



AEROSPACE RECOMMENDED PRACTICE

ARP6887™

Issued

2024-09

Validation and Verification of Integrated Vehicle Health Management Systems

RATIONALE

This ARP provides objectives and activities of Validation and Verification Processes required to assure high quality and/or criticality level of IVHM (Integrated Vehicle Health Management) systems and software. IVHM covers a vehicle's monitoring and data processing functions inherent within its subsystems, providing the tools and processes used to manage and provide the information needed to assist in maintenance decisions to restore the vehicle's health in a timely manner, whether component, subsystem, system, and system of systems. This document presents a recommended approach for IVHM stakeholders to achieve the Validation and Verification of IVHM hardware, IVHM software, and the overall integrated IVHM system. This ARP contributes to a hierarchy of IVHM guidance documents, along with organizational goals, system requirements, system architecture, detailed system design, and sustainment/support.

TABLE OF CONTENTS

1.	SCOPE.....	3
1.1	Purpose.....	3
1.2	Field of Application.....	4
1.3	Overview of this Document.....	4
2.	REFERENCES.....	4
2.1	Applicable Documents.....	4
2.1.1	SAE Publications.....	4
2.1.2	A4A Publications.....	5
2.1.3	EASA Publications.....	5
2.1.4	FAA Publications.....	5
2.1.5	IEEE Publications.....	6
2.1.6	ISO Publications.....	6
2.1.7	RTCA Publications.....	6
2.1.8	Transport Canada Publications.....	7
2.1.9	U.S. Government Publications.....	7
2.1.10	Other Publications.....	7
2.2	Definitions.....	7
2.3	Acronyms and Abbreviations.....	9
3.	IVHM BASICS.....	11
3.1	The IVHM Development Process.....	11
3.2	IVHM Design and Development Principles.....	13
3.3	Development Rigor and Assurance Levels.....	14
3.4	Health-Ready Components.....	15
3.5	Achieving IVHM System Capability Levels.....	16
4.	VALIDATION AND VERIFICATION.....	16
4.1	Validation and Verification Methods.....	18
4.2	Validation and Verification Steps.....	19

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2024 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or used for text and data mining, AI training, or similar technologies, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE ARP6887

For more information on this standard, visit
<https://www.sae.org/standards/content/ARP6887>

Documents

Standard, visit Sharing Hub

4.3	Qualification	19
4.4	IVHM System Validation and Verification Comparison to Traditional System Validation and Verification	20
4.5	IVHM System Baseline Verification	21
4.6	IVHM Operational Use Case Validation	23
4.7	IVHM System Requirements Validation	24
4.8	IVHM System Architecture and Design Validation	24
4.9	IVHM Hardware and Software Verification	25
4.9.1	Airborne Equipment	25
4.9.2	Ground Equipment	25
4.10	IVHM Integrated System In-Service Verification	25
4.10.1	Idealistic Validation and Verification Methods	26
4.10.2	Intended Functions	27
4.11	Additional IVHM Validation, Verification, and Regulatory Acceptance	28
4.11.1	Fault Data Based Validation	29
4.11.2	In-Service Validation	30
4.11.3	Natural/Seeded Fault Based Validation	30
4.12	Validation and Verification of Ground-Based Data	30
5.	OTHER CONSIDERATIONS	31
5.1	Considerations for MSG-3	31
5.2	The Use of COTS Software	31
6.	SUMMARY	32
APPENDIX A	LANDING GEAR EXAMPLES	33
Figure 1	IVHM validation and verification	12
Figure 2	Stakeholder value proposition	13
Figure 3	Safety objective approach	15
Figure 4	IVHM capability levels for aerospace and automotive applications	16
Figure 5	V-diagram showing IVHM life cycle	21
Figure 6	General IVHM system architecture view	22
Figure 7	Example of system boundary diagram	23
Figure 8	Validation and verification roadmap and role of simulation framework	27
Figure 9	Different types and stages of diagnostics and prognostics	28

