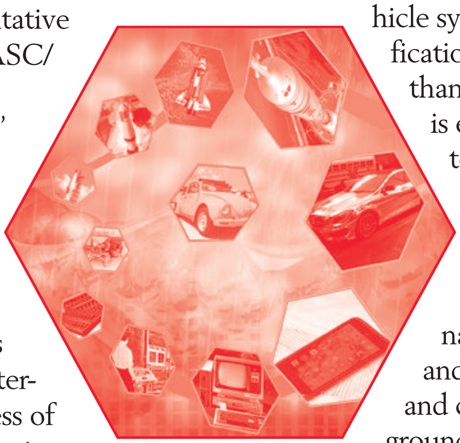
Applicability of MIL-HDBK-516B to Certifying Autonomous Decision-Making Air Vehicle Systems

by Dr. Alan Burkhead and Matthew Clark, MSEE
Wright-Patterson Air Force Base, Ohio

Airworthiness certification of military aircraft is accomplished by the developing military service. Air Force programs use the qualitative criteria outlined in MIL-HDBK-516B, "ASC/EN Airworthiness Certification Criteria Expanded Version of MIL-HDBK-516B" (September 26, 2005) to aid the development of program-specific airworthiness criteria. The generalized criteria in this document are used to construct the specific criterion and associated artifacts — evidence of compliance — as the basis for making an airworthiness determination. This paper describes the process of transitioning from qualitative to specific criteria, and then examines the applicability of the existing guidance in MIL-HDBK-516B to autonomous decision-making adaptive air vehicle systems. Recommendations are made for future research and criteria expansion. An integrated approach that uses the most promising emerging and existing design, analysis, and validation and verification techniques is proposed as a means to develop the artifacts for certification coverage of autonomous adaptive unmanned air vehicle systems.



Background

Air Force studies identified that unmanned air vehicle systems can be considered a viable alternate to accomplish a range of traditionally-manned missions [Ref. 1]. An Air Force Technology Horizons Studies by the Air Force Chief Scientist found that "….advanced technologies can allow the Air Force to gain the capability increases, manpower efficiencies, and cost reductions available through far greater use of autonomous systems in essentially all aspects of Air Force operations" [Ref. 2]. Since there is high-level interest and recognition in the worth of unmanned air vehicles that can function autonomously, it is a certainty that systems with increasing levels of decision autonomy will be developed.

All air system configurations, regardless of the amount of inherent autonomy, will undergo an airworthiness certification process before being released for Air Force use. This paper will look at the robustness of the current military airworthiness process for use on highly autonomous decision-making systems.

"Airworthiness" is an air vehicle-level attribute, and military guidance for airworthiness is focused at the air vehicle system level [Ref. 3]. Airworthiness certification considerations generally involve more than just the flying part of an air system. This is especially important for unmanned systems, which must be considered integrated systems consisting of elements such as the control station (ground or airborne); telemetry; launch and recovery equipment; and communications and navigation equipment, including ground and/or air equipment used for command and control of the vehicle, equipment on the ground and in the air used for communication with the chase aircraft, other members of the flight crew, observers, air traffic control (ATC) and other air vehicles in the same air space.

Determination of airworthiness for military air vehicles is accomplished using the guidance and criteria contained in the tri-service coordinated document MIL-HDBK-516B [Ref. 4]. This document defines airworthiness as, "The property of a particular air system configuration to safely attain, sustain and terminate flight in accordance with the approved usage and limits."

This paper will focus on MIL-HDBK-516B and, in the next few sections, will outline the process of going from the general guidance of MIL-HDBK-516B to airworthiness criteria tailored to a specific program.

MIL-HDBK-516B Purpose and Format

The purpose of the guidance in MIL-HDBK-516B, as stated in the document, is: *"This document establishes the airworthiness certification criteria to be used in the determination of airworthiness of all manned and unmanned, fixed and rotary wing air vehicle systems. It is a foundational document to be used by the system program manager, chief engineer, and contractors to define their air system's airworthiness certification basis. This handbook is for guidance only. The handbook cannot be cited as a requirement. If it is, the contractor does not have to comply."*

The purpose of MIL-HDBK-516B is the determination of airworthiness of all manned and unmanned, fixed and rotary wing air vehicle systems. This hardware-centric emphasis is reflected in the structure of the document. MIL-HDBK-516B contains certification criteria

Para #	Certification Criteria	Applicable? (Y/N)	Rationale for Non-Applicable Criteria	Standard	Method of Compliance (MOC)	Data Artifacts	Compliance? (Y/N)	Risk Assessment Level for Non-Compliances
1	2	3	4	5	6	7	8	9
#.#.#	Criteria Statement per MIL-HDBK-516 B Expanded	Identify those criteria applicable at the aircraft system level	Provide explanation for non-applicability of criteria	State the standard per MIL-HDBK-516B Expanded; Tailor as appropriate and provide justification;	State the MOC per MIL-HDBK-516B expanded; Tailor as appropriate and provide justification;	Verfication evidence	Identify if criteria and standard are fully met. A risk hazard assessment will be required for each unsatisfied criteria	Risk Assessment level

Figure 1 — TACC/MACC Compliance Matrix [Ref. 5].

that are grouped by a mixture of major aircraft systems and/or technology disciplines. These major headings are: systems engineering, structures, flight technology, propulsion and propulsion installations, air vehicle subsystems, crew systems, diagnostics systems, avionics, electrical system, electromagnetic environmental effects, system safety, computer resources, maintenance, armament/stores integration, and passenger safety and materials. Under each of these major headings are listed the certification criteria. Each criterion has associated with it a standard, compliance method and a listing of potentially applicable industry, military and FAA standards, handbooks or guidance documents appropriate for that criterion.

