

DOT/FAA/AR-09/37

Air Traffic Organization
NextGen & Operations Planning
Office of Research and
Technology Development
Washington, DC 20591

Commercial Off-the-Shelf Validation Criteria

July 2010

Final Report

This document is available to the U.S. public through the National Technical Information Services (NTIS), Springfield, Virginia 22161.

This document is also available from the Federal Aviation Administration William J. Hughes Technical Center at actlibrary.tc.faa.gov.



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 United States Government assumes no liability for the contents or use thereof. The United States Government does not endorse products or manufacturers. Trade or manufacturer's names appear herein solely because they are considered essential to the objective of this report. This document does not constitute FAA certification policy. Consult your local FAA aircraft certification office 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).

1. Report No. DOT/FAA/AR-09/37	2. Government Accession No.	3. Recipient's Catalog No.	
4. Title and Subtitle COMMERCIAL OFF-THE-SHELF VALIDATION CRITERIA		5. Report Date July 2010	
		6. Performing Organization Code	
7. Author(s) R. Robinson		8. Performing Organization Report No.	
9. Performing Organization Name and Address Goodrich Sensors and Integrated Systems 100 Pantan Road Vergennes, VT 05491		10. Work Unit No. (TRAVIS)	
		11. Contract or Grant No. DTFACT-06-R-00002	
12. Sponsoring Agency Name and Address U.S. Department of Transportation Federal Aviation Administration Air Traffic Organization NextGen & Operations Planning Office of Research and Technology Development Washington, DC 20591		13. Type of Report and Period Covered Final Report March 2006 – May 2008	
		14. Sponsoring Agency Code ASW-100	
15. Supplementary Notes The Federal Aviation Administration Airport and Aircraft Safety R&D Division technical monitor was Dr. Felix Abali.			
16. Abstract <p>This report presents a summary of the regulatory background for addressing the issue of validating a Health and Usage Monitoring System (HUMS) Ground Station that incorporates and/or relies on commercial off-the-shelf (COTS) components. It provides guidance on the establishment of a service history program, with specific emphasis on the roles and responsibilities contributed by operators, original equipment manufacturers, and HUMS equipment vendors. A process for gathering indirect evidence suitable for use during validation of the system is examined in greater detail. The technique of multiple-dissimilar software validation is explored, with emphasis on using existing collected data to establish a method that is both compliant with the existing validation guidelines and can potentially save significant cost compared to typical methods that rely on redundant or parallel processing for a period of time. Research conclusions are provided, as are opportunities for further study regarding the incorporation of COTS components.</p>			
17. Key Words Software validation, Commercial off-the-shelf		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 32	22. Price

TABLE OF CONTENTS

	Page
EXECUTIVE SUMMARY	ix
1. INTRODUCTION	1
1.1 Purpose	1
1.2 Background	1
1.3 Related Documents	1
2. DISCUSSION	2
3. The COTS Validation Criteria	3
3.1 Reglulatory Requirements	3
3.1.1 DO-178B—Multiple-Version Dissimilar Software Verification	4
3.1.2 AC 29-2C, Section MG-15	4
3.2 Service History	10
3.2.1 Operators	10
3.2.2 The OEMs	11
3.2.3 Vendors	12
3.2.4 Guidelines for Establishing a Service History Program	13
3.3 Process for Gathering Direct and/or Indirect Evidence	14
3.3.1 Collecting Data	14
3.3.2 Collected Data	15
3.4 Independent Verification Means for the COTS Portion Under Study	16
3.4.1 Structural Usage Computation	16
3.4.2 Multiple-Dissimilar Software	16
3.4.3 Verification Using Dissimilar Software	20
3.4.4 Verification Results	20
3.4.5 Verification Conclusions	21

3.5	Opportunities for Further Study	22
3.5.1	Development Guidelines for COTS	22
3.5.2	Operational Guidelines for COTS	23
4.	CONCLUSIONS	23
5.	REFERENCES	23

LIST OF FIGURES

Figure		Page
1	Damage Distribution	19

LIST OF TABLES

Table		Page
1	Partitions Used for Damage Factors	19
2	Detailed Verification Results	21

LIST OF ACRONYMS

AC	Advisory Circular
CFR	Code of Federal Regulations
COTS	Commercial off-the-shelf
FAA	Federal Aviation Administration
GBE	Ground-based equipment
GBS	Ground-based system
GSS	Ground support station
HUMS	Health and Usage Monitoring System
ICA	Instructions for Continued Airworthiness
JAR	Joint Aviation Requirements
MG	Miscellaneous guidance
OBS	Onboard system
OEM	Original equipment manufacturer

EXECUTIVE SUMMARY

The inclusion of commercial off-the-shelf (COTS) components in the Health and Usage Monitoring System (HUMS) Ground Stations is subject to specific regulatory requirements that extend beyond those covered in RTCA DO-178B and for which the Federal Aviation Administration has issued an Advisory Circular (AC 29-2C, Section MG-15).

This report provides an overview of the regulatory background covering the issue of validating a HUMS Ground Station that incorporates COTS components; explores the issues related to COTS during the three phases of implementation outlined in the regulations (HUMS Installation, Credit Validation, and Instructions for Continued Airworthiness); and presents a specific variation of the multiple dissimilar software technique, which could be used as a method of establishing the viability and acceptability of the incorporation of COTS into the Ground Station portion of an overall for-credit HUMS.

Specific guidance to establish of a service history program is provided, which focuses on the roles and responsibilities of three major parties: operators, original equipment manufacturers, and HUMS vendors. The process of gathering direct and/or indirect evidence of HUMS validation was examined, with specific emphasis on using existing collected data as the input to a multiple-dissimilar software verification technique designed to assess the impact of COTS in the resulting system.

Details of this validation technique are provided as explored during the practical implementation of this approach taken during the research, including the results of the comparison and guidance on establishing a similar approach for HUMS credit validation. Suggested further study topics related to the inclusion of COTS in a HUMS Ground Station are also provided.

1. INTRODUCTION.

1.1 PURPOSE.

This report documents processes and specific techniques that can be used to establish the acceptability of a Health and Usage Monitoring System (HUMS) Ground Station, including commercial off-the-shelf (COTS) hardware and software, using the guidance provided in Advisory Circular (AC) 29-2C, Section MG-15. This process was developed over the course of a research program aimed at providing additional assistance to manufacturers seeking certification of their HUMS equipment.

1.2 BACKGROUND.

HUMSs are increasingly finding acceptance in the rotorcraft community. From their inception in the 1990s as little more than ruggedized instrumentation packages temporarily mounted as data collection equipment for airframes that were suspected of generating abnormal vibrations or as a stop-gap measure to warn of incipient mechanical or structural failure, these systems have continually evolved into more sophisticated avionics-level equipment capable of continuous usage and health monitoring of rotorcraft systems throughout their lifetime.

