2013-01-2333

Developing IVHM Requirements for Aerospace Systems

Ravi Rajamani[1], Abhinav Saxena[2,3], Frank Kramer[4], Mike Augustin[5], John B. Schroeder[6], Kai Goebel[3], Ginger Shao[7], Indranil Roychoudhury[2,3], Wei Lin[3]
[1]Meggitt, [2]SGT inc., [3]NASA Ames, [4]Airbus, [5]IVHM Inc., [6]AFRL, [7]Honeywell,

ABSTRACT

The term Integrated Vehicle Health Management (IVHM) describes a set of capabilities that enable sustainable and safe operation of components and subsystems within aerospace platforms. However, very little guidance exists for the systems engineering aspects of design with IVHM in mind. It is probably because of this that designers have to use knowledge picked up exclusively by experience rather than by established process. This motivated a group of leading IVHM practitioners within the aerospace industry under the aegis of SAE's HM-1 technical committee to author a document that hopes to give working engineers and program managers clear guidance on all the elements of IVHM that they need to consider before designing a system. This proposed recommended practice (ARP6883 [1]) will describe all the steps of requirements generation and management as it applies to IVHM systems, and demonstrate these with a "real-world" example related to designing a landing gear system. The team hopes that this paper and presentation will help start a dialog with the larger aerospace community and that the feedback can be used to improve the ARP and subsequently the practice of IVHM from a systems engineering point-of-view.

INTRODUCTION

At the very highest level, an integrated vehicle health management (IVHM) system satisfies the sustainability needs of an aircraft. It is comprised of a set of hardware components, software components, and operational and maintenance processes that work together to ensure that the vehicle performs according to its specifications in the most cost effective manner, without unexpected failures. While IVHM is typically focused on a particular vehicle, it is clear that fleet level constraints can impact the operations and maintenance decisions of individual aircraft. These constraints should be considered during the system design process.

IVHM is expected to support the cost, safety, and performance benefits of a vehicle. Each IVHM functionality must "buy" its way onto the platform. In other words, IVHM functionality will only be implemented if it improves some or several requirements as determined by a cost-benefit analysis. See AIR4176 [2] for a comprehensive discussion of conducting cost benefit analysis (CBA) for an engine health management (EHM) system. The asset may be different, but the thought process is the same as for a vehicle.

The premise of ARP6883 is that such a CBA has already been conducted and that the decision to move forward with the implementation of the IVHM system. Also, we assume that the IVHM system is being developed as part of a new aircraft, and therefore is an integral part of the system from the design phase. This is not the case for many IVHM systems today, partly because the concept of IVHM did not exist when many of these systems were designed and developed. With these systems, a specific monitoring or maintenance issue might result in the retrofit incorporation of IVHM systems. While there is a place for such systems, we expect that in the future the vast majority will be part of the vehicle design. Particularly, given rising challenges resulting from increasingly constrained budgets and requirements to keep vehicles operational for longer periods, it is imperative that a more cost effective and robust solution be considered. It is argued that building an IVHM system integrated into the vehicle from early in the design phase allows for a more cost effective and robust solution. Engineers may be able to identify design solutions that can "design out" the issues in the first place. If this is not cost effective, or technically infeasible, then they could consider IVHM as a solution. The key is to do the trade studies to figure out costs and benefits of an IVHM solution so that we can arrive at the most rational solution. For example, if time-on-wing is an overriding requirement, it is probably possible to design a system that flies for a very long time before maintenance is needed, but some of the design changes to do this might be onerous; whereas a properly designed and executed IVHM system may extend time-on-wing without design trade-offs.

The implementation of specific IVHM objectives for a given air vehicle is best described as a process which (in most cases) will be carried out by a multidiscipline team working in close coordination with other parts of the integrated product team (IPT). These teams will include not just the mechanical and electrical component IPTs but also, critically, the controls, and the reliability, safety & maintainability (RM&S) teams.