1. SCOPE

This SAE Aerospace Recommended Practice (ARP) provides guidance to plan and perform validation and verification of IVHM systems. The intent of this ARP is to help the reader appreciate and understand additional objectives and activities of validation and verification processes, beyond validation and verification of the vehicle, that arise due to the nature of an IVHM System. This includes an end-to-end evaluation of the entire IVHM system, noting that IVHM is a “system of systems.” In order to perform validation and verification, the user must determine what they are using IVHM for, including the criticality of the application. The process should then determine appropriateness of the data corresponding to the application criticality.

This document provides validation and verification guidance for IVHM as: (1) a system of systems, (2) a system, and (3) elements within a system. While this document is not intended to be prescriptive, it is a reference guide that highlights and discusses some attributes of IVHM and its uses that typically necessitate special handling during validation and verification.

For more information about validation and verification processes required for onboard aerospace applications, please refer to ARP4754 (for development process), ARP4761 (for safety assessment process), RTCA DO-178 (for software), RTCA DO-254 (for hardware), and FAA guidance provided by AC 25.1309-1A. The validation and verification processes identified in the standards cited above must be considered where IVHM elements are part of an airborne system. See 1.3 for a more detailed overview.

1.1 Purpose

The main purpose of the document is to provide the following:

- Guidance for the validation and verification of IVHM systems during design of ground-based hardware and software.
- Guidance for the validation and verification of IVHM systems during design of airborne hardware and software.
- Guidance on the development of scenarios used for the validation and verification of the off-board capabilities of IVHM systems.
- Guidance on the development of scenarios used for the validation and verification of the onboard capabilities of IVHM systems.
- Functionality guidance on integrated requirements-based verification performed at the appropriate level of rigor required by the development assurance level (DAL), which was assigned based on the system safety analysis process. The basic requirements-based verification process based on the DAL is covered in ARP4754. However, IVHM systems have systems with complex interactions and intertwined DALs, leading to functionality challenges. This entails including validation and verification of the operational use cases that support the overall concept of operations.

In general, validation and verification of an IVHM system should be no different than any other vehicle system. Having said that, there are two main areas of particular interest when performing validation and verification on IVHM:

1. IVHM is a “system of systems.” IVHM is not a federated, compartmentalized, isolated system that performs one main function. IVHM is often distributed across a vehicle onboard, on-ground, and up to enterprise level, such that IVHM requirements can be found throughout all vehicle systems (and ground support systems). All systems need to work together to fulfill IVHM's intended function.
2. IVHM is focused on “off-nominal” operations. The main function of IVHM is the unified capability of a “system of systems” to assess current or future state of health. IVHM performs this via the detection of problems, anomalies, failures, etc., and assisting in the recovery to achieve nominal operations (i.e., by advising other systems to take action according to design or by generating alerts, advisories, and information for recommended actions in a timely manner).

Item 1 above implies that much of the validation and verification effort should be performed at the systems level, using end-to-end scenario testing based on the concept of operations and use cases.

Item 2 implies that the sections of RTCA DO-178 and RTCA DO-254 that deal with “Requirements-Based Test Selection” of “Normal Range Test Cases” and “Robustness Test Cases” take on a whole new meaning. Often in the validation and verification of a typical function, the robustness test simply looks at limits testing or envelope testing (i.e., this means test cases that ensure that a function works within required limits and fails predictably when limits are exceeded, often resulting in a function disconnect or generation of a warning). For IVHM, there is much more to consider than just limits testing, for example, single fault and multiple fault cases, function reconfiguration and recovery, assessment of false positives and false negatives, etc.

1.2 Field of Application

This document may be applied by IVHM stakeholders to assist with verification and validation of IVHM hardware, IVHM software, and an integrated IVHM system. The stakeholders may include different types of users already within an IVHM system. The different types of users may have different goals and will use different kinds of datasets. However, they should all be part of the end-to-end scenario testing.

