Towards Requirements in Systems Engineering for Aerospace IVHM Design

Abhinav Saxena[1] *and Indranil Roychoudhury*[2]

SGT Inc., NASA Ames Research Center, Moffett Field, CA, 94035

Wei Lin[3] *and Kai Goebel*[4]

NASA Ames Research Center, Moffett Field, CA, 94035

Health management (HM) technologies have been employed for safety critical system for decades, but a coherent systematic process to integrate HM into the system design is not yet clear. Consequently, in most cases, health management resorts to be an after-thought or 'band-aid' solution. Moreover, limited guidance exists for carrying out systems engineering (SE) on the subject of writing requirements for designs with *integrated* vehicle health management (IVHM). It is well accepted that requirements are key to developing a successful IVHM system right from the concept stage to development, verification, utilization, and support. However, writing requirements for systems with IVHM capability have unique challenges that require the designers to look beyond their own domains and consider the constraints and specifications of other interlinked systems. In this paper we look at various stages in the SE process and identify activities specific to IVHM design and development. More importantly, several relevant questions are posed that system engineers must address at various design and development stages. Addressing these questions should provide some guidance to systems engineers towards writing IVHM related requirements to ensure that appropriate IVHM functions are built into the system design.

I. Introduction

The term *Integrated Vehicle Health Management* (IVHM) describes a set of *health management* (HM) capabilities *integrated* into a system's design that enable sustainable and safe operation of components and subsystems within vehicle platforms. For some systems such as deep space robotic spacecraft systems health management, the focus is on *fault management* (FM)[1] with safety and reliability goals during operation. For others, such as aircraft, terrestrial vehicles, or long duration serviceable space platforms, the emphasis is on improving uptime and maintaining safety during system life cycle. For those systems, HM includes accommodation of both faults and effects of normal wear due to usage and ageing. The discussion in this paper addresses both safety and maintainability objectives. Despite significant advances in HM technologies and their application in flight-critical operations over the last few decades, commercial success stories of HM are relatively few[2]. System engineers and designers have to use knowledge gained from experience or adapted from other processes rather than through an established system engineering (SE) process. The engineering 'discipline' of health management is not well recognized in most organizations and hardly practiced consistently within the same organization[1, 2]. In many cases the top level requirements for IVHM are themselves so vague that systems engineers struggle to define the scope and functions of HM. In the past, it was, therefore, not uncommon that design for HM suffered from several shortcomings[3]. These included, for example, that designers did not identify the right stakeholders; customer needs were not properly articulated; the link of top level requirements to the design rationale including a cost-benefit-analysis were missing; the flow-down to lower level requirements was not well established; and, the links to other

[1] Research Scientist, Intelligent Systems Division, Discovery and Systems Health, MS 269/4, AIAA Member.
[2] Computer Scientist, Intelligent Systems Division, Discovery and Systems Health, MS 269/3.
[3] Systems Engineer, Engineering Systems Division, Systems Engineering Technical Area, MS 213/13.
[4] Senior Scientist, Intelligent Systems Division, Discovery and Systems Health, MS 269/1, AIAA Senior Member.

SE processes (such as verification and validation (V&V), architecture design, program milestones, and so on) were not clearly defined early on in the design-phase. It is not surprising that most, if not all, of the recently fielded examples of HM fall into the category of retrofitting piecewise solutions implemented on need basis within a multitude of constraints[4]. These usually result in very high costs that are far from optimal when compared to a system design with built-in health management functions.

As HM technologies continue to mature there has been a rise in the number of efforts where aerospace professionals have come together to carve out standardized processes or systematic guidelines for IVHM design within system development. Ranging from workshops and conference meetings to reference texts[2, 4, 5] and standards documents, a lot of information about IVHM theory and practice is being formalized. For instance, SAE's HM-1 technical committee has the charter to develop standards documents on Aerospace IVHM. These documents endeavor to distill the practical experience from industry such that they give engineers and program managers guidance on the elements of IVHM that they need to consider for designing and operating a system. Similarly, there has been a concerted effort within NASA to organize fault management practice by way of fault management workshops[4, 6] and development of a fault management handbook[7]. It is well understood that coming up with good requirements for IVHM early on during systems design phase would be the most effective towards its implementation. One of the proposed SAE documents is an aerospace recommended practice (ARP6883) that is being developed. This aerospace recommended practice will describe all the steps of requirements generation and management as it applies to IVHM systems, and demonstrate these with "real-world" examples[8]. Earlier works have explored the requirement flowdown for IVHM from high level user objectives[9, 10] that will allow upfront assessment of IVHM complexity commensurate with mission objectives and scope[11]. Furthermore, it is also realized that it is not only important to establish the product requirements but also process requirements to actually realize a truly *integrated* HM system as opposed to a 'band-aid' HM system[7, 12]. The project management structure should regard IVHM engineering as an activity on its own with clear roles and responsibilities, formal documentation for design, implementation, and reviews of IVHM, upfront resource allocation, and adequate planning for IVHM testing and validation[11].

