Chapter 9

Safety and IVHM

Kai Goebel, NASA Ames Research Center

Salus populi suprema lex esto...—Cicero

9.1 Introduction

When we address safety in a book on the business case for IVHM, the question arises whether safety isn't inherently in conflict with the need of operators to run their systems as efficiently (and as cost effectively) as possible. The answer may be that the system needs to be just as safe as needed, but not significantly more. That begs the next question: How safe is safe enough? Several regulatory bodies provide guidelines for operational safety, but irrespective of that, operators do not want their systems to be known as lacking safety. We illuminate the role of safety within the context of IVHM.

9.2 Does Safety Matter?

Two of the core elements in IVHM are providing a state assessment of the system and supporting the resiliency of systems. Abnormal states not only are an inconvenience, but also they can impact safety and lead to loss of equipment, personal injury, and loss of life. Of course, not all events that lead to degraded safety can be prevented by IVHM. However, there is a significant proportion of cases where IVHM can play an important role in informing about, preventing, or mitigating unsafe conditions. The following sections provide a brief summary of accident statistics and incidents in commercial aviation and terrestrial transportation that were caused by—

or attributed to—equipment malfunction (and therefore are a candidate for IVHM systems). By way of example, this section will mainly focus on statistics gathered in the USA. The findings are thought to be applicable to other regions of the world as well.

9.2.1 Accidents Due to Equipment Malfunction in Aeronautics

Accidents in aeronautical applications get a lot of attention because they tend to be dramatic, and often a large number of civilians perish (they also tend to be relatively uncommon). The National Transportation Safety Board (NTSB) is an independent federal agency that investigates, among others, civil aviation accidents in the United States, conducts special investigations and safety studies, and issues safety recommendations to prevent future accidents. The information the NTSB investigators collect during their investigations of these aviation events resides in the NTSB Aviation Accident and Incident Data System [Aviation 2011]. Between 1989 and 2008 there were 2151 fatalities in 600 accidents. Of those, 109 accidents (777 fatalities) were due to equipment malfunction. This amounts to 18% of all accidents and 36% of all fatalities.

The Aviation Safety Reporting System (ASRS) is a joint NASA/FAA database of aviation incident reports submitted on a voluntary basis by pilots, air traffic controllers, ground personnel, and others involved in aviation operations. Because the incidents are reported voluntarily, they are subject to self-reporting biases, and are not corroborated by the Federal Aviation Administration (FAA) or the National Transportation Safety Board (NTSB) and cannot be considered a representative sample of the underlying population of events they describe [ASRS 2001]. However, because it relies on additional information sources, it is a more inclusive repository than the incidents reported to the NTSB. An analysis of 38,894 component failure incidents from January 1993 to April 2011 found that 25,049 of the incidents listed aircraft

equipment as the primary problem and 29,253 listed it as a contributing factor. Table 9.1 lists the numbers by affected component for NTSB-reported accidents and incidents reported in the ASRS database.

Table 9.1 Accidents and Incidents Due to Equipment Malfunction and/or Failure

	NTSB Accidents	NTSB Accidents (%)	ASRS Incidents	ASRS Incidents (%)
Engine	40	*32%*	2036	*14%*
Landing Gear	29	*23%*	1200	*8%*
Fuel	2	*2%*	456	*3%*
Structure	8	*6%*	634	*4%*
Electrical	10	*8%*	1230	*8%*
Flight Control	9	*7%*	2269	*15%*
Hydraulic	11	*9%*	1199	*8%*
Other	13	*10%*	2677	*18%*
Instrumentation/ Communication/ Navigation	5	*4%*	3309	*22%*
Total	127		15010	

9.2.2 Future Safety Risk Analysis

Reveley et al. [2010] performed a survey to identify future aviation safety risks. They include, among others, in-flight loss of control. Loss of control during flight may occur as a result of a stall, an icing-related event, a severe atmospheric turbulence or wake vortex encounter, or a malfunction or failure of a flight-critical system or equipment. As outlined earlier, analysis of NTSB accident data and FAA incident data has established that system/equipment failures and malfunctions are significant contributing factors to aviation safety risk. In addition, the National Aeronautics Research and Development Plan [National 2010] cited several fundamental safety challenges that are relevant to preventing loss of aircraft control accidents caused by system or subsystem malfunctions or failures. Among these are:

- Predicting, monitoring, and assessing the health of aircraft, at the material, subsystem, and component level, more efficiently and effectively.
- Rapidly but safely incorporating technological advances in avionics, software, automation, and aircraft and airspace concepts of operation and operating procedures, by assuring their safety through a rigorous verification and validation process in a cost- and time-effective manner.
- Developing aircraft-level health management systems that can identify problems before accidents occur. Research in health management requires not only monitoring and detecting, but also confident prognostics of latent potential failures before they occur.

9.2.3 Accidents Due to Equipment Malfunction in Terrestrial Transportation

The National Highway Traffic Safety Administration (NHTSA) reports that there were more than 5.5 million police-reported motor vehicle crashes in the United States in 2009. A total of 1.52

million of those crashes resulted in an injury, and 30,797 resulted in a death. Equipment malfunction accounts for somewhat less than 5% of all motor vehicle accidents. The NHTSA report "National Motor Vehicle Crash Causation Survey" [National 2008] lists 6.8% of all cases as equipment malfunction being a contributing factor. The most cited types of equipment failure are loss of brakes, tire blowouts or tread separation, and steering/suspension failure [National 2008].