This document addresses IVHM in the context of aerospace vehicle types; however, the guidance provided is generic and may also be relevant to other industrial domains and vehicles outside of aerospace. Specifically, much of the guidance in this document leans to commercial aviation (fixed wing and rotorcraft), which utilizes the Airlines for America (A4A) MSG-3 document to create a list of scheduled maintenance tasks for aircraft models under a given type certificate.

NOTE: This document does not directly address certification of IVHM. Although guidance such as this may be critical to successful implementation of an IVHM system, use of this guidance alone cannot be assumed to constitute or ensure regulatory agency acceptance. Any regulatory accepted use to fulfill requirements will require collaboration and agreement with the appropriate regulatory agency. This SAE document is not a regulatory document and neither the applicants nor the regulatory agency is compelled to follow them unless there is associated regulatory agency policy.

1.3 Overview of this Document

This document provides a brief background of IVHM before delving into validation and verification. Section 3 addresses the IVHM development process, IVHM design principles, development rigor and assurance levels, health ready components, and IVHM system capability levels. Several existing SAE documents cover these, and this validation and verification document is intended to be a part of this IVHM hierarchy. Later in the document, the concept of qualification and integration tests are incorporated in the view of validation and verification.

Section 4 discusses steps of IVHM validation and verification, qualification, system baseline verification, operational use case validation, system requirements validation, system architecture validation, hardware and software verification, integrated system implementation verification, fault-based validation, in-service data validation, natural/seeded fault-based validation, and validation and verification of ground-based data. Section 5 discusses MSG-3 considerations along with the use of commercial off-the-shelf (COTS) hardware and software and the differences between ground and airborne systems. Section 6 provides a summary, while Appendix A shows some examples.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

AIR6900 Applicable Aircraft Integrated Vehicle Health Management (IVHM) Regulations, Policy, and Guidance

AIR7121	Applicability of Existing Development Assurance and System Safety Practices to Unmanned Aircraft Systems
ARP4754	Guidelines for Development of Civil Aircraft and Systems
ARP4761	Guidelines for Conducting the Safety Assessment Process on Civil Aircraft, Systems, and Equipment
ARP5783	Health and Usage Monitoring Metrics, Monitoring the Monitor
ARP5987	A Process for Utilizing Aerospace Propulsion Health Management Systems for Airworthiness Credit
ARP6275	Determination of Costs and Benefits from Implementing an Integrated Vehicle Health Management System
ARP6290	Guidelines for the Development of Architectures for Integrated Vehicle Health Management Systems
ARP6407	IVHM Design Guidelines
ARP6461	Guidelines for Implementation of Structural Health Monitoring on Fixed Wing Aircraft
ARP6803	IVHM Concepts, Technology and Implementation Overview
ARP6883	Guidelines for Writing IVHM Requirements for Aerospace Systems
ARP7122	Utilizing Aircraft Integrated Vehicle Health Management Systems for Maintenance Credit
SAE JA6268	Design and Run-Time Information Exchange for Health-Ready Components

2.1.2 A4A Publications

Available from Airlines for America, 1301 Pennsylvania Avenue, NW, Suite 1100, Washington, DC 20004, Tel: 202-626-4000, www.airlines.org.

A4A MSG-3 Operator/Manufacturer Scheduled Maintenance Development

2.1.3 EASA Publications

Available from European Union Aviation Safety Agency, Konrad-Adenauer-Ufer 3, D-50668 Cologne, Germany, Tel: +49 221 8999 000, www.easa.europa.eu.

CS-23 Certification Specifications for Normal, Utility, Aerobatic, and Commuter Category Aeroplanes

CS-25 Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes

EC 748/2012 Annex Part 21: Certification of Aircraft and Related Products, Parts and Appliances, and of Design and Production Organizations

2.1.4 FAA Publications

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866-835-5322, www.faa.gov.

