Certification strategies using run-time safety assurance for part 23 autopilot systems

Loyd R. Hook
University of Tulsa – ECE Dept.
800 S. Tucker Dr., Rayzor 1130
Tulsa, OK 74104
918-631-3272
Loyd-hook@utulsa.edu

Matthew Clark
Air Force Research Laboratory
2210 Eighth St.
Wright-Patterson AFB, OH 45433
937-713-7044
Matthew.clark.20@us.af.mil

David Sizoo
FAA Aircraft Certification Service,
Small Airplane Directorate,
901 Locust St., Kansas City, MO 64106
816-329-4158
David.sizoo@faa.gov

Mark A. Skoog
NASA-Armstrong Flight Research Center
P.O. Box 273 / M.S. 4830E
Edwards, CA 93523
661-276-5774
Mark.a.skoog@nasa.gov

James Brady
FAA Aircraft Certification Service,
Small Airplane Directorate
901 Locust St., Kansas City, MO 64106
816-329-4132
James.brady@faa.gov

Abstract— **Part 23 aircraft operation, and in particular general aviation, is relatively unsafe when compared to other common forms of vehicle travel. Currently, there exists technologies that could increase safety statistics for these aircraft; however, the high burden and cost of performing the requisite safety critical certification processes for these systems limits their proliferation. For this reason, many entities, including the Federal Aviation Administration, NASA, and the US Air Force, are considering new options for certification for technologies which will improve aircraft safety. Of particular interest, are low cost autopilot systems for general aviation aircraft, as these systems have the potential to positively and significantly affect safety statistics. This paper proposes new systems and techniques, leveraging run-time verification, for the assurance of general aviation autopilot systems, which would be used to supplement the current certification process and provide a viable path for near-term low-cost implementation. In addition, discussions on preliminary experimentation and building the assurance case for a system, based on these principles, is provided.**

TABLE OF CONTENTS

1. INTRODUCTION

The Federal Aviation Administration (FAA) has been interested in alternate certification strategies for small aircraft systems for several years. The Agency recognizes that new technologies are available that could significantly increase safety. However, many of these technologies are not being implemented or certified due to several barriers. Some of these barriers include the certification burden of outdated regulations. 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 mishaps that afflict small aircraft are: loss of control (LOC), controlled flight into terrain (CFIT), and component failure involving the power plant [1]. Of particular interest is LOC, which accounts for over 40% of the total fatal mishaps. In many instances, LOC statistics—as well as CFIT statistics - which are due to spatial disorientation or pilot distraction - could be significantly improved with the addition of even very simple autopilot systems, such as a simple wing leveler. In addition, there are other automatic aircraft systems which will be able to improve mishap rates in many other categories in the near future. For instance, an automatic LOC prevention and recovery system could have a dramatic impact on safety of small aircraft. This would also be true for a flight director or automatic ground collision avoidance system (Auto GCAS) or an automatic forced landing system (Auto FLS). Even so, these systems will all require an integrated autopilot system to provide safety decision actuation in order 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 and/or facilitate a significant increase in safety for this type of airplane. Autopilots can be found on some new small aircraft; however, due to current certification costs, the business case

978-1-4673-7676-1/16/$31.00 ©2016 IEEE
Approved for Public Release Distribution Unlimited
CASE NUMBER 88ABW-2015-4093

is not favorable for development of low cost autopilots for the small aircraft retrofit market and many new lower cost aircraft. For example, a simple 2 axis, rate based autopilot (that was state of the art 15 years ago) costs $20,000- $25,000 to install on a simple Cessna C-182. This high cost means that sometimes the hull value of the aircraft is less than the installed autopilot system. Furthermore, modern attitude based autopilots are even more expensive and harder to justify on older retrofit aircraft.