9.2.4 Safety Does Matter

The previously cited statistics illustrate that safety (or the lack thereof) affects us constantly. The statistics focused on the cases where equipment malfunction or failure was the direct cause and therefore where IVHM methods could help to detect or predict failure, and thus improve safety. While not all accidents due to equipment malfunction are preventable, many are. For example, the UK CAA estimates that around 80% of aircraft mechanical defects (on helicopters) are detectable, so an assumed accident and death/injury prevention rate could be derived using advanced IVHM principles. It has to be recognized that the implementation of IVHM for safety improvement comes at a cost. A system has to have a certain payoff to justify the investment, irrespective of the safety gains. Even regulatory authorities will not mandate safety at infinite cost. Outside that region, the system would not be built. Figure 9.1 illustrates the conceptual connection between safety and cost for both unmanned and manned systems, where the hashed area indicates the infeasible area.

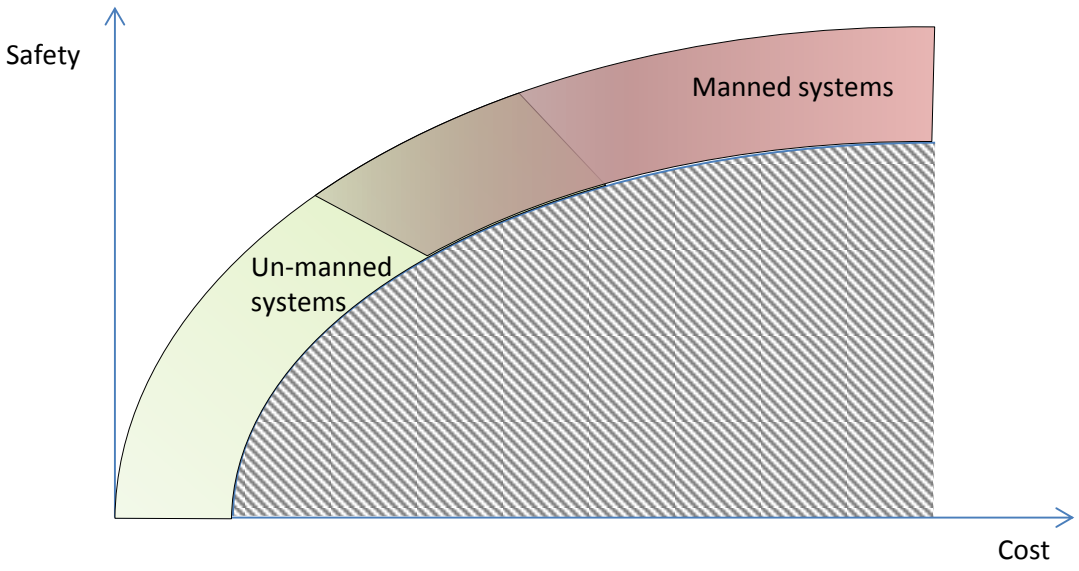

Figure 9.1 Cost-safety balance for IVHM systems.

9.3 Safety as a Driver for Operations in Space and Aeronautics

The following sections illuminate the experience and efforts for IVHM in space and aeronautics that have been at the forefront of health management development.

Space Flight

Fundamentally, the objective of safety in space flight is similar to other domains, namely to protect personnel and equipment from damage or loss. But in space operations, the risk to personnel from equipment failure and the financial implications for equipment loss are usually significantly higher than in terrestrial applications. This, in turn, motivates the use of health management technology. The strategy followed is to employ several layers of protection that start with a fault avoidance strategy. The latter seeks to prevent faults from happening in the first place through conservative design practices (e.g., reducing moving parts) and performance margins. The next layer seeks to make the system fault tolerant through the appropriate level of

redundancy, fault containment, or design for graceful degradation. These measures are categorized as fault masking where the occurrence of a fault is compensated through hardware measures. The last layer of fault management is active fault detection, identification, and recovery. These are the functions that are typically also found in IVHM approaches and include the same range of technology solutions. Figure 9.2 illustrates this taxonomy.

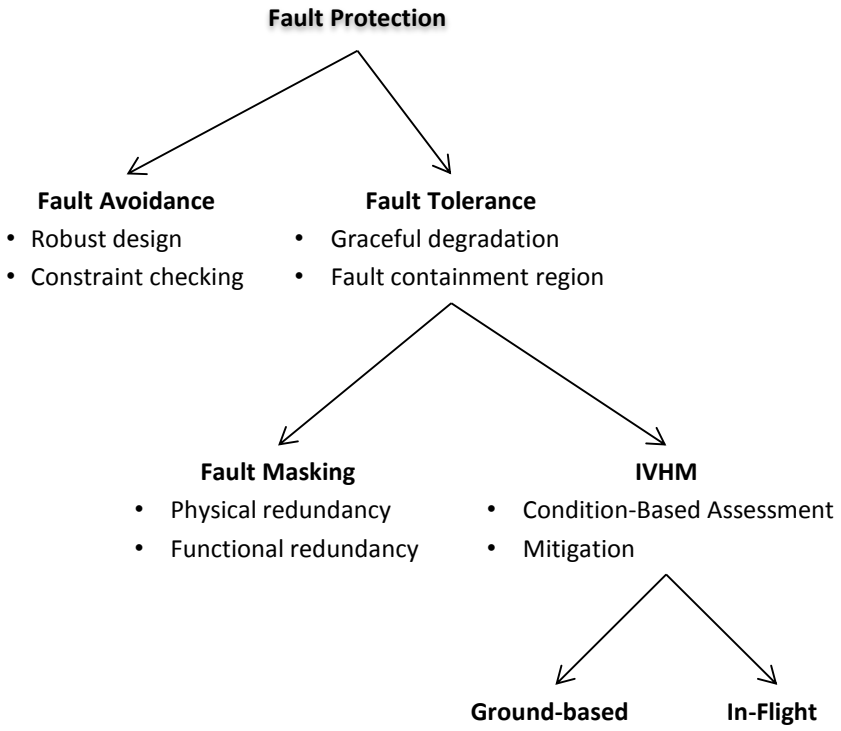

Figure 9.2 Taxonomy for fault protection in unmanned space applications (adapted from [Day and Ingham 2011]).