14 CFR Part 21 Certification Procedures for Products and Parts

14 CFR Part 23 Airworthiness Standards: Normal, Utility, Acrobatic, and Commuter Category Airplanes

14 CFR Part 25 Airworthiness Standards: Transport Category Airplanes

14 CFR Part 26 Continued Airworthiness and Safety Improvements for Transport Category Airplanes

14 CFR Part 27	Airworthiness Standards: Normal Category Rotorcraft
14 CFR Part 29	Airworthiness Standards: Transport Category Rotorcraft
14 CFR Part 33	Airworthiness Standards: Aircraft Engines
14 CFR Part 35	Airworthiness Standards: Propellers
AC 20-115	RTCA DO-178, Software Considerations in Airborne Systems and Equipment Certification
AC 20-152	RTCA DO-254, Design Assurance Guidance for Airborne Electronic Hardware
AC 20-156	Aviation Data Bus Assurance
AC 25-19	Certification Maintenance Requirements
AC 25.1309-1A	System Design and Analysis
AC 29-2C MG 15	Airworthiness Approval of Rotorcraft Health Usage Monitoring Systems
AC 43-218	Operational Authorization of Integrated Aircraft Health Management System
AC 121-22	Maintenance Review Board Procedures
FAA CPI Guide	The FAA and Industry Guide to Product Certification, Sept 2004.

2.1.5 IEEE Publications

Available from IEEE Operations Center, 445 and 501 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, www.ieee.org.

IEEE STD 610.12 IEEE Standard Glossary of Software Engineering Terminology

2.1.6 ISO Publications

Copies of these documents are available online at <https://webstore.ansi.org/>.

ISO 13374 Condition Monitoring and Diagnostics of Machines

ISO 26262 Functional Safety Standard for Modern Road Vehicles

2.1.7 RTCA Publications

Available from RTCA, Inc., 1150 18th Street, NW, Suite 910, Washington, DC 20036, Tel: 202-833-9339, www.rtca.org.

DO-160	Environmental Conditions and Test Procedures for Airborne Equipment
DO-178	Software Considerations in Airborne Systems and Equipment Certification
DO-200	Standards for Processing Aeronautical Data
DO-201	Industry Requirements for Aeronautical Information
DO-254	Design Assurance Guidance for Airborne Electronic Hardware
DO-278	Guidelines for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) System Software Integrity Assurance

DO-331	Model-Based Development and Verification Supplement to DO-178C and DO-278A
DO-333	Formal Methods Supplement to DO-178C and DO-278A
DO-355	Information Security Guidance for Continued Airworthiness
DO-380	Environmental Conditions and Test Procedures for Ground Equipment
ED-206	EUROCAE ED-206, Guidance on Security Event Management
SC-240	EUROCAE WG-117, Topics on Software Advancement

2.1.8 Transport Canada Publications

Available from Transport Canada, Tower C, Place de Ville, 330 Sparks Street Ottawa, Ontario K1A 0N5, Tel: 1-800-305-2059, www.tc.gc.ca.

CARs 2012-1 Part I - General Provisions, Subpart 1 - Interpretation (CARs 101.01).

CARs 2012-1 Part V - Airworthiness, Regulations, Subpart 21 - Approval of the Type Design or a Change to the Type Design of an Aeronautical Product (CARs 521.01 to 521.456), Division IV - Changes to a Type Design (CARs 521.151 to 521.161)

AC 521-004 Changes to the Type Design of an Aeronautical Product

2.1.9 U.S. Government Publications

Copies of these documents are available online at <https://quicksearch.dla.mil>.

MIL-STD-461 Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment

MIL-STD-810 Environmental Engineering Considerations and Laboratory Tests

MIL-STD-1472 Design Criteria Standard: Human Engineering

2.1.10 Other Publications

Adhikari, P., Rao, H., and Buderath, M. (2018, October). *Machine Learning based Data Driven Diagnostics and Prognostics Framework for Aircraft Predictive Maintenance*. 10th International Symposium on NDT in Aerospace, Dresden, Germany.