In response to this reality, the FAA is partnering with NASA, with the University of Tulsa and AFRL, to develop strategies to ease the certification burden for small aircraft autopilots in order to improve the business case for their inclusion in both existing aircraft and lower cost new aircraft. One particular strategy for accomplishing this is to transfer the authority and certification burden to a simpler and standardized system that would monitor an autopilot during operation to 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 condition which mitigates loss of control during this transition (See Figure 1). Techniques to provably assure safety in this manner are currently being established based on work in the hybrid systems verification and run-time verification fields as well as being used during testing of experimental air and spacecraft control systems. Therefore, confidence in this method of alternate certification is high; however, there remains a large amount of work that must be accomplished before certification authorities will have the data required to make decisions based on this alternate method of certification.

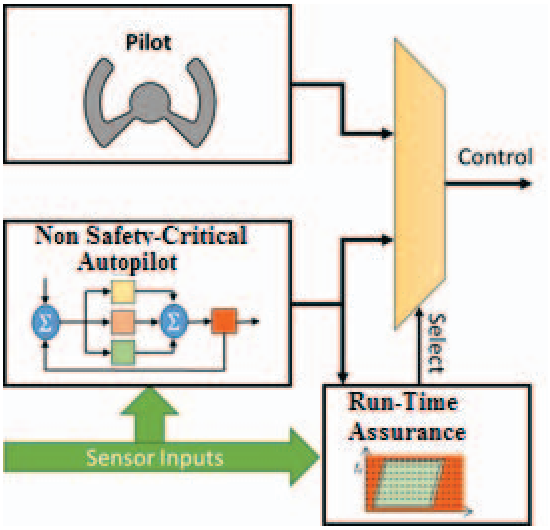

Figure 1. Autopilot monitor and control switch strategy which may relieve certification burden for an autopilot

2. Acronyms

AFRL	Air Force Research Laboratory
ATC	Air Traffic Control
Auto FLS	Automatic Forced Landing System
Auto GCAS	Automatic Ground Collision Avoidance
CFIT	Controlled Flight into Terrain
COTS	Commercial off the Shelf
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulations
GA	General Aviation
GAJSC	General Aviation Joint Steering
IFR	Instrument Flight Rules
IMC	Instrument Meteorological Conditions
LOC	Loss of Control
NASA	National Aeronautics and Space Admin.
RTA	Run Time Assurance
ROA	Region of Action
ROR	Region of Recovery
SARA	Small Aircraft Revitalization Act
SOUP	Software of Unknown Pedigree

3. Revitalized Certification for Part 23 Aircraft

Part 23 of the Federal Aviation Regulations (FAR) details airworthiness standards for the certification of airplanes that fall within the normal, utility, acrobatic, and commuter categories. These categories consist of nearly all general aviation airplanes along with other small commuter aircraft. Therefore, when the United States Congress wanted to tackle the "overly prescriptive and outdated certification process [2]" for general aviation (GA) aircraft and systems, they passed H.R. 1848, *The Small Aircraft Revitalization Act of 2013*, or SARA. SARA provides the FAA the opportunity to reorganize the certification requirements for part 23 aircraft in order to streamline the approval of new technologies designed to improve safety. In addition, SARA stipulates to remove prescriptive based certification requirements in favor of performance based regulations, thereby opening up untraditional methods to airplane certification.

In this context, the FAA has been looking into alternate methods of certification which will continue to assure safety in small aircraft without the current, overly burdensome and expensive certification process. This has led to collaboration with partners in government, academia, and industry in order to determine the best ways to solve this difficult issue. In particular, the FAA has begun coordinating with NASA to develop alternate methods of certification for autopilot systems which could enable the largest increase to overall safety for GA aircraft.