Developing a Tailored Airworthiness Certification Criteria/Modified Airworthiness Certification Criteria (TACC/MACC) from MIL-HDBK-516B

The guidance information contained in MIL-HDBK-516B cannot be directly used as airworthiness certification requirements. The information in MIL-HDBK-516B is only qualitative in nature and must be converted to program-specific requirements. This is accomplished by the program office when it creates what is called a Modified Airworthiness Certification Criteria (MACC) or a Tailored Airworthiness Certification Criteria (TACC) document. A TACC is used by a program building a new air vehicle, while the MACC is for a modification of an existing air vehicle. Both documents have the same format and consider the same core criteria. Program-unique criteria can be inserted into a TACC/MACC, but all the criteria in MIL-HDBK-516B have to be included in the TACC/MACC [Ref. 5].

A part of the TACC/MACC documentation is a description of the system configuration, including the airframe identifier, software build number, engine types and quantity, crew and passenger capabilities. This description includes any differences between configurations and how those configurations are identified, as well as any limitations, temporary restrictions and procedures that the operator must use and observe to safely operate the system. This section includes a reference to the risk hazard assessment required for any unsatisfied criteria and a listing of the non-compliances, with their associated risk(s) and mitigations.

The major part of the TACC/MACC is the Compliance Matrix. The format for this matrix is shown in Figure 1. Each criteria listed in MIL-HDBK-516B is evaluated to determine if it is appropriate for the program of interest. These criteria cannot be modified. But if only a portion of a criterion applies, and a portion does not apply, one should include the applicable portion in the certification basis and provide justification for the non-applicable portion. Rationale has to be supplied for any criteria or portion thereof that is judged not applicable. Program-unique criteria can be included in the TACC/MACC Compliance Matrix.

For each applicable criterion listed in the Compliance Matrix, tailored specific standards and a method of compliance for the program of interest must be developed. This is accomplished by tailoring (as necessary) the recommended standard from MIL-HDBK-516B. Also, the method of compliance (MOC) for each applicable criterion needs to be tailored appropriately for the program. This is accomplished by tailoring (as necessary) the recommended method of compliance from MIL-HDBK-516B. To help construct the standards and methods of compliance, MIL-HDBK-516B lists suggested sources, such as industry standards, DoD/military standards and FAA documents. The MOC should identify what specific tests, analysis methods and measures of merit will be used.

Airworthiness Bulletin (AWB-004A), uses the image of a high jumper [Ref. 6]. The criterion is analogous to an athlete in a track and field competition. To successfully perform a high jump, the athlete must jump over the bar without knocking it off its stand. This criterion cannot be changed. The standard is how high the bar is set. The bar, or standard, may be set at different heights depending on the athlete: male, female, or age. Similarly, for the same given airworthiness criterion, the standards for a fighter aircraft may be significantly different from that required for a tanker aircraft. The method of compliance is analogous to the execution technique the athlete uses to successfully complete the jump. Does the athlete use the “Fosbury Flop” or the “Scissors and Straddle” jumping technique?

MIL-HDBK-516B criteria are written in such a way that a simple “yes/no” answer is not adequate. These criteria are written in the form “Verify that....” In this form, the criterion asks if something has been studied, analyzed or demonstrated. This form of criterion enables — and almost demands — a dialogue between the project team and airworthiness certification authority subject matter experts (SME), who are independent of the program office. Adequacy of evidence to satisfy the term ”verify” is not fully defined in the handbook. The depth and width of what needs to be done to “verify” that the criteria is satisfied has to be determined between the program office and airworthiness authority for the program in question. This is consistent with the tailoring trend instituted in many military standards where rigid requirements that enveloped all possible conditions were replaced by more tailored requirements [Refs. 21 & 22].

The text in columns one and two of the Compliance Matrix is directly copied from MIL-HDBK-516B. In the third column, it is noted whether the criterion is applicable for the program, and in the fourth column, the rationale for this decision is given. The standard and method of compliance columns five and six start with their respective text copied from MIL-HDBK-516B for this criterion, which then can be tailored, added or modified as necessary.

Columns seven, eight and nine of the table are filled in as the planned compliance activities are completed. The first of these three columns lists all of the artifacts or evidence generated by the compliance method. A determination is made as to whether the planned compliance activity did, in fact, fully satisfy the MIL-HDBK-516B criteria and what residual risk level exists for this airworthiness issue. This is documented in columns eight and nine.

Using MIL-HDBK-516B to Certify Autonomous Decision-Making Air Systems

From an airworthiness perspective, a major impact of air vehicle autonomy is on the vehicle controls, communication, where decisions are made and the removal of equipment needed to support an onboard pilot. Removal of equipment reduces the complexity of the air vehicle, while the complexity of controls, communication and software subsystems increases.

Therefore, for the purposes of this paper, the focus will be on the software criteria of MIL-HDBK-516B. Software issues are scattered among major aircraft system headings such as flight technology, propulsion and propulsion installations, air vehicle subsystems, and computer resources. As part of the current planned revision to 516, the intent is to consolidate the majority of existing software criteria, along with any new criteria, into the computer resource section. This consolidation should not impact the essence of the following discussion.