Space operations can point to a series of successful fault protection events in manned and unmanned space flight. The range of successfully resolved faults include despun power bus reset caused by debris shorts (Galileo); a software flaw that caused heartbeat termination (Magellan); attitude estimator transient during backup star tracker checkout (Cassini); cosmic ray upset of attitude control electronics (Dawn); overvoltage due to unexpected power interaction at launch

(Kepler) [Day and Ingham 2011]; and various non-catastrophic glitches during the space shuttle missions.

It should be noted here that unmanned space flight is encumbered with additional constraints such as operation with only limited ground contact. In particular, there may be extended periods with no planned contact that range from 1 to 4 weeks; the planned contact periods may be short (1 to 2 hours); ground contact may not be established even for planned contacts (5% to 10%); and large one-way transmission times in the range of minutes to hours as well as very low downlink data rates, possibly only 10 to 40 bps, may be experienced. In addition, a system must possibly survive without maintenance for primary missions lasting a decade or longer and survive in harsh radiation and thermal environments.

Manned space flight has its own constraints. For example, astronauts on the International Space Station (ISS) spend roughly 10% of their time with scientific work; 67% of the time is consumed with life-sustaining activities (sleep, meals, exercise). The rest is spent on maintenance, routine operations, inventory, public affairs events, and others [Falls 2012]. Most of the monitoring is augmented through the ground station, where data are analyzed by specialists around the clock. Some automated health management tools have found their way into operations, such as the Inductive Monitoring System (IMS) Tool, an abnormal condition detection tool based on clustering technology that is employed at NASA Johnson Space Center to monitor various subsystems.

Aeronautics

Because military aircraft operate under different usage scenarios than commercial aircraft and are subject to a strict internal safety review (but not FAA certification), the military can look back at a long history of integrating IVHM principles. Starting with a simple time-temperature recorder

for the engine hot-section on the F-8 (during deployment in Vietnam), and later the A-7 aircraft engine health monitoring program of the early 80s, IVHM principles found their way in various degrees onto numerous platforms, as shown here (roughly in order of time of implementation): F-8, A-7E, TA-7, AV-8B, F/A-18 A/B, T-45A, F-14 D, E-2C, SH-60, and H-53, as well as some versions and models of the AH-1 and UH-1, V-22, F/A-18 C/D, and the JSF [Engel et al. 2000; Hess 2012].

Commercial airlines have also adopted IVHM principles where they help to reduce cost and at the same time assist in maintaining safety of operations. To that end, engine manufacturers, for example, offer service contracts that provide round-the-clock monitoring of the engines. Reports are generated where off-nominal engine conditions (before they reach safety-critical levels) are detected and forwarded to airline operators [O'Flarity 2009; Calhoun 2009]Error! Reference source not found.. The economic benefits of these systems are that faults can be dealt with before they result in a delay or cancellation or that the remote monitoring system can prevent secondary damage. The safety benefit is that degradations can be detected and dealt with before they become equipment failures. Similar to engine service providers, aircraft frame manufacturers are providing service offerings [Maggiore and Kinney 2009] that inform on the health of a variety of aircraft subsystems and help in an operational setting in a similar fashion.

In addition to these fielded examples, NASA has been spearheading research in IVHM for aeronautics. The premise is that public benefits resulting from continued growth in the air transport of passengers and cargo are dependent on the improvement of the inherent safety attributes of current and future aircraft that will operate in the Next Generation Air Transportation System (NextGen).

One of NASA's programs within the Aeronautics Mission Directorate is the Aviation Safety Program (AvSafe). Its research mission is motivated in large part by the challenges that arise from NextGen, which strives to make travel through increasingly crowded skies more efficient

and speedy while maintaining or increasing safety [NASA 2012]. AvSafe lists as some of the top technical challenges vehicle health assurance, prognostic algorithm design, assurance of flight critical systems, and loss of control prevention, mitigation, and recovery. All these have an IVHM flavor. Indeed, AvSafe continues to sponsor IVHM-related programs.

These programs seek to provide increasing capabilities to predict and prevent safety issues, to monitor for safety issues in-flight and lessen their impact should they occur, to analyze and design safety issues out of complex system behaviors, and to constantly analyze designs and operational data for potential hazards. These technologies, many of which are at a lower technology readiness level (TRL), can be leveraged to support safety in other complex systems such as NASA long-duration missions in space science and exploration. IVHM research technologies were found to map to the Joint Planning and Development Office's (JPDO) National Research and Development (R&D) Plan as well as the Safety Working Group's National Aviation Safety Strategic Plan (NASSP) [Reveley et al. 2010].

9.4 Safety as a Mandate

It is often voiced that safety is upheld by commercial operators to the degree required by regulatory bodies. That has implications for how commercial operators respond to safety. In particular, they will meet those requirements but not voluntarily exceed them, unless there is a perceived commercial value. This, in turn, has implications for the role of IVHM as an enabling technology for safety in aviation in that it is seen primarily from a cost reduction perspective. At NASA or within DoD, there tends to be a different balance between safety and cost, where safety of human-rated systems trumps other considerations due to the unique situation of the mission. And, as Cicero pointed out a few thousand years ago: “Salus populi suprema lex esto—Let the good of the people be the supreme law.”