4. Small Aircraft Safety Statistics

At the heart of the issue that SARA and the FAA are trying to address is the relatively poor safety record of general

978-1-4673-7676-1/16/$31.00 ©2016 IEEE

aviation travel compared to other common forms of transportation. In the ten year period from 2001-2010, the average number of general aviation accidents was over 1600 per year, with over 300 of those causing at least one fatality [3]. This produced over 550 fatalities per year on average or over 1.5 fatalities per day. When adjusted for the number of general aviation flight hours flown during these years and assuming a conservative average velocity of 100 miles/hr. and average occupancy of 2 persons per vehicle, the fatality rate per personal mile traveled was over 11.6 fatalities per 100 million personal miles traveled. When comparing this rate to other common forms of transportation, the data reveal that GA pilots and occupants are over 11 times more likely to be killed per mile traveled compared to travel in a car. This number increases to over 1100 times more likely when compared to commercial air travel. Only when compared against travel in motorcycles, which is known to be one of the most dangerous forms of travel, does general aviation have an advantage in safety and this advantage is only by a factor of around 2.5 [4, 5].

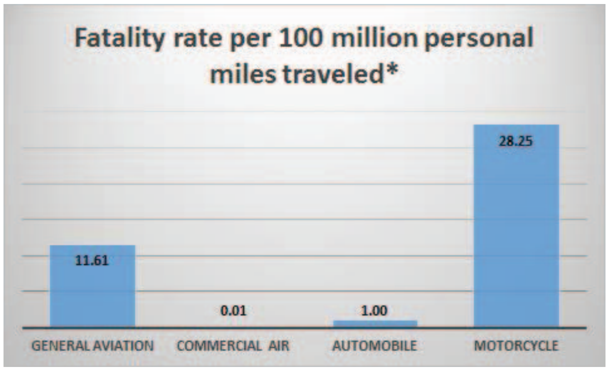

Figure 2. Comparing fatality rates in transportation categories per personal mile traveled. [3, 4, 5]

Of these relatively large number of fatal accidents, over 60% can be attributed to three specific causes: loss of control (LOC), controlled flight into terrain (CFIT), and component failure of the power plant [1]. Of these 3 major causes, loss of control heavily dominates, being the cause of over 40% of the total fatal mishaps in general aviation. Therefore, targeting solutions to these three major causes, with special emphasis on loss of control, would provide the largest contributions to increases in safety for GA aircraft.

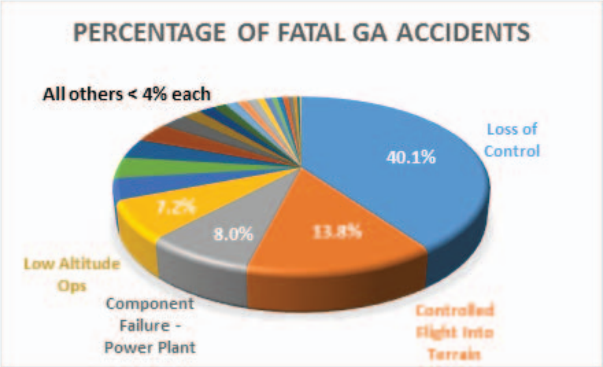

Figure 3. Categorization of fatal GA accidents from the GAJSC [1]

5. EFFECT OF AUTOPILOT INCLUSION AND AUTOMATIC SYSTEMS ON GA SAFETY

Fortunately, automated systems are currently available which are able to have a major impact on fatality statistics of these three major causes. Of immediate interest, loss of control and CFIT accidents caused by poor situational awareness produced by environmental, geographical, or time-of-day factors, we believe, 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 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 which would provide a significant increase in the safety for other accident categories as well. For instance, automatic ground collision avoidance systems (Auto GCAS), have been developed and are being deployed on United States Air Force F-16s [6]. These Auto GCAS systems may have the ability to reduce CFIT accidents by as much as 98% in military aircraft, and development of similar systems for GA aircraft is underway. In addition, systems to automatically avoid and/or recover from loss of control situations are being developed which, when applied to the GA regime, would have a dramatic impact in safety for all types of loss of control situations. Even fatalities from power plant failure could be significantly reduced with the inclusion of automatic forced landing systems (Auto FLS) or flight directors with energy management cues that provide the highest probability for a safe and successful emergency landing [7]. These Auto FLS systems are currently under development for commercial and general aviation 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 (or flight director) system 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 the fatal accident rates, it would also allow for

978-1-4673-7676-1/16/$31.00 ©2016 IEEE
Approved for Public Release Distribution Unlimited
CASE NUMBER 88ABW-2015-4093

more advanced automatic systems to be integrated providing even further safety enhancement.