Azzam, H. and McFeat, J. (2016). *Validation, Verification and Certification of Structural Health Monitoring Systems for Military Aircraft* (MASAAG Paper 123). Prepared for The Military Aircraft Structural Airworthiness Advisory Group, Issue 2a.

Buderath, M., Adhikari, P., and Rao H. (2016, November). *Simulation as Key Enabler to Support ISHM Certification*. 8th International Symposium on NDT in Aerospace, Bangalore, India.

Buderath, M. and Adhikari, P. (2012, July). *Simulation Framework and Certification Guidance for Condition Monitoring and Prognostic Health Management*. European Conference of Prognostics and Health Management Society, Dresden, Germany.

Menon, P. and Robinson, B. (2012). *Validation and verification Process for CBM Maintenance Credits*. 67th American Helicopter Society International Annual Forum, Virginia Beach, VA, United States.

2.2 Definitions

AIRWORTHINESS: The condition of an aircraft, aircraft system, or component in which it operates in a safe manner to accomplish its intended function (refer to ARP4754).

APPROVAL: The act of formal sanction of an implementation by a certification authority (refer to ARP4754).

ASSURANCE: The planned and systematic actions necessary to provide adequate confidence and evidence that a product or process satisfies given requirements (refer to RTCA DO-178).

CERTIFICATION: The legal recognition that a product, service, organization, or person complies with the applicable requirements. Such certification comprises the activity of technically checking the product, service, organization, or person, and the formal recognition of compliance with the applicable requirements by issue of a certificate, license, approval, or other document as required by national laws and procedures (refer to ARP4754).

CERTIFICATION AUTHORITY: Organization or person responsible for granting approval in accordance with applicable regulations (refer to ARP4754).

CONDITION BASED MAINTENANCE: Performing maintenance based on evidence of need (i.e., based on the condition or health of a component or system rather than on a periodic or scheduled basis).

CONDITION MONITORING: The process of observing the health state of an asset in order to provide data, which can be used to determine a maintenance need. The observations can be through continuous real-time data or periodic sampling.

CRITICALITY: Indication of the hazard level associated with a function, hardware, software, etc., considering abnormal behavior (of this function, hardware, software, etc.) alone or in combination with external events (refer to ARP4761).

DAMAGE MONITORING: Any direct measurement methods that allow the detection of damages in the structure.

FAILURE CONDITION: A condition caused or contributed to by one or more failures or errors that have either a direct or consequential effect on the airplane, its occupants, and/or other persons. In identifying failure conditions, the flight phase, relevant adverse operational or environmental conditions, and external events should be considered (refer to AC 25-19).

FUNCTIONAL HAZARD ASSESSMENT: A systematic, comprehensive examination of functions to identify and classify failure conditions of those functions according to their severity (refer to ARP4754).

INDEPENDENCE: (1) A concept that minimizes the likelihood of common mode errors and cascade failures between aircraft/system functions or items. (2) Separation of responsibilities that assures the accomplishment of objective evaluation (e.g., validation activities not performed solely by the developer of the requirement of a system or item) (refer to ARP4754).

INSTRUCTIONS FOR CONTINUED AIRWORTHINESS (ICA): Documentation that sets forth instructions and requirements for the maintenance that is essential to the continued airworthiness of an aircraft, engine, or propeller (refer to AC 25-571-1).

INTEGRITY: Attribute of a system or an item indicating that it can be relied upon to work correctly on demand (refer to ARP4751).

OPERATIONAL MONITORING: Any indirect measurement methods that can contribute to the evaluation of a structure's condition or utility.

