



AEROSPACE RECOMMENDED PRACTICE

ARP6407™

Issued

2019-07

IVHM Design Guidelines

RATIONALE

Integrated vehicle health management (IVHM) systems are increasingly being designed and incorporated on different aerospace platforms, but very little guidance exists for the systems engineering aspects of IVHM design. This document provides information and guidance to system program managers and IVHM developers for the IVHM design process. This document can serve as a framework from which to develop specific design plans as an integrated part of the overall IVHM systems engineering process.

TABLE OF CONTENTS

1.	SCOPE.....	3
1.1	Purpose.....	3
1.2	Applicability.....	3
2.	REFERENCES.....	3
2.1	Applicable Documents.....	3
2.1.1	SAE Publications.....	3
2.1.2	ISO Publications.....	4
2.1.3	MIMOSA Publications.....	4
2.1.4	IEEE Publications.....	4
2.1.5	INCOSE Publications.....	4
2.1.6	ARINC Publications.....	4
2.1.7	U.S. Government Publications.....	4
2.1.8	Other Publications.....	4
2.2	Abbreviations.....	5
3.	THE IVHM DEVELOPMENT PROCESS.....	6
3.1	Organizational Goals Influence on IVHM Design.....	7
3.2	Vision.....	8
4.	DESIGN ANALYSIS AND CONSIDERATIONS.....	9
4.1	Design Principles.....	9
4.2	IVHM Design Analysis.....	10
4.2.1	System Safety Analysis.....	10
4.2.2	Failure Modes and Effects (Criticality) Analysis (FMEA/FMECA).....	11
4.2.3	System Reliability Predictions.....	11
4.2.4	Diagnostic (Testability) Analysis.....	11
4.3	IVHM Functional Reference Model.....	12
4.4	Vehicle Health Monitoring Functions.....	13
4.5	Core IVHM Functions and Processes.....	14
4.6	New System Design versus Retrofit Design.....	16

SAE Technical Standards Board 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 © 2019 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, 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 ARP6407

SAE values your input. To provide feedback
on this Technical Report, please visit
<http://standards.sae.org/ARP6407>

Documents
Document Sharing Hub

5.	SUBSYSTEM HEALTH MONITORING AND INTEGRATION	17
5.1	Subsystem IVHM Design Analysis	17
5.2	Subsystem IVHM Models	18
5.2.1	Subsystem IVHM Design Process - Clean Sheet System	18
5.2.2	Subsystem IVHM Design Process - Retrofit System	19
5.2.3	Health-Ready Subsystems	20
5.3	Subsystem IVHM Architectural Considerations	21
6.	PLATFORM LEVEL HEALTH MONITORING AND INTEGRATION	22
6.1	Platform IVHM Design	22
6.2	Platform IVHM Design Process - Clean Sheet System	23
6.3	Platform IVHM Design Process - Retrofit System	25
6.4	Platform Level Failure Reasoning	26
7.	ENTERPRISE (FLEET) IVHM DESIGN	29
7.1	Realizing Organizational Goals	30
7.2	Enterprise IVHM Design - Clean Sheet Program	30
7.3	Enterprise IVHM Design - Retrofit Program	32
8.	INTEGRATED IVHM DESIGN	34
8.1	IVHM Function and Process Implementation Considerations	35
9.	Summary	38
10.	NOTES	38
10.1	Revision Indicator	38
Figure 1	SAE HM-1 document mapping to the IVHM development process	6
Figure 2	IVHM system hierarchical view (adapted from System Health Management with Aerospace Applications, S.B. Johnson, et al.)	13
Figure 3	Primary IVHM design stages	17
Figure 4	IVHM design flowchart for new system/subsystem design	19
Figure 5	Design flowchart for retrofit system/subsystem design	20
Figure 6	Illustration of interaction between subsystem IVHM design and enterprise processing	21
Figure 7	IVHM subsystem design phases	22
Figure 8	Design flowchart for new platform solutions	24
Figure 9	Design flowchart for retrofit platform level solutions	26
Figure 10	Representative diagnostic model fragment	27
Figure 11	Building the fault model or propagation rules	27
Figure 12	IVHM platform design phases	29
Figure 13	Design flow for enterprise processing (EP)	31
Figure 14	Design flow for enterprise process working with retrofit IVHM	33
Figure 15	Detailed design of an IVHM enterprise process	34
Table 1	IVHM functional reference model (ISO 13374)	12
Table 2	Common functions and processes within the IVHM functional blocks	15
Table 3	Enterprise processing design consideration for retrofit IVHM	33
Table 4	Typical IVHM design implementation across levels	35