Figure 4. USAF F-16 with integrated Auto GCAS [16]

6. AUTOPILOT RUN-TIME CERTIFICATION STRATEGIES

Currently, there exist low cost, off the shelf, advanced autopilots designed for the experimental market with a mixed track record of capability and performance. In addition to these low cost solutions, several companies have invested resources in creating more robust, commercially available autopilot options. These autopilot technologies, under a well-defined set of operating conditions, perform safely and effectively. However, most of these systems have what is considered commercially off the shelf software (COTS) or software of unknown pedigree (SOUP), software that has been developed without investing the resources to ensure compliance with current FAA certification guidance (specifically, the airworthiness design criteria highlighted within the SAE ARP4761, ARP 4754A, and the RTCA DO-178C standards). To address this concern, one approach would be to invest the significant time, resources, and funding required to create an autopilot that is Flight Critically rated “safe to fly”. However, the end product most likely would be cost prohibitive for private owners, rated for specific vehicle configurations, and limited in usability [8]. Another option could be to assume that these autopilot systems, from the certification perspective, are considered capable at a lower certification standard. This would assume that, without additional testing and inspection, the autopilot software may not be compliant with all FAA certification standards at the rated criticality level. For these types of systems, several military and civilian aviation documents have identified a notion of a real time monitor and failsafe switching system, referred to as Run Time Assurance (RTA), as a key component to enabling the certification of automated, increasingly autonomous, and highly complex systems that are either cost prohibitive or impossible to certify using the current standards or guidelines.

Run Time Assurance

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. As illustrated in Figure 5, a run time assurance system 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 sufficiently 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 general aviation aircraft, a low cost autopilot could be considered the untrusted component. The core idea 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 civilization 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.

The key advantage to a Run Time Assurance approach is that lower cost autopilot systems can be employed without costly certification, allowing only the behaviors that are protected by certified monitors and recovery systems. At the surface, this may seem concerning, allowing a system to function without exhaustive testing / analysis. However, such an inference relies on the assumption that current software systems are exhaustively tested and are without errors or defects, which is actually 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 Run Time Assurance framework for untrusted flight critical software within any control layer from mission planning to trajectory planning to inner loop control. Below are some design considerations that were noted within the program that may be applicable to a Run Time Assurance based certification paradigm for a low cost GA Autopilot system:

(1) 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 at real time.

(2) The RTA framework can be implemented using multiple recovery or failsafe mechanisms, which cover differing 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.

(3) 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.

(4) 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.

7. HIGH LEVEL ASSURANCE CASE FOR SIMPLE RTA/AUTOPILOT SYSTEMS

In what may be the most tractable near-term implementation of an RTA system which could provide benefit for general aviation aircraft, a COTS type non-safety-critical autopilot would be monitored by a configurable and certified RTA system. The "recovery" controller (from Figure 5) for this implementation, would be the human pilot in command which 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. This setup, which will be referred to for the remainder of this section as a "Non-Critical Autopilot - Run Time Assured - with Manual Pilot Recovery" System (NCA-RTA-MPR), is shown in Figure 6.