IVHM requirements will be derived from system cost, safety, and performance requirements that cover the needs of external stakeholders. In addition to these, the internal stakeholders need to be considered as well. Traditionally, IVHM systems have been designed primarily to derive economic benefit for the operator, in the form of diagnostics and prognostics of potential systems failures. However, this has not required any major certification efforts because IVHM systems have not been essential to any safety critical function in the air vehicle. There are, of course, notable exceptions (maximum continuous thrust monitoring, automated oil debris monitoring, etc.) where PHM systems play more safety-critical roles, but these are not the norm. However, with advances in IVHM technology and reliability these systems will be increasingly used for obtaining maintenance credits. Such systems will require certification as well as approval from the governing authorities for continued air worthiness. The SAE recommended practice (ARP5987 [3]) does a good job discussing such systems.

In this short paper we will summarize the basic thesis of ARP6883 and use the example of a landing gear system to demonstrate how IVHM requirements should be developed. The hope is that the feedback from the larger community will help in enhancing the quality of the ARP. The next section presents some general considerations for IVHM systems, followed by thoughts on how systems engineering processes apply to IVHM systems. Finally we present guidelines for writing IVHM requirements developed via the example of a landing gear system.

GENERAL CONSIDERATIONS

Writing IVHM requirements is no different from writing any other system or subsystem requirements except for a few key differences. From a systems engineering perspective, IVHM can be thought of as another subsystem that fulfills sustainability goals of the vehicle. However, it can differ from other subsystems in that it can be a spatially-distributed set of hardware and software components that may reside within other subsystems. In fact in many instances, an IVHM system is not even necessarily a physical system; rather it is a system function that has elements that reside on-board the vehicle, on the ground, and in processes that are distributed across the globe. Therefore, when compared to other systems, IVHM systems typically have many more stakeholders whose needs have to be considered. These could include:

- Maintenance personnel and management (e.g. line, overhaul, MRO personnel)
- Operator (e.g. the airline, USAF, etc., if not the owner)
- Crew (the actual operator such as the pilot)
- Fleet manager (e.g. mission commander)
- Owner (e.g. airline / lease company / USAF)
- Regulatory authorities (e.g. airworthiness, certification)
- General public
- Health Management (HM) system integrator (e.g. third party IVHM provider)
- Original Equipment Manufacturer (OEM, e.g. Internal integrated engineering teams developing the product)

Each of these groups is looking for something different from the system. For example, the vehicle operator, who is often also the owner, is looking for fuel savings, increasing availability in the fleet, reducing turn times in the shops, and lowering maintenance cost, etc. The maintainer (both line and shop) is looking for parts availability, highest throughput, reducing no-fault-found (NFF) incidences, reducing parts inventory, reducing maintenance cost, etc. If the maintainer has a long-term service agreement (LTSA) with the customer his needs are very different than if he only has a time & material (T&M) contract with the operator or owner. The OEM and the ultimate customer also have stakes in the recommendations of the IVHM system.

All these factors have to be considered and prioritized when developing the requirements, because they may lead to significantly different designs. While this document focuses on new systems, it is clear that retro-fit solutions have their own unique set of requirements of cost, weight, compatibility, and the need to get supplemental certification. The highest desires of the stakeholders are translated by the IVHM systems analyst into high level (HL) requirements. Once analyzed, these can be translated to low level (LL) requirements that are more specific and verifiable. It is crucial that the needs of the stakeholders are translated to actionable high level requirements. If sufficient time is spent on this step, the chances of developing and deploying a successful IVHM system improves dramatically.

A system safety analysis (SSA) that takes into consideration all failure modes and effects, functional hazard analysis, etc., will typically begin the IVHM development process. Among the options for failure mitigation are design changes that eliminate non-critical components, beef up structural components, or take into consideration special monitoring systems. That is why having this analysis done as early as possible in the preliminary design stage is so critical to a successful system design.