1. SCOPE

This Aerospace Recommended Practice (ARP) provides guidance for the design of an integrated vehicle health management (IVHM) capability that will extend the vehicle's inherent design to enable health management of the platform and its components. This guidance is technology-independent; the principles are generally applicable to the majority of potential IVHM design scenarios, including "clean sheet" system design, where IVHM is considered as a primary design consideration, and the retrofit design, where existing systems are modified and leveraged with the IVHM capability. In either case, this ARP provides guidance for designing the IVHM capability from the feasibility assessment to the conceptual design analysis and to the development design phases, with considerations given to trade studies, metrics, and life cycle impacts.

1.1 Purpose

The purpose of this ARP is to provide information and guidance for the IVHM design process. The information can serve as a framework from which to develop specific design plans as an integrated part of the overall IVHM systems engineering process, as described in Section 1. As such, this ARP is not intended as a legal document, but only as a technical guide to help IVHM system designers understand the engineering trade-offs between different solution alternatives, improving developer productivity and encouraging adoption of the technology.

1.2 Applicability

This document applies primarily to aerospace systems, either commercial or military. The principles expressed herein, however, are largely independent of the application and may have general applicability to ground vehicles or any complex system.

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.

AIR5109	Applications of Probabilistic Methods
ARP1587	Aircraft Gas Turbine Engine Health Management System Guide
ARP4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
ARP5580	Recommended Failure Modes and Effects Analysis (FMEA) Practices for Non-Automobile Applications
ARP6275	Determination of Cost Benefits from Implementing an Integrated Vehicle Health Management System
ARP6803	IVHM Concepts, Technology and Implementation Overview
JA6268	Design & Run-Time Information Exchange for Health-Ready Components

Jennions, I., "Integrated Vehicle Health Management: Perspectives on an Emerging Field," (Warrendale, PA, SAE International, 2011), doi:10.4271/R-405.

Jennions, I., "Integrated Vehicle Health Management: The Technology," (Warrendale, PA, SAE International, 2013), doi:10.4271/R-429.

2.1.2 ISO Publications

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

ISO 13374-1 Condition Monitoring and Diagnostics of Machines - Data Processing, Communication, and Presentation, - Part 1: General Guidelines

ISO 13374-2 Condition Monitoring and Diagnostics of Machines - Data Processing, Communication, and Presentation, - Part 2: Data Processing

ISO/IEC 15288 Systems and Software Engineering - Systems Life Cycle Processes

2.1.3 MIMOSA Publications

Available at <http://www.mimosa.org/mimosa-osa-cbm/>.

OSA-CBM 3.3.1 Open System Architecture for Condition-Based Maintenance

2.1.4 IEEE Publications

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

1232-2010 Standard for Artificial Intelligence Exchange and Service Tie to All Test Environments

Wilmering, T., "A Practical Examination of Model Reuse," IEEE Autotestcon. Salt Lake City, Utah, 2008.

2.1.5 INCOSE Publications

Available from the International Council on Systems Engineering, 7670 Opportunity Road, Suite 220, San Diego, CA 92111-2222, USA, Tel: 858-431-1725, www.incose.org.

TP-2003-002-03.1 Systems Engineering Handbook - A Guide for System Life Cycle Processes and Activities, Fourth Edition

2.1.6 ARINC Publications

Available from ARINC, 2551 Riva Road, Annapolis, MD 21401-7435, Tel: 410-266-4000, www.arinc.com.

ARINC 624-1 Design Guidance for Onboard Maintenance System

2.1.7 U.S. Government Publications

Systems Engineering Fundamentals, Department of Defense, January 2001, https://ocw.mit.edu/courses/aeronautics-and-astronautics/16-885j-aircraft-systems-engineering-fall-2005/readings/sefguide_01_01.pdf.

