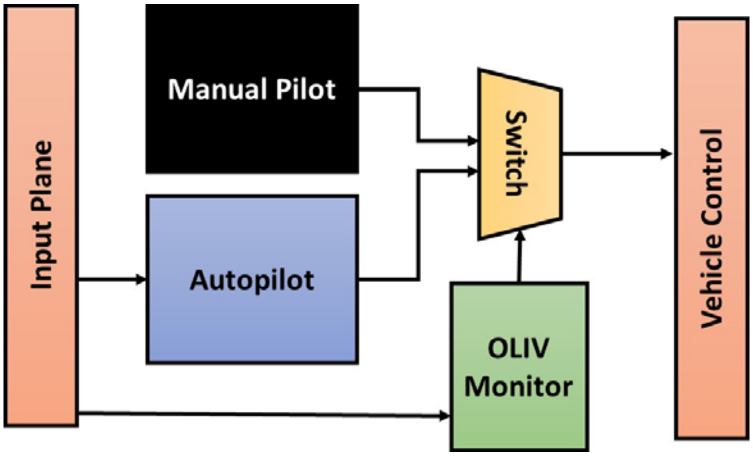


Figure 7. Functional block diagram for preliminary OLIV system

This limited example provided invaluable experience into the implementation of such a system. For example, the need for comprehensive instrumentation of the RTA monitor for flight testing was found to be critical to understanding the behavior of the system. For instance, because of the nature of the position data source, the RTA monitor was tripped multiple times during each flight test. Having RTA switch from autopilot to pilot was such a regular event from a pilot perspective that determining who was controlling the aircraft was at times ambiguous. Interestingly, this unexpected result was also seen in the USAF Auto GCAS flight testing because the pilots thought they flew the recovery maneuver only to find out during post-flight analysis that the Auto GCAS system actually initiated and flew the maneuver slightly before the pilot [6]. After experimentation with delaying the pilot alert of RTA switching, it was found that prompt and aggressive indications should be added to rapidly alert the pilot that he was being transferred control. Each of these findings indicate the importance of the development effort that must be applied to the pilot vehicle interface for this type of system.

Because of the limited safety risk of testing these small-scale UAVs in highly controlled environments, making the safety case for their testing was rather straightforward. However, testing of the OLIV system on larger scale UAVs and manned GA aircraft is planned beginning in late 2015 continuing through 2016. On these test platforms, the safety assurance case will be a critical factor in determination of flight safety and the ability to perform the requisite testing. It is hoped the results of this testing will be twofold: 1) the design and implementation of the system itself, and 2) the process required to convince experimental airworthiness certification authorities at NASA and the FAA of the safety of the system and aircraft. The results of both should provide much-needed direction to the NASA/USAF/FAA group and the community at large.

2.3 ASSURANCE CASE

We agree that the most important component of an RTA-based certification approach may be the assurance case (or safety case). Fundamentally, the overarching RTA claim is that a subsystem does not provide enough evidence to achieve the level of confidence required for the predetermined level of risk, but in combination with a higher confidence-monitoring and recovery system, the entire system provides sufficient evidence to achieve the level of confidence required for the predetermined risk. Our goal is to provide an NCA-RTA-MPR system that will not reduce the confidence in existing GA aircraft and will lay the framework for future safety and recovery systems that rely on autopilot. The goal of these future systems is to increase confidence in future GA, providing evidence to support the claim that aircraft will have a higher confidence of safety with the existence of these systems.

However, this approach in many ways does not align with existing design and verification processes as prescribed in documents such as the SAE DO-178C standard. It is assumed that the standard processes will be followed, when feasible, to achieve a sufficient level of confidence in an OLIV system. However, it is understood that the underlying assurance argument that governs such processes is implicit. Therefore, if any deviation to the existing standards is proposed, much care must be taken in constructing a new explicit argument and evidence to achieve the level of confidence desired. To further illustrate this point, the following examples would need to be constructed to articulate the explicit high-level arguments, sub-arguments, and required evidence that might support an OLIV assurance case. A complete and thorough assurance case is better suited for follow-on research and engineering efforts and is out of scope for this report; however, the following is offered for example purposes:

Argument 1. The pilot in command is responsible for the safety of the aircraft, including separation from other aircraft, ground avoidance, air traffic control (ATC) compliance, weather avoidance, controllability, and GA “rules of the road.”

Required evidence:

- The pilot in command has been trained to be responsible for these safety factors and is “certified” to command the aircraft.

Argument 2. The autopilot will be able to be used only under the authority of the pilot-in-command.

Sub-argument a. The autopilot can be engaged only by the pilot in command.

Sub-argument b. The autopilot can be disengaged at any time by the pilot in command.

Required evidence:

- The RTA system must be assured through appropriate safety-critical certification activities to enable autopilot control only through the input of the pilot in command and to allow disengagement at any time by the pilot in command.

Argument 3. The autopilot will not be allowed to operate in an unsafe or uncontrollable region of its flight envelope.

Sub-argument a. If the aircraft is within the unsafe portion of its flight envelope and under manual control of the pilot in command, the autopilot will not be allowed to be enabled.

Sub-argument b. If, while under autopilot control, the aircraft enters into the unsafe or uncontrollable region (whether due to aircraft failure, environmental anomaly, or other emergency or unknown reason), the autopilot will be disengaged.

Required evidence:

- The RTA system must be assured through appropriate certification activities to be able to monitor aircraft state and disengage the autopilot if the state falls outside the safe region.
- The aircraft must be assured to be safe and controllable within a pre-defined region of operation. Any state space outside this safe region is considered unsafe for these purposes.

Argument 4. The autopilot will not be allowed to cause LOC or entry into an unsafe or uncontrollable region of the aircraft operating space.

Sub-argument a. If the aircraft is tending toward the unsafe region of operation, the RTA system will disengage the autopilot in a timely manner to allow for the pilot in command to accomplish an appropriate recovery action, such that the aircraft never enters into the unsafe region of operation.

Required evidence:

- The RTA system must be assured through appropriate certification activities to be able to monitor aircraft state and disengage the autopilot in time to allow for appropriate recovery actions to be performed by the pilot.

- The pilot must be qualified and have the time needed to react and respond to the condition causing disengagement of the autopilot to keep the aircraft in the safe and controllable region of its operation space.

More information and background on the construction and usage of assurance and safety cases can be found in Reinhart, et al [15].

3. CASE STUDIES

3.1 ROLL AXIS AUTOPILOT

The following case study was performed by the University of Tulsa to uncover design considerations for an OLIV system using a simplified example. The approach is based on a rich history of work in run-time assurance, safety kernels, and hybrid systems reachability [16–22]. Work accomplished during this case study uncovered four basic objectives that should be included when considering the design of any system of this type:

1. Build the safety requirements for the OLIV system.
2. Develop and understand the model for the vehicle state dynamics.
3. Provide verifiable boundaries for safe and recoverable regions of the vehicle state space, either analytically, numerically, or through simulation.
4. Implement logic to enforce control decisions using robust and certifiable means and methods.