To implement IVHM requirements there may be a need to add dedicated sensors and signal processing and other hardware, as long as they are justified by cost, safety, or performance benefits. These, in many cases, will only be realized over the lifetime of the vehicle. Other significant impacts that should be considered are technology readiness levels and gaps, reliability, operational and cost impacts due to false or missed detects, data delivery and security issues, the governing business model that might need additional infrastructure investment, etc.

Therefore, one of the biggest challenges for the IVHM team will be the need to present a well-articulated cost-benefit analysis. Past experience and guides such as ARP4176 [2] can help with this process. Note that the benefit may not be immediate and may take some time after aircraft fleet introduction before it can be realized [4]. In the following sections we will go into more details about how IVHM requirements can be developed and implemented.

THE PROCESS OF DEVELOPING REQUIREMENTS

The intent of ARP6883 is not to reinvent the wheel as far as systems engineering (SE) is concerned. We direct the reader to several very good references that do a great job expounding on the general principles of SE ([5], [6]). Our intent here is to concentrate on the IVHM requirements-writing process and borrow as much machinery from SE as is needed to make our job easier. Because the IVHM system is being developed along with the vehicle system, the key concepts and steps are enumerated at the system level and details specific to IVHM design and development are provided for each of these system level steps.

Various government agencies and commercial organizations use different life cycle stages from a variety of stakeholders' viewpoints. Although these stages differ in detail or terminology they all follow a similar process that includes systems engineering steps at its core. The high level SE process (blue, as described by INCOSE [5]) is juxtaposed with the ISO's generic lifecycle (white, [7] in Figure 1).

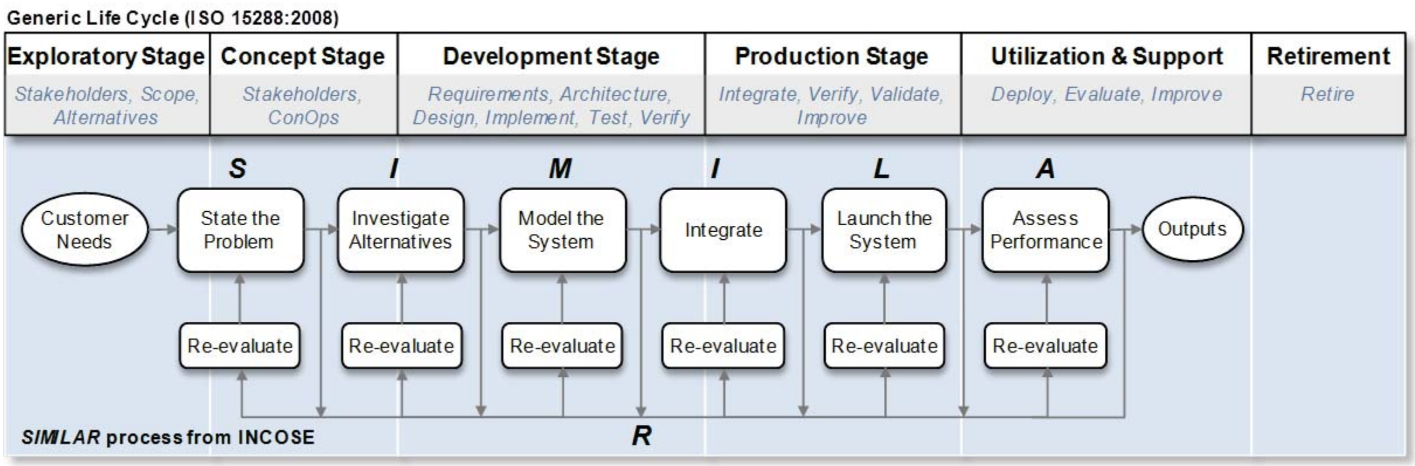

Figure 1: A generic approach to system engineering process (adapted from INCOSE and ISO)