2.1.8 Other Publications

ISBN 978-0-470-74133-7, *System Health Management with Aerospace Applications*, Johnson, S.B., Gormley, T., Kessler, S., Mott, C., Patterson-Hine, A., Reichard K., Scandura, P.A. Jr., editors, 2011.

ISBN 978-146668490, *Emerging Design Solutions in Structural Health Monitoring Systems*, Tibaduiza Burgos, D., Mujica, L. Rodellar, J. editors, 2015, pp. 234-273.

ISBN: 978-0-4701-9590-1, *Systems of Systems*, Jamshidi, M., editor, 2009.

2.2 Abbreviations

AG	Advisory Generation (ISO 13374 layer)
ARINC	Aeronautical Radio, Incorporated
ARP	Aerospace Recommended Practice
BIT	Built in Test
CA	Corrective Action
CBA	Cost Benefit Analysis
CBM	Condition Based Maintenance
DA	Data Acquisition (ISO 13374 layer)
DM	Data Manipulation (ISO 13374 layer)
EP	Enterprise Processing
FHA	Functional Hazard Assessment
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects and Criticality Analysis
HA	Health Assessment (ISO 13374 layer)
HI	Health Indicators
IEEE	Institute of Electrical and Electronics Engineers
INCOSE	International Council on Systems Engineering
IP	Intellectual Property
IVHM	Integrated Vehicle Health Management
KMS	Knowledge Management System
LCC	Life Cycle Cost
LRU	Line Replaceable Unit
MBD	Model Based Development
MIMOSA	Machinery Information Management Open Systems Alliance
OEM	Original Equipment Manufacturer
OSA-CBM	Open Systems Architecture for Condition Based Maintenance
PA	Prognostics Assessment (ISO 13374 layer)
ROI	Return on Investment

RUL	Remaining Useful Life
SD	State Detection (ISO 13374 layer)
SE	Systems Engineering
SRU	Shop Replaceable Unit
TTF	Time to Fail
UBL	Usage Based Lifting
V&V	Verification and Validation
U.S.	United States

3. THE IVHM DEVELOPMENT PROCESS

The goal of this ARP is to provide recommendations for how to approach the design of an IVHM system, given a satisfactory set of goals, requirements, and architectural specifications with which to begin. The SAE HM-1 Integrated Vehicle Health Management Committee is creating a series of related documents that provide guidance for each of these major IVHM system development activities, as shown in Figure 1. The reader may refer to the other ARPs for information on the related health management process activities. This document tree reflects the current SAE IVHM document configuration as of the date of publication—some listed may still be in development. Future documents that are released will be included in the tree in future updates of this document.