The remainder of this section follows the sequence of these objectives for an example air vehicle containing an autopilot that can only control angular motion around the *x*-axis (i.e., roll). Furthermore, in this example case, the vehicle's roll dynamics are neither affected by nor affect the other degrees of freedom of the vehicle. The roll autopilot has full control authority and controls the roll through an input that is defined as the set of inputs that impose a roll moment on the vehicle producing a roll acceleration $\ddot{\phi} \in [-90, 90]\ deg/s^2$ in the absence of any other moments. This roll control is directly related to the acceleration value, abstracting away the actual interfaces of the controllers with the airframe.

The simplified state space for this vehicle is

$$x = \begin{bmatrix} \phi \\ p \end{bmatrix}, \tag{1}$$

where ϕ is the bank angle and p is the roll rate. The dynamics of this roll state are:

$$\dot{x} = \begin{bmatrix} p \\ u + L_p{*}p \end{bmatrix}, \tag{2}$$

where $L_p = -2$ is the roll damping factor, $\dot{\phi} = p$, and:

$$\dot{p} = u + L_p{*}p = u - 2p \tag{3}$$

SAFETY REQUIREMENTS. The safety requirements for the system fall into two main categories defined by concepts of safety and recoverability. This example defines safety with the *Do No Harm Requirement* somewhat arbitrarily defined as: the OLIV shall not allow the controller to cause the bank angle ϕ to exceed 90 degrees in either direction.

Therefore, the safe region is only dependent ϕ and is defined as $\phi_{safe} \doteq [-90,\ 90]$ and the unsafe region $\phi_{unsafe} \doteq [-180,\ -90) \cup (90,180]$. To guarantee that we can fulfill our one safety requirement, we must monitor the vehicle state and allow operation of the autopilot only in a pre-defined region of the state space. However, there are regions of the state space that are labeled safe but will inevitably lead to an unsafe condition. This is because u is limited (in this case to between [-90, 90]), making it impossible to counteract the vehicle's roll rate before ϕ falls outside the safe region. An area of the safe region of the state space that makes such recovery impossible is labeled unrecoverable; the area within the safe region is labeled safe and recoverable. The job of the OLIV system is to allow operation of the autopilot only in the pre-defined safe and recoverable region.

MODEL. The definition of the safe region is straightforward, but the boundaries of the recoverable region require some explanation. The natural starting place is the definition of the roll dynamics:

$$\phi(t) = \int p(t)\,dt + \phi_0, \tag{4}$$

$$\dot{\phi}(t) = p(t) = \int u(t)\,dt + \int p(t)\,L_p dt + p_0, \tag{5}$$

where ϕ_0 and p_0 are the initial bank angle and roll rate, respectively. We can treat $u(t)$ as a constant expression u since we will be considering only piecewise constant control input signals (a decision that will become clear in a later section). Integrating the $\int u(t)dt$ term and substituting (4) into (5) for $\int p(t)dt$ results in the following linear ordinary differential equation:

$$\dot{\phi}(t) - L_p\phi(t) = ut - L_p\phi_0 + p_0, \tag{6}$$

Solving (6) for $\phi(t)$ gives equation (7):

$$\phi(t) = \phi_0 - k + k{*}e^{L_p t} + \frac{u}{-L_p}t\ , \tag{7}$$

where $k = \frac{u}{L_p^2} + \frac{p_o}{L_p}$.

To find an extreme value of $\phi(t)$ for a given constant control input u, set $\dot{\phi}(t^*) = 0$ and solve for the time, t^*. Then, find the value of $\phi(t^*)$, which is the extreme value:

$$\dot{\phi}\left(t^*\right) = \frac{u}{-L_p} + \left(\frac{u}{L_p} + p_0\right)e^{L_p t^*} = 0 \tag{8}$$

$$t^* = \frac{1}{L_p}\ln\left(\frac{u}{u + L_p p_0}\right) \tag{9}$$

Evaluating (7) for $t = t^*$ yields:

$$\phi^* \equiv \phi\left(t^*\right) = \phi_0 - \frac{p_0}{L_p} - \frac{u}{L_p{}^2}\ln\left(\frac{u}{u + L_p p_0}\right) \tag{10}$$

The extreme value of (7) is defined in terms of constants with no dependence on any time variable. When the current state of the vehicle $\begin{bmatrix}\phi_0\\ p_0\end{bmatrix}$ is such that $|\phi^*| \geq 90$, the RTA system must switch control away from the uncertified autopilot. All such points in the safe region make up the unrecoverable region of the state space. The applicability of equation (10) is subject to some minor interpretation. One can see that the system is not in danger of leaving the safe region when $sgn(\phi_0) \neq sgn(p_0)$, because such a roll rate will tend away from the boundary of the safe region and toward its interior. In such cases, equation (10) is not applicable. For compactness of notation in further discussion, let $\xi_p = sgn(p_0)$ and $\xi_\phi = sgn(\phi_0)$.

If we define a set Ω as the set of points in x that are on the boundary of the safe and recoverable region, such a set would be defined:

$$\Omega = \begin{cases} \phi_0 = 90\xi_p + \dfrac{p_0}{L_p} - \dfrac{u\xi_p}{L_p{}^2}\ln\left(\dfrac{u}{u - L_p\xi_p p_0}\right) & ,\xi_\phi = \xi_p \\ \phi_0 = 90\xi_p & ,otherwise \end{cases} . \tag{11}$$

SAFE AND RECOVERABLE REGIONS. Three recovery scenarios will illustrate the effects on the recoverable region based on three types of recovery that might be expected of a certified pilot when the RTA system switches control away from the autopilot: no recovery (zero control input), immediate optimal recovery (maximum corrective input), and optimal recovery after reaction time (maximum corrective input after some pre-defined delay).

Scenario 1 – No Recovery. In this scenario, the system is designed for the case in which it cannot depend on the certified pilot to supply any control input at all. The "recovery" control input will stay fixed at $u = 0$. This substitution, applied with values for system constants, simplifies equation (10) considerably:

$$\phi_{nr}^* = \phi_0 + \frac{p_0}{2}, \tag{12}$$

where ϕ_{nr}^{*} is the extreme value of ϕ (in this case as $t \rightarrow \infty$) with “no recovery.” This means the vehicle’s angular momentum will cause the bank angle to change by, at most, $\frac{p_0}{2}$ degrees. The simplification also applies to Ω:

$$\Omega_{nr} = \begin{cases} \phi_0 = 90\xi_p - \dfrac{p_0}{2} & ,\xi_\phi = \xi_p \\ \phi_0 = 90\xi_p & ,otherwise \end{cases} . \tag{13}$$

A graphical depiction of the safe and recoverable region appears in figure 8.