Systems with IVHM capability have unique challenges that require the designer to look beyond their own domain and consider the constraints and specifications of other interlinked systems. There is a strong need to clearly identify and lay out a process that gives engineers and program managers crisp guidance on all the elements of IVHM that they need to consider before designing a system. This paper presents a view on how IVHM design and development should be included in the overall system design. Details specific to IVHM design and development are provided for each of these system level steps. A brief overview of SE processes, followed in various government and commercial organizations, is presented in Section II by mapping similar steps onto a common process and then describing IVHM specific activities. Section III then enumerates specific activities during the concept and exploratory stages, which define the goals for IVHM and lay the foundation for IVHM requirements. Development of IVHM ConOps is described in Section IV. Special emphasis is given to the activity of requirements-development for correct and a complete set of requirements in Section V, which lays the foundation of a well-built engineering system. Deriving 'good' requirements is the key in this process since a requirements-document is referenced throughout the development cycle and becomes the basis of verification and validation activities at all stages. Several relevant questions are posed that system engineers must address at various design and development stages to ensure that appropriate IVHM functions are built into the system design. Therefore, as discussed later, moving from 'exploratory stage' to 'concept of operation' and developing 'system requirements', it is argued that if the relevant questions are identified and answered early on, the chances of a successful outcome are greatly enhanced. This paper sheds some light on the topic of which questions to ask and at what stage.

II. The Systems Engineering Process as Applied to IVHM

The intent of this section is not to reinvent the wheel as far as SE is concerned. Several references[13-15] expound the general principles of SE. The intent here is to concentrate on the IVHM requirements writing process by reusing as many methods from SE as needed to make the integration of HM into a system's design a seamless process. This paper assumes that IVHM functions are being developed as part of the aerospace system and hence the IVHM specific SE tasks are a part of overall SE for that system.

A. Context – Where Does IVHM Fit in a System's Development Program?

There is often a debate whether IVHM should be regarded as a subsystem of a system or a function of a system (Figure 1) both from implementation architecture point of view and program management point of view[16]. A

significant difference practically becomes evident in the program structure and how IVHM specific development and activities get managed. Due to its unique distributed nature it becomes a critical question to answer and if not crystallized early on could lead to poor implementation of IVHM.

Unlike other subsystems, such as structure, propulsion, avionics, etc., which can be developed and tested separately given specifications in interface control documents (ICDs), IVHM development has to be integrated into each of the monitored subsystems. It is, therefore, a crosscutting function with a distributed implementation such that it monitors different subsystems and components by collecting data from spatially distributed sensors and, in some cases, processing information in a distributed manner as well[4]. Therefore, it does not quite fit the usual picture of a consolidated subsystem with a centralized teaming structure. Furthermore, it requires IVHM engineers to be fairly familiar with the subsystem design and function. However, from the SE perspective, treating IVHM as a subsystem allows allocating requirements and responsibilities to a dedicated health management team led by an IVHM lead engineer (Figure 1(a)). The IVHM team, in this case, must interface very closely with the individual subsystem teams. Additionally, the IVHM team must also interface and coordinate well with the organization's safety assurance team that maintains an oversight of program wide safety, reliability, maintainability, and quality assurance policies and procedures. Specifically, there are potential overlaps in activities such as FMECAs, fault tree analyses, and other risk analyses that must be coordinated. Some of the programmatic risks can be alleviated through program management structure. For example, a large portion of success in Boeing 777's IVHM implementation was attributed to the fact that the chief mechanic (top IVHM stakeholder) was elevated to the same approval level as the chief engineer[17].