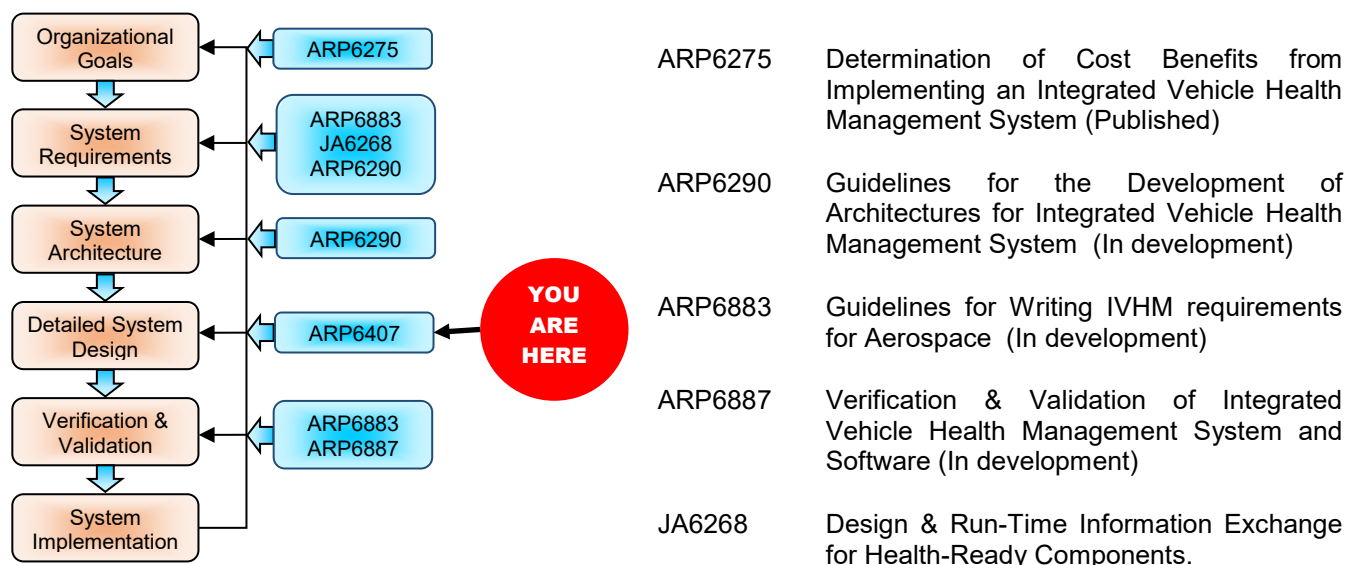


Figure 1 - SAE HM-1 document mapping to the IVHM development process

The IVHM development process should be approached in the way one approaches the development of any complex system. One starts by determining the organizational goals of all stakeholders. The requirements for the system are evolved from these goals, and system architecture is then produced that provides the framework to support the instantiation of the system requirements. A detailed system design process is then undertaken that should lead to a robust and efficient implementation that will support organizational goals and requirements for the planned life of the system. At each step along the way there are numerous “reality checks” to ensure one is aligning with the constraints of previous steps, and these naturally lead to iterations in the process.

Detailed design ultimately derives from the developing entity's organizational goals. An IVHM business case can be thought of as a part of the justification for an organizational investment in the provision of system health management capability. Any business case should be based upon a firm understanding of the business goals for the sponsoring organization. By documenting the expected costs, benefits, and risks, the business case serves as a repository for the rationale and justification for decisions on system needs and whether it is prudent to proceed with a project from an organizational perspective. The business case typically identifies, at a very high level, initial views of interfaces between the IVHM system characteristics to be developed and its users and dependencies, as well as quantifiable goals on system performance and life cycle costs which help define system success criteria. There may be other organizational goals beyond quantifiable performance and "return on investment" criteria, such as technological imperatives. For example, an examination of whether the proposed project aligns with an existing business strategy. Together, these organizational goals provide a primary input to IVHM system requirements from a business perspective, which drives system architecture as well as subsequent system design and implementation.

The overall design of an IVHM system can be viewed as a series of decisions, each serving to satisfy an organizational goal. The approach taken to an IVHM business case analysis is dependent on many factors, which are detailed in Section 4. In general, organizational direction and cost goals are used as input to the IVHM development process.

3.1 Organizational Goals Influence on IVHM Design

While IVHM processes typically seek to maximize one or more aspects of product safety, availability, or operation, there is often a goal to simultaneously reduce total system ownership costs. Furthermore, other organizational goals may frequently drive initial desires to pursue various technological solutions. A disciplined process is required to determine how to best allocate financial and technological resources to best satisfy requirements for system availability at an optimum value of life cycle cost (LCC). Ultimately, IVHM may cease to be thought of as an up-front supportability price tag to be paid, but rather be recognized as an essential function in producing affordable aerospace systems. To that end, the business analysis should be derived from top level functional requirements and directly influence IVHM system design requirements and, therefore, the overall system design. A good introduction to possible ways of developing a cost benefit analysis for IVHM systems is given in ARP6275.

Approaches to a particular IVHM problem can vary significantly and can be:

- a. A diagnostic approach, in which a system is allowed to run to failure; where the failure signature is typically mapped to the corresponding set of repair procedures.
- b. A predictive (or prognostic) approach, in which system failure is predicted at some time before the failure will affect system operation.
- c. As a preplanned integrated approach, in which scheduled maintenance, flight operations, logistics, and supplier/OEM operations are optimized using the IVHM decision support system.