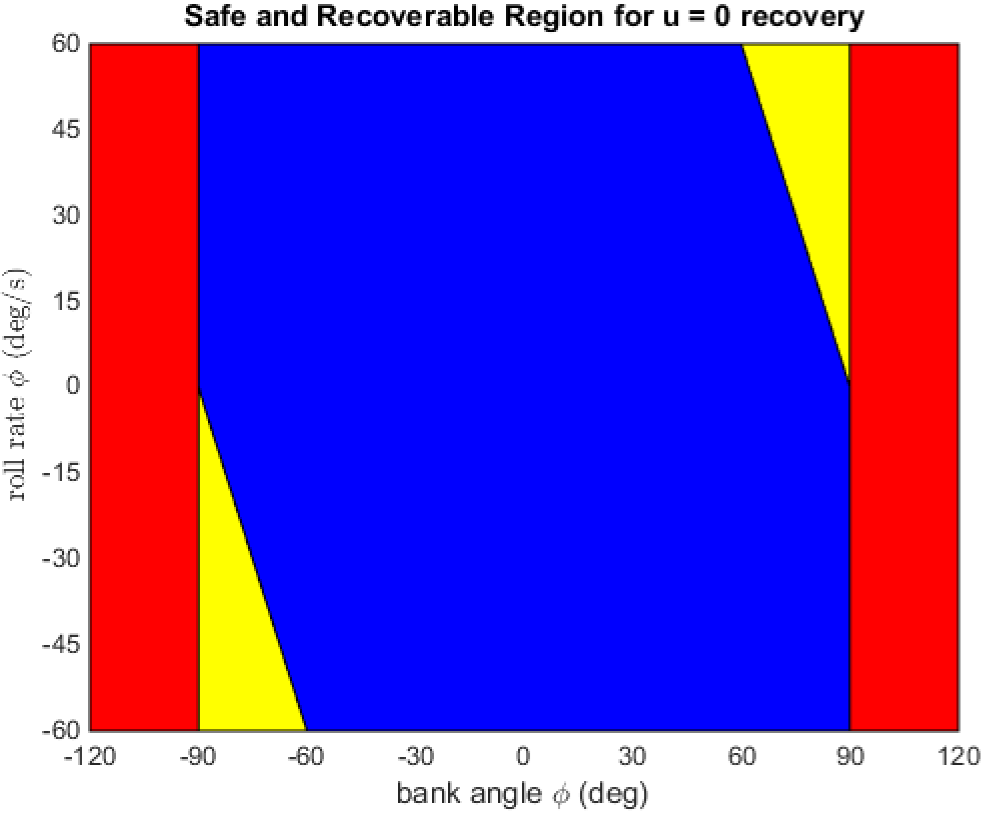


Figure 8. Safe and recoverable region for the “No Recovery” case; the triangular regions denote safe but unrecoverable regions, and the central, hexagonal region is safe and recoverable

Scenario 2 – Immediate Optimal Recovery. In this scenario, the system is designed for the case in which the certified pilot reliably supplies the optimal control recovery action immediately when needed. The control input for this recovery action will be the maximum magnitude input in the direction away from the boundary, applied at time $t = 0$ (RTA control switching time):

$$u_{ior} = \begin{cases} -90 & if\ \phi_0 \geq 0 \\ 90 & if\ \phi_0 \leq 0 \end{cases} \tag{14}$$

Equation (10) then becomes:

$$\phi^{*}_{ior} = \phi_0 + \frac{p_0}{2} - \frac{u_{ior}}{4}\ln\left(\frac{u_{ior}}{u_{ior}-2p_0}\right). \tag{15}$$

This yields the smallest possible unrecoverable region, as shown in equation (16) and figure 9:

$$\Omega_{ior} = \begin{cases} \phi_0 = 90\xi_p - \dfrac{p_0}{2} - 22.5\xi_p \ln\left(\dfrac{u}{u+2\xi_p p_0}\right) & ,\xi_\phi = \xi_p \\ \phi_0 = 90\xi_p & ,otherwise \end{cases} \tag{16}$$

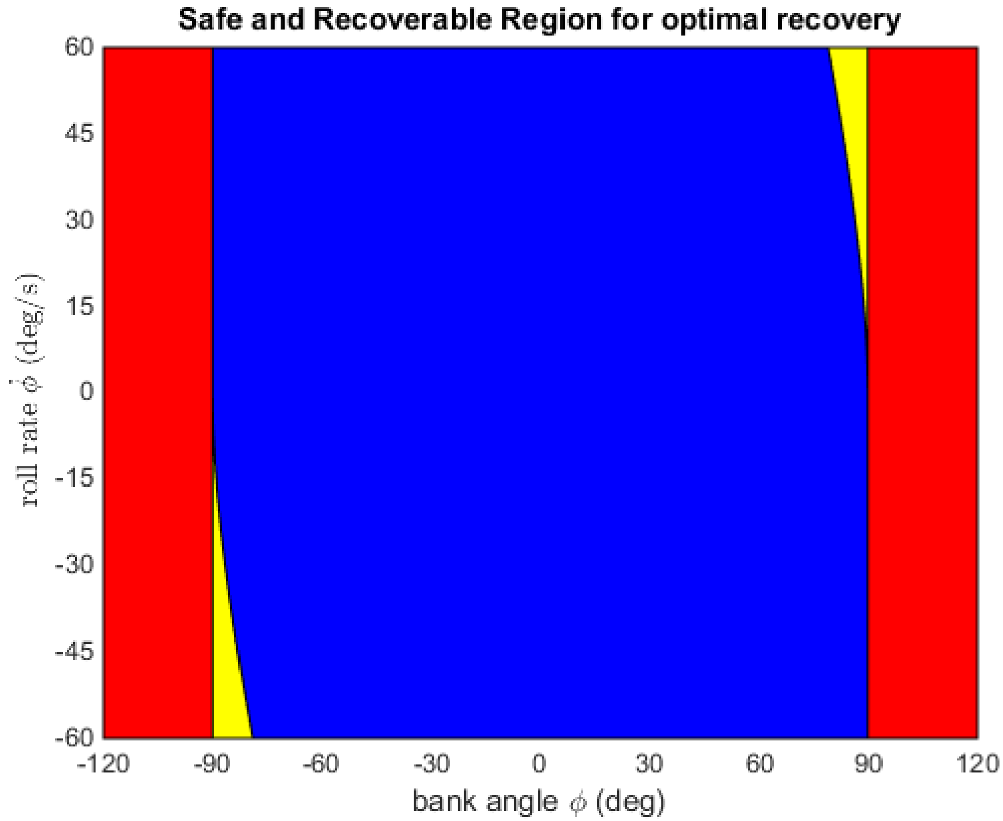


Figure 9. Safe and recoverable region for the "Immediate Optimal Recovery" case.; the darker, central region is safe and recoverable (Note the diminished size of the unrecoverable regions in contrast to the "No Recovery" case)

Scenario 3 – Optimal Recovery After Reaction Time. In this scenario, the system is designed for when the pilot performs the optimal control recovery action after a certain maximum time elapses for him or her to react to the situation. (In this case we will give a 0.5 second maximum reaction time for demonstration purposes.) The recovery control input is the same as equation (14), but it is not applied until time $t = t_r = 0.5$ (*i.e.*, t_r seconds after RTA control switching time).