As this class of avionics has advanced, so too has the need to ensure that the equipment, techniques, algorithms, and data collection procedures employed by HUMS follow the regulatory and safety guidance already established for equivalent classes of avionics systems that contribute to the continued safe operation of the rotorcraft.

However, in addition to the airborne component of a HUMS, this class of avionics also generally includes additional, nonairborne components that allow for the efficient processing of information generated by the HUMS, and the efficient notification and handling of the data generated by these systems. Unlike more traditional avionics systems, the data generated by a HUMS is not only interpreted by the flight crew, but is also used postflight as a means to assess the overall health of the rotorcraft; it also contributes information to the maintenance program for that rotorcraft to help determine the appropriate time for component overhaul, replacement, and retirement. In this context, validation criteria established to demonstrate the appropriate reliability of the system extends not only to the airborne component, but can also be required to support the ground processing and subsequent handling of HUMS data outside the airborne equipment itself.

1.3 RELATED DOCUMENTS.

This document is one in a series generated during the course of this research. A HUMS functional assessment document was produced at the beginning of the program that summarizes the overall capability and architectural design considerations of the HUMS used during this research. A key feature of that system is its design, which incorporates a multiple-partitioning scheme designed to recognize and take advantage of the RTCA DO-178B levels of criticality that can be assigned to an overall system such as HUMS. By incorporating processing in the onboard system for those tasks deemed a higher criticality level (up to Level B), according to the

aircraft's System Safety Assessment, and performing only those functions assigned to a lower criticality level (Level D) in the ground support station (GSS) component, compliance with the certification criteria in AC 29-2C, Section MG-15, is more likely to be achieved, and more appropriately addresses the issues involved with extensive use of COTS typically found in the GSS environment.

A HUMS COTS GSS process guidance report was generated as a result of this research. This report provides specific guidance to assist organizations interested in meeting the criteria found in AC-29-2C, Section MG-15, and focuses on the operational nature of a deployed HUMS system that incorporates COTS components. This includes the establishment of a service history program, guidelines for establishing a process of indirect and/or direct evidence to correlate HUMS outputs and actual component lifing issues, and guidelines for use by the operator of a HUMS-equipped aircraft to remain compliant with the Federal Aviation Administration (FAA) Instructions for Continued Airworthiness (ICA) program.

2. DISCUSSION.

The inclusion of COTS software in any system that falls under the scrutiny of DO-178B has traditionally been a cause of concern, not only on the part of the developer of the product, but also on the part of the regulatory agencies responsible for its certification. Unlike application-specific software development and the very type of software for which the regulatory guidelines were written and for which access to the software development process, source code, verification methods, and complete development environment and life cycle is not only assumed but must be proven—COTS software arrives in the end product without any sort of pedigree. By its very nature, COTS software presents itself as a “black box” to the rest of the system. Its internal architecture, design, coding standards, error handling, robustness, and performance are virtually unknown, and its functionality can only be characterized by external means. Since the regulatory guidance's fundamental approach is to use development process controls to establish a minimum level of software reliability in the resulting system, this presents a significant roadblock to accepting the inclusion of COTS software anywhere in the system.

However, the high degree of integration and sophistication expected by modern aviation software systems has continued to fuel the trend to incorporate signification functionality in those systems. Developers often rely on the built-in functionality included in COTS software to provide a higher degree of integration and commonality and to reduce development costs and time-to-market. In addition, many real-time operating systems are available to provide support for advanced features (such as tasking and partitioning) that require the inclusion of COTS run-time systems to enable these features within the application-specific software. Given this trend, it is becoming more difficult to identify aviation-related software systems that do not have some element of COTS software in the run-time system, either to provide additional functionality for the system or as a means of providing native operating system support directly to the application itself.

It must be recognized that, by its very nature, DO-178B guidelines are applicable to airborne systems and equipment certification. Systems that directly control or influence the continued safe operation of an aircraft in flight must be designed and verified according to the rigorous

safety criteria contained within those guidelines. Traditionally, airborne systems performed their functions in an autonomous manner using signals and data obtained in real time, and produced their outputs (control, indication, warning, alarm, etc.) in real time as well. By restricting the functionality of such systems to very specific domains (such as fuel gauging, avionics, and flight instrumentation), designing ‘brick wall’ systems to prevent one isolated failure from propagating into multiple systems, and including secondary and tertiary “backup” systems (which can be used in the event of a primary system failure), isolation and redundancy have resulted in the ability to safely operate the aircraft even during one or more primary system failures.

By contrast, HUMS typically rely not only on an airborne portion (usually responsible for the collection of component health and aircraft operating environment data), but also on at least one ground-based component to provide the required amount of data storage, usage computation and storage, component health visualization, health trending information, and interfaces to external systems that enable operations and maintenance personnel to work more efficiently in an automated maintenance environment. Also, in contrast to the application-specific dedicated HUMS airborne equipment, the ground station portion of a HUMS is typically required to be hosted on an industry-standard, compatible personal computer workstation that integrates well into the office environment of the operations and maintenance organizations. As such, this workstation may be loaded with non-HUMS, application-specific software in addition to the HUMS ground station application.

This report targets the ground station workstation environment. In recognition of the differing operational environment of HUMS airborne and ground station systems, the FAA has issued AC 29-2C, Section MG-15, Airworthiness Approval of Rotorcraft Health and Usage Monitoring Systems (HUMS). This report is aimed specifically and directly at the unique issues involved with approval of HUMS systems, which are comprised of both airborne and ground elements.

This research involves a particular approach aimed at using the technique of multiple-dissimilar software (one of the alternative certification methods found in DO-178B) in conjunction with a special case of controlled introduction into service to evaluate the suitability of the COTS included in multiple versions of ground station software. The goals are to examine two unique systems built as multiple-dissimilar software, run actual HUMS data through the two systems, and detect any differences in the systems that would be attributable to the COTS elements of two systems. If sufficient predictability in the outcome of data can be developed, such a technique would support the ability to use this method for COTS validation, which would be used to support the integration of the system into an operational HUMS program to be used for credit applications.

3. THE COTS VALIDATION CRITERIA.

3.1 REGULATORY REQUIREMENTS.

The primary regulatory guidance driving this effort is found in AC 29-2C, entitled “Certification of Transport Category Rotorcraft.” Chapter 3, “Airworthiness Standards Transport Category Rotorcraft,” contains a Miscellaneous Guidance (MG) Section, AC 29 MG-15, entitled “Airworthiness Approval of Rotorcraft Health Usage Monitoring Systems (HUMS),” which

provides, as stated in the *Purpose* section, “...guidance to achieve airworthiness approval for rotorcraft Health and Usage Monitoring System (HUMS) installation, credit validation, and Instructions for Continued Airworthiness (ICA) for the full range of HUMS applications.” [1]

AC 29-2C MG-15 additionally references many parts of the Code of Federal Regulations (CFR), the corresponding European Joint Aviation Requirements (JAR), and the latest revisions of DO-160/ED-14, DO-178/ED-12, and SAE documents ARP 4754 and ARP 4761.