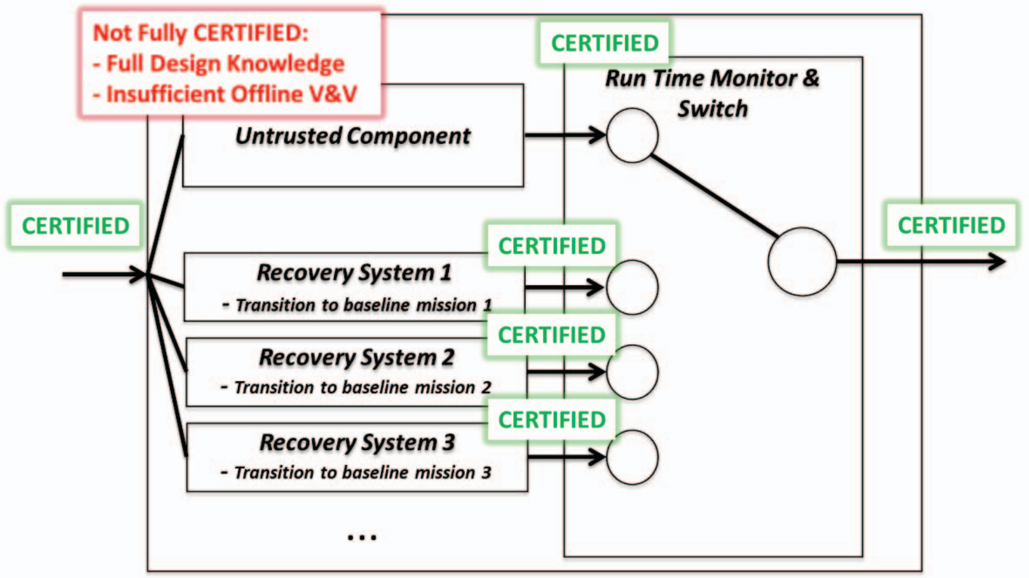

Figure 5. Generic Run Time Assurance Architecture

978-1-4673-7676-1/16/$31.00 ©2016 IEEE
Approved for Public Release Distribution Unlimited
CASE NUMBER 88ABW-2015-4093

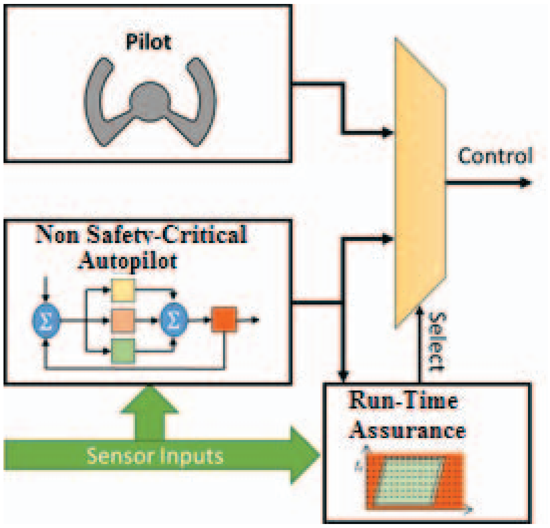

Figure 6. Non-Critical Autopilot - Run Time Assured - with Manual Pilot Recovery (NCA-RTA-MPR) System

We agree that the most important component of a Run Time Assurance based certification approach may be the Assurance Case (or Safety Case) itself. Fundamentally, the overarching Run Time Assurance claim is that a subsystem, by itself, does not provide enough acceptable evidence to achieve the level of confidence required for the predetermined level of risk, but that, 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 a NCA-RTA-MPR system that will NOT REDUCE the confidence in an existing GA aircraft and will lay the framework for future safety and recovery systems that rely on an autopilot. The goal of these future systems is to actually 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 than without.

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, where feasible, to achieve a sufficient level of confidence in a NCA-RTA-MPR 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 which might support an NCA-RTA-MPR 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 initial paper; 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, ATC compliance, weather avoidance, controllability, and general aviation “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 system will only be able to be used under the authority of the pilot-in-command.

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

Sub-arguement 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 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 state space.

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

Sub-arguement 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 loss of control or entry into an unsafe or uncontrollable region of the aircraft operating space.

Sub-arguement 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 in order 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 [9].

8. Run time assurance for GA and Small UAV autopilots: preliminary experimentation

Experimentation and implementation of the systems and concepts advocated in this paper (that being of the NCA-RTA-MPR system) is beginning to be applied at the NASA Armstrong Flight Research Center with support from the FAA and NASA. Initial testing on small unmanned aircraft has already provided limited but successful results and proved the feasibility of testing both in simulation and on the small scale. For these initial tests, a small UAV autopilot was driven by 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).