9.4.1 Regulatory Requirements

The task to regulate the safety for different application domains lies with various government entities. The following sections give a brief overview over a few selected regulatory bodies.

Federal Aviation Administration (FAA)

The FAA has a prominent role in enforcing safety of operations in aviation. Traditionally, it has focused on a risk and hazard analysis approach as the main element in ensuring safe operations. This includes time-based inspection of components. While it acknowledges in its System Safety Handbook [FAA 2012] that "warning devices" (i.e., pieces of equipment that issue an alert when an off-nominal condition is encountered) can be a part of a safety strategy, the use of condition-based health assessment to ensure safe operations is coming only slowly into practice. The goal of operators to use IVHM principles to reduce cost of ownership by performing as-needed maintenance finds itself in conflict with regulatory concerns about airworthiness [Sigma-Technik 2012]. In principle, there is an acknowledgement that condition-based principles can result in "maintenance credits" toward ensuring safe operations, which allow condition monitoring to reduce or replace time-based inspection. FAA Advisory Circular (AC) AC 29-2C, Section MG-15 provides guidance for transport category rotorcraft to attain airworthiness approval for installation, and credits validation of health and usage applications. The primary concern is to ensure that the probability of failure is as low as reasonably practicable, and is compliant with the quantitative regulatory requirements.

The FAA does require the use of engine condition monitoring (ECM) and oil consumption monitoring to issue extended operations (ETOPS) certification for certain classes of aircraft.

ETOPS certification is meant to ensure that a multi-engine aircraft can reach an airport even when a subset of its engines is no longer operational. Specifically, the ECM should provide a system for data collection and timely analysis to detect engine deterioration and preclude failure [FAA 2011]. The goal of this monitoring program is to detect deterioration at an early stage, and to allow for corrective action before safe operation is affected. The UK CAA has a similar requirement [CAA 2002]. ETOPS maintenance requirements are also meant to reduce diversions through engine condition and oil level/consumption monitoring. Some commercial providers cite that this practice has resulted in maintenance interval increases over OEM recommended practice [Eaton 2006]. In addition, the CAA has issued a requirement to install health and usage monitoring systems (HUMS) on helicopters to address failure rates of operation in the North Sea [CAA 2006]. The benefits that have been demonstrated after its implementation are part of the reason why most of the world's offshore drilling helicopter fleets now have HUMS.

Nuclear Regulatory Commission (NRC)

NRC defines a so-called "Maintenance Rule" in 10 CFR 50.65 which states that “each holder of an operating license for a nuclear power plant under this part and each holder of a combined license under part 52 of this chapter after the Commission makes the finding under § 52.103(g) of this chapter, shall monitor the performance or condition of structures, systems, or components, against licensee-established goals, in a manner sufficient to provide reasonable assurance that these structures, systems, and components, as defined in paragraph (b) of this section, are capable of fulfilling their intended functions” [§ 50.65 Requirements 2012]. It further states that “performance and condition monitoring activities and associated goals and preventive maintenance activities shall be evaluated at least every refueling cycle provided the interval between evaluations does not exceed 24 months.” The regulatory objective of the Maintenance

Rule is to require licensee monitoring of the overall continuing effectiveness of their maintenance programs to ensure that:

- Safety-related structures, systems, and components (SSCs) and certain SSCs that are not safety related are capable of performing their intended functions.
- For equipment that is not safety related, failures will not occur that prevent the fulfillment of safety-related functions.
- Failures resulting in scrams (emergency shutdowns) and unnecessary actuations of safety-related systems are minimized.

As part of these regulatory requirements, nuclear power plant operators have been exploring for several decades how best to implement health management principles to assess the state of health of their equipment. Early solutions included expert systems [Ancelin et al. 1991] and other artificial intelligence approaches [Uhrig, Hines, and Nelson 1998]. The connection to operational safety is made [Attieh et al. May 2000; Nov. 2000]. It should be noted, however, that the Nuclear Regulatory Commission requests the Utilities to meet the requirements without specifically telling the Utilities what to do. The Utilities merely need to file documents that state how they will meet the requirements, and the NRC determines if the proposed activities will meet the requirements.

National Highway Traffic Safety Administration (NHTSA)

The NHTSA has a legislative mandate under Title 49 of the United States Code, Chapter 301, Motor Vehicle Safety, to issue Federal Motor Vehicle Safety Standards (FMVSS) (CMVSS in Canada) and Regulations to which manufacturers of motor vehicle and equipment items must conform and certify compliance.

Recent advances include the monitoring of tire pressure, which has been articulated in FMVSS standard No. 138 (49 CFR Parts 571 and 585). It requires installation of a tire pressure monitoring system (TPMS) capable of detecting when one or more of a vehicle's tires is significantly under-inflated. This rule requires installation in all new light vehicles of a TPMS capable of detecting when one or more of the vehicle's tires, up to all four tires, is 25% or more below the manufacturer's recommended inflation pressure or a minimum activation pressure specified in the standard, whichever is higher [49 CFR 2012]. NHTSA has further regulations and is discussing the monitoring of other safety-related equipment such as brakes, air bags, electronic stability control and—beyond that—has also begun to investigate safety-related systems that are not strictly part of IVHM such as frontal collision warning systems and lane departure warning systems [Commission 2008].

Other advances that are being pursued outside NHTSA include onboard monitoring systems for commercial motor vehicles, a project sponsored by PATH, the Partners for Advanced Transportation TecHnology, a multi-disciplinary program with researchers from universities statewide, and cooperative projects with private industry, state and local agencies, and nonprofit institutions. Research is under way for semi-autonomous proximity warning devices and driver fatigue warning devices [Misener et al. 2006].