The extreme value is now calculated in two stages: first, evaluate equation (7) and its derivative at $t = t_r$, then substitute the results for ϕ_0 and p_0, respectively, in equation (10).

$$\phi^*_{orart} = \phi_0 + \frac{p_0}{2} - \frac{u_{ior}}{4} \ln\left(\frac{u_{ior}}{u_{ior} - 2 p_0 e^{-2t_r}} \right) \tag{17}$$

The overall effect of adding a delay time is the inclusion of an exponential decay term based on the constant length of the delay. Substituting $t_r = 0.5$, the expression for Ω becomes:

$$\Omega_{orart} = \begin{cases} \phi_0 = 90\xi_p - \frac{p_0}{2} - 22.5\xi_p \ln\left(\frac{u}{u + 2\xi_p p_0 e^{-1}} \right) & , \xi_\phi = \xi_p \\ \phi_0 = 90\xi_p & , otherwise \end{cases} \tag{18}$$

A graphical depiction of the safe and recoverable region appears in figure 10.

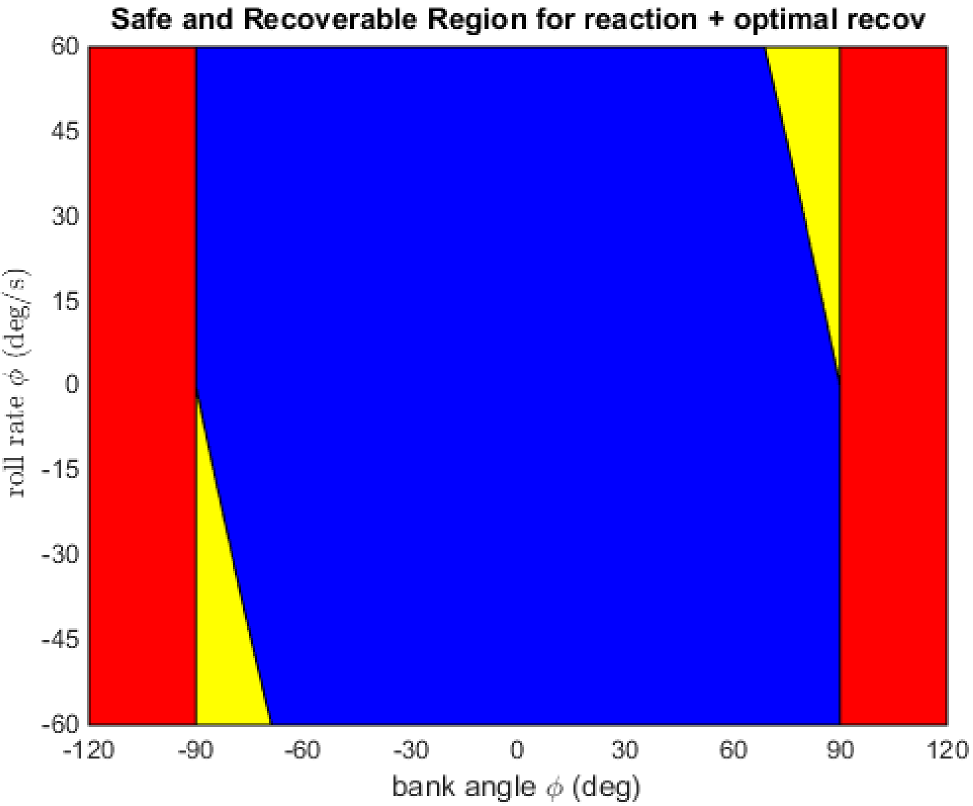


Figure 10. Safe and recoverable region for the "Optimal Recovery after Reaction Time" case; the darker, central region is safe and recoverable, and the size of the unrecoverable regions is intermediate in reference to the other two cases

Comparisons and Conclusions. It can be shown that all three scenarios are related and generalized by scenario 3. The expression for ϕ^*_{nr} is a degenerate case of ϕ^*_{orart} for $t_r \to \infty$.

Likewise, the expression for ϕ_{ior}^{*} is a degenerate case of ϕ_{orart}^{*} for $t_r = 0$. The boundary Ω is therefore a function of the reaction time t_r and the optimal control with scenario 1 calculating the boundary with $t_r \to \infty$ and scenario 2 calculating the boundary with $t_r = 0$. Thus, it would be expected that the boundary for the $t_r = 0.5$ case would fall between the boundaries for the $t_r = 0$ and $t_r \to \infty$ cases. This matches our results, which are depicted in figure 11.

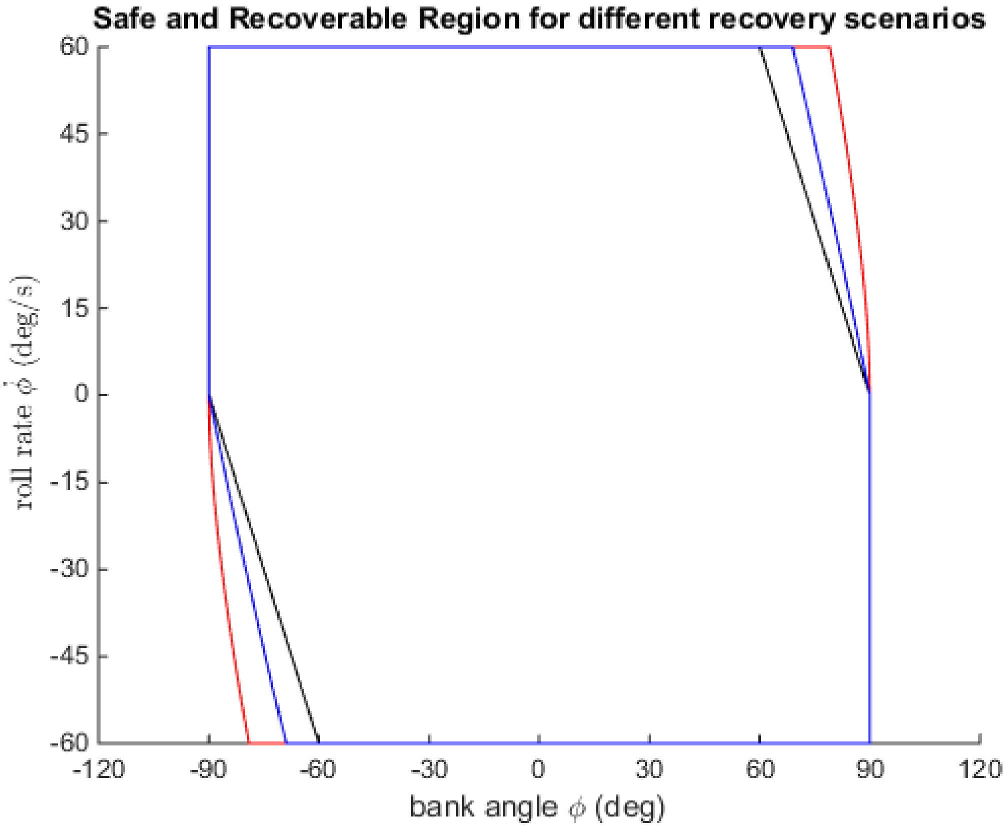


Figure 11. Comparison of the boundaries for the three scenarios: $t_r = 0$ (innermost, black), $t_r = 0.5$ (intermediate, blue), and $t_r \to \infty$ (outermost, red)

FUTURE WORK. The robust and certifiable implementation of such a system is complicated by several factors, all of which are outside the scope of this report but which present opportunities for continuing development of this topic. For example, translating the idealized equations to an actual computing platform will require quantifying and managing any quantization error due to the limits of the numerical representation and the discretization of the time domain. The computations involved get much more complex with removal of the unrealistic assumption that the roll behavior is independent of the other degrees of freedom. Such state space explosion, necessary to model realistic air vehicles, will most likely not provide an analytical solution. It will be necessary to use more advanced techniques, such as problem reformulation, leveraging previous work on hybrid systems, viability theory, and reachability theory. Further, optimization may be necessary or desirable by bounding the state space under consideration to a prudent time horizon or by using efficient search algorithms to analyze possible outcomes from arbitrary current states.