The primary additional reference applicable to this research is found in DO-178B, Section 12.3, “Alternative Methods,” and subsequent subparagraphs, which provide a launching point for “Additional Considerations” when evaluating airborne systems and equipment certification from a systems and software certification standpoint.

3.1.1 DO-178B—Multiple-Version Dissimilar Software Verification.

DO-178B provides a broad set of guidelines concerning the software verification process when evaluating multiple-version dissimilar software. By definition, this is “a set of two or more programs developed separately to satisfy the same functional requirements. Errors specific to one of the versions are detected by comparison of the multiple outputs.” [2] This verification methodology differs from traditional “white-box” testing in that the credibility of the output of the unit under test software is evaluated in comparison to another separate software result, rather than via explicit internal testing criteria (which forms the bulk of the guidance found in previous sections in this document). As such, it holds great promise as a means of evaluating and verifying software that does not lend itself to internal, or “white-box,” examination. This aspect of the technique makes it a good match for the verification and validation of COTS software portions of a HUMS.

3.1.2 AC 29-2C, Section MG-15.

One of the potential criticisms of applying DO-178B to a HUMS application is that it addresses only “airborne systems and equipment certification.” Since a HUMS application includes both airborne and ground-based equipment, the applicability of the document in dealing with the ground-based components of the system is questionable. If DO-178B is construed as applying only to airborne equipment, then no portion of any ground-based equipment would need to be considered with regard to software reliability, software partitioning, system safety, or the effects of unintended or incorrect operation in the context of the entire aircraft system. However, if DO-178B is construed as applying to all aspects of a HUMS system, then it is likely that not only would the ground-based portion of the system be subject to conditions found in the document, but potentially any system that communicates with the ground-based HUMS portion also might be called into question. A typical discourse on software functionality and system safety involving HUMS processing usually suggests that any part of any automated system that might inject erroneous data or cause the system to generate an error with respect to the health and/or usage (life) of a critical component on the aircraft could result in serious or catastrophic damage to life and property. This line of reasoning could pull any number of software systems under the scrutiny of DO-178B, including those that were clearly never intended to be covered originally.

Fortunately, the FAA has been proactive in defining the scope of the regulatory guidance as it applies specifically to HUMS by specifying this applicability in AC 29-2C, Section MG-15, and in defining the guidance as limiting itself to three specific areas:

1. HUMS Installation
2. Credit Validation
3. Instructions for Continued Airworthiness

The impact of COTS within each of the three areas is discussed below.

3.1.2.1 Ground-Based Equipment Installation and the Role of COTS.

Following is a discussion of the various aspects of ground-based equipment (GBE) installation and the role of COTS as provided in the subsections of AC 29-2C, Section MG-15.

3.1.2.1.1 Independent Verification.

The AC states that service history alone is not sufficient to satisfy compliance to integrity requirements. In addition to service history, an independent means of verifying the results of ground station processing is required. Further, the independent means may be discontinued (with the certifying Authority's agreement) once "significant quantities of the processed data consistently agree with the verifying means." [1]

A number of acceptable methods are listed in the AC for satisfying the requirement for an independent verification means, including physical inspection, redundant processing, comparison of directed action to actual maintenance performed, or any other means of comparing the directed action to the HUMS processed data.

In this report, the focus is to perform redundant processing by a second dissimilar system using a significant amount of data that had already been collected from operational HUMS aircraft platforms. By doing so, and performing a detailed comparison of the results of the two dissimilar systems, a methodology is provided that simultaneously satisfies the requirement for independent verification, but which also does not need to be continued into actual end-user operations, thereby relieving operators from the burden of maintaining two dissimilar systems under normal operations.

3.1.2.1.1 Integrity Level Considerations.

The AC states that these methods are appropriate for meeting the initial integrity requirements for DO-178B Criticality Levels B through D (and that, effectively, only the timing of the independent verification is different—in the case of Level D systems, the verification can be performed after certification).

3.1.2.1.3 Ground-Based Equipment Hardware.

It is assumed that the GBE is comprised largely (if not exclusively) of COTS components, so independent verification is required to ensure that the hardware is compatible with both the intended application (as a HUMS ground station) and the software (both the COTS portion and the HUMS application-specific portion).

3.1.2.1.4 Software.

The AC acknowledges the presence of two types of software within the GBE: “Operational” software (referring to the operating system and its included interface software, such as display and disk drivers and peripherals) and “HUMS-specific” software.

In reality, however, even the HUMS-specific software may be comprised of both “application-specific” software (that is, custom-developed source code that performs the HUMS-specific processing tasks necessary to satisfy overall system processing requirements), and COTS software, usually in the form of third-party components that provide an enhanced user experience (e.g., user interface, reports, graphing components), extend general processing capabilities of the system (e.g., databases used to persist HUMS data over time, or general processing engines used to calculate or convert HUMS data), and provide the ability to interface to other, non-HUMS-specific software (such as external maintenance management, configuration management, or flight operations systems).

Therefore, the influence (and resulting potential impacts to HUMS operation) of COTS software can extend to the entirety of the GBE processing, both within the HUMS application software and outside of it.

The AC position on COTS software is the same as for COTS hardware: independent verification is required due to the opaque nature of the software and the necessary tasks that COTS performs within the context of the entire HUMS end-to-end performance. Regarding HUMS-specific software, the guidance provided within DO-178B applies. However, it must be recognized that even in the course of DO-178B development, it is possible to cross the application-specific/COTS software boundary one or more times. In such cases, an evaluation of the potential risks should be performed; appropriate responses should be made to those risks generated in the form of software design and techniques that would either eliminate those risks, or at the very least, identify when data integrity or other violations make the resulting HUMS function unreliable or erroneous.

3.1.2.1.5 Data Processing.

This section of the AC states the requirements for general performance and accuracy of the data processing portion of the GBE. It requires that the processing speed be acceptable to the end user. In addition, it requires the data processing portion of the GBE must not cause any monitored parameters to go out of specification based on the accuracy requirements originally specified for a particular parameter. Primarily, this section discusses the difference between a dedicated and shared data processing environment based upon the DO-178B criticality level of

the GBE. Level B and C systems that contain COTS are required to either be part of a dedicated system or demonstrate adequate protection from anything else processed on the same equipment. Level D systems need not be part of a dedicated system.

3.1.2.1.6 Display and Peripheral Equipment.

Similar to section 3.1.2.1.3, display and peripheral equipment must be shown to be compatible with other parts of the system and provide a clear and usable presentation. It is likely that different installations may support different models and types of such equipment, especially in a COTS or user-supplied hardware environment; the AC requirement is that whatever equipment is employed should not interfere with the proper operation of the system.