Software-Related Criteria in MIL-HDBK-516B

The airworthiness certification criteria listed in MIL-HDBK-516B are flexible since they do not prescribe a process, but instead function much like a checklist of issues that a program has to show have been adequately addressed. Often, there is more than one way that particular issues can be addressed. The technology method selected by the program of interest to satisfy the criteria generally impacts the method of compliance, as well as the nature and form of the evidence of compliance. The artifacts from the method of compliance can be the result of specific engineering analyses done during system design, component tests, simulations, hardware/software audits, and open air test and evaluation (T&E) activities accomplished by the T&E community.

The airworthiness certification criteria for software in MIL-HDBK-516B can be categorized generally as:

- There are criteria on specific performance behavior of the system for which software is a key component.
- There are also criteria that address the nature/structure and pedigree of the software itself.

Each category of software-related criteria will be discussed separately later.

Software Performance Criteria

The first type of criteria has as its measure of merit the desired performance and behavior of the entire air system configuration related to the criterion of interest. These criteria include the integration of software into the air vehicle and the qualification of integrated hardware/software elements. These criteria are scattered throughout MIL-HDBK-516B in the various hardware-related sections. These are not identified as being software criterion in MIL-HDBK-516B, but rather criterion about a function or issue that needs to be verified. As a TACC/MACC is being generated from MIL-HDBK-516B for a specific program, the nature of the system being built has to be taken into account. Embedded software issues need to be made overt so that the method of compliance selected appropriately exercises these software elements.

Software Development Criteria

The second set of criteria are concerned with how the software was developed and the configuration of the hardware/software component of the entire air system configuration. These criteria type more closely line up with the issues and focus of DO-178B, as reflected by the fact that DO-178B is one of the suggested sources for MIL-HDBK-516B criteria standards and methods of compliance [Ref. 7].

(Note: MIL-HDBK-516B references DO-178B. This document has been revised to the "C" version, which is an essential update to the "B" version. The "C" version contains corrections of found errors and inconsistencies, along with new text to add clarity and consistency, and new supplements for tool qualification and specific technologies such as formal methods, object-oriented technology and model-based design and verification.)

Even though DO-178B/C is a suggested source for selecting activities or methodologies for tailoring the method of compliance, DO-178B/C by itself is not an adequate method of compliance for military applications [Ref. 7 & 8]. DO-178B/C was designed to be used within the civil certification environment. More specifically, DO-178B/C is part of a larger body of guidelines described in the Society of Automotive Engineers (SAE) ARP 4754, "Guidelines for Development of Civil Aircraft and Systems" document, which states, "The guidelines herein are directed toward systems that support aircraft-level functions and have failure modes with the potential to affect the safety of the aircraft" [Ref. 37]. This document guides a designer/validator through the process of designing, assessing risk and providing evidence for certification. Using these guidelines assists the developer in identifying the level of criticality, or risk of causing injury, loss of life or significant cost. The higher the criticality level, the more stringent/thorough the guidelines are in ensuring the software is sufficiently correct and has minimal error, and that the hardware has an acceptable reliability. Within this library of guidelines, DO-178B/C is the software quality document, documenting assurance steps that must be taken given a particular level of criticality. For example, Level A flight-critical software (i.e., the flight control computer) has the potential, if it fails, to cause the entire aircraft to lose control, potentially killing everyone on board. When using DO-178B/C outside of that environment, the context changes so that regulations and guidance that are assumed to be in place are no longer valid. At Level A criticality, DO-178B/C has 66 objectives that must be met. However, these objectives give limited insight as to why they are sufficient to ensure that a particular level of criticality/risk mitigation is achieved. Additionally, for military aircraft in certain operating conditions, such as in combat situations, risk may be assessed by different methods than those prescribed in the SAE guidelines. Different risks potentially result in different software design and verification objectives. But which objectives need to be changed? There is a need to evaluate and clearly define for the program of interest how the use of DO-178B/C would (or would not) apply when used within a non-civil certification process, such as the United States Air Force (USAF) Airworthiness Process.

> "Different risks potentially result in different software design and verification objectives. But which objectives need to be changed?"

An exception to following MIL-HDBK-516B for airworthiness certification criteria for a military air vehicle system is for commercial-derivative Air Force aircraft. The FAA-type certification is the preferred method of certifying the airworthiness of a commercial-derivative aircraft for Air Force operations. This is provided that the military usage is no more severe than the FAA certification flight envelop and usage environment [Ref. 5]. In these cases, the software certification criteria is highly likely to be essentially what is outlined by DO-178B/C guidance because the FAA recognizes DO-178B as a means, but not the only means, to seek FAA approval of airborne software [Refs. 9 and 10]. (Note: Reference 10 gives the FAA recognition of the "C" version of DO-178).

Addressing the Challenges in Certifying Software for Unmanned Military Air Vehicle Systems

McNeil, using his airworthiness certification experience at Redstone Arsenal, reported that for remotely controlled unmanned air vehicles, the MIL-HDBK-516B criteria is insufficient as a guide for doing airborne software certification. McNeil proposed additional certification criteria that should be added to MIL-HDBK-516B for unmanned remotely controlled air vehicle systems [Ref. 23]. These additional criteria do not address the additional complexity when the airborne software can autonomously make decisions.