3.2 CASE STUDY FOR RTA IN GA AUTOPILOTS

The following case study was performed by Adaptive Aerospace Group (AAG) to study approaches to developing, integrating, and evaluating an OLIV (additionally referred to as the autopilot integrity monitor or AIM in this case study) for use on a certified GA aircraft. Specifically, the paper describes the current systems and proposed modifications needed to develop and test the OLIV concept on AAG's Cessna R182.

Current Aircraft Systems

AAG's test airplane is a 1979 Cessna R182 (Skylane RG) with modern avionics installed to allow data to be gathered in flight. AAG has developed and verified the functionality of a derived angle-of-attack algorithm that uses data from the Aspen Primary Flight Display (PFD). In addition to certified avionics, an Aeroprobe multihole probe can be mounted on the wing strut and has been calibrated for airspeed and angle of attack. AAG's data acquisition system can gather data from the Global Positioning System (GPS) units, Air Data Attitude and Heading Reference System (ADAHRS), and Aeroprobe probe during flight. AAG is in the process of developing a means to gather control surface position and expects to have an initial version of the system tested before the end of 2015. N736WP also has a JPI 930 engine monitor and can obtain data from it post-flight and synchronize it with the other data. AAG spoke with JPI at Oshkosh 2015 and was told they would provide an interface to obtain the data during flight; to date JPI has not come through with the interface. AAG will keep pursuing this option and is considering swapping the engine monitor for an Electronics International one as we know that can provide data during flight. The aircraft is shown in figure 12, and the instrument panel and some of the data connections are shown in figure 13. Some details of the existing avionics and data systems follow in this section, and a high-level diagram of the components pertinent to this work are shown in figure 14 along with two proposed AIM-related modifications that are described in Modifications to Support AIM Flight Evaluations section.

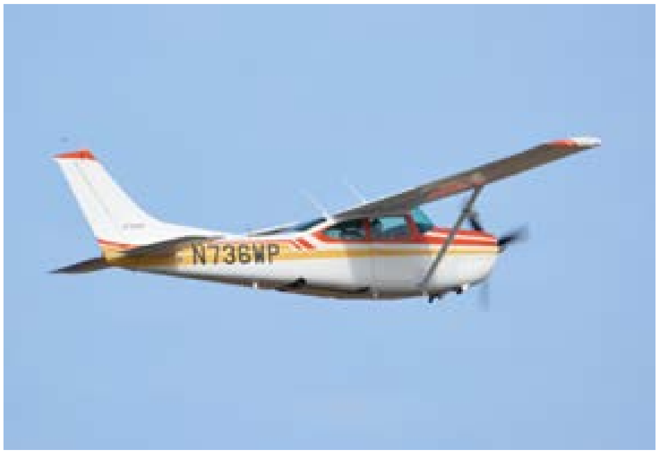
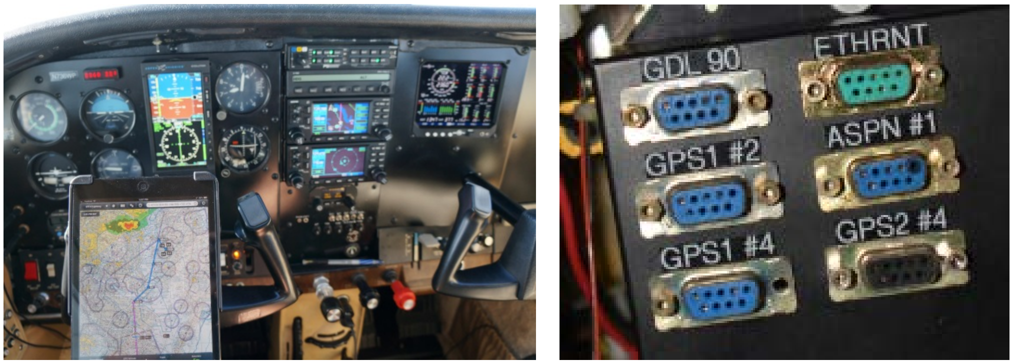


Figure 12. N736WP is a 1979 Cessna R182 equipped to obtain calibrated ADAHARS and angle-of-attack data



(a) (b)

Figure 13. N736WP instrument panel (a) and data connections under panel (b)