Another way of representing the detailed SE process is with the classic V-diagram as depicted in Figure 2. This has been distilled from many sources and is fairly well known and widely used in the industry. This shows the various tasks that need to be carried out during the development of a system. These tasks map directly onto the Development and Production stages in the system lifecycle. We will use this as

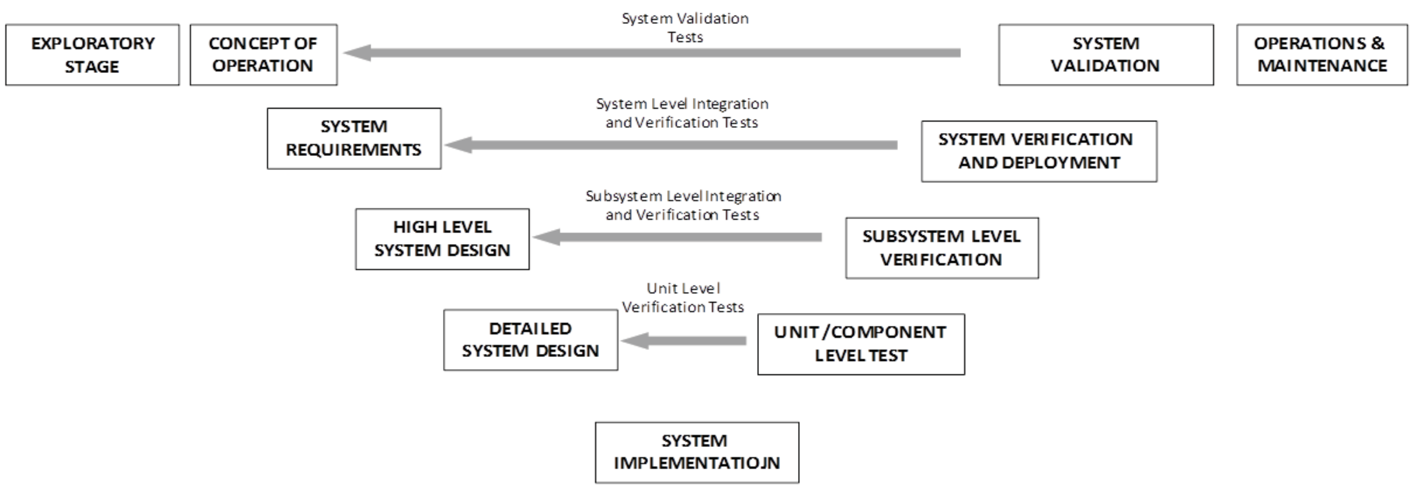

Figure 2: A generic V-diagram depicting key systems engineering steps

the basis for discussing the requirements development process. Since this document deals with requirements, the Utilization, Support, and Retirement stages will not be discussed.

Also, many references can be found giving general guidance on how to write good requirements (see e.g., [8]). Some of the authors of this ARP have also published (or contributed to works) on this subject (see e.g. [9] for general aerospace systems and [10] for rotorcrafts).

Exploratory and Concept Stage

The first step is to document the need to develop the intended system. This involves clearly understanding, and justifying, the need before formalizing requirements. This stage includes identifying user needs, exploring various concepts that meet those needs, and selecting a concept solution that can be developed and tested. Some key steps for the IVHM system are:

- Identify stakeholders and needs
- Define scope of the system
- Identify various interfaces between components and the vehicle for which the IVHM is being developed
- Develop Concept of Operations (ConOps)
- Identify data needs
- Setup upfront coordination activities between various actors
- Identify future opportunities for system upgrades

Development and Production Stage

A formal SE process starts during development stage where all requirements and activities are systematically documented and thorough review cycles are implemented as decision gates. The ConOps developed during exploratory stage are used to derive requirements for the overall system, which are then flown down to specifics at lower levels for individual subsystems and components.