Another source of guidance for unmanned military air vehicle systems is the North Atlantic Treaty Organization (NATO) Standardization Agreement (STANAG) 4671, "Unmanned Aerial Vehicle (UAV) Systems Airworthiness Requirements," which was specifically formulated for unmanned aircraft systems [Ref. 24]. STANAG 4671 points to RTCA/DO-178B for software assurance of these systems and, in its scope section, clearly states that it is not for:

> *Non-deterministic flight, in the sense that UAV flight profiles are not pre-determined or UAV actions are not predictable to the UAV crew,….*

Therefore, there still exists a clear need to address airworthiness certification issues for more advanced, autonomous decision-making systems.

MIL-HDBK-516B Applicability to Autonomous Decision-Making Air Vehicles

The response behavior of autonomous decision-making air vehicle systems can be different for the same environmental conditions. This type of behavior is the result of adapting to and learning how to handle previously encountered environmental conditions. This behavior presents an emerging challenge to airworthiness certification, since most current techniques assume that the behavior observed during the certification process will be the same and invariant throughout the actual usage.

Existing airworthiness certification methods are able to adequately certify autonomous decision-making air systems that use scripted scenarios. Scripted scenarios are response behaviors built into the software for failures or unusual environmental conditions that were anticipated by the designers. The decision making by the autonomous system is limited to deciding which certified script to implement.

Scripted systems with limited autonomy decision making can handle unanticipated situations by defaulting the decision to the pilot or vehicle controller, who is either on or in the loop. Manpower requirements and the increased capability pointed to in References 1 and 2 could be realized if the air vehicle system could handle unanticipated situations autonomously via real-time adaptation. The decision making is not dependent on a person in or on the loop. Such autonomous decision-making air systems for military applications would have to be certified by criteria from MIL-HDBK-516B. MIL-HDBK-516B has a few criteria that start to address certifying such software. Consider paragraph 11.1.4 of MIL-HDBK-516B:

> "Verify *(that)* the overall avionics system operates in a deterministic or bounded manner and limits latency of any time-critical data, including primary flight data, as needed to support all safety-critical functions."

The criteria cited above could be considered to be opening the door for certifying adaptive software, provided the adaptive behavior is bounded in some manner. Currently, the recommended standard in MIL-HDBK-516B for compliance methods for this criterion deals with latency limits and time-critical issues. But with the ability to tailor the standard and method of compliance when writing a TACC/MACC, autonomous adaptive air vehicle software could also be considered. Additional criteria will be required to fully handle the challenges in certifying autonomous decision-making software.

Addressing Challenges in Certifying Software for Adaptive Air Vehicle Systems

The bulk of the research looking at the problems and challenges in certifying adaptive software for airborne applications has been looking at DO-178B/C as the frame of reference for certification of such software [Refs. 16, 17, 19 and 20]. This is a natural reference point, since these investigators are concerned with airworthiness certification for civil air vehicles.

DO-178B/C asserts that its prescriptive process-based approach and the artifacts developed from it result in software that is suitable for the intended application. As pointed out by Holloway, there are many implicit assumptions on which DO-178B/C is based, one of which is the assumption that the software being certified safe does not change during usage [Refs. 14 and 15] (DO-178C requires that any change in software or software loading has to be re-examined for recertification). While DO-178C as currently structured does not address certification of adaptive software, it is not to say that some of its techniques could not be useful and valid for such software.

The researchers looking at the problems and challenges in certifying adaptive software considered the use of formal methods, high-fidelity simulations, model checkers like run-time monitors and/or real-time bound checkers, individually or in combinations, as potential methods for certification of autonomous adaptive software [Refs. 16, 17, 19 and 20]. In general, they found that each of these methods can address specific aspects of the certification challenge, but no one method can do it all.

Proposed Modifications to MIL-HDBK-516B to Handle Adaptive Decision-Making Software

As currently structured, MIL-HDBK-516B certification criteria give guidance for specific attributes to be verified. These criteria do not overtly give guidance as to when in the product development cycle this verification is to be accomplished. It has been proposed that the classic "V" used to describe the software development process be modified to have verification accomplished throughout the development cycle, as shown in Figures 2 and 3 [Ref. 25]. Figure 3 shows an integrated development and verification and validation (V&V) process in which V&V activities occur between each major development activity. The same type of tools used by the software developer should be used to verify the work at each step along the way.

Another modification to MIL-HDBK-516B is the regcognition that airworthiness should be thought of differently for adaptive autonomous air vehicle systems. Currently, "airworthiness" is defined as the ability of an air system configuration to safely attain, sustain and terminate flight in accordance with the approved usage and limits [Ref. 4]. What is meant by the term "safely" could be different for an autonomous adaptive air vehicle system than for a manned air vehicle system. For a manned system, this means the vehicle with a trained onboard pilot can attain, sustain and terminate flight in accordance with the approved usage and limits without causing damage to the vehicle or others. For an unmanned autonomous adaptive air vehicle system, airworthiness should take into account the decision-making ability of the system. For example, the ability of the manned air vehicle to not fly into a "keep out" zone is not normally considered part of the airworthiness certification. For an adaptive air vehicle system, it is highly likely that the ability of the system to avoid "keep out" zones (unless commanded to do so) could be part of the airworthiness determination. This expanded scope for airworthiness determination could be handled by the addition of certification criteria to MIL-HDBK-516B or by having the guidance in 516 closely linked to another guidance document for the decision-making attribute of an adaptive unmanned air vehicle system.