3.1.2.1.7 Data Communications.

Finally, this section covers those portions of the system that are used to share data with other systems (such as network applications). Such features are allowed in Levels C and D, provided that the independent verification means (associated with section 3.1.2.1.3) covers the use of these features. Level B applications must show that sufficient protection is provided to maintain that level of integrity throughout any foreseeable failure, malfunction, or mistake in any associated application (in addition to the independent verification means).

3.1.2.2 Credit Validation.

Although the issue of HUMS installation has been satisfactorily addressed, the issue of COTS (hardware or software) is not addressed in the AC during the period of Credit Validation. This phase primarily focuses on identifying the practices and procedures that are sought to be modified as a result of the operation of HUMS-equipped aircraft in the fleet. This phase was not studied in depth in this research because the effect of COTS during this phase is not covered in the AC.

3.1.2.3 Instructions for Continued Airworthiness.

The final phase in the AC pertains to the on-going process of establishing ICA for HUMS operators. An approved ICA program is mandated by 14 CFR/JAR Part 29 and Appendix A, and the AC provides supplemental guidance to address “aspects unique to HUMS” in this regard.

Although this section of the AC also does not specifically mention COTS, it is well recognized that the inclusion of COTS hardware and software will impact the activities and effort performed within the ICA program, which continues essentially for the life of the platform and its associated HUMS equipment.

The primary concern regarding COTS during this phase is the update, enhancement, modification, and maintenance of COTS components during the operational life of the HUMS. Since COTS represents the current state-of-the-art in both hardware component design and software functionality, as these disciplines advance, so will the capabilities of the COTS portions of the HUMS system. Faster processors, increased storage (both run-time memory and persisted

storage), faster data sharing, and new and denser memory devices are a given in today's electronics industry. Beyond the mere replacement and enhancement of hardware, continued maintenance, enhancement, and expanded capabilities are also common expectations of COTS software. Furthermore, entire operating systems are likely to evolve and become outdated over the life time of a HUMS. Therefore, many of the fundamental COTS components of a HUMS application are likely to change, possibly dramatically, over that time period.

During the course of this research, a few general categories appropriate for consideration during the ICA phase of the HUMS lifecycle have emerged. They are broadly classified as follows and are discussed in sections 3.1.2.3.1 through 3.1.2.3.3.

- Failure and repair
- Upgrades and updates
- New systems

3.1.2.3.1 Failure and Repair.

The failure and repair category of COTS changes may cause the least significant impact to a HUMS. Those COTS components (both hardware and software) that fail outright under normal usage and require repair or replacement with identical, or at least functionally similar, components fall into this category. A hardware failure of a COTS networking card, display unit, keyboard, or mouse, require that component to be either repaired or replaced. The hardware replacement returns the system to normal operation with no evident change. COTS software could become damaged or corrupted, necessitating that it be repaired or replaced (usually via features found in the original setup or installation media), and this repair would also return the system to a normal, functional state with no evident change in its behavior or performance. There would be no additional verification requirement for this type of COTS change other than confirming that the system returns to normal operation.

3.1.2.3.2 Upgrades and Updates.

The next level of COTS changes possibly could affect HUMS operations and should be considered for additional verification scrutiny. In contrast to replacing a failed component with an equivalent one, upgrades and updates aim to enhance or improve some aspect of the system. Hardware upgrades (such as faster processors and more memory), faster network interfaces, larger or more capable display systems, or even wholesale motherboard or computer refits can affect many more COTS components (hardware and driver software) than a simple repair. Software updates, where a COTS component undergoes an update to add additional protection or error processing, additional features (which do not change the original product family), or even bug fixes, are much more likely and numerous than hardware upgrades on any given system. Most major operating system providers now routinely send out "patches" or "service packs," which can be automatically detected and downloaded into a system without user intervention (depending on the system administrators preferences). Such updates include not only changes to the underlying operating system, but can also include updates to third-party device drivers, malware software, networking protocols—running the entire gamut of functionality provided by the operating system and its helper software is subject to update at any time.

Generally, it is impractical to prevent the practice of periodic COTS software updates on any system, HUMS ground stations included. In fact, most organizations responsible for computer systems require the timely and complete update of computer systems to limit their exposure to malware (viruses, worms, denial-of-service attacks, etc.), which the updates usually strive to prevent. As a result, ground station equipment, which is part of a shared or multipurpose computing environment, is likely to receive many COTS software updates over its lifetime.

In addition to operating software, any HUMS system that incorporates COTS components as part of the HUMS application will also experience a degree of COTS software updates over the life of a program. However, unlike operating system updates, usually the effects of HUMS-specific COTS component updates is evident in the update of the HUMS-specific software itself.

HUMS-specific software, unless already developed and so mature as to not require any changes, is likely to experience several updates over the life of the aircraft. As of this writing, even though the scope of many HUMS systems has become relatively well-defined, it is likely that HUMS in production today will include additional functionality and capability. The very nature of modern software- and field-loadable HUMS equipment lends itself to software and configuration data updates over the lifetime of the product.

When a change to the HUMS falls into the upgrades and updates category, an assessment should be made to understand the potential impact to that update, and some level of verification may be necessary under the operator's ICA program. Minor device changes (such as an upgrade from a 15" display to a 23" display) may not impact the HUMS functionality in any way (as long as the new device and associated drivers can be shown to function as expected within the system). Upgraded memory or network devices may increase the performance of the system, but not substantially alter the initial validation of the system in any way. In these two examples, simply demonstrating the continued operation of the system would be sufficient to verify that the HUMS applications are not impacted and may continue to be used in normal operations.

However, if a substantial upgrade or update is made, a more extensive evaluation of the system may be warranted. Replacement of a computer with a substantially different device, upgrading the motherboard from a single processor to a multi-processor system, or adding a new networking device (like a mobile wide-area network card) may result in changes to the hardware system that could impact HUMS functionality. Similarly, installation of a new operating system service pack, upgrading the HUMS software from one major release to another, or the installation of a substantial update to an existing third-party COTS software component might also require a more extensive evaluation of the new change on existing HUMS functionality. In these cases, a method to verify the continued correct operation of the HUMS should be established, executed, verified, and documented by the supplier, original equipment manufacturer (OEM), or operator (as specified in the ICA) to ensure that no negative impact to HUMS functionality is evident.

3.1.2.3.3 New Systems.

The final category involves the replacement of major portions of COTS hardware or software. A brand-new computer system must be installed in accordance with the manufacturer's guidelines, all peripheral software installed and configured, and the HUMS software application and associated software also installed and verified. In this case, as long as the HUMS application and associated software are compatible with the new hardware, a functional check should suffice to verify that the new system is up and operating.