High Level Requirements

The bulk of the work for developing IVHM requirements is done during this stage of the process. The stakeholders' needs are captured in the ConOps document and get translated to high level requirements. From an IVHM point of view system requirements stay at the level of specifying reliability, maintainability, and availability requirements without compromising safety in general, and include cost requirements and constraints (pertaining to loss, incomplete missions, unscheduled maintenance, downtime, cost of false alarms, etc.). It is important to note that in many cases the primary reason for an IVHM system is to provide a margin of design assurance for system shortfalls that cannot be cost effectively designed out. An HM system may be conceptualized at high level indicating what it will do – diagnosis, prognosis, real-time decision support, decision making for logistics, etc. While it still does not lay out exact details at the software and hardware implementation level, the functional roles and interactions of the HM modules are well defined in the system design at this high level.

Detailed Design

It is at this level that IVHM design and development become dedicated activities. IVHM ConOps are translated to detailed use cases, leading to relevant low level (LL) requirements. The LL requirements are spelled out in sufficient details to allow system designers to develop all the necessary IVHM functionality including implementation and integration details, verification and validation (V&V) tests, and qualification steps, etc. Detailed design identifies which subsystems or components to focus on, data and sensing requirements, processing and interface requirements, etc. It should be noted that the SE process is iterative in nature and can be applied to lower level subsystems all over again so that all elements can be refined and optimized.

System Implementation and Testing

While not strictly a part of requirements development it should be noted that no requirements document is complete without a comprehensive V&V test document. Many of these are unit tests that can be completed via simulation and on components and subassemblies. But some of the critical validation tests must be done at the vehicle level.

In the next section we illustrate these steps with a concrete example.

GUIDELINES AND AN EXAMPLE

We will illustrate how this might work in practice with an example that is closely related to real life. We will consider an aircraft landing gear system (LGS, Figure 3).

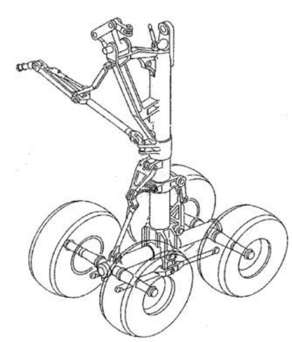

Figure 1: Generic aircraft landing gear system

For the sake of this example, the system stakeholders are restricted to:

- Owner (in this case, a leasing company)
- Maintainer (line and overhaul shop)
- Operator (airline)
- Crew (pilot)

Clearly, there are a few more stake holders such as the regulatory authorities, the landing gear OEM, etc., but let us stick with these for now. Also, even for these stakeholders, the list of requirements would typically be much larger than given below. These are only a subset, included here to illustrate the requirements management process.

Typically in commercial aviation the LGS is designed and certified along with the aircraft by an LG supplier whereas the wheels and brakes are a customer specified item that might have other suppliers involved.

Exploratory and Concept

During this process we will gather vehicle level goals from the stakeholders that may be supported by an IVHM system directly. In other words we try to identify what IVHM can do for these stakeholders in scenarios that involve health related issues for a landing gear subsystem. One can prioritize among various possibilities and develop a suitable concept of operations (ConOps) document. This will lay out the envisioned processes and role of IVHM (information, interfaces, caution and warning, etc.) and methods of presenting this information to the respective stakeholders. Here we list only the high level stakeholder needs that can be extracted from the ConOps. For example these might be (all numbers have been replaced by X):

Owner: Cannot exceed a certain initial cost for the system and spares, as well as lifetime cost numbers. Need to be able to track health of the LGS so as to enhance resale value. Need to track abuse to the system.

Maintainer: Need to obtain enough real-time information about system health to be able to support gate turnaround of X minutes or less. Should have the ability to change any line replaceable unit (LRU) in less than X minutes, and the wheels and brakes during an overnight visit to the hanger. Need to diagnose precise failure conditions for applying minimum equipment list (MEL) conditions for next flight as well as having failure or trend data available for forecasting future trouble with the system for deferred maintenance planning. Need to track remaining useful life. Need to put in place a spare parts management plan.