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, due to 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 trivial and regular event from a pilot perspective that accurate determination of who was controlling the aircraft was at times ambiguous. This unexpected result was also seen in the USAF Automatic Ground Collision Avoidance System flight testing as 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]. In addition, 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 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 small scale and 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 NCA-RTA-MPR system on larger scale UAVs and manned general aviation 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 thus the ability to perform the requisite testing. It is thus envisioned that the results of this testing will be twofold, one being the design and implementation of the system itself, and the other being 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.

9. Recommendations and Future Work

As has been discussed, the development of the Run Time Assurance methodologies, to date, has been largely academic. However, this group is interested in not only the theoretical basis but also early experimentation and implementation to uncover problems early in the development process. In pursuing this theme, work has begun on identifying a candidate autopilot system considered for small GA aircraft to test the concepts presented in this paper. With this system, we plan on utilizing conventional but novel assume-guarantee reasoning techniques to abstract allowable and non-allowable behaviors from the candidate autopilot. In addition, plans to identify and implement recovery mechanisms like pilot takeover, collision avoidance, etc., and instrument the candidate autopilot to monitor undesired behavior or behavior that induces an unsafe or unrecoverable condition are underway.

After development, certification, and flight testing of the NCA-RTA-MPR system, other systems that are of interest to the community could be developed as well. For instance, the FAA is interested in the concept of adaptive autopilots which can change their control properties based on changes to aircraft control or aerodynamics. These types of autopilots are designed to provide controllability even in the event of a control surface failure and therefore may be highly desirable. However, certification of these highly complex systems has not been successfully accomplished to date, making them great candidates for certification under an RTA approach. In addition, RTA acceptance could open up many further areas of research for autonomy in part 23 aircraft which could increase safety and open up general aviation to a much larger percentage of the population.

APPENDIX

A. DEFINITION OF TERMS

Assurance Case – A structured argument, supported by documentation, which builds confidence of safety and security to an acceptable level within a particular context. The assurance case provides a means to structure the reasoning that engineers implicitly use to gain confidence that systems will work as expected. It also becomes a key element in the documentation of the system and provides a mapping to more detailed information. The concept of an assurance case has been derived from the safety case, a construct that has been used successfully in Europe for over a decade to document safety for nuclear power plants, transportation systems, automotive systems, and avionics systems. Much like a legal case presented in a courtroom, an assurance case requires arguments linking evidence with claims of conformance to dependability-related requirements. [10] Several certification standards and guidelines in the defense, transportation (aviation, automotive, rail), and healthcare domains now recommend and/or mandate the development of assurance cases for software-intensive systems [11, 12]

Design Time – The period within a system lifecycle pertaining to all design, integration, verification and validation activities performed PRIOR to full rate production.

Run Time – The period within a system lifecycle after deployment, fielding, or full rate production as opposed to referring to the system during the "design time" or design phase prior to full rate production.

Run Time Assurance (RTA) - A structured argument supported by evidence, justifying that a system is acceptably safe and secure not through reliance on offline tests but through reliance on real time monitoring, prediction, and failsafe recovery.

Run Time methods – Methods and techniques to monitor, diagnose, and evaluate pre-defined (at design time) constraints that always must hold. Other terms may refer to fault diagnosis, isolation, and recovery with the exception that FDI & R methods predominantly refer to off-nominal physical component failures and not necessarily to software based failures not previously identified at design time.

Run Time Assurance Based Certification – The act of providing acceptable arguments and evidence that leads to the certification of a system that contains a design time uncertified subsystem. The certification argument relies on additional, complementary subsystem components designed to monitor, interrupt, and recover from a failure from the uncertified subsystem component.

Autopilot assurance – A structured argument, supported by evidence that an autopilot system is acceptably safe and secure within the specific operational context in which it was intended.

Hybrid System Verification – The discipline and methods to verify Hybrid Systems, or systems that contain both discrete decisions and continuous dynamics.