Our vision, graphically depicted in Figure 4, concentrates on compartmentalizing the self-governing autonomous decision making within systems through formally specified architectures and requirements, enforcing (either at design time or at run time) "assume-guarantee" contracts between the interfaces of these components. From these component contracts, multiple paths of verification and validation can be realized to provide a convincing (formally provable) argument of safety and security that can be reused, composed and analyzed rapidly, enabling the transition of the next generation of autonomous systems capability.

For these systems of systems, a new set of arguments for safety is needed, arguments that are formally (mathematically) documented,

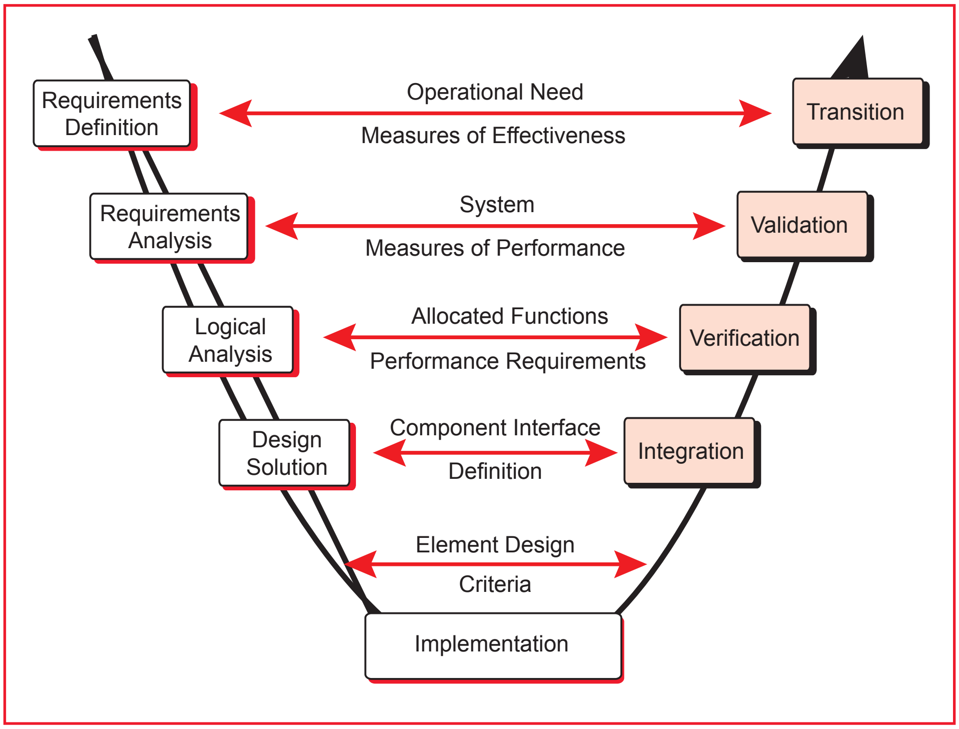


Figure 2 — Classic "V" Development Cycle.

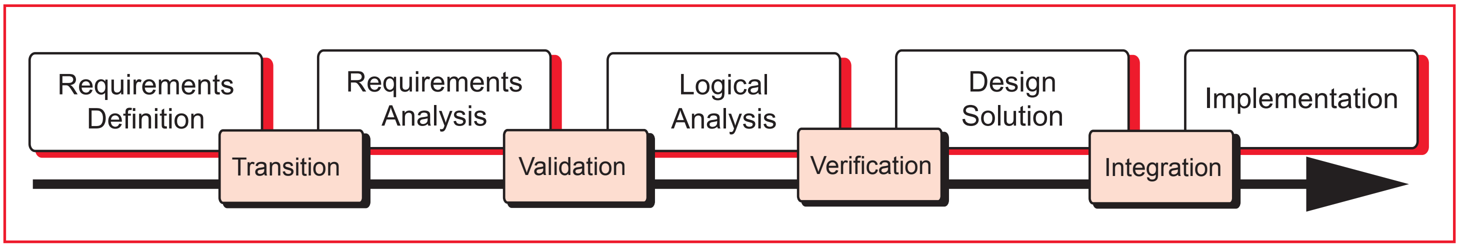


Figure 3 — Integrated Development and V&V Cycles [Ref. 25].