California Air Resources Board (CARB) and Environmental Protection Agency (EPA)

The California Air Resources Board (CARB) required that all new vehicles sold in California starting in 1991 have some basic on-board diagnosis (OBD) capability. The purpose was not strictly to enhance the safety of operations. Instead, this regulation was motivated by a desire to reduce the exhaust emissions and to institute a state-wide tailpipe emissions testing program. The

specifications were refined in the so-called “OBD-II” with mandated adoption for all cars sold in California starting in model year 1996 [CARB 2006] and allowed OBD to perform on-board monitoring of a wide range of emissions controls. The Environmental Protection Agency (EPA) followed suit and made OBD-II mandatory for all cars sold in the United States [EPA 2005]. In 2001, the European Union adopted a similar directive [EU 1998] for vehicles with gasoline engines and in 2004 for vehicles with diesel vehicles sold in the European Union. SAE and ISO both defined OBD-II standards as summarized in Table 9.2.

Table 9.2 OBD Standards

Organization	**Standard**	**Scope**
SAE	J1962	Physical connector used for the OBDII interface
SAE	J1850	Serial data protocol
SAE	J1978	Operating standards for OBDII scan tools
SAE	J1979	Diagnostic test modes
SAE	J2012	Trouble codes and definitions
ISO	9141	Diagnostic systems
ISO	14230	Diagnostic systems—Keyword Protocol
ISO	15031	Communication between vehicle and external equipment for emissions-related diagnostics

9.4.2 Certification Bodies

Minimized life-cycle cost at a high safety level is arguably the primary business case for IVHM . The fundamental idea is that the application of IVHM algorithms and methodologies will be able

to detect incipient mechanical faults and allow preventive maintenance intervention. If these principles are followed, the operator would be issued "maintenance credits," which would relieve them from performing maintenance at fixed intervals. The result would be that the operation of the vehicle is as safe (or safer) as with fixed maintenance intervals while the cost of maintenance would be reduced because it would be performed based on an as-needed basis, as opposed to somewhat blindly at fixed intervals. The interval of the latter is always chosen to be conservative, usually based on statistical analysis of component life, with a safety margin built in. That is, the interval will be based on an expected average mean time to failure from which some number of standard deviations will be subtracted, with a further reduction for safety (often of 50%). The result is that most components are inspected or serviced significantly sooner than they need to be.

The condition-based maintenance concept with associated maintenance credits was adopted by the U.S. DoD and has been put into practice for the AH-64 Apache fleet. Obtaining maintenance credits for civil operators has been more difficult, as the accreditation process is still a work in progress.

In the absence of maintenance credits, the business case for IVHM is more complicated because one ends up detecting either additional failures (which, if one catches them early, may save money, but one ends up performing additional maintenance and has to bear the cost of the IVHM system implementation). Alternatively, one would catch the onset of faults and failures that impact other business metrics such as delays and cancellations which are legitimate and have led most major jet engine OEMs to adopt an engine monitoring program. However, they are not primarily geared toward improving safety.

FAA

The regulatory agencies have not developed much guidance for implementation of IVHM on transport category aircraft. In part, this has to do with the fact that industry needs typically lead the guidance that regulatory agencies disseminate. Compounding this issue is the fact that the industry need for IVHM is driven by economic benefits, not safety. In general, the more the system to be certified impacts the potential safety of the system, the more stringent the certification steps are. Safety may be potentially impacted where systems provide information to the flight crew that can influence in-flight decisions; where traditional inspection intervals are extended; and where traditional inspections are replaced with automated monitoring. It is thought that an easier route is, therefore, an IVHM system that provides post-flight information to maintenance personnel, thus avoiding the safety implications for the flight crew (one would still have to address the condition-based maintenance aspect). It should be noted that software per se does not get certified. IVHM functions may be certified with another system, such as an engine FADEC system or aircraft display and monitoring system [Rajamani et al. 2010].

Certification involves development and execution of a certification plan that lists test and analysis steps with pass/fail criteria and outlines a system safety assessment (SSA) that includes ample documentation to address all elements of airworthiness as outlined in FAR 14 CFR Part 21 [FAA 2012]. The SSA is hierarchical in nature, from the subsystem level through the aircraft platform level (i.e., the system itself needs to be safe, and needs to be safe as part of the installation). In addition, product support documents have to be furnished that include maintenance and operating manuals.

DO-178C “Software Considerations in Airborne Systems and Equipment Certification” is the primary document by which the FAA (and its European counterpart EASA) will approve all

commercial software-based aerospace systems, and in particular, safety-critical software [SAE 2012]. DO-178C builds on the work of DO-178B, which was released 20 years earlier. FAA Advisory Circular AC 20-115B established DO-178B as the accepted means of certifying all new aviation software. Adhering to DO-178B and DO-178C in itself does not guarantee the safety of software, and it is not intended as a software development standard. Instead, it is meant as a software assurance plan that uses a set of steps to meet certain levels of rigor ("Design Assurance Levels"). Companion document DO-278A deals with software assurance of non-airborne systems [SAE 2002].

At this point, it should also be noted that Verification and Validation (V&V) can be a bottleneck in certification of IVHM solutions, depending on the type of credit sought. If no maintenance credits are sought (i.e., all standard maintenance is conducted regardless), and if the IVHM solution does not adversely affect the safety of operations, V&V is not more burdensome than for other health management solutions. However, if a move to CBM is sought, the burden may substantially increase. The current approach to performing V&V for health management algorithms is to carry out massive amounts of simulation and testing. Unfortunately, this approach increases the cost of safety assurance prohibitively. Furthermore, advanced IVHM algorithms may incorporate nonlinear, nondeterministic methods to improve the accuracy of predictions under uncertainty. V&V methods for nondeterministic mission-critical systems are still in their infancy.