Which approach or a combination of them are selected depends on consideration of the pros and cons of each with respect to system performance, maintenance, safety, and life cycle cost attributes. Even though prediction of failures (or prognostics) is often considered to be the ultimate IVHM design goal, a prognostic approach should be considered to be only one means towards an effective, integrated health management solution. Diagnostic or integrated, scheduled maintenance approaches may prove to be more cost effective over the life of a product. When considered in the broader view of platform and fleet level health management requirements, implementation of a balanced and efficient methodology will achieve a balance of health management technologies with the right mix of diagnostic, prognostic, and scheduled maintenance approaches based on available resources and life cycle cost considerations.

The organizational goals regarding an IVHM system may include scheduled reliability for a new or operating vehicle, cost reduction (fault detection, isolation, and prognostics goals directly affect maintenance and operation costs), and business opportunities such as new products and services.

The three levels of IVHM design, namely the designs at the level of subsystem, platform, and enterprise, are detailed in the following sections and each must support achievement of organizational goals. As platform subsystems provide the sensing, processing, and interfaces to feed platform and enterprise health management systems with the necessary information, the subsystems must be optimized for these qualities to achieve health management goals as early in the design cycle as possible. The platform must effectively communicate with both subsystems and the enterprise, and further provide some level of integration of health information across system boundaries. Enterprise level health management considerations should be integrated with other enterprise actors (maintenance, operations, regulators, logistics) to provide effective decision support.

3.2 Vision

The recommendations of this ARP are strictly advisory in nature and are suggested to be used in concert with the other ARPs as shown in Figure 1. There might be situations where good design requires that these design guidelines be extended or modified to maximize use of the vehicle's inherent design and optimize the benefits of a chosen solution. The guidelines were developed by drawing from the experiences of key aerospace defense programs and commercial IVHM initiatives and implementations.

This document presents an overview of how IVHM implementations for systems with different degrees of complexity should be designed to provide maximum effectiveness across a system's life cycle. The overview is agnostic to the type of system the IVHM design may be applied to; different technologies (e.g., hydraulic, pneumatic, or avionic systems) may require quite different approaches. Technology-specific guidelines might be developed for such specific technologies in the future.

The primary, and most challenging, requirement is to integrate the IVHM design with the overall system design to the greatest extent possible. This reflects a concurrent engineering view. While the benefits of concurrent engineering for system health have long been recognized, it is nonetheless typically a challenge in most engineering organizations to elevate system health management requirements to the same level of priority as other system design goals.

This is not to say that all IVHM designs are implemented at system design time; the need for health management solutions is often made apparent long after the system has been designed and deployed. When IVHM solutions must be implemented within a "legacy" system framework, the IVHM approach must still be integrated into the existing system design in the most symbiotic way possible.

The approaches described in this document assume that every effort is made to equate IVHM functional and physical requirements with system operational requirements, and to consider the ramifications of IVHM as a design attribute of a system for its entire life cycle. Because IVHM cuts across all aspects of system design and implementation throughout the system life cycle in this way, this necessitates the adoption of a systems engineering view of IVHM design. Refer to *Integrated Vehicle Health Management - Perspectives on an Emerging Field* (Jennions, 2011) and *System Health Management: with Aerospace Applications* (Johnson, 2011).

Design and implementation of IVHM systems necessarily integrates contributions from multiple disciplines, communicates with multiple physical and logical subsystems, and involves human interaction from designers, owners, operators, and maintainers. IVHM system developers must be keenly aware of IVHM dependencies and influences on system design and subsequent implementation. Trade studies are required to assess system interactions and influences to ensure that the symbiosis of IVHM and system primary function is mutually effective and ultimately supports customer operational and support goals. For example, a key consideration is an upfront life-cycle cost (LCC) evaluation that explores the benefit of integrating IVHM to different degrees for different components and subsystems, contrasting the technical implementation issues and goals with customer cost and operational considerations. These LCC analyses are more specific in nature than the top-level business case described previously, and typically compare different technical implementations of solutions for the specific IVHM issues under consideration.