PRELIMINARY SYSTEM SAFETY ASSESSMENT: A systematic evaluation of a proposed system architecture and its implementation, based on the Functional Hazard Assessment and Failure Condition classification, to determine safety requirements for systems and items (refer to ARP4754).

PRODUCT: (1) Hardware, software, item, or system generated in response to a defined set of requirements (refer to ARP4754). (2) Aircraft, aircraft engines, propellers, as well as appliances and components or parts (refer to FAA CPI Guide).

QUALIFICATION: The processes of verifying that a product (system, hardware, and software) complies with a specified set of performance and airworthiness requirements.

REGULATORY ACCEPTANCE: The process of formally accepting, certifying, or "selling-off" a system against one or more regulatory or industry standards.

REGULATORY ACCEPTANCE TESTING: The verification (usually testing) activities involved in formally accepting, certifying, or “selling-off” a system against one or more regulatory or industry standards.

SYSTEM COMPLEXITY: An attribute of systems or items that makes their operation difficult to comprehend. Increased system complexity is often caused by such items as sophisticated component and multiple interrelationships.

SYSTEM SAFETY ASSESSMENT: A systematic, comprehensive evaluation of the implemented system to show that the relevant safety requirements are met (refer to ARP4754).

VALIDATION (REQUIREMENTS): The determination that the requirements for a product are correct and complete. It answers the question, “Are we building the right aircraft/system/function/item?” (Refer to ARP4754.)

VALIDATION (SYSTEM): The demonstrated assurance that the IVHM system meets the value proposition and benefits stated in the business case (refer to ARP6803).

VERIFICATION: The evaluation of an implementation of requirements to determine that they have been met. It answers the question, “Did we build (implement) the aircraft/system/function/item right?” (Refer to ARP4754.)

2.3 Acronyms and Abbreviations

A4A	Airlines for America, formerly known as Air Transport Association of America, Inc. (ATA)
AC	advisory circular (FAA) or airworthiness certificate
AL	assurance level
ARP	Aerospace Recommended Practice
BIT	built-in test
BSCU	braking system control unit
CCA	common cause analysis
CFR	Code of Federal Regulations
COTS	commercial off-the-shelf
CNS/ATM	communication, navigation, surveillance, and air traffic management system
CONOPS	concept of operations
CBM	condition-based maintenance
CMS	central maintenance system
DA	design authority
DAL	development assurance level
DAQ	data acquisition
DoD	Department of Defense
DoDAF	DoD architecture framework
DTS	data transfer system

EASA	European Aviation Safety Authority
EMI	electromagnetic interference
FAA	Federal Aviation Agency
FAR	Federal Aviation Regulations
FHA	functional hazard assessment
FMEA	failure modes and effects analysis
FMECA	failure modes, effects, and criticality analysis
FTA	fault tree analysis
HRC	health-ready component
HUMS	health and usage monitoring system
ICA	instructions for continued airworthiness
IEEE	Institute of Electrical and Electronics Engineers, Inc.
ISO	International Organization for Standardization
IT	information technology
IVHM	integrated vehicle health management
LGCU	landing gear control unit
MoDAF	Ministry of Defense (UK) architecture framework
MRB	maintenance review board
MRBR	maintenance review board report
MSG-3	Maintenance Steering Group 3
MTBF	mean time between failures
OEM	original equipment manufacturer
OPS	operations
PSSA	preliminary system safety assessment
RTCA	RTCA, Inc.
RUL	remaining useful life
SSA	system safety assessment
TSO	technical standard order
UK MOD	United Kingdom Ministry of Defense
WOW	weight on wheel

3. IVHM BASICS

The recommended best practice and guidance provided in this ARP are strictly advisory in nature and can be used with other IVHM ARPs and an organization's existing engineering design practices. There are situations where good design requires that these guidelines be extended or modified to utilize the vehicle's inherent design to realize the benefits of the particular IVHM system solution.