FAA Advisory Circular AC 29-2C, Section MG-15

As mentioned earlier, FAA Advisory Circular AC 29-2C, Section MG-15 provides guidance for transport category rotorcraft to attain airworthiness approval for installation, and it credits validation of health and usage applications. Using the certification of HUMS on a helicopter as an example, the recommended steps for certification are [Michael et al. 2004]:

- Establish a certification project with the responsible aviation authority
- Develop an end-to-end system design concept by:
  - Defining the desired maintenance credit(s)
  - Determining the functional partitioning between airborne and ground
  - Establishing the functional partitioning between HUMS and the maintenance system
  - Selecting COTS software and hardware with an established service history,
  - Clearly identifying the end of the credit function (algorithm)
  - Defining a user interface that will meet desired objectives
- Prepare and submit hazard assessments for:
  - Airborne installation
  - Maintenance credits expected or desired
- Perform system development to:
  - Obtain hardware to meet the system qualification requirements
  - Establish application software to the required DO-178B levels
- Test the application in the COTS environment
- Validate the COTS using an independent means of verification
- Develop a user operating manual for the system defining credit requirements
- Modify maintenance and/or flight manuals for the proposed credits
- Certify the airborne installation
- Conduct a controlled service introduction for credit validation
- Helicopter operator to obtain credit approval for his aircraft

While there is interest of the FAA and industry to show how this process can be used with success on an example, there have not yet been any approvals of substance. At the root of this is that the software certification applies the airborne software certification paradigm of DO-178B/C.

A usage credit for fatigue limited parts requires level B software certification in the airborne system and an equivalent level for any ground processing according to DO-178B/C [Michael et al. 2004]. This has rendered all attempts too difficult or expensive.

Underwriters Laboratories

Underwriters Laboratories (UL) is a company addressing "safety science" that focuses, among others, on product safety, environment, life and health, and verification services. UL has distinguished itself by issuing trusted certification marks that assure a certain standard of safe operation. To that end, UL employs principles from health management, including failure modes and effects analysis (FMEA). Beyond that, UL has also certified monitoring equipment in certain fields, including the medical field. Indeed, UL certification is the U.S. national standard for safety testing of electrical medical devices. Most hospitals will not allow installation of medical monitoring devices in their facilities without proof of the equipment meeting the IEC (International Electrotechnical Commission) 60601-1 regulation. IEC 60601-1 is the harmonized standard for medical electrical equipment that covers requirements for functional safety, software, and EMC, among others. For more generic safety-related control systems in machine applications, UL follows standard IEC 62061, which defines safety integrity in terms of safety integrated levels (SIL). This includes also the degree of diagnostic capabilities. The range of UL listed monitoring equipment includes monitoring for server rooms, cold storage, and industrial processes, and others.

9.4.3 Standards

While fielded IVHM tools are not yet common practice, a fair number of standards exist that aid in their implementation. The following sections discuss several of the standards that have been developed with IVHM in mind.

SAE International

E-32 Aerospace Propulsion Systems Health Management has issued Aerospace Recommended Practice (ARP) 1839 (Recommended Practices for Aircraft Turbine Engine Vibration Monitoring Systems) [SAE 2008]. This Aerospace Recommended Practice gives general guidance for typical turbine engine vibration monitoring (EVM) systems applicable to fixed or rotary wing aircraft applications, with an emphasis on system design considerations.

ARP 6461 (Guidance on Structural Health Monitoring for Aerospace Applications) [ARP 6461 2011] is applicable to civil and military aerospace airframe applications in which stakeholders are seeking guidance on the development and certification of Structural Health Monitoring (SHM) technologies for SHM applications. It is also recognized that many stakeholders (such as regulatory agencies, airlines, OEMs, academia, and equipment suppliers) are interested in the process of certifying SHM solutions. To that end, a common language, framework, and recommended practices are needed to promote fruitful and efficient technology development.

Additionally, SAE has published ARP 5987 “Guidelines for Engine Health Management System Software Assurance Levels.” ARP 5987 is intended to provide guidance for IVHM systems with a propulsion-centric focus with a process to determine the assurance levels and appropriate

airborne electronic hardware elements. The document addresses the various stages and functions of the IVHM system (i.e., on-engine, on-aircraft, communications, and ground-based elements). In addition to the assurance levels, the document addresses mitigation techniques and system architectures necessary to support the certification of the IVHM systems and functions [ARP 5987 2008].

ISO

As another standardization body, ISO has long worked on harmonizing condition monitoring practices. These are encapsulated in a host of standards, some of which are summarized in Table 9.3. Technical committee 108, in particular, has focused on condition monitoring and diagnostics of machines.