Operator: For an airline it should be able to see current system health through a web-based interface for fleet operation purposes. Should have adequate prediction of future health to optimize fleet operations. Should have direct access to hard landing reports to support inspections and maintenance. For the pilots, they would not want specific actions traced back to individuals, and they would like to see the availability of advance warning about performance issues to allow them to plan accordingly (Figure 2)

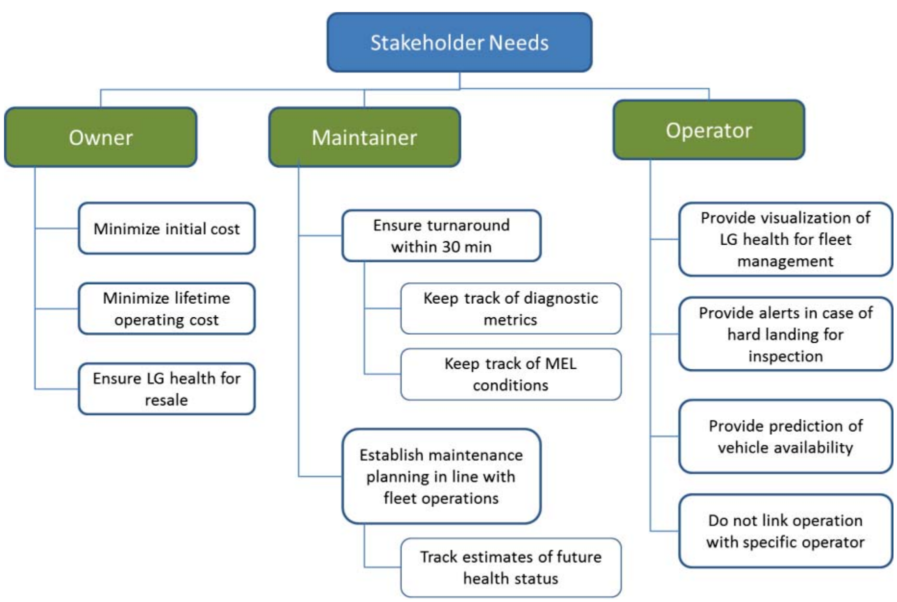

Figure 2 Stakeholder Needs

High level requirements

From these high level articulation of the stakeholders' needs we need to sketch out actual requirements and specifications that will be applicable to a real system. Being aware that there won't be a 1-to-1 relationship between stakeholder and product requirements a first set of high level technical requirements shall be envisaged (Note that we have used X to represent values that are not relevant to the discussion):

The system artifact addressed here shall provide technical capabilities for fulfillment of needs in the domain of stakeholders. These technical capabilities are linked to the hardware design of the system and define a certain output of the system for further processing on the ground. Apart from requirements definition for a purchaser, technical specification designers and suppliers are obliged to respond with a data model (or you might say: some kind of interpretation of core parameters) used in a data base on which applications for health data analysis, prediction, etc. can be performed.

For an initial set of requirements regarding the technical system solution we can assume the following ones

R-1 The Landing Gear System (LGS) shall monitor LGS usage and the state of the electrical, structural, and hydraulic subsystems
- R-1.1 The LGS shall measure stress inside the LGS structural system within a tolerance of X %.
- R-1.2 The LGS shall measure vibration within the LGS components
- R-1.3 Environmental and usage conditions shall be monitored and recorded

R-2 The LGS shall perform Health Assessment of the LGS subsystems
- R-2.1 The LGS shall perform fault detection as defined in the Health Assessment Plan
- R-2.2 The LGS shall perform fault isolation as defined in the Health Assessment Plan
- R-2.3 The LGS shall perform fault identification (damage severity estimation) as defined in the Health Assessment Plan
- R-2.4 There shall be prediction of the growth of critical fault modes as defined in the Health Assessment Plan
- R-2.5 The LGS shall perform anomaly detection as defined in Health Assessment Plan
- R-2.6 The LGS shall perform degradation detection as defined in Health Assessment Plan.