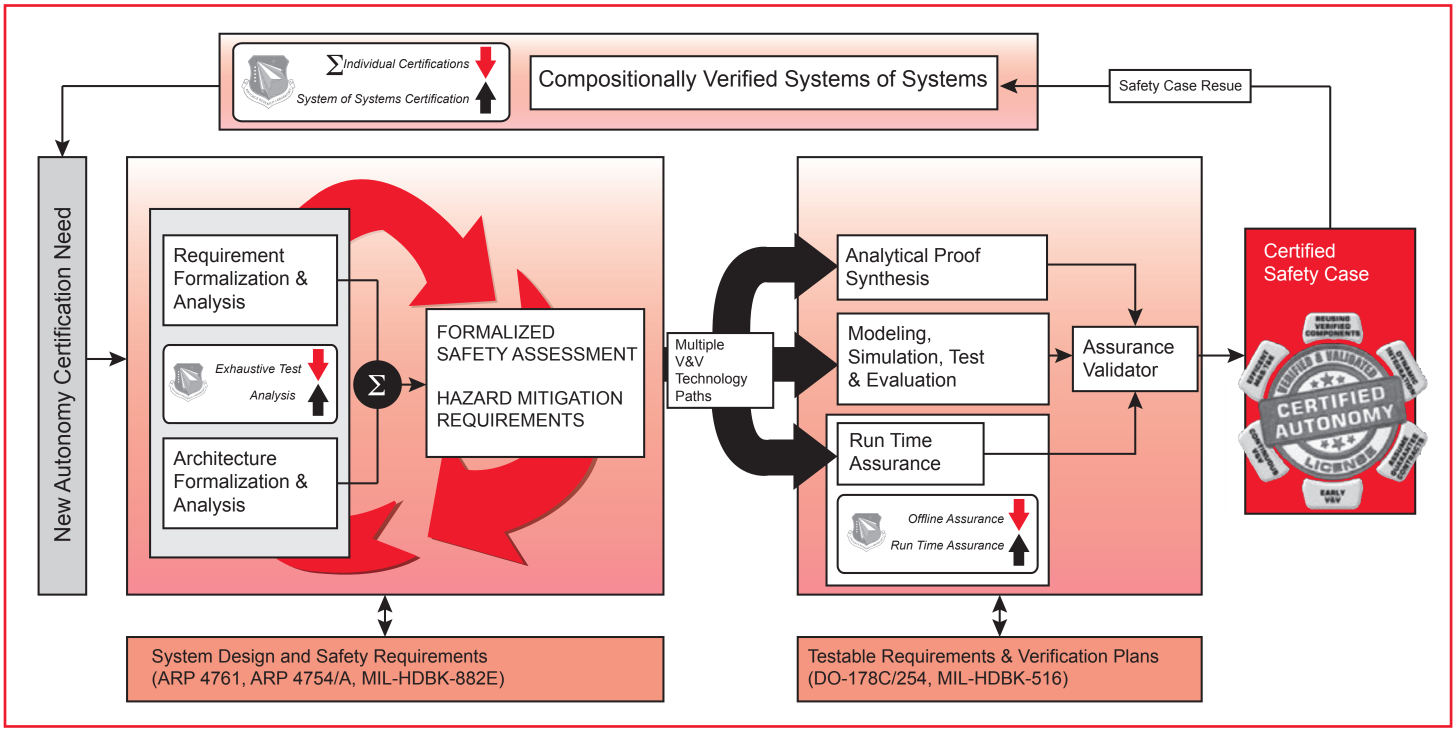

∑Individual Certifications
System of Systems Certification
Compositionally Verified Systems of Systems
Safety Case Resue
New Autonomy Certification Need
Requirement Formalization & Analysis
Exhaustive Test
Analysis
Architecture Formalization & Analysis
Σ
FORMALIZED SAFETY ASSESSMENT
HAZARD MITIGATION REQUIREMENTS
Multiple V&V Technology Paths
Analytical Proof Synthesis
Modeling, Simulation, Test & Evaluation
Run Time Assurance
Offline Assurance
Run Time Assurance
Assurance Validator
Certified Safety Case
REUSING VERIFIED COMPONENTS
VERIFIED & VALIDATED
CERTIFIED AUTONOMY
LICENSE
EFFICIENT MAS T&E
DYNAMIC INTEGRATION
CONTINUOUS V&V
ASSUME GUARANTEE CONTRACTS
EARLY V&V
System Design and Safety Requirements (ARP 4761, ARP 4754/A, MIL-HDBK-882E)
Testable Requirements & Verification Plans (DO-178C/254, MIL-HDBK-516)

Figure 4 — Trust and Certification of Autonomous Systems Process.

analyzable, provable and reusable. The technology that supports these new arguments must eliminate excessive certification, as heterogeneous machines are combined during operation. We must be able to enforce guarantees at the subsystem or system level to prevent unintended emergent behavior as systems are composed into systems of systems. Also, this technology must allow one element of a fractionated capability to be modified while minimizing the re-certification requirements of other components. Our goal is to provide a reusable and composable set of comprehensive and defensible arguments that a system of systems is acceptably safe to operate in a particular context.

The Air Force Research Laboratory, Aerospace Systems Directorate, Power and Control Division, AFRL/RQQ, in conjunction with other organizations, is researching the development of pieces of the Trust and Certification of Autonomous systems process shown in Figure 4. The goal of this integrated approach is to increase trust in the next generation of highly complex and autonomous systems, providing new arguments for flight safety and security, and closing future gaps in current test and evaluation methods.

- **Formal Design and Analysis of Requirements and Architectures**
  - o The focus of this work is to create a mathematically rigorous framework to compartmentalize and guarantee interactions between components and functions within a system. Current work leverages assume guarantee contracts at the architecture abstraction level between subsystems and systems and between systems and systems of systems to ensure that requirements are satisfied at all levels of interaction [Refs. 26 and 27].
- **System Safety Analysis and Design**
  - o The focus of this work is to incorporate system safety and analysis techniques within a framework that enables early analysis of failure modes [Ref. 28], alternate safety analysis techniques [Ref. 29], and specific and efficient tests automatically generated from designs [Refs. 30 and 31].
- **Multiple Paths to Verification Through…**
  - o Run-time Assurances – Reducing the reliance on offline tests by increasing the reliance on real-time monitoring and failsafe reversionary backup systems [Ref. 32].
  - o Progressive sequential tests – Reducing the reliance on isolated subsystem component testing by increasing the reliance on reusable, composable, progressive modeling, simulation, test and evaluation.
  - o Formal proofs – Reducing the reliance on exhaustive testing through early analysis, and correction by construction design [Ref. 33].
- **Composable and reusable assurance cases based on multiple paths of evidence**
  - o Systems of systems re-certification through the reuse of assurance cases as a basis of evidence of safety and security [Ref. 34-36].