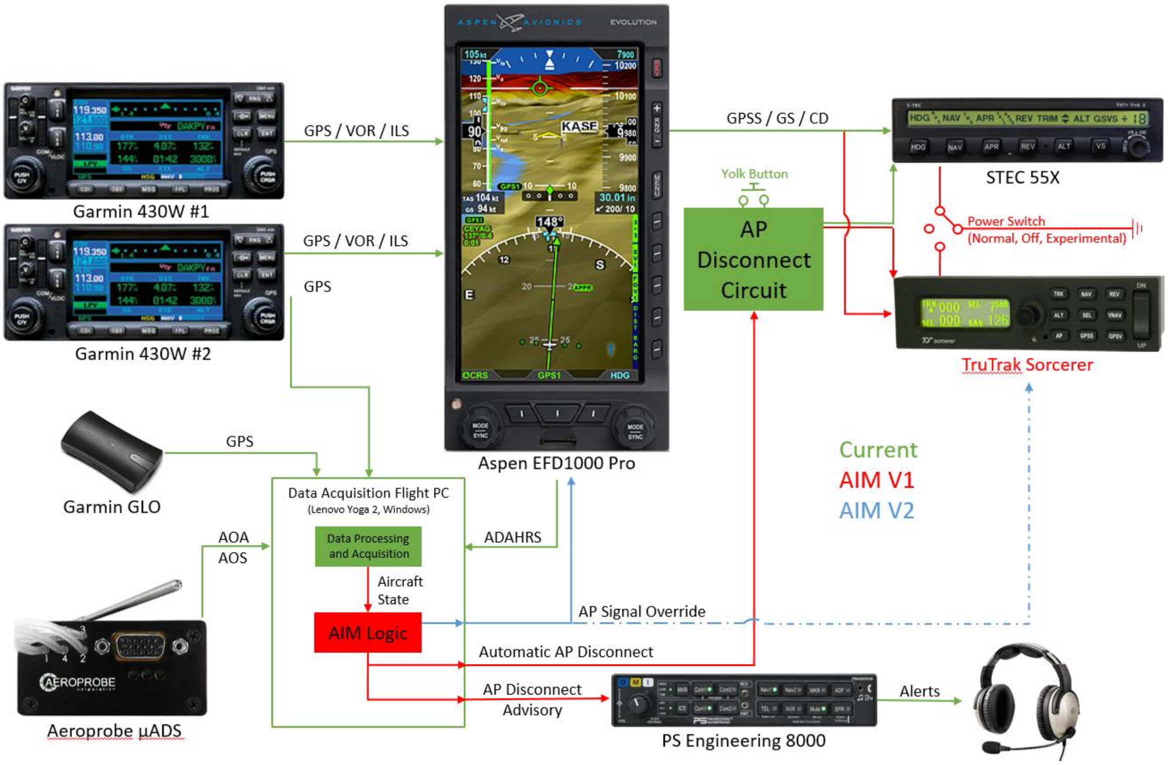


Figure 14. High-level system diagram showing current system (green), AIM V1 (red), and AIM V2 (blue)

ADAHRS – Aspen EFD1000, Sandia Quattro

The Aspen EFD1000 is a certified glass-panel-type PFD that provides ADAHRS data via a proprietary protocol with which AAG has experience and approval to use for flight testing. The PFD also provides switching between the navigation sources and drives the heading/track functions of the autopilot.

AAG conducted the TSO flight tests of Sandia Aerospace's Quattro glass panel ADAHRS indicator, which provides a secondary source of attitude information via a proprietary protocol.

The pre-production Quattro also provides ADAHRS data that can be used as a second source if desired.

Autopilot – S-TEC System 55X

The S-TEC (now Genesys) System 55X autopilot currently installed is a certified analog, rate-based autopilot that commands servos for aileron, elevator, and elevator trim control. The airplane has manual rudder trim control used to adjust for power changes. An electric turn coordinator is part of the autopilot and provides yaw rate, and a pressure transducer provides a pressure altitude reference from static ports on the left and right of the empennage. These static ports are not part of the original aircraft pitot/static system. The autopilot disconnect button is located on the pilot yolk. Pressing it closes a circuit allowing the pilot to quickly disconnect the autopilot returning the aircraft to manual control if desired, including if it exhibits unexpected or undesirable behavior. The pilot can also manually overpower the servos or use a circuit breaker to remove power from the autopilot and auto-trim if necessary.

The autopilot uses standard differential voltage commands from the glide slope and course deviation indicators, and as GPS steering information from the selected navigation system, Garmin® 430w, via a standard ARINC 429 protocol. The Aspen EFD1000 selects a heading to hold. The selected 430w provides the option to follow GPS or VHF omni directional radio range/localizer navigation. The selected system is sent to the S-TEC for directional control and in approach mode can provide vertical guidance. In other modes, altitude rate and hold are controlled by the pilot via a mode control panel. The autopilot has no envelope protection, so it will attempt to hold a commanded climb or descent rate, constant track or heading, or a standard rate turn no matter the speed and power setting of the aircraft.

GPS–Garmin 430W, Garmin GLO

AAG's data-acquisition system gathers data from both Garmin 430w units and the non-certified Garmin GLO to capture standard GPS information in-flight. The GLO provides the highest rate GPS data at 10 Hz.

Angle of Attack—Adaptive Aerospace Group Derived, Aeroprobe µADS 1.0, Aspen EFD1000

AAG developed an in-house algorithm that computes a derived angle-of-attack estimate based on ADAHRS and GPS information for the four nominal flap positions (up, 10°, 20°, and 40°). AAG's data-acquisition system also incorporates an Aeroprobe multi-hole probe mounted on the right wing strut that provides 100 Hz calibrated and true airspeed, sideslip, and angle of attack calibrated for the four nominal flap positions. AAG has experience with the Aspen EFD1000 displays and its output of a derived angle-of-attack estimate associated with the no-flap configuration. It was calibrated at two flap positions. The other angle-of-attack system is used for the pilot display but not output.

Modifications to Support AIM Flight Evaluations

The initial autopilot integrity monitor (AIM V1) will simply disconnect the autopilot if it starts to drive the aircraft outside the predetermined flight envelope and possibly if it starts to drift from the intended course, altitude, vertical rate, or speed depending on the autopilot and mode. A definitive approach to implementing AIM V1 is described in this section. A second and more sophisticated AIM V2 would attempt to keep the autopilot from going out of the envelope before resorting to disconnecting it. Figure 14 shows the existing systems on the aircraft (green), additions required for AIM V1 (red), and for AIM V2 (blue). The components of V1 would also be required for V2. It is suggested that V1 be developed and tested first. Lessons learned from V1 development can be used when considering development of V2. The lessons learned may include that V2 is not practical or would not add sufficient benefit to offset the added complexity and cost.

The existing STEC 55X autopilot is a certified analog autopilot. The certification assures the autopilot's behavior is predictable and correct, with one exception. The 55X has no awareness of aircraft speed; therefore, it is possible for it to stall or speed up the aircraft if the power setting is not compatible with the commanded vertical rate. Adding an electronic switch (relay) to close the autopilot disconnect circuit (same circuit as the disconnect switch on the yoke) via a command from the AIM algorithm running on AAG's data acquisition computer would be relatively straight forward. However, given that this system is certified and our team has no access to the inner workings, what can be learned or proven is limited. A more flexible approach is to add a second, non-certified autopilot to the aircraft for development and testing of AIM systems. TruTrak Flight Systems has a good reputation in the experimental aircraft industry, and their autopilots have been installed in Cessna aircraft in countries outside the U.S. AAG talked with TruTrak and Bay Avionics about this approach. Installation of the TruTrak Sorcerer autopilot is possible with a switch added to the instrument panel to select which autopilot is powered (55X or Sorcerer). Installing and flying with the Sorcerer would require the aircraft to be put in the experimental category, as would installing the AIM-activated autopilot disconnect switch. The autopilot selection switch would be implemented in a way that allows the AIM relay to disconnect whichever autopilot is being used when the AAG data-acquisition computer is connected with the AIM application running.

The proposed TruTrak Sorcerer is an existing low-cost, non-certified digital autopilot that uses the same standardized communication protocol for control as the 55x. However, it may require some tweaking of the interface with the Aspen EFD1000 to achieve full functionality. (Aspen and TruTrak are interested and have agreed to work with AAG on development and testing of the AIM. Software changes can be made to the autopilot/ PFD to introduce known problems for the AIM to detect and interrupt.) The install would include a manually operated double-pole multi-position switch to provide power to only one of the autopilots at a time. The signal routing for the aforementioned autopilot disable button and parallel relay controlled by the AIM software running on AAG's data-acquisition computer would be used to disconnect whichever autopilot is powered. AIM V1 obtains and analyzes the available ADAHRS, AOA, and GPS data and either visually or audibly alerts the pilot and automatically triggers the autopilot disconnect switch when necessary. This transfers control and recovery back to the research test pilot. Discussion of the AIM envelope limits used to trigger the autopilot disconnect is in AIM Protected Envelope section.