R-3 The LGS shall report Health Assessment and Monitoring information
- R-3.1 The LGS shall visually report State of Health to the operator within X minutes of the occurrence of a critical event as defined in Interface Specifications Document
- R-3.2 The LGS shall report State of Health time-history to the maintainer within X minutes of landing
- R-3.3 The LGS shall report additional State of Health or historical state measurements within X sec of request
- R-3.4 The LGS shall report abnormal usage conditions to the maintainer within X minutes of landing
- R-3.5 The LGS shall report parameters used for anomaly and degradation detection
- R-3.6 The LGS system shall not link the specific operator (pilot) to the abnormal usage report.

Note that the last requirement (R-3.6) derives from one of the needs of a specific stakeholder. Had this not been articulated during the initial stages, this might not have been captured correctly.

Allocation of Requirements to the Platform

It is obvious that stakeholder requirements related to IVHM will have a deep impact on the design of the system including the kinds of sensors and other means of monitoring capabilities that will be required to be installed on the LGS. Beyond that there will be requirements for acquiring and storing parameters either locally at the system level or centrally by another system onboard the vehicle. Therefore requirements should be written at a higher "function" level so that no attempt is made to identify where the capability will ultimately be implemented. The optimized mapping to potential hardware platform(s) shall happen when all requirements are made available.

Flow down process and low level requirements

For illustration, let us look at R-1.1 and R-3.4, and specifically let us look at:

1. Stress and overload conditions experienced by the LGS
2. Loss of performance of the LGS
3. Unreliability of proximity sensors for LG position and looked / unlocked state indicators.

There might be two options as corresponding design solutions for the LGS according to these requirements:

OPTION A

LGS REQ 1.1A. The system shall provide a monitoring device related to the shock absorber assembly in order to report the maximum forces applied to the LGS during touchdown (e.g. hard landing) for diagnosing potential damage of the LGS and the surrounding structure.

LGS REQ 1.2A. The system shall memorize the monitoring data of the shock absorber compression greater than X tons in the time window of pre-event (X msec) and post-event (X msec) with a sample rate of X samples/sec.

Once a hard landing detection capability has been allocated, there is a need to enable reconfiguration of the monitoring logic, to fix the maximum number of reports, and to specify the way an overload or hard landing report shall be transmitted for awareness.

LGS REQ 1.3A. The system shall have the capability to store at least X hard landing reports.

LGS REQ 1.4A. The system shall transmit hard landing reports to the cockpit and maintenance system for awareness.

These requirements do not impose any specific requirements on sensor technology (either measurement of temperature or deflection). This would be up to the system or equipment supplier.

There might be another option for this case if the vehicle is equipped with an Aircraft Condition Monitoring System (ACMS), which is the case in most of civil aircraft. For that case R-1.1 and R-3.4 can be solved by the following ones:

<u>OPTION B:</u>

LGS REQ 1.1B. The system shall provide monitoring input for the ACMS regarding potential LGS hard landing together with aircraft parameters like acceleration values, vertical speed, etc.

Furthermore for LGS REQ 1.1B a process requirement is necessary:

LGS REQ 1.2B. The LGS supplier shall provide parameters and logic for implementing overload and hard landing report in ACMS.

For the second option, ACMS is in charge to alert the operator in case of extensive stress on the LGS.

<u>REQUIREMENTS FOR LGS PERFORMANCE INDICATION</u>

LGS REQ 2.1. The system shall provide monitoring of extension and retraction operation for anomaly and degradation detection by means of following parameters:

- Travel time for extension and retraction
- High resolution power consumption over time for electrical or hydrauliSc actuator

LGS REQ 2.2. The LGS supplier shall provide anomaly detection pattern for the identification of deviations in power consumption and time period for extraction and retraction operation with evidence for future function failure for prognosis purpose.

LGS REQ 2.3 The LGS supplier shall provide degradation detection model for prolonging initial trends up to future function failure for prognosis purpose.