Assume-Guarantee Reasoning – A form of compositional proof, performed by systematically defining and verifying the pre-conditions (assumptions) and post-conditions (guarantees) that govern the interconnections between all subcomponents within a system [13, 14, 15].

Region of Attraction (ROA) – The region or multi-dimensional constraint space that guarantees a system, given the initial conditions start within the ROA, will always remain within the ROA.

Region of Recovery (ROR) – The region or multi-dimensional constraint space that is defined by a Run Time Assurance recovery system, guaranteeing that once a transition from advanced control to recovery control occurs, the system will safely traverse from the failed state space to a less capable, certified controller's region of attraction (ROA).

(RTA) Untrusted or Uncertified Component – The software component within an RTA system not certified at the same criticality level that is required of the system as a whole (i.e., a software system being used within a safety critical application that has not been tested to current safety critical standards).

(RTA) Recovery System – Set of transition and baseline components providing overall assurance that at any given time, the RTA protected system can recover from an untrusted component failure.

(RTA) Baseline Component – Software component(s) certified to maintain RTA protected critical functions under specific and limited conditions using deterministic and reliable decision procedures.

(RTA) Transition Component – Software component(s) certified to transition the system from any condition at which the untrusted component failed to an operating condition suitable for the baseline controller to engage.

(RTA) Monitor & Switch – Certified run time executive that compares the untrusted component behavior with a set of known, acceptable constraints based on the assume-guarantee contracts of each subcomponent interaction and behavior. The monitor determines, based on the violation of a constraint and the time required to recover, when to switch from the untrusted to recovery components.

(RTA) Instrumentation Considerations – The process by which an untrusted or uncertified component is designed with software instrumentation (i.e., software based triggers, outputs, or assertions) such that run time monitoring against pre-defined constraints can be performed.

Worst Case Execution Time (WCET) – The maximum time a particular algorithm, compiled on the target platform, requires to perform all executions within a given period of time.

REFERENCES

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

[2] 113th US Congress, "H.R. 1848," 2013.

[3] National Transportation Safety Board, "Preliminary Aviation Statistics, Data for years 2001-2010," 2013.

[4] U.S. Department of Transportation, "Fatality Reporting System Data for years 2001-2010," 2012.

[5] Insurance Institute of Highway Safety, "Traffic Safety Facts 2011, Data for years 2002-2011," 2011.

[6] D. E. Swihart, A. Barfield, E. Griffin, R. Lehmann, S. Whitcomb, B. Flynn, M. Skoog and K. Processor, "Automatic Ground Collision Avoidance System Design, Integration, & Flight Test," *IEEE Aerospace and Electronic Systems Magazine,* vol. 26, no. 5, pp. 4-11, 2011.

[7] L. Hook and C. Tomlin, "Development of a “Where-to-Land” Decision Function for an Expert Piloting Systems (EPS) in Man-rated Autonomous Air Vehicles," NASA NARI, 2013.

[8] J. Rushby, "New challenges in certification for aircraft software," in *Proceedings of the ninth ACM international conference on Embedded software*, 2011.

[9] D. Reinhart, J. Knight and J. Rowanhill, "Current Practices in Constructing and Evaluating Assurances Cases with Applications to Aviation," NASA Technical Report, 2015.

[10] "Assurance Cases," [Online]. Available: http://www.sei.cmu.edu/dependability/tools/assurancecase/. [Accessed August 2015].

[11] *1st International Workshop on Assurance Cases for Software-Intensive Systems (ASSURE 2013).*

[12] R. Hawkins, I. Habli and T. Kelly, "The Principles of Software Safety Assurance," Boston, 2013.

[13] K. L. McMillan, "Circular Compositional Reasoning about Liveness," Cadence Berkeley Labs, , Berkeley, CA, 1999.

[14] G. Frehse, Z. Han and B. Krogh, "Assume-Guarantee Reasoning for Hybrid I/O Autonomata by Over-Approximation of Continuous Interaction," *Decision and Control 2004, CDC 43rd IEEE Conference,* vol. 1, 2004.