The barriers to concurrent engineering often turn out not to be technical, but rather political and organizational in nature. While this document does not address these latter issues, the suggestions contained herein provide the basis for a reasoned set of arguments for optimizing IVHM as a function of system design, thus providing “design-for-IVHM” methodology that fundamentally alters the way systems are designed by including health management design attributes. For example:

- Materials and design strategies that are amenable for monitoring or other health management purposes.
- Modular building blocks that lend themselves to evolving systems where partial (as opposed to complete) redundancies can be leveraged.
- An architecture that responds in real-time to the needs of the system with the goals of satisfying primary mission objectives (e.g., “bring the system home safely” or “on-time dispatch”) and supporting IVHM system maturation as operational experience is accumulated.
- Data management systems that can accommodate the data acquisition, storage, and processing needs of an IVHM system.

4. DESIGN ANALYSIS AND CONSIDERATIONS

4.1 Design Principles

The term “integrated vehicle health management,” as used in this document, is meant to encompass both the monitoring and data processing functions inherent within the vehicle subsystems, the vehicle itself, and the tools and the processes used to manage and restore the vehicle’s health at the enterprise level. These functional elements are required to deliver a complete IVHM system solution and drive the operational, safety, and economic benefits desired by an organization.

There are four system design principles that should be considered when designing an IVHM solution for aerospace platforms. Each principle is followed by referencing the associated general design guidelines included in this ARP:

1. *Design of health management functionality of engineered systems should be cast as a “systems engineering” task.* Because IVHM is a systems engineering discipline, the system designer must have a systems view of the platform to define the solution that best leverages the inherent design of the system, subsystem, vehicle interfaces, and data processing capabilities.
2. *Health management is not a self-contained, stand-alone function.* Unlike other platform capabilities, health management is a function designed (inherently) within a system. That is, while caution and advisory panels on a vehicle are part of the vehicle’s health management function, monitoring and reporting of the system’s health state is done within the system itself. IVHM design at the platform level should integrate the inherent subsystem capabilities into an optimized solution.
3. *Health management consists of health monitoring functions and the management processes enabled by health state data and information.* The health monitoring function provides the data and information required to assess the health state of the overall system. The management processes encompass the activities, resources, and tools used to identify, manage, mitigate, and resolve actual and impending faults and failures within the vehicle to restore the vehicle to a “healthy state.”
4. *Health management exploits the integration of the system’s inherent design with enabling data processing technologies.* A practical view of IVHM is that its focus is on providing enabling capabilities over the life of the component (or systems) that typically revolve around providing safety and/or affordability. This focus is realized with automated systems and managing the health state data and information across systems and subsystems.

4.2 IVHM Design Analysis

A solid IVHM design approach requires that the IVHM implementations be integrated as a constituent of the overall system design. Critical to the success of the IVHM design is a detailed understanding of intended system functional and physical implementation, and the effects of system failures on functional and physical operation. This understanding is accomplished by undertaking a series of failure propagation trade studies that analyze the impact of system failures on system safety and reliability, as well as the implications of the potential means for detecting and isolating failures (Wilmering, *A Practical Examination of Model Reuse*, 2008). These analyses provide the basis for understanding the options available for the mitigation of system failure and can be used in conjunction with cost benefit studies to ascertain the most effective means of failure mitigation and to prioritize health management resources. Traditionally, most organizations perform these analyses independently, often within different engineering departments. However, an integrated failure propagation analysis that integrates the following traditional engineering analyses is recommended as the most coherent and beneficial approach to supporting a solid IVHM design and implementation.

Throughout this document there is discussion about the creation and use of models. Models in general are representations of real world concepts and may take many forms (e.g., physics models, data models). While there are numerous kinds of models that are extremely useful and indeed central to IVHM Design analysis and implementation, the discussions of models in this document are not meant in any way to imply that IVHM design must utilize model-based development (MBD) engineering design processes, although one could choose to employ MBD if desired. This ARP is agnostic, in general, to the engineering design approach that may be used to implement the IVHM design.