<u>REQUIREMENTS FOR PROXIMITY SENSOR DEGRADATION</u>

LGS REQ 3.1 The system shall monitor proximity sensor output for degradation detection of in the near/far status detection.

LGS REQ 3.2 The sensor supplier shall provide degradation pattern for the identification of any offset resulting in false near/far indication.

System verification and validation

Let us look now at above low level requirement that we have given above and see how we can structure V&V tests for these. Note that these are only examples. For the subsequent section we assume that OPTION A has been selected. Following verification requirements:

V-R-1 Lab test procedure shall allow the measuring of shock absorber compression level in the range X to X in X steps
V-R-2 Ground test procedure shall perform loading of X tons stepwise by X tons
V-R-3 Flight test procedure shall perform hard landing touchdown with a vertical speed of max. X ft/sec for triggering hard landing reports.

For all procedures listed above, the hard landing report shall be analyzed to verify that the output matches LGS REQ 2A.

The analysis of the hard landing report shall confirm whether initial stakeholder requirement R-1.1 and R-3.4 had been achieved (validation cycle).

CONCLUSIONS

In this brief paper we have given a summary of ARP6883 [1]. This forthcoming SAE document lays out some guidelines for developing good requirements for IVHM systems.

REFERENCES

1. SAE Aerospace Recommended Practice ARP6883, "Guidelines for Writing IVHM Requirements for Aerospace Systems," expected publication, December 2013.
2. SAE Aerospace Recommended Practice ARP4176, "Determination of Costs and Benefits from Implementing an Engine Health Management System," February 2013.
3. SAE International Aerospace Recommended Practice, "Establishing Software Assurance Levels for Engine

Health Management Systems Utilized for Maintenance Credit," ARP 5987, under review, Aug 2013.
4. Byer, B., A. Hess, and L. Fila, Writing a convincing cost benefit analysis to substantiate autonomic logistics, in IEEE Aerospace Conference2001. p. 3095-3103.
5. International Council on Systems Engineering (INCOSE), Systems Engineering Handbook, Version 3.0, June 2006.
6. Saxena, A., et al., "Requirements Flowdown for Prognostics and Health Management, AIAA Infotech@Aerospace Conference, Garden Grove, CA, 2012
7. International Organization for Standardization ISO15288:2008, "Systems and software engineering -- System life cycle processes," 2008.
8. Firesmith, D. Specifying Good Requirements, Vol. 2, No. 4 Journal of Object Technology 79, July-August, 2003. Pp. 77-87.
9. Prognostics Center of Excellence, "Attributes of Good Requirements for Verification and Validation of Health Management Systems," NASA Ames Research Center, Moffett Field, CA 94035. Draft 2012.
10. US Army Aviation and Missile Command (AMCom), Aeronautical design standard, ADS-79b-HDBK: Handbook on Condition Based Maintenance Systems for US Army Aircraft Systems, January 2011.

ACKNOWLEDGMENTS

The authors are grateful to the larger SAE HM-1 committee for stimulating discussions and helpful suggestions. We are also grateful to an anonymous reviewer for many of the improvements to the document.

DEFINITIONS/ABBREVIATIONS

ACMS	Aircraft condition monitoring system
CBA	Cost Benefit Analysis
ConOps	Concept of operations
EASA	European Aviation Safety Agency
FAA	Federal Aviation Administration
HL	High level
IPT	Integrated Product Team
IVHM	Integrated Vehicle Health Management
LG(S)	Landing gear (system)
LL	Low level
LRU	Line replaceable unit
LTSA	Long term service agreement
MEL	Minimum equipment list
MRO	Maintenance, repair, and overhaul
NFF	No fault found
OEM	Original Equipment Manufacturer
RM&S	Reliability, Maintainability, and Safety
SE	Systems Engineering
SSA	System Safety Analysis
T&M	Time and material
USAF	United States Air Force
V&V	Verification and validation