Table 9.3 Selected ISO Standards Related to IVHM

ISO standard	**Title**
	Condition monitoring and diagnostics of machines
13372	Vocabulary
13373-1	Vibration condition monitoring—Part 1-2
13374-1	Data processing, communication and presentation—Part 1-7
13379	General guidelines on data interpretation and diagnostics techniques
13381-1	Prognostics—Part 1
17359	General guidelines
18434-1	Thermography—Part 1: General procedures
18436-X	Requirements for training and certification of personnel—Part 1-7

22096	Acoustic emission
29821-1	Ultrasound—Part 1: General guidelines
	Road vehicles
16844-6	Tachograph systems—Part 6: Diagnostics
	Industrial automation systems and integration
18435-1	Diagnostics, capability assessment and maintenance applications integration—Part 1: Overview and general requirements
2041	Mechanical vibration, shock and condition monitoring—Vocabulary
16587	Mechanical vibration and shock—Performance parameters for condition monitoring of structures
14963	Mechanical vibration and shock—Guidelines for dynamic tests and investigations on bridges and viaducts
	Freight thermal containers
10368	Remote condition monitoring
	Cranes
12482-1	Condition monitoring—Part 1: General
	Transport Information and Control Systems (TICS)
17687	General fleet management and commercial freight operations—Data dictionary and message sets for electronic identification and monitoring of hazardous materials/dangerous goods transportation

9.4.4 Discussion

This section discussed how IVHM addresses safety in several application domains and thereby implicitly answers the question whether safety matters as far as IVHM is concerned. Various regulatory bodies have implemented processes for certification, but considerable differences are noted. It can be speculated that the difference is explained in part in how many systems have to be considered by the regulatory bodies. When there are few systems (as in nuclear power plants) it may be feasible to deal with each of them on an individual basis. When there are many (e.g., airplanes), it may be more logical to go with a process-based approach. Besides the mandate from regulatory bodies, there are also business justifications to implement IVHM. The latter are subject to cost-benefit calculations that should be flexible enough to incorporate safety metrics. In addition, various standards exist that aid in the development of systems for IVHM.

9.5 Closing Thoughts

Safety concerns drive the use of IVHM in a number of different application areas, particularly where human safety is affected. Regulatory bodies are establishing rules in commercial settings to guarantee a minimum degree of safety and—in some cases—require the use of IVHM methods. Voluntary additional safety improvements need to justify the investment of resources into development of IVHM technologies or, alternatively, need to help reduce lifetime cost or reduce maintenance costs. Some examples exist where the application of IVHM helped to improve safety and cost, such as the case in which a HUMS system was credited with preventing several accidents with an associated savings of $49M on three AH-64 [avionicstoday.com 2012], but, generally, good cost-benefit models are lacking that would promote the penetration of IVHM technology. While IVHM can undoubtedly contribute to safety improvements, its acceptance will

hinge to a large degree on the cooperation of regulatory authorities and—beyond that—on the ability to calculate a positive cost-benefit.

A reasonable body of standards exists, and additional standards are actively being developed to assist in the development and implementation of IVHM with a safety perspective.

It should be expected that more emphasis will be placed on quantifying the impact of safety improvements on systems operations in the future. In addition, as IVHM systems mature, the benefit of IVHM will not only be in providing safety-relevant information. but will also be in taking action that will improve the state of safety of a system through autonomous action (although the certification of such systems will pose a considerable hurdle). Lastly, due to increasing software complexity, the topic of software health will become more prevalent [Leveson 2005] as we see more safety-related incidents. While software assurance is expected to make strides, it should be contemplated how IVHM principles can be adopted to aid in dealing with these issues.

In the past, IVHM has often been treated as an afterthought, when it became apparent that systems' safety was not up to par (e.g., HUMS on helicopters). It would be advantageous (and presumably cheaper) to consider IVHM during the design process to optimally divide the authority of safety-enhancing IVHM methods (and of means to reduce life-cycle cost) and safety-enhancing design modifications at the conceptual design stage. While some manufacturers are starting to embrace this philosophy, an industry-wide adoption is still in its infancy.

IVHM undoubtedly and demonstrably has the capability to improve safety. The challenge is to be able to calculate the economic benefits and to overcome regulatory constraints so that both the economic needs of commercial operators are satisfied so that Cicero's vision can be realized.

9.6 References

§ 50.65 Requirements for monitoring the effectiveness of maintenance at nuclear power *plants*. 2005. NRC Regulation 10 CFR.

49 CFR Parts, 571, Department of Transportation, National Highway Traffic Safety Administration.

Ancelin, J., F. Cheriaux, J.-P. Gaussot, D. Pichot, G. Sancerni, and G. Voisin. 1991. KSE: a real-time expert system to diagnose nuclear power plant failures; Real Time Systems. In Proceedings., *Euromicro '91 Workshop on*, 70 – 76.

ARP6461, *Guidance on Structural Health Monitoring for Aerospace Applications*, SAE Standard, 6/6/2011, SAE International, Warrendale, PA 15096.

ARP5987: *Guidelines for Engine Health Management System Software Assurance Level*, E-32 Aerospace Propulsion Systems Health Management, 4/22/2008.

ASRS: The Case for Confidential Incident Reporting Systems, ASRS Research Paper, Pub. 60, http://asrs.arc.nasa.gov/docs/rs/60_Case_for_Confidential_Incident_Reporting.pdf, 2001.

Attieh, I. K., A. V. Gribok, J. W. Hines, and R. E. Uhrig. 2000. "Pattern Recognition Techniques for Transient Detection to Enhance Nuclear Reactors' Operational Safety," In *Proceedings of the Maintenance and Reliability Conference (MARCON 2000)*, Knoxville, TN, May 7-10.

Attieh, I. K., A. V. Gribok, J. W. Hines, and R. E. Uhrig. 2000. "Transient Detection Module to Enhance Nuclear Reactors' Operational Safety," In *Proceedings of The Third American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation and Control and Human-Machine Interface Technologies*, Washington DC, November 13-17, 2000.

Aviation Accident and Incident Data System, NTSB , online database http://www.ntsb.gov/aviationquery/index.aspx, last accessed 3/10/2011.

avionicstoday.com. 2012. HUMS Technology, *Avionics Magazine*, pp. 24-28, May 2012.