[15] M. Huth and M. Ryan, Logic in Computer Science, Modelling and Reasoning about Systems, Cambridge: Cambridge University Press, 2004.

[16] Photo by Jim Ross, "NASA Dryden Past Projects: Automatic Collision Avoidance Technology / Fighter Risk Reduction Project," 2013. [Online]. Available: http://www.nasa.gov/centers/dryden/research/ACAT_FRRP/.

BIOGRAPHY

Loyd R. Hook *received a Ph.D. from the University of Oklahoma in Electrical and Computer Engineering in 2012. He is currently an assistant professor at the University of Tulsa in the Electrical and Computer Engineering Department and director of the TU Vehicle Autonomy and Intelligence Lab (TU VAIL). Previously, he worked for NASA’s Armstrong Flight Research Center where he served as principle investigator and flight test engineer primarily pursuing projects investigating and implementing automatic and autonomous air vehicle systems. His current research focus is the development of safety assured autonomous vehicle systems.*

Matthew A Clark *is the Technical Area Lead for the verification and validation of autonomous control systems within the Autonomous Controls Branch, AFRL/RQQA. Mr. Clark started his career in the Air Force Research Lab in 1998 supporting large scale aircraft component thermal, acoustic, and static combined environment structural testing. In 2000, 2010 respectively he received his Bachelor’s and Master’s Degree in Electrical Engineering from Wright State University in Dayton, OH. From 2000 to 2005, Mr. Clark worked as an industrial power and control engineer at Delphi Automotive, in Warren Ohio. In 2005, Mr. Clark returned to AFRL as Technical Area Lead for the combined environment structural testing facility. In 2010, Mr. Clark served at the Air Force Material Command headquarters providing support for the test and evaluation infrastructure, strategic planning, and operational cyber security, receiving the Exemplary Civilian Service Award. In 2011 he returned to the Air Force Research Laboratory to work on the verification and validation of autonomous control systems and applications. His research interests include verifiable intelligent control systems and Run Time Assurance of intelligent systems.*

David Sizoo *earned both M.S. and B.S. degrees in Aerospace*

978-1-4673-7676-1/16/$31.00 ©2016 IEEE
Approved for Public Release Distribution Unlimited
CASE NUMBER 88ABW-2015-4093

Engineering from M.I.T. He has been an Experimental Test Pilot and Human Factors Specialist with the FAA for 6 years. Prior to joining the FAA, his 23 year career spanned work in both the military and civilian sectors. In the U.S. Air Force and at Gulfstream Aerospace he served as a Developmental Test Pilot on programs including the F-35 Joint Strike Fighter, F-16, and Gulfstream G-150. His passion is General Aviation flying and he is currently leading research to bring advanced technology and safety enhancements to the aviation community.

***Mark A. Skoog** works for NASA's Armstrong Flight Research Center as the Principle Investigator for their Automatic Systems Project Office which leads the Center's autonomy research. He also leads the Collision Avoidance Technical Stewardship Group for the Office of the Undersecretary of Defense for Personnel and Readiness. He graduated from California Polytechnic State University at San Luis Obispo. Over the past 34 years he has supported numerous NASA and the Air Force fighter and UAV research efforts as well as initial flight test of the B-2. Focus areas have included the integration of flight controls and avionics with high authority autopilots to automatically accomplish all phases of fighter combat missions. More recently, much of his career has been in the development of full vehicle autonomy and automatic collision avoidance systems, for both ground and air.*

***James Brady** received a B.S. in Aerospace Engineering from Wichita State University, a M.S. in Engineering from Kansas University, a MBA from Avila University and a Ph.D. from Ohio State University. He spent more than 25 years with Lucent Technologies Bell Laboratories where he supervised product engineering and system groups for military and space projects. In 2006 he joined the FAA as the Avionics and Electrical Systems Specialist in the Small Airplane Directorate*

978-1-4673-7676-1/16/$31.00 ©2016 IEEE
Approved for Public Release Distribution Unlimited
CASE NUMBER 88ABW-2015-4093