AIM V2 would be more sophisticated, with the ability to attempt to limit or correct the autopilot's actions before resorting to the disconnect switch and returning the airplane to the pilot. As shown in figure 14, the AIM V2 could modify autopilot commands through either the Aspen or by directly altering the autopilot commands. As with AIM V1, the system will obtain and analyze the available ADAHRS data but also receive and interpret standardized autopilot control commands () and either regenerate or pass through the autopilot control commands to the autopilot. AIM V2 could also slightly modify the commands with the intent of finding sensitive parameters that may be causing the autopilot to perform in an undesirable manner and correct this behavior. If the attempt to modify the autopilot command is unsuccessful, the integrity monitor will disconnect the autopilot as the AIM V1 does, and transfer full control back to the pilot.

We anticipate that the commercial application would have the AIM residing in the certified Aspen EFD1000 or a similar unit. However, it could function in a unit external to the PFD as this test implementation is done. The external unit would require access to some or all ADAHRS data. A very limited AIM capability may be possible using GPS information alone, making a low-cost, stand-alone AIM possible with no ADAHRS required. Part of the effort will be determining the minimum useful set of data that could support an effective AIM and to assess the tradeoff between the safety benefits and cost of an AIM that uses the minimum set and one that uses other potentially available parameters.

Specifically, modifications to the existing R182 systems for the AIM testing would include the following (figure 14):

1. Installing the TruTrak Sorcerer autopilot.
2. Installing a switch to select whether the 55X or Sorcerer is powered.
3. Developing the AIM logic and software to run on AAG’s data acquisition computer and implement it as a separate application or integrated with the data-acquisition software.
4. Installing an electronic switch that allows the AIM logic to close the powered autopilot’s disconnect switch. The current audio panel install allows for the data-acquisition computer to be plugged in for auditory pilot alerts.

We suggest in this report that an electronic autopilot disconnect switch can be used by the AIM to disconnect an autopilot that is not behaving properly, thus giving control back to the pilot. Only through discussions with the FAA can there be certainty that this approach is certifiable, given that the autopilot is not certified, including its response to the disconnect circuit. An alternative installation of the AIM could use a relay to remove power from the autopilot, assuring it does not interfere with the pilot’s inputs. The choice only impacts the install by the type and location of the relay used to interrupt the autopilot. If autopilot power is interrupted, it will take longer to re-engage the autopilot after AIM interruptions.

AIM Protected Envelope

The AIM will be designed to operate within a very conservative flight envelope. Given that the system will automatically disconnect the autopilot with little or no warning, the airplane should not be in a state that is difficult for the pilot to recognize and recover from. Consideration of different envelope protection limits for different phases of flight should also be made. More conservative limits may be applied during precision approaches, for example, because small errors can have bigger, more immediate consequences during approaches. Only one envelope is considered in this initial report. It is suggested that more “special case” envelopes be considered and developed when the AIM development and implementation work is done.

Table 1 provides initial thoughts on a list of conservative envelope parameters for AAG’s Cessna R182 as a starting point for discussion and development of an AIM tailored for that model aircraft.

The table includes a list of parameters, a proposed limit, and a brief discussion on the reason for the limit. An installed autopilot, certified or not, is expected to remain within the boundary parameters listed here to provide comfortable, non-aggressive, and predictable flight characteristics. It may be reasonable to start the testing with one control axis, but many of the parameters are dynamically coupled; therefore, it likely makes sense to tackle the problem together. A fully developed AIM is expected to relinquish control to the research pilot if the provided ADAHRS and GPS indicate the aircraft has exceeded or is trending toward a limit. Trending toward the limit is key, because going through the limit at a high rate could cause the aircraft to stall or enter an unusual attitude that is difficult to recover from before the autopilot disconnects, giving the pilot very little time to observe, determine, and act. Part of the philosophy of selecting the limits has to do with the intended function of autopilots. They are used to fly normal maneuvers akin to IFR flight, so they should stay well within the speed envelope and not exceed standard rate turns. Some of the discussion assumes the AIM knows the aircraft's current configuration. However, flap position is not generally an available parameter on GA aircraft. AAG is developing an approach to provide a flap-position detection capability. However, given that flap position will not be readily available on GA aircraft, two versions of the AIM logic should be developed for when configuration information is available and when it is not. Likewise, if engine status is available, power setting could be included in the AIM development. Power setting would likely only support prediction capability in GA aircraft because auto-throttles do not exist in GA aircraft of interest for these systems.

Table 1. Aircraft envelope parameters

Parameter	Limit	Reasoning
Minimum speed flaps up	80 KIAS	This is a safe, stable speed and is 10 KIAS below downwind, a “slow” ILS/approach speed, and 8 KIAS below best rate of climb speed. It provides a 20 KIAS margin to stall. Note 1: Hoffler generally flies approaches at 120 KIAS prior to taking manual control on “short” final. Note 2: 80 KIAS is above best glide speed, which may be a problem or require an exception.
Minimum speed 10° flaps	80 KIAS	Similar to flaps up. The biggest difference is drag.
Minimum speed 20° flaps	65 KIAS	75 KIAS is a good final approach speed with 20° of flaps. It provides a 10 KIAS margin to stall and is roughly 15 KIAS above stall warning buzzer.
Minimum speed 40° flaps	60 KIAS	65 KIAS is a good final approach speed with 40° flaps. It provides a 20 KIAS margin to stall. A short field is 61 KIAS but would be hand-flown currently. Note: The aircraft can lose speed rapidly in this configuration.
Maximum speed 20° and 40° flaps.	90 KIAS	5 KIAS below flap extended speed for these settings. This provides some margin and is nominally faster than the airplane would be flown with 20° or more flaps.
Maximum speed 10° flaps and/or gear down.	135 KIAS	5 KIAS below 10° flap and gear down speed.
Maximum speed gear and flaps up.	160 KIAS	V_{NO} – Maximum structural cruising speed in smooth air (top of the green arc). Also, it is roughly 6 KIAS faster than fastest level speed.
Maximum bank angle	30°	Will never limit a standard rate turn and is a benign angle to recover from. Note: It would be more conservative to limit bank angle to 5° more than the bank required for a standard rate turn. With GPS ground speed, this is easy to compute. However, it also introduces more complexity.
Maximum nose up theta	15°	This is 5° higher than liftoff theta. Note: This needs additional consideration.
Maximum nose down theta	5°	This is conservative. Note: This needs additional consideration.

Table 1. Aircraft Envelope Parameters (continued)

Parameter	Limit	Reasoning
Maximum time to speed boundary	5 seconds to speed boundary	The system should not allow acceleration that will “bust” a minimum or maximum speed in less than 5 seconds. At 8 seconds, it should warn the pilot. The times clearly need to be researched or better thought-out.
Maximum altitude rate	?	May not be needed and should be covered by the other parameters. If the autopilot has a known level-off altitude, this could be time to achieve parameter. 1000 fpm would not limit normal vertical rates with autopilot engaged and should possibly be used.
Maximum N_z	1.25 g	This is slightly higher than a 30° level turn. It corresponds to the level turn limit with a 0.1 g margin.
Minimum N_z	0.75 g	This is just opposite the maximum g limit. Note: This needs additional consideration.