Ultimately, an IVHM system should deliver the operational improvements targeted by the enterprise stakeholders. These operational improvements may be documented in the system concept of operations (CONOPS) and operational use cases, which are, in turn, used to develop the system requirements specification (refer to ARP6883) employed in developing the IVHM system architecture (refer to ARP6290). Given that the concept of operations and operational use cases drive the system design, the guidance in this document focuses on validation and verification of elements traditionally not covered by the myriad of existing validation and verification specifications and standards in our industry. Hence, this document addresses verification of onboard and off-board IVHM system elements and validation of the IVHM system using end-to-end test scenarios based on the operational use cases. Validation performed during different phases of the design also need to be considered (i.e., requirements validation, architecture validation, etc.) in addition to any final regulatory acceptance activities that occur post system integration.

SAE technical committees created documents to provide guidance on aspects of the IVHM development process (see 3.1). These documents utilize the system engineering activities outlined by the International Council on Systems Engineering (INCSE) and the more specific IVHM systems engineering process described in SAE IVHM texts (see 2.1.1). In addition, ISO 13374 provides guidance on functional layers for health management systems. Since an IVHM practitioner may not have an extensive systems engineering background, some fundamentals of this discipline are restated in an IVHM context. Systems engineers may find IVHM-specific considerations that may not be obvious without prior IVHM experience.

3.1 The IVHM Development Process

IVHM system development starts, like most systems, by determining the organizational goals of the sponsoring and user communities. Requirements for the system evolve from these goals. The system architecture then provides a framework to inform and govern the system design. The architecture must enable a detailed system design process to be completed. Together, these steps lead to a robust and efficient implementation that supports organizational goals and requirements for the planned system life cycle. At each life cycle step, there are checks to ensure alignment with the constraints of previous steps. This leads to iterations in the process, where the design space is explored and new opportunities, risks, and constraints are revealed.

Several SAE standards cover various portions of the IVHM system development process. ARP6803 is the cornerstone document, anchoring the hierarchy of IVHM standards. Organizational goals and business cases are covered in ARP6275. Requirements development is addressed in ARP6883. These documents serve as the basic inputs to the architecture development process. Another potential input is covered in SAE JA6268, which covers health-ready components (HRC) and systems. The concepts from SAE JA6268 can help the IVHM architect standardize interfaces at various levels of the architecture (refer to ARP6290). Finally, the architecture drives detailed design as covered in ARP6407. ARP6461 provides guidance on structural health monitoring applications. Other IVHM standards (both current and future) may provide additional context.

The validation and verification activities that should be performed during the various development phases of IVHM system are depicted in Figure 1 (refer to Buderath et al. [2016]). System validation is the demonstrated assurance that the IVHM system meets the value proposition and benefits stated in the business case. See Figure 2 for an example of stakeholder value proposition (refer to ARP6803).

A clear understanding and representation of the functions to be accomplished provide the framework for capturing how a system can fail, the manifestations of the failure, its consequences, and its impact on the vehicle as a whole. Thus, the left side of Figure 1 provides inputs (and vice versa) to IVHM design and development. Maintenance strategy aims to map all fault modes at individual and system levels to different maintenance categories (decision logic based on existing guidelines: SAE JA1011, SAE JA1012, NAVAIR 00-25-403, and ATA MSG-3 with suitable modification).

ARP4754 primarily emphasizes the validation of airborne system requirements with the expectation that the system requirements should be fully matured and frozen before moving on to the system design. The expectation that system requirements are mature and frozen is heavily influenced by the waterfall model of system development and may not be sufficient to address the IVHM system development, which happens in an iterative manner. There is a need to revalidate or redefine the system requirements based on the findings and learnings from other phases like design and integration. Hence, while using the guidelines of ARP4754 for the IVHM system requirements validation, there is a need for continuous validation of the system through all other phases against IVHM-specific considerations.