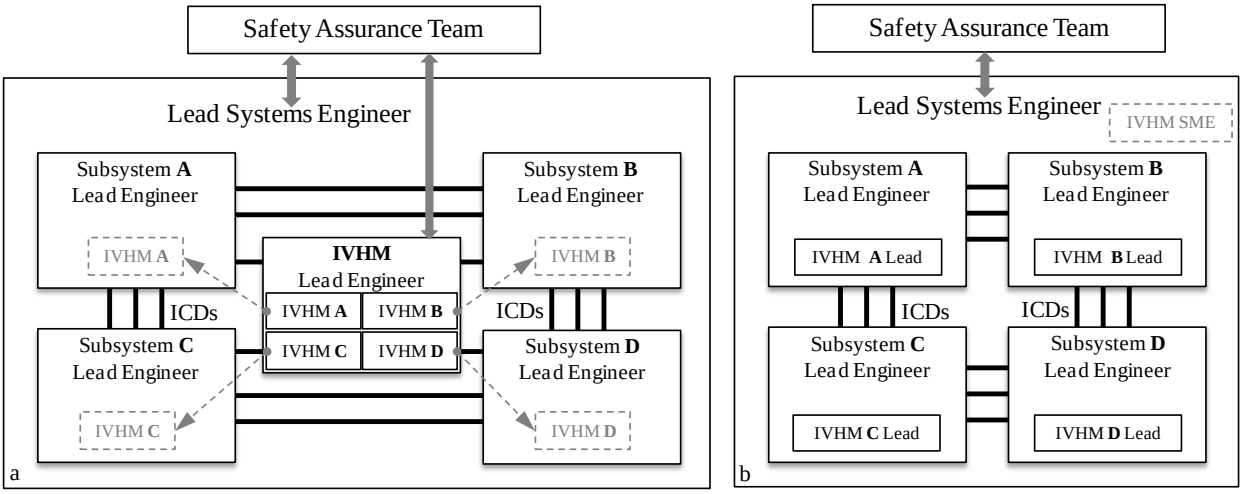

Figure 1. (a) IVHM as a subsystem within system engineering. (b) IVHM as a capability residing within multiple subsystems of a system.

On the other hand, IVHM can be regarded as a set of functions or capabilities[18] that other subsystems ought to possess to ensure safety, reliability, and maintainability (Figure 1(b)). This expands the scope of design and development of individual subsystems and requires dedicated HM engineers as part of respective subsystem development teams. Here each subsystem team must include an IVHM expert to guide IVHM design. There may not be a lead IVHM engineer for the overall system and each of the subsystem leads owns the IVHM requirements. There is a danger that this could result in unclear/incomplete system level IVHM requirements. A lack of dedicated leadership of overall IVHM may lead to overlaps and inconsistencies in IVHM terminology, design, implementation, and validation[3, 4, 11]. Therefore, care must be taken and a crisp program structure (with well defined reporting and work breakdown structure) should be put in place especially for IVHM development. The importance of getting an early buy-in from the program management and allocation of adequate test time cannot be emphasized enough.

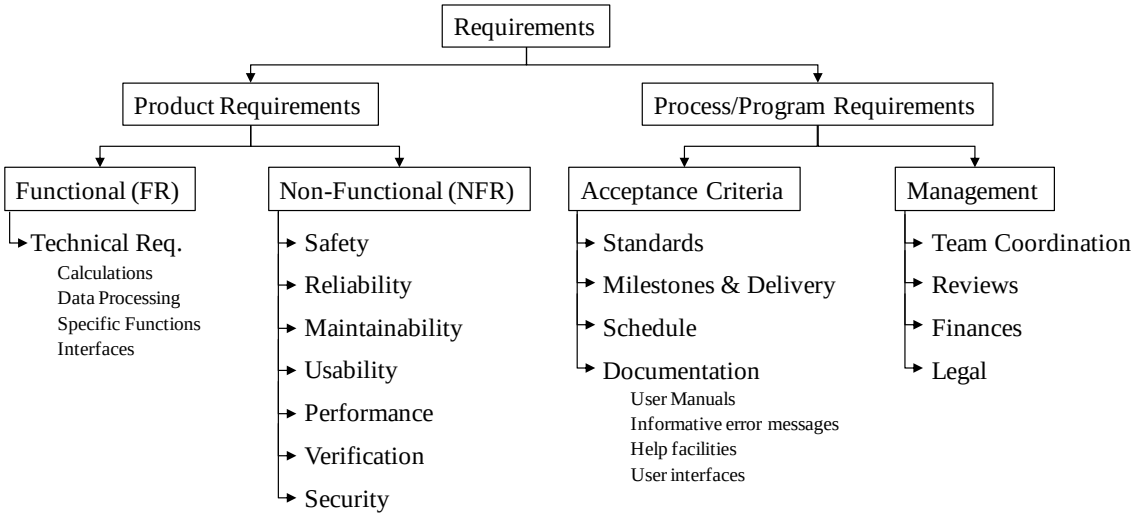

Figure 2. Classification of requirements for SE.