4.2.1 System Safety Analysis

System safety analyses (ARP4761) are commonly performed on aerospace platforms and subsystems, and can be used to inform the IVHM design process. These typically include failure modes and effects analysis (FMEA), fault tree analysis (FTA), event tree analysis, functional hazard assessment (FHA), and probabilistic risk assessments. In an FHA, safety engineers identify unacceptable design features and propose design or usage changes that will mitigate the failure effects and satisfy safety requirements. The idea is that one first identifies system level failures that could result in loss of life or system equipment. For each of these critical functions, a functional analysis is performed of how the system works in normal operating conditions, then determines which failure modes could lead to the occurrence of the critical system functional failure. A key element of FTA is to try and quantify the probabilities associated with various failure modes, thereby assessing the criticality levels of these modes. This is a necessary element in the safety assessment of a system and becomes part of the certification records. The model constructed is typically referred to as a fault tree. Specifically, the FTA process looks like this:

1. Select a top-level event for analysis.
2. Identify “local” functional failures that would produce the top-level event should they occur. These failures are then related to the top-level event either directly or by representing their logical relationship to the top-level fault. That is, it may be the case that several lower level failures need to occur to produce the top-level failure, which is represented via an AND gate. Alternatively, it may be the case that one or more of a select number (“m of n”) failures must occur to produce the top-level failure; this is represented as either a simple or constrained (specific “m of n”) OR relationship.
3. Continue in this manner until a “root cause” is reached, represented in most cases as a physical fault in some hardware component (although an FHA may be purely functional, as well). Root cause may also be an external system event, such as human error, for example.
4. Identify mitigating conditions, such as the addition of redundancy in one or more systems, or the increase of reliability of some physical component, or even an operational method that may mitigate the failure effect in some way. In rare cases, this may result in a complete redesign.

Most FTAs also include the notion of probability of occurrence; the failure rates of the lowest level faults are considered and the hazard (or risk) probability is calculated as the probability of occurrence of each of the events in the failure tree that is constructed.

4.2.2 Failure Modes and Effects (Criticality) Analysis (FMEA/FMECA)

In a failure modes and effects analysis (or failure modes and effects criticality analysis) (ARINC 724), all possible failure modes of the system/parts are identified together with the failure rate (and criticality), that will help the IVHM design focus on the potential failures most harmful to the system health. The process typically starts with the lowest level hardware (piece part FMEA/FMECA) or system functions (functional FMEA/FMECA), determines the fundamental failure modes that have a direct effect on those piece parts or elemental functions, and then represents system functional effects at successive indenture levels of the system. The failure rates of the associated failures are often taken into consideration. A FMECA adds the notion of failure criticality to a FMEA. There are several different standards that organizations may choose to adhere to, and many FMEAs are variations on one of several themes. For instance, many organizations include the notion of monitors, or the tests that detect the failure of a function at some level of indenture. Other FMEAs may include the notion of failure mitigation as well.

4.2.3 System Reliability Predictions

This analysis calculates the probability that a series of system operations will conclude successfully. For instance, a commercial aircraft flight might be composed of five distinct phases: takeoff, climb, cruise, descent, and landing. The reliability of the entire flight is the series reliability of each of the flight's phases that is based on the probability of failure of the system functions required to support that phase. This probability is a function of the duty cycle of the required functions, the related failure modes, and their probability of occurrence.

Each system phase is modeled by creating a block diagram of system operation, where the blocks usually represent system functions, (but in some approaches, might represent system components). The blocks are connected to represent system functional flow, and redundant or reconfigurable functions are connected via AND and OR gates to represent the system design for fault tolerance. The reliability of each block is calculated based on its constituent reliabilities, and the overall reliability of the system is then calculated based on the series reliability of the operational phases.

This topology has some fundamental traits in common with the safety fault tree analysis.

4.2.4 Diagnostic (Testability) Analysis

Diagnostic models are typically used for either analysis of a system's potential to realize health management goals, as a design aid, or to support execution of fault isolation reasoning. Great synergies and consistency may be realized if the analytical model is used to support the reasoning process.