Conclusion

MIL-HDBK-516B is a guidance document from which one can construct a Modified Airworthiness Certification Criteria (MACC) or a Tailored Airworthiness Certification Criteria document (TACC) for the accomplishment of airworthiness determination of a military air vehicle system. The guidance in MIL-HDBK-156B needs to include additional guidance for autonomous adaptive unmanned air vehicle systems. Researchers have investigated several different emerging techniques that hold promise in that they could individually address some of the certification challenges for such systems. An integrated approach that uses the most promising emerging and existing design, analysis, and Validation & Verification techniques has been proposed so there will be no gaps in the certification coverage for autonomous adaptive unmanned air vehicle systems.

About the Authors

Dr. Alan Burkhard received his Ph.D. in engineering mechanics from the University of Wisconsin. He has more than 33 years of experience as an Air Force Research Laboratory researcher working on the development of testing methods and techniques for all types of mechanical, electrical and avionics subsystems. His experience includes being the chief engineer and team leader of a joint Navy and Air Force program for the development of integrated subsystems technology (JIST) for the Joint Strike Fighter. He currently is a Booz Allen Hamilton consultant to the Air Force Research Laboratory working on the development of verification and validation approaches for safety of flight software. He has authored and/or co-authored more than 20 technical papers and reports on test methods and criteria development.

Matthew A Clark, MSEE is the technical area lead for the verification and validation of autonomous control systems within the Autonomous Controls Branch, Power and Control Division, Aerospace Systems Directorate, Air Force Research Laboratory (AFRL/RQQA). He leads a team of 10 in-house researchers in the design, analysis, verification and validation of autonomous control systems. He is also the primary subject matter expert for the AFRL Autonomy Test and Evaluation, Verification and Validation (TEVV). Additionally, he is the co-leader of the Assistant to the Secretary of Defense, Research and Evaluation, Autonomy Community of Interest, Test and Evaluation. He started his career in the Air Force Research Lab in 1995 supporting large-scale aircraft component thermal, acoustic and static combined environment structural testing. In 2000 and 2010, respectively, he received his bachelor's and master's Degree in electrical engineering at Wright State University with a concentration on electrical power and intelligent control systems. From 2000 to 2005, he worked as an industrial power and control engineer at Delphi Automotive in Warren, Ohio. In 2005, he returned to AFRL as technical area lead for the combined environment structural testing facility. In 2010, he 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 power and control systems and run time assurance of intelligent systems. ⬢

References

1. *United States Air Force Unmanned Aircraft Systems Flight Plan 2009-2047*, Headquarters, United States Air Force, Washington, D.C., May 18, 2009, http://fas.org/irp/program/collect/uas_2009.pdf.
2. Office of the U.S. Air Force Chief Scientist. *Report on Technology Horizons, A Vision for Air Force Science & Technology During 2010-2030, Vol. 1*, AF/ST-TR-10-01, May 15, 2010.
3. Air Force Departmental Standardization Office (SAF/AQRE), "Developmental Engineering USAF Airworthiness," *Air Force Instruction 62-601*, June 11, 2010.
4. "ASC/EN Airworthiness Certification Criteria Expanded Version of MIL-HDBK-516B," September 26, 2005, http://www.wpafb.af.mil/shared/media/document/AFD-120319-032.pdf
5. United States Air Force (USAF). "TACC/MACC Construction & Format," *Airworthiness Bulletin (AWB-005)*, September 27, 2010.
6. United States Air Force (USAF). "Certification Basis," Airworthiness Bulletin (AWB-004A), June 17, 2011.
7. Radio Technical Commission for Aeronautics (RTCA). "Software Considerations in Airborne Systems and Equipment Certification," DO-178B, 1992.
8. Radio Technical Commission for Aeronautics (RTCA). "Software Considerations in Airborne Systems and Equipment Certification," DO-178C, 2011.
9. Federal Aviation Administration (FAA) Advisory Circular. "Alternatives to RTCA/DO-178B for Software in Airborne Systems and Equipment," AC-20-171, January 19, 2011.
10. FAA Advisory Circular. "Airborne Software Assurance," AC-20-115C, July 19, 2013.
11. Grimsley, Frank. "USAF Task Force On UAS Airspace Integration," Presentation at 2013 Ohio UAS Conference, Dayton, April 23-25, 2013.