ILS = instrument landing system; KIAS=knots-indicated air speed

Partners and Path Forward

In addition to NASA, the FAA, the DOD, and the University of Tulsa team, AAG has talked about this work and the potential benefits to GA with TruTrak Flight Systems and Aspen Avionics. Both are interested and have agreed to work with us on the project. TruTrak can modify the software in their Sorcerer autopilot to intentionally cause “bad behavior” for testing and verifying the behavior of the AIM implementation. AAG is currently working with Aspen and using data from their EFD1000 on another project. Aspen may have to make minor modifications to their autopilot interface to work correctly with the TruTrak Sorcerer. This would be part of the AIM effort. Note that if the AIM development is successful, it will result in a set of requirements for such a system and a quick path to certification and implementation with the combination of Aspen and TruTrak being involved.

Additionally, AAG has a long-standing working relationship with the National Institute of Aerospace (NIA) located in Hampton, VA. The NIA has a task order contract in place with the FAA that could be used for the work. The NIA also has formal methods expertise that could be useful in formally proving the integrity of the AIM functional requirements and software implementation..

The scope of what elements to address, or doing a complete development of AIM V1, needs to be discussed to determine the costs of development and testing. Some pilot evaluations should be done in simulation to keep costs under control. Flight tests most likely should be relegated to proving functionality in flight with real systems and data. AAG is a member of Partnership to Enhance General Aviation Safety, Accessibility and Sustainability (PEGASAS) and should be able to work with University of Tulsa (not a PEGASAS member) and others to set up a simulation evaluation at one of the PEGASAS universities, Tulsa, or AAG. AAG also has a long history with the simulation facilities at NASA Langley Research Center (LaRC). LaRC’s facilities include a 6-DOF motion facility and may be an option, though likely an expensive one by comparison.

4. CONCLUSIONS AND FUTURE WORK

This report has provided an initial look into a new concept for certification of small aircraft autopilot systems. This study was motivated by the relatively poor safety record of GA aircraft, which could be significantly improved with the addition of new technologies. However, these technologies have not been adopted due to, in large part, the cost and burden associated with the somewhat outdated certification process. The OLIV architecture, which is based on assurance of system safety at run-time, has been proposed to help alleviate this burden through the bounding of autopilot control to regions of the aircraft state space, which are known to be safe and recoverable. This report has discussed an example of how these state boundaries should be constructed given the ability of a pilot to correct autopilot actions. It has also discussed considerations of a safety case for OLIV, which may be the most important aspect of its initial design. In addition, this report has provided a first look into flight-test considerations for the OLIV system on a representative GA aircraft.

The findings found in this report are meant to be seen as a first step to development of the OLIV architecture. A complete pilot-reaction model should be developed to quantify the ability of the pilot to recover from a potential autopilot fault. This model then should be used in the calculation of safe and recoverable boundaries for the full-envelope of aircraft states and dynamics. Certification considerations for the RTA monitor and switch must also be explored, as should any components of the system common across multiple aircraft. Last, and potentially most important, a large amount of OLIV flight and simulation data should be produced so certifiers can assess the appropriateness of the concepts in this report. Only then will new technologies made possible by these concepts have an opportunity to advance small aircraft safety.

5. REFERENCES

1. General Aviation Joint Steering Committee (GAJSC) Loss of Control Work Group Report. (2012). Approach and Landing Report..

2. National Transportation Safety Board Report. (2013). Preliminary Aviation Statistics, Data for years 2001-2010.

3. U.S. Department of Transportation Report. (2012). Fatality Reporting System Data for years 2001-2010.

4. Insurance Institute of Highway Safety Report. (2011). Traffic Safety Facts 2011, Data for years 2002-2011.

5. Swihart, D. E., Barfield, A., Griffin, E., Lehmann, R., Whitcomb, S., Flynn, B., Skoog, M., Processor, K. (2011). Automatic ground collision avoidance system design, integration, & flight test. *IEEE Aerospace and Electronic Systems Magazine, 26*(5), 4–11.

6. Ding, J., Hook, L. R., Tomlin, C. J., (2016). *Initial Designs for an Automatic Forced Landing System for Safer Inclusion of Small Unmanned Air Vehicles into the National Airspace.* Proceedings from the Digital Avionics Systems Conference, Sacramento, CA.

7. NASA NARI Report. (2013). Development of a "Where-to-Land" Decision Function for an Expert Piloting Systems (EPS) in Man-rated Autonomous Air Vehicles.

8. General Aviation Manufactures Association. (2012). *General Aviation Statistical Databook and Industry Outlook*. Washington, DC: GAMA.

9. RTCA Report. (2011). Software Considerations in Airborne Systems and Equipment Certification. (DO-178C).

10. Jackson, S. (2012). *Certification of Safety Critical Software Under DO-178C and DO-278A*, Paper presented at Infotech@Aerospace 2012, Garden Grove, CA.

11. NASA Report. (2001). A Practical Tutorial on Modified Condition/Decision Coverage. (NASA/TM-2001-210876).

12. Goldberg, A., Horvath, G. (2007). *Software Fault Protection with ARINC 653*. Presented at the 2007 IEEE Aerospace Conference, Big Sky, MT.

13. 113th US Congress. (2013). "H.R. 1848, the Small Aircraft Revitalization Act."

14. Department of Defense - Autonomy Community of Interest, Test and Evaluation, Verification and Validation Working Group, (2015). Technology Investment Strategy 2015-2018..

15. NASA Report. (2015). Current Practices in Constructing and Evaluating Assurances Cases with Applications to Aviation. (NASA/CR2015-218678).

16. Hinchman, J., Clark, M., Hoffman, J., Hulbert, B., Snyder, C. (2012). *Towards Safety Assurance of Trusted Autonomy in Air Force Flight Critical Systems*. Proceedings from the Computer Security Applications Conference, Orlando, FL.

17. Mitchell, I. (2002). *Application of Level Set Methods to Control and Reachability Problems in Continuous and Hybrid Systems*. (Ph.D. thesis). Stanford University.

18. Mitchell, I., Tomlin, C. (2002). *Level set methods for computation in hybrid systems.* Hybrid Systems: Computation and Control, vol. 1790, 310–323.

19. Bayen, A., Mitchell, I., Oishi, M., Tomlin, C., (2007). Aircraft Autolander Safety Analysis Through Optimal Control-Based Reach Set Computation. *Journal of Guidance, Control, and Dynamics, 30*(1), 68–77.

20. Lygeros, J., (2004). On Reachability and Minimum Cost Optimal Control. *Automatica, 40*(6), 917–927.

21. Rushby, J. (1986). Kernels for Safety. In Anderson, T. (Ed.), *Safe and Secure Computing Systems* (210–220). Glasgow, UK: Blackwell Scientific Publications, 1986.

22. Leveson, N. G., (1995). *Safeware: System safety and computers*. New York, NY, USA: Addison-Wesley.