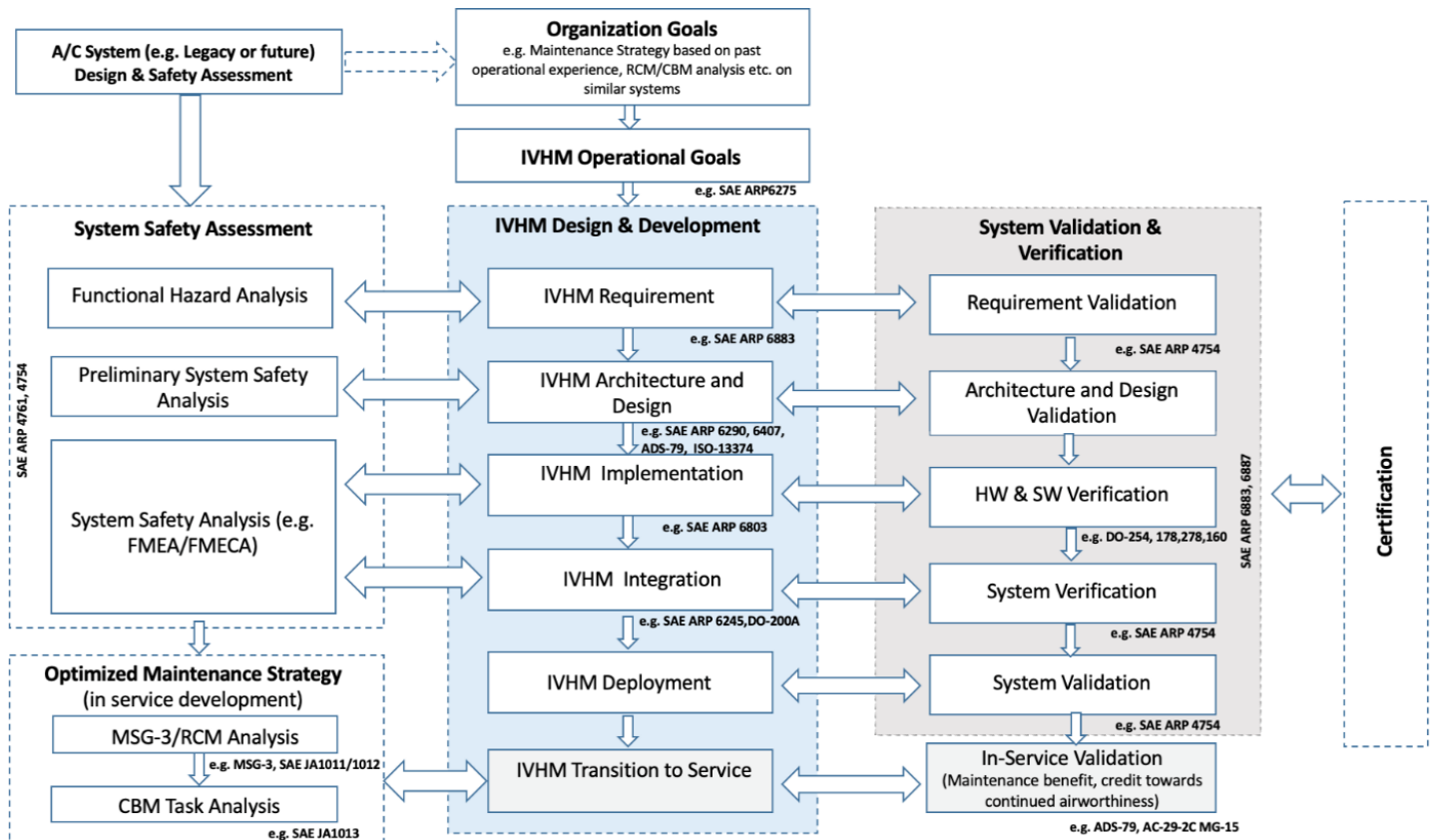


Figure 1 - IVHM validation and verification