Calhoun, K. 2009. Health Management at Rolls-Royce, Presentation, https://www.phmsociety.org/sites/phmsociety.org/files/FieldedSystems_Calhoun.pdf, last accessed 3/20/2012, Fielded Systems Session at 1st Annual Conference of the PHM Society, 1. October 2009, San Diego, CA.

CAA. 2002. CAP 513, Extended Range Twin Operations (ETOPS).

CAA. 2006. CAP 753, Helicopter Vibration Health Monitoring (VHM), Guidance Material for Operators Utilising VHM in Rotor and Rotor Drive Systems of Helicopters.

CARB. 2006. CCR Title 13 Section 1968.1.

Commission of the European Communities, Commission Staff Working Document, SEC(2008) 1908, Annex to the Proposal for a Regulation of the European Parliament and of the Council concerning *Type-approval requirements for the general safety of motor vehicles - Impact Assessment*, COM(2008) 316, SEC(2008) 1909, Brussels, 23.05.2008.

Day, J. and M. Ingham. 2011. Fault Management at JPL: Past, Present and Future, Presentation Slides, *ESA Workshop on Avionics Data, Control and Software Systems (ADCSS)*, 25-27 October 2011.

Doel, D. 1990. "The Role for Expert Systems in Commercial Gas Turbine Engine Monitoring," Proc. of the Gas Turbine and Aeroengine Congress and Exposition, Brussels, Belgium.

Eaton. 2006. Eaton Aerospace Oil Debris Monitoring Technology, Presentation to the Aircraft Builders Council, Inc. September 26, 2006.

Engel, S. J., B. J. Gilmartin, K. Bongort, and A. Hess. 2000. "Prognostics, the real issues involved with predicting life remaining," Aerospace Conference Proceedings, 2000 IEEE, Vol. 6, pp. 457 – 469.

EPA. 2005. 40 CFR 86.1806-01 - On-board diagnostics.

EU. 1998. European emission standards Directive 98/69/EC.

FAA. 2011. 14 CFR 121.161 - Airplane limitations: Type of route, rev. 2011.

FAA. 2012. 14 CFR Part 21, Certification Procedures for Products, Articles, and Parts.

FAA. 2000. System Safety Handbook, Chapter 13: Launch Safety, December 30, 2000.

Falls, M. 2012. ISS Logistics & Maintenance, Presentation slides from Defense Maintenance & Sustainment Summit, San Diego, CA, February 28, 2012.

Hess, A. 2012, Personal Communication, April 2012.

Leveson, N. 2005. Safety in Integrated Systems Health Engineering and Management, Integrated System Health Engineering and Management Forum, Napa Valley, November 2005.

Maggiore, J. and D. Kinney. 2009. Monitoring Real-Time Environmental Performance, Aero, Qtr_03 09.

Michael, J., G. Collingwood, M. Augustine, and J. Cronkhite. 2004. Continued Evaluation and Spectrum Development of a Health and Usage Monitoring System, DOT/FAA/AR-04/6, Final Report.

Misener, J., C. Nowakowski, D. Cooper, and J. Margulici. 2006. Onboard Monitoring for Truck Safety: From Concept to Prototype to Field Operational Test, *Intellimotion*, Volume 12, No. 2.

National Aeronautics Research and Development Plan, Biennial Update, National Science and Technology Council, February 2010.

NASA Aviation Safety Program, Program Home page, http://www.aeronautics.nasa.gov/programs_avsafe.htm, last accessed 3/8/2012.

National Motor Vehicle Crash Causation Survey, Report to Congress, DOT HS 811 059, July 2008.

O'Flarity, S. 2009. PHM Experience at UTC and Pratt & Whitney, Presentation, https://www.phmsociety.org/sites/phmsociety.org/files/FieldedSystems_OFlarity.pdf, last accessed 3/20/2009. Fielded Systems Session at 1st Annual Conference of the PHM Society, 1. October 2009, San Diego, CA.

Rajamani, R., D. Chase, C. Queitzsch, H. Larsen, G. Iverson, and D. Simon. 2010. Presentation of Panel Discussion, Guidelines for Engine Health Management System Software Assurance Levels, Annual Conference of the PHM Society.

Reveley, M., J. Biggs, J. Evans, S. Jones, T. Kurtoglu, K. Leone, C. Sandifer, and M. Thomas. 2010. Commercial Aircraft Integrated Vehicle Health Management Study, NASA/TM-2010-215808.

Reveley, M. 2010. Systems Analysis of NASA Aviation Safety Program - Final Report.

SAE. 2012. DO-178C, *Software Considerations in Airborne Systems and Equipment Certification*, Radio Technical Commission for Aeronautics, SC-205, Issued: 1/5/2012.

SAE, 2002. DO-278A, *Guidelines for Communication, Navigation, Surveillance, and Air Traffic Management (CNA/ATM) Systems Software Integrity Assurance*, Radio Technical Commission for Aeronautics, SC-190, Issued: 3-5-2002.

SAE. 2008. AIR 1839C, A Guide to Aircraft Turbine Engine Vibration Monitoring Systems, E-32 Aerospace Propulsion Systems Health Management - 2008-02-16.

Sigma-Technik. 2012. Engineering Study Paper, "Gaining Regulatory Approval for Helicopter CBM Programs," http://www.sigma-technik.com/uploads/Gaining_Regulatory_Approval_for_Helicopter_CBM_Programs.pdf, last accessed 3/10/2012.

Uhrig, R. E., J. W. Hines, and W. Nelson. 1998. Integration of Artificial Intelligence Systems into a Monitoring and Diagnostic System for Nuclear Power Plants," In *Proceedings of Special Meeting on Instrumentation and Control of the Halden Research Center*, Lillehammer, Norway, March 28-21, 1998.