In the case of new COTS software, such as a new operating system, or a new database version, it is likely that extensive changes to the underlying COTS and HUMS-specific application may be necessary. In these cases, a return to the validation phase is likely, where the underlying new COTS component is subjected to independent validation, just as the original system would have been. Typically, the vendor or OEM would be involved in migrating the existing HUMS product line from one version to the next and would perform a series of formal verification activities to verify the required functionality of the HUMS in an end-to-end system test. Using this method, the HUMS in its entirety would be revalidated to function as designed in the updated software environment.

3.2 SERVICE HISTORY.

In Section f (3) (ii), the AC mandates that the installation of GBE containing COTS hardware and software must have a satisfactory service history and an independent means of verifying the results of its processing. It further indicates that compliance to the integrity requirements for COTS is based on equivalence, which is a subjective process. Taken together, these statements indicate that while service history is an important consideration for the COTS portions of the system, it must be supplemented with an approved process of independent verification (at least initially, and likely for a period of time into the operation of the system).

Service history, gathered continuously over the lifetime of a HUMS product, can provide significant benefits, not only in the interest of certification and AC compliance, but also for the continued proper operation of the HUMS product. Since COTS updates, i.e., the type discussed in section 3.1.2.3.2, can occur asynchronously from planned HUMS installations and updates, it is important to have a program focused on continuous monitoring of the overall system to enable timely identification and mitigation of any interruptions to service, no matter what the cause.

Operators, OEMs, and vendors each share a role in the administration of an effective service history program. The following sections provide broad guidance in the activities of each party in establishing and conducting an effective service history program designed to monitor the effect of COTS in an overall HUMS environment.

3.2.1 Operators.

The operator is the primary component of any service history program. Since the operator routinely conducts the day-to-day activities of flying and maintaining the rotorcraft, they would be the first to be impacted by any issues with functionality of the system. Since the primary

purpose of the HUMS technology is to provide ample warning of any impending failure, any failure of that warning system should be identified before it compromises the continued safe operation of the rotorcraft. It is important that daily operations include sufficient checks and redundancy so that any anomaly in the operation of the system can be spotted early, and that no single point of failure could allow the anomaly to go undetected for a significant period of time.

Operators perform the following HUMS-related tasks and provide the following inputs to a service history program:

- Monitor routine HUMS indications provided during normal operation.
- Report action taken when identified by the HUMS and associated additional inspections.
- Identify components replaced due to HUMS indications.
- Maintain HUMS active and archive data (locally).
- Transfer HUMS data to OEM/vendor as indicated by service history program.
- Report unusual indications during operation onboard system (OBS) or ground-based system (GBS).
- Report any issues with OBS data recording or system data transfer (OBS to GBS).
- Log error messages and system faults.
- Track HUMS built-in test and system faults, including replaced components of the monitoring system.
- Initiate alternate means of data collection in the event of a HUMS collection failure.

3.2.2 The OEMs.

The OEM is a key strategic partner in the establishment and routine conduct of an effective service history program. Though the OEM is usually not directly involved with day-to-day operations, they do serve as a key point of contact for a wide range of topics regarding the rotorcraft, including operational use and limitations, rotorcraft and system maintenance, the effects of fatigue on life-limited components, structural and design considerations, design changes and the implementation of modifications to components, and a wide range of other information and services designed to maximize the value of the rotorcraft to the operator.

The OEM is also a primary consumer of the subset of HUMS information, which is targeted toward gathering overall trend data on the health and usage of the rotorcraft. This long-term trend data can be used in a variety of ways, including validation of rotorcraft design,

identification of any key trends in components or structures, early identification of fleetwide trends, the establishment of thresholds for early detection, to name a few.

It must be recognized that any HUMS data evaluated by the OEM is likely to be processed on a delayed basis. Even those programs that support near real-time transmission of HUMS data from an operator to an OEM will incur a delay of that processing due to the nature of gathering this data from a widely disbursed fleet of rotorcraft. It is also important to recognize that the nature of the information being extracted from the HUMS by the OEM may be fundamentally different than that extracted by the operator. The operator's primary focus is on the continued safe and effective operation of its available rotorcraft, and compliance with all mandated procedures, inspections, maintenance, and operational limitations. At the OEM level, HUMS data is usually examined on a broader level to establish a statistical framework for anomaly detection, overall fleet health and usage trends, and broader maintenance and design information, which requires the collection of data from among many operators across the variety of flight and usage scenarios encountered in the field.

OEMs can perform the following tasks for the service history program:

- Obtain overall HUMS fleet data from various operators.
- Analyze fleet data for statistical behavior and establish thresholds, which can be used to differentiate normal versus abnormal indications in the collected data.
- Analyze fleet data for overall component trend and aggregate usage information.
- Identify coverage gaps in fleet data requiring additional data collection.
- Identify missing data resulting from monitoring or collection anomalies.
- Participate with component analysis, overhaul, and retirement.
- Assist with the movement of HUMS-related data as required for component analysis.
- Obtain indirect and direct evidence comparing data to component status.

3.2.3 Vendors.

The HUMS vendor is typically the party furthest removed from day-to-day operations of a HUMS-equipped fleet (with the exception of those vendors who also supply on-site support), but they can also provide valuable assistance in the establishment and maintenance of an effective service history program.

The vendor is typically focused on the proper operation of the HUMS product over one or more aircraft product lines, possibly for multiple customers and OEMs. The vendor usually works directly with the OEM (for factory-installed systems) or primary customer (when retrofitting) to perform initial verification of the overall system in the target environment (both on-aircraft and

within an established COTS environment) and is also the primary focus for any HUMS maintenance, modification, or enhancement over the life of the product line.

The vendor is usually in the unique position of being able to perform detailed analysis of any reported issue arising from use at the operator or OEM level. They can be a valuable resource for verifying any field-reported issue with the operation of the HUMS. This makes the vendor another important partner in the establishment and conduct of an effective service history program.

Vendors can add the following to service history programs:

- Identification and investigation of common reports provided by operators and OEMs.
- Analysis of unique issues identified across the HUMS fleet.
- Support for deployment and installation of HUMS product hardware and software.
- Analysis of HUMS functional enhancements or modifications.
- Assistance with the proper operation, maintenance, and replacement of HUMS equipment.
- Correction and verification of identified anomalies in fielded systems.
- Support for credit validation during controlled introduction and/or ICA activities.

3.2.4 Guidelines for Establishing a Service History Program.

An effective service history program requires consistent participation by all relevant parties responsible for HUMS data collection and analysis. The following guidelines are provided for the establishment of a service history program.

- Identify the key participants in the program—At a minimum, the participants should include each end-user operator of the HUMS-equipped system, the rotorcraft OEM, and the HUMS equipment vendor or their representative. In addition, major component suppliers to the OEM and other organizations involved in the collection, dissemination, analysis or storage of the HUMS data should be considered for participation in the service history program.
- Assign roles and identify collection requirements for each participant—A clear set of roles and responsibilities should be established for each member of the service history program. Each assigned duty should be consistent with that member's function within the program and should be aligned with their activities performed in support of aircraft operations, data analysis, or HUMS product responsibilities. The specific type of data to be collected and/or reported from each role should also be identified at this time.