12. Rusby, J. “A Safety-Case Approach for Certifying Adaptive Systems,” AIAA Infotech Aerospace Conference, AIAA Paper No. 2009-1992, Seattle, Washington, April 2009.
13. Hawkins, Richard, Ibrahim Habli, Tim Kelly and John McDermid. “Assurance Cases and Prescriptive Software Safety Certification: A Comparative Study,” *Safety Science*, Vol. 59, pages 55-71, 2013.
14. Holloway, C.M. “Towards Understanding the DO-178C/ED-12C Assurance Case,” 7th Institution of Engineering and Technology (IET) International Conference on System Safety, Incorporating the Cyber Security Conference, Edinburgh, 2012.
15. Holloway, C.M. “Making the Implicit Explicit: Towards An Assurance Case for DO-178C,” 31st International System Safety Conference, NASA Report # 20140002745, Boston, Massachusetts, August 12-16, 2013.
16. Rushby, John. “How Do we Certify for The Unexpected,” AIAA Guidance, Navigation and Control Conference and Exhibit, AIAA paper No. 2008-6799, Honolulu, Hawaii, August 18-21, 2008.
17. Rushby, John. “Just-In-Time Certification,” 12th IEEE international Conference on Engineering Complex Computer Systems (ICEEECCS), pp. 15-24, Auckland, New Zealand, June 2007.
18. Sun, Linling, et al. “ Do Safety Cases Have a Role in Aircraft Certification?” 2nd International Symposium on Aircraft Airworthiness (ISAA 2011), http://www.sciencedirect.com/science/article/pii/S1877705811027202
19. Jacklin, Stephan. “Closing the Certification Gaps in Adaptive Flight Control Software,” AIAA Guidance, Navigation and Control Conference and Exhibit, AIAA paper No. 2008-6988, Honolulu, Hawaii, August 18-21, 2008.
20. Cortellessa, Vittorio, et al. “Certifying Adaptive Flight Control Software,” Proceedings of the 2nd International Software Assurance Certification Conference, (ISACC), Washington, D.C., 2000.
21. Bello, Michael. “MIL-Prime – The Performance Oriented Approach,” IEEE 1990 National Aerospace and Electronics Conference (NAECON), Dayton, Ohio, Vol.3, pp. 987 – 994, May 1990.
22. “Specification & Standards – A New Way of Doing Business,” Memorandum from the Secretary of Defense to Various Military Departments,” Washington, D.C., June 1994.
23. McNeil, Josh, et al. “Practical Software Airworthiness/Safety and Computer Resources Criteria for Airworthiness Qualification of Military Unmanned Aircraft Systems,” *Journal of System Safety*, Vol. 48, No. 3, May-June 2011.
24. “Unmanned Aerial Vehicles Systems Airworthiness Requirements (USAR),” NATO STANAG 4671 (Edition 1), September 2009, http://www.nato.int/docu/stanag/4671/4671_ed1_e.pdf
25. Clark, M. “Test and Evaluation, Verification and Validation of Autonomous Systems From AFRL/RQ to DoD,” Safe & Secure Systems and Software Symposium (S5), Air Force Research Laboratory (AFRL), Dayton, Ohio, 2014, http://www.mys5.org/Proceedings/2014/Day_1_S5_2014/2014-S5-Day1-02_Clark.pdf
26. Whalen, M., A. Gacek, D. Cofer, A. Murugesan, M. Heimdahl and S. Rayadurgam. “Your ‘What’ is My ‘How’: Iteration and Hierarchy in System Design,” *Software*, Institute of Electrical and Electronics Engineers (IEEE), Vol. 30, No. 2, pp. 54-60, March 2013.
27. De Alfaro, Luca, and Thomas A. Henzinger. “Interface Theories for Component-Based Design,” *Embedded Software*. Springer Berlin Heidelberg, 2001.
28. Joshi, Anjali, et al. “Model-Based Safety Analysis.” University of Minnesota, Minneapolis, Minnesota, Rockwell Collins, Inc., Cedar Rapids, Iowa, NASA/CR-2006-213953, Langley Research Center, 2006.
29. Leveson, Nancy. *Engineering A Safer World: Systems Thinking Applied to Safety*, MIT Press, 2011.
30. Joshi, Anjali, Pam Binns and Steve Vestal. “Automatic Generation of Fault Trees from AADL Models.” DSN 2007 Workshop on Architecting Dependable Systems, June 2007.
31. Ammann, P.E, P.E. Black, and W. Majurski. “Using Model Checking to Generate Tests from Specifications,” *Proceedings of the 2nd International Conference on Formal Engineering Methods*, pp. 46-54, 1998.
32. Clark, M., X. Koutsoukos, R. Kumar, I. Lee, G. Pappas, L. Pike, J. Porter and O. Sokolsky. “A Study on Run Time Assurance for Complex Cyber Physical Systems,” Technical report, http://www.dtic.mil/docs/citations/ADA585474, Wright-Patterson Air Force Base (WPAFB), 2013.
33. Clarke, E. and J. Wing. “Formal Methods: State of the Art and Future Directions.” ACM Computing Surveys (CSUR), Vol. 28, No. 4: pp. 626-643, 1996.
34. Kelly, T.P. “Arguing Safety — A Systematic Approach to Safety Case Management,” Ph.D. dissertation, University of York, 1999.
35. Graydon, Patrick, et al. “Arguing Conformance.” *Software*, IEEE, Vol. 29, No. 3, pp. 50-57, 2012.
36. Cobleigh, Jamieson M., Dimitra Giannakopoulou, and Corina S. Păsăreanu. “Learning Assumptions for Compositional Verification,” *Tools and Algorithms for the Construction and Analysis of Systems*, pp. 331-346, Springer Berlin Heidelberg, 2003.
37. Radio Technical Commission for Aeronautics (RTCA). “Guidelines for Development of Civil Aircraft and Systems,” Aerospace Recommended Practice (ARP) 4754, 2012.