Diagnostic analysis models are typically created to support one or more of three primary goals: predictions of fault detection, fault isolation, or the design of a preliminary test strategy (results of these analyses may then be used to influence design to optimize these characteristics). Fault detection analysis calculates the percentage of system faults (defined as specific component failure modes) that can be detected by the prescribed tests. Fault isolation analysis determines the failure ambiguity groups that will result from exercising the tests over the fault universe, and test strategy analysis will determine the optimal sequence of tests to be performed based on the fault universe, prescribed tests, and other optimization criteria. In addition to tests and faults, these analyses typically take into consideration system failure rates and system components (failure ambiguities are typically mapped to components and expressed in terms of replaceable components). Optimization criteria may include failure rates, test times or costs, component costs, or other significant attributes of the system or associated resources required to support the test process. Additionally, diagnosis sometimes focuses on isolating system functional failure.

Diagnostic analysis models or their test strategies may be used as input to tools that create, or help direct the creation of, executable system diagnostics. There are numerous examples of applications in practice today where test strategies are used to support creation of test requirements documents for automatic test equipment, and where diagnostic models and test strategies are used in diagnostic development tools to support real time diagnostic reasoning applications.

Diagnostic reasoning models support a wide variety of fault isolation approaches. Diagnostic reasoning methods may be simple or quite complex. Some of the most common include the processing of static pre-computed binary decision trees (by far the most prevalent approach to fault isolation reasoning), dynamic (i.e., not pre-computed) causal reasoning from data structures such as causal graphs or D-matrices, Bayesian reasoning on causal graphs, or formal logical inference. While each of these approaches (and models) possess their own unique characteristics and information elements, they all utilize common elements, such as the entities representing the relationships among system components, failures, tests, functions, etc. An IEEE industry standard for diagnostic reasoning model representation, exchange, and application support services describes each of these approaches and supports model integration across systems (IEEE 1232).

4.3 IVHM Functional Reference Model

This document incorporates the design principles within ISO 13374 and the underlying principles of the open systems architecture for condition-based maintenance (OSA-CBM) that encapsulate the primary design functions in an IVHM system component or subsystem. This guidance provides practitioners with a common functional reference model for characterizing specific subsystem, system, and enterprise health monitoring functions in support of modular design and interoperability. A description of these functional elements is given in the first two columns of Table 1.

Table 1 - IVHM functional reference model (ISO 13374)

IVHM Functional Block	Description	IVHM Process Stage
Advisory Generation (AG)	This function provides actionable information to operational and maintenance personnel or external systems.	Act
Prognostics Assessment (PA)	This function provides future state of health, performance life remaining, or remaining useful life (usage) indicators.	Analyze
Health Assessment (HA)	This function provides information to determine the current state of health of equipment.	
State Detection (SD)	This function evaluates equipment state conditions against normal operating profiles and generates normal or abnormal condition indicators.	
Data Manipulation (DM)	This function processes and transforms the sensor data and health state information collected by the DA.	Transfer
Data Acquisition (DA)	This function collects the sensor data and health state information from the equipment internal monitors, the system data bus or data recorder.	Acquire Store

The IVHM Functional Reference Model facilitates functional analysis and partitioning between and within the subsystem, platform, or enterprise levels of indenture to develop an IVHM system integration strategy and gap analysis. For example, propulsion, avionics, payload sensors, and digital communications systems normally have some inherent health monitoring capabilities (DA, DM, SD). The addition of functional layers (HA, PA, AG) to such systems should be evaluated with respect to integration and cost impacts. Electrical and other vehicle components (drive train, pumps, actuators, landing gear, etc.) that lack inherent foundational HM capability may require the investment in the elements required to perform lower level DA, DM, or SD functions.

A functional model of the system to be designed provides a structured way to think about how the various components of an IVHM system might be partitioned and organized within the IVHM system architecture. Architecture development is a parallel, yet integral, element of any IVHM design process, providing an optimal solution for distribution and integration of the data acquisition, processing, and decision support elements that comprise a design. Table 1 also maps IVHM functional blocks (ISO 13374 layers) to the IVHM (operational) process stages in the last column of the table to provide context for the functions performed at each level. This ARP does not cover architectural specifics.