- Establish a process for personnel replacement—Since the service history program is likely to extend over a long period of time, the program should establish procedures to handle the reassignment of key personnel from time to time. Each established role should be identified and a process established to ensure that each role is filled whenever an assigned individual is transferred or no longer able to serve in their designated capacity.
- Establish periodic review schedule—Collected service history should be evaluated routinely in a periodic manner to allow for identification of any trends or anomalies in the program. The timeframe for this review should be commensurate with established component lifetimes and known failure scenarios to ensure that the review cycle will be likely to identify key indicators prior to component failure.
- Identify a suitable archive solution—As service history data is collected over time, this data should be archived in a format allowing for later analysis and use. A method to collect and store this information should be identified during the establishment of the service history program.

3.3 PROCESS FOR GATHERING DIRECT AND/OR INDIRECT EVIDENCE.

The AC requires that the validation process used for HUMS certification be based on “suitably representative physical data...which may use either direct or indirect evidence or a combination of the two, depending on the credit type and the criticality on the aircraft of any HUMS failure or modification” [1].

3.3.1 Collecting Data.

As envisioned in the AC, the process of gathering both direct and indirect evidence to correlate component failures with collected HUMS data is an ongoing effort over the life of the system. For most newly developed HUMS applications, this can present a significant obstacle to both the vendor and the operator. At the outset of a program, no such data will exist for any given platform because a HUMS is not present to start with. Even on rotorcraft with a pre-existing service history, the introduction of HUMS onto that rotorcraft may require a substantial period of time before sufficient data can be collected in the full range of operational characteristics for the platform and even longer before sufficient failure data could be obtained to provide direct correlation with the condition of any given component.

In addition, to enter into the validation phase, the AC requires a separate controlled introduction into a service period. This can be a significant obstacle to both the vendor and the operator as it requires operation of the system in parallel with alternative or standard procedures to provide back-to-back comparison. Not only may there be significant differences between the multiple procedures, but the additional workload of performing parallel procedures on a given rotorcraft may result in the decision to not attempt a HUMS solution due to the actual or perceived additional workload that the operator may incur. Such a result could negate any possible

operational or safety gains that the installation of a HUMS system could provide for that operator and would inhibit the application of HUMS technology in general.

Traditionally, the process of HUMS credit validation has been evolutionary. In the first phase, approval for initial HUMS equipment installation is sought and pursued in accordance with applicable standards for the installation and operation of airborne equipment. Once the HUMS is installed and routinely collecting data, the process of comparing reported HUMS data with the actual condition of the rotorcraft and its components can begin. After a sufficient amount of time, which may include actual component failures during monitored operations, correlation of the HUMS data and resulting component condition and health may be established. Once that relationship is established, the process of applying for credit validation of specific HUMS-monitored components can be sought.

The goal of a HUMS installation is to increase the readiness and reliability of a rotorcraft system by providing an automated means of constant component condition monitoring, accurate and reliable usage monitoring, and effective and actionable indications to both operations and maintenance personnel on the status, health, and condition of all monitored components and systems. Once established, this level of monitoring integrity becomes the basis for validated credits, which can be applied to the routine operation and maintenance of the system.

3.3.2 Collected Data.

In contrast to the method of collecting data in parallel using alternative or standard procedures during a controlled introduction into service, for the purpose of this research, the researchers have attempted to show that a process based on existing collected data could be established with the goal of providing equivalent justification of the system using the concept of a controlled introduction to service, but without the added burden of operating systems in parallel at the operator's location. The following paragraphs cover this concept in more detail.

This research focused on using a variation of the multiple-dissimilar software method to provide for an independent means of verification of the COTS portion of the HUMS ground station system under test. This was accomplished by isolating a specific HUMS function (structural usage computation) for analysis and running that function on two dissimilar COTS operating systems (Microsoft® Windows® XP Professional and Linux™ WS v.4 for x86) across a large history of previously collected HUMS data. Direct comparison of the results from the two systems was the means to verify any impact of the COTS portions of the system (hardware and software).

Key to this effort was the availability of existing HUMS data for the retroactive analysis of a proposed added function, such as the structural usage computation. By using existing data that spanned a significant period of time, sufficient data was available to provide for valid processing and comparison of the results across the dissimilar operating systems.

By conducting thorough processing and verification of the resulting output at the system level, the goals of the controlled introduction to service process can be met without incurring the added

burden of parallel operation of the system on the part of the operator for an extended period of time, thereby providing an alternate method of establishing the sought credit.

3.4 INDEPENDENT VERIFICATION MEANS FOR THE COTS PORTION UNDER STUDY.

The following sections detail the process used for independent verification of the COTS portion of the HUMS under this study. Information in this section is specific to the study itself and is provided to supply a context for the verification methods discussed.

3.4.1 Structural Usage Computation.

For the purpose of this study, a proposed method of performing structural usage computations was implemented as an extension of existing HUMS ground station functionality. Inputs to this processing capability included time spent in each pre-existing flight regime and the parts structure of the rotorcraft, as provided from the existing configuration management system in use at the time of the HUMS data collections. A variety of structural damage factors were pre-allocated and assigned to the various parts in the rotorcraft structure. It must be noted that the structural damage factor values themselves were generated and assigned randomly—they were in no way validated as actual damage factors for the parts evaluated under this study. The validation of structural usage damage factors is beyond the scope of this effort and is not included in the results of this study. However, the process by which independent verification could be obtained using multiple-dissimilar software is illustrated and examined by this method.

3.4.2 Multiple-Dissimilar Software.

At the heart of this research was the use of the multiple-dissimilar software technique as a means to independently verify the results of the structural usage computations performed by the ground station. The research goals were accomplished using the following techniques:

- Data input to the system consisted of identical HUMS data, collected over approximately 2.5 years from a homogeneous fleet of HUMS-equipped rotorcraft.
- The structural usage algorithm created for study was identical across the two independent systems. Identical parts and flight regime data served as the input to both systems, as well as identical assigned factors for structural damage factors.
- Data was consumed and generated by the two systems in an identical fashion, enabling a direct back-to-back comparison of the resulting output data via a 'file difference' program, and was analyzed manually for any differences between the two systems.

Once the software was designed and implemented, it was compiled for native execution on each of the intended target systems (one for Microsoft Windows, the other for Linux).

3.4.2.1 Structural Usage Module Design.

This report focuses on the development of a prototypical software module designed to compute the structural usage life of rotorcraft components. When compared to traditional “usage-based” parts life measurements, structural usage computations have several distinguishing characteristics.

Operational usage-based, life-limit metrics traditionally are used to track the number of hours that the aircraft component has been in use. Usually tied to a single metric, such as Aircraft Flying Hours, Engine Hours, or possibly Airframe Hours, this type of measurement tracks the cumulative number of operating hours that a particular aircraft component has been subject to. When the airframe manufacturer determines that a particular part’s useful life is limited to a specified number of hours, the hours against this component are tracked and the component is removed from service when it reaches the specified life limit. Assemblies consisted of one or more life-limited components are also tracked, and the life of the assembly is limited to the life of the most limiting component within the assembly. When the life limit is reached, the assembly is pulled and either retired from service or overhauled for removal and replacement of the designated life-limited components. A new life limit for the resulting assembly is established by the cognizant overhaul authority, and the assembly is returned for service with the new life limit established.

By contrast, structural usage life considers not only the time a component is in operation, but also the flight conditions under which that time is accumulated. When an aircraft HUMS is installed and used to monitor flight operations, the various flight regimes encountered by the aircraft can be detected, and this flight regime data (also known as regime recognition data) can be used to compute the structural usage life of installed aircraft components. By convention, structural usage is usually computed in terms of equivalent hours so that systems that track hour-based component usage can be used to store and display structural usage values as well.

To perform this transformation, life-limited components are assigned damage factors, which represent the loss of useful life to that component as it is exposed to a specific flight regime for a specified period of time. Damage factors vary from component to component, and for a given component, will also vary from regime to regime, reflecting the imputed amount of damage (or loss of useful life) that a particular flight regime may incur on any given component during normal (or abnormal) operation.

Mathematically, this relationship for a single part in a single regime can be expressed as follows:

$$S_u = F_d \times R_d$$

where S_u = Structural usage
 F_d = Damage factor
 R_d = Regime duration

To compute the total amount of Structural Usage applied to a given aircraft component for an entire monitored operation (a single flight, for example), the following equation can be used:

$$SU_p = \sum_{1...n} (\sum_{1...r} DF_p * TT_r)$$

where

- SU_p = Structural usage (damage) for a Part
- DF_p = Damage factor for a part
- TT_r = Total time in the regime
- n = Operation(s)

3.4.2.2 Software Implementation.

Two software modules were compiled to perform the Structural Usage computations described above. These modules were compiled using the same C++ source code, but one was targeted to run on the Microsoft Windows operating system and the other was targeted to run on the Linux operating system. Since these modules used identical source code, their structural usage algorithms are also identical.

3.4.2.3 Regime Data Extraction.

An extensive database of HUMS-equipped aircraft data was accessed to provide input data over a period of several years. This study leveraged that data for the purpose of providing a significant history of already-collected regime data for input to this study.

3.4.2.4 Damage Factor Assignment.

A series of damage factors were constructed to simulate the spread of potential damage factor values expected over an aircraft's life-limited installed components. Figure 1 shows this distribution in graphical form. Table 1 indicates the exact values used in tabular form.

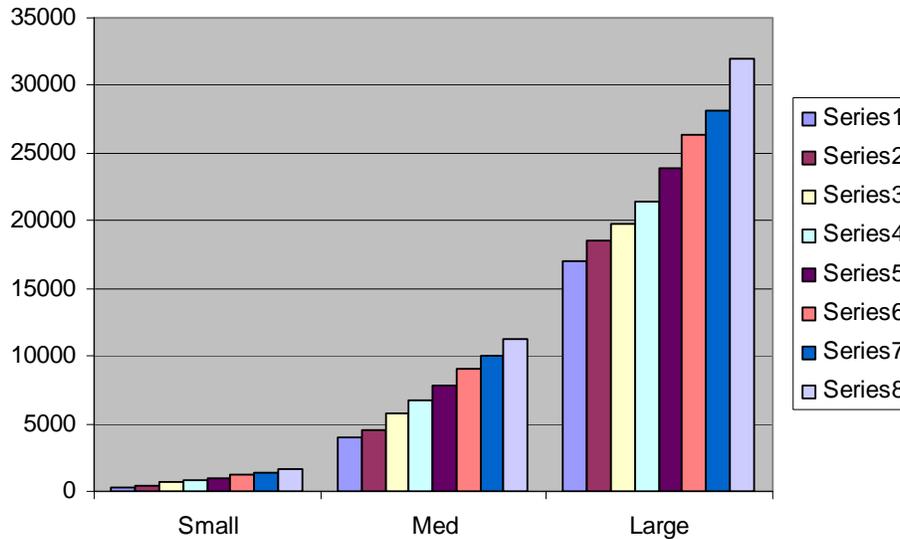


Figure 1. Damage Distribution

Table 1. Partitions Used for Damage Factors (Hours before replacement)

Set	Small	Medium	Large
1	300	4,000	17,000
2	430	4,498	18,589
3	715	5,760	19,702
4	785	6,773	21,420
5	893	7,883	23,874
6	1200	9,018	26,301
7	1380	10,001	28,127
8	1656	11,200	32,000

3.4.2.5 Regime Data Source.

Regime data used for the final extraction consisted of the full set of aircraft data that was available as of November 12, 2007. The cumulative data spanned 3.5 years (April 7, 2004 to November 8, 2007) and included a total of 35,561 aircraft operations.

3.4.2.6 Data Analysis.

A number of data extraction experiments were conducted to evaluate the differences found when computing Structural Usage from the same algorithm executed within two disparate COTS software environments. The first experiment was conducted using a relatively small input data set as a means of verifying the overall experimental data flow as well as gauging the relative performance of the two different systems. Following that run, a second experiment was

conducted using much larger input data sets to stress the applications themselves and to provide a more statistically significant cross section of Structural Usage computation results.

Several additional experiments were conducted to refine the software. The software was modified to reduce the likelihood of differences in output when run on different operating systems and was also modified to improve performance such that the experiments could be conducted in a reasonable time period. The concluding experiment ran against the full set of regime data and damage factors and is considered the final run for this research project, upon which the verification conclusions are based.

3.4.3 Verification Using Dissimilar Software.

In the final verification process, several data runs were executed under each target operating system, and the results compared directly between the two systems. Two modes of operation were examined. In the first, the resulting incremental structural damage values for each operation were compared back-to-back. The second mode of operation had the software under study accumulate the structural damage across multiple operations to examine any COTS impact on the summation of this data over time.

To establish detailed metrics, each large set of aircraft data was run multiple times, specifying a different level of numeric precision between each run. This controlled change to how the data was computed and outputted for comparison allowed for multiple levels of verification against increasing expected numeric precision.

3.4.4 Verification Results.

The resulting output data sets were compared directly against one another by mode and precision.

As indicated table 2, there was significant agreement achieved between the two dissimilar COTS environments. Thirteen of the sixteen tests produced identical output results in the final phase of testing. This shows that a substantial agreement between the two systems was achieved and serves to support the concept that multiple-dissimilar software verification for the purpose of validating the COTS software environment is a viable concept that can be demonstrated in actual practice.

The final three tests that consisted of the large data set, which performed the most complex computations and carried higher levels of numeric precision, did not produce identical results when the Linux system output was compared to the Windows system output.

Detailed examination of the data indicated that between the two systems, the method of rounding used to report the specified numeric precision of each output value varied. After exhausting various options over the control of rounding behavior among the two systems, the end result was that for precisions higher than three decimal places, each system chose to implement a different behavior when rounding the (n)+1 digit. As a result of this different behavior under specific circumstances, the computed summations of structural usage values across all the data summed

for a specific aircraft model were not identical between the two systems when the numeric precision was greater than three decimal places. The error varied in proportion to the requested precision, from 0.22% at 6 digits, to 0.03% at 12 digits.

Table 2. Detailed Verification Results

Test	Group*	Linux†‡	Windows†‡	Result
1	Small	P3_M1	P3_M1	Identical
2	Small	P6_M1	P6_M1	Identical
3	Small	P9_M1	P9_M1	Identical
4	Small	P12_M1	P12_M1	Identical
5	Small	P3_M2	P3_M2	Identical
6	Small	P6_M2	P6_M2	Identical
7	Small	P9_M2	P9_M2	Identical
8	Small	P12_M2	P12_M2	Identical
9	Large	P3_M1	P3_M1	Identical
10	Large	P6_M1	P6_M1	Identical
11	Large	P9_M1	P9_M1	Identical
12	Large	P12_M1	P12_M1	Identical
13	Large	P3_M2	P3_M2	Identical
14	Large	P6_M2	P6_M2	Out of 72,819 lines of data, 159 (0.22%) had rounding errors in the 6 th decimal place.
15	Large	P9_M2	P9_M2	Out of 72,819 lines of data, 48 (0.07%) had rounding errors in the 9 th decimal place.
16	Large	P12_M2	P12_M2	Out of 72,819 lines of data, 24 (0.03%) had rounding errors in the 12 th decimal place.

Legend: *Small = Limited input data set; Large = Final data set (35,561 aircraft operations)

† P(n) indicates numeric precision of (n) digits was specified.

‡ M1 = Damage values per operation; M2 = Damage values per aircraft

3.4.5 Verification Conclusions.

Several conclusions may be drawn from this study regarding the use of the multiple-dissimilar software verification technique for validation of the COTS portion of a HUMS Ground Station, as listed below.

1. This study has shown that the use and analysis of pre-existing HUMS data is a viable alternative to conducting an analysis in parallel with the operation of the system. As long as the existing data is available and can be formatted for use in the proposed system, it serves as a valuable resource for the conduct of a retroactive study of the behavior of the system.

2. The use of the multiple-dissimilar software comparison technique has also been shown to be a viable method of producing useful verification outputs. By creating a common software solution that can be implemented in multiple environments, the effort usually associated with multiple-dissimilar software design and implementation (i.e., duplication) can be greatly reduced. It requires a slightly larger effort than the design and implementation of a solution in a single environment and requires sufficient skill sets in the chosen environments. However, a duplication of effort can be avoided if the task is well planned and executed.
3. Direct comparison of outputs from the disparate environments provides an immediate and exact method of verifying agreement or disagreement between the two systems.
4. Additional design iterations are likely to be required when using the multiple-dissimilar verification technique. In addition to the normal design cycle for a particular solution, it will also be necessary to compare the interim results of the dissimilar systems when using this technique and additional passes through this cycle are likely to account for any observable differences the initial design may impart. Once these additional iterations are completed, the direct comparison of outputs will have significant bearing on the final results.
5. The use of the multiple-dissimilar verification technique itself may impose an additional error margin in the overall verification results. In this study, a small epsilon error was noted in the most complex computations when one system was compared to the other. An understanding of the cause of that difference and an analysis of the acceptable size of that difference would both be required before establishing the Pass/Fail criteria to apply for any given verification effort. In this study, at the highest precision and most complex computation, a difference of 0.03% was noted between the two otherwise identical systems. Pass/Fail criteria would have to be established prior to formal qualification testing to use the comparison technique as a viable test result.
6. One important negative conclusion of this study is that use of the multiple-dissimilar software verification technique may not provide any assistance in determining which (if any) of the systems under test is the “correct” system when the end result is disagreement between the dissimilar systems. Since the criteria for this technique is substantial (within the established epsilon) agreement between the systems, any failure would only serve to fail the verification itself, but not necessarily supply any indication as to which of the disagreeing systems is more accurate or correct than the other.

3.5 OPPORTUNITIES FOR FURTHER STUDY.

3.5.1 Development Guidelines for COTS.

A more detailed look into guidelines to assist developers of HUMS products that incorporate COTS hardware and software is a possible area for future study. This research provided a focused, hands-on implementation of one suggested method of credit validation (independent

verification using multiple-dissimilar software); but this method may not prove the most cost-effective or useful for all types of HUMS functionality developed in software. A set of development guidelines that provides alternate methods of fulfilling the intent of credit validation would prove very useful as a means of exploring other techniques that allow the participation of COTS hardware and software as part of a for-credit HUMS product.

3.5.2 Operational Guidelines for COTS.

The nature of COTS hardware and software is that of near-continual change and adaptation. Even after a rigorous COTS validation activity with a given version of the available hardware and software, it is very likely that the COTS components of the system will change over the life of the HUMS product that it supports. Given the likelihood of change, a set of guidelines focused on maintaining the integrity of the system for which credit has been obtained over the lifetime of the changing COTS baseline would assist operators, OEMs, and vendors.

Another study [3] includes guidance specifically covering this topic, based upon the results of this research program and experience with support of existing systems in the field. Additional research, methods, and techniques may also prove useful in this critical area for future programs.

4. CONCLUSIONS.

This study has shown that the multiple-dissimilar software verification technique can be applied to the process of providing validation of the commercial off-the-shelf (COTS) portions of a Health and Usage Monitoring System (HUMS) Ground Station. It has further shown that evaluation of pre-existing data can provide valuable benefits in the verification of a specific HUMS capability without an unreasonable increase in the cost or scope of that verification effort. This study has also outlined several criteria for using this technique for validation, and has identified a few limitations and items to consider when planning such an activity. In addition, the study has provided background for the establishment of several guidelines related to the establishment and conduct of a Service History program as outlined in Advisory Circular 29-2C, Section MG-15.

5. REFERENCES.

1. United States Department of Transportation, Federal Aviation Administration, Advisory Circular 29-2C, Miscellaneous Guidance Section MG-15.
2. RTCA DO-178B, "Software Considerations in Airborne Systems and Equipment Certification, RTCA, Inc., Washington, DC, 1992.
3. Robinson, R., "Commercial Off-The-Shelf Ground Support Station Process Guidance," FAA report DOT/FAA/AR-09/66, to be published.