Irrespective of which view is taken, IVHM SE process is a subset of the overall SE process. Therefore, IVHM requirements are part of overall system requirements. Requirements are typically divided into *functional requirements* (FR) and *non-functional requirements* (NFR) categories (see Figure 2). Functional requirements define the function of a system whereas non-functional requirements define the attributes (such as safety, reliability, maintainability, usability, performance, security, etc.) of the system. As shown in Figure 3, the high level requirements for IVHM trace back to non-functional requirements of the overall system, such as maintainability, safety, and reliability requirements. IVHM requirements then can be further broken down into corresponding FRs (monitoring, diagnosis, prognosis, mitigation, etc.), and NFRs (metrics such as allowable false positives (FP), false negatives (FN), and desired accuracy, fault coverage, etc.). Therefore, the high level (HL) goals for the system that call for IVHM system development are considered as the starting points for IVHM concepts. An overview of the SE process is provided next with an emphasis on IVHM specific activities that must be carried out during a system's development.

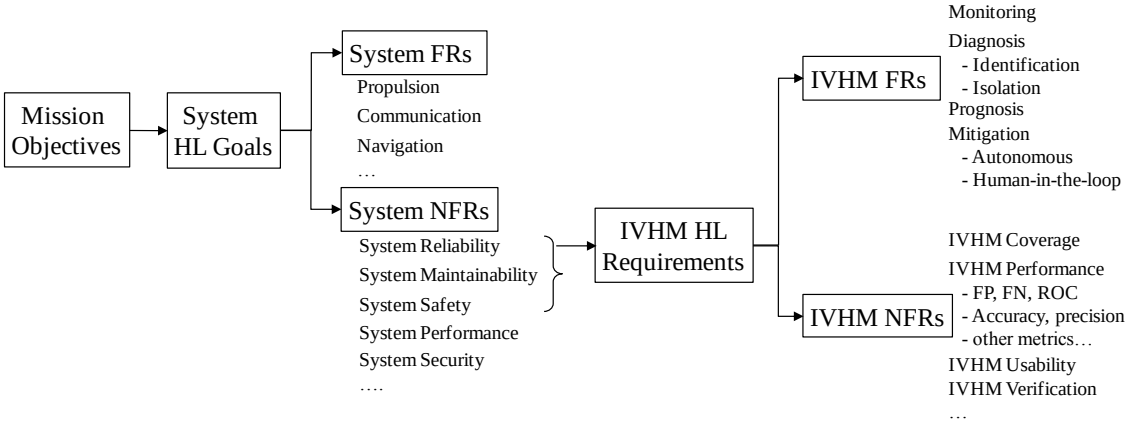

Figure 3. Derivation of IVHM requirements from system requirements.

B. The Systems Engineering Process

Various government agencies and commercial organizations use slightly different but similar definitions for stages in the life cycle of a system. Although these stages differ in detail or terminology they all follow a similar sequential process with core systems engineering activities of definition, development, utilization, and retirement. For instance, the high level *SIMILAR* SE process[14], as described by the INCOSE organization, is juxtaposed to the ISO's generic lifecycle[15] in Figure 4 to show that the two map on to each other well with slight change in scope of definitions for each of these stages. Processes from other organizations such as NASA, US Department of Defense, and US Department of Energy as well as non-governmental commercial entities map on these very well[13]. The key

points to note here are that the basic steps remain the same, there are often several feedback loops for iterative developments, and each organization may have customized processes to implement these.

Expanding on the core Systems Engineering stages the classic V-diagram (see Figure 4) enumerates various tasks that need to be carried out during the development of a system. These tasks map directly onto the *Concept*, *Development*, and *Production* stages in the system lifecycle and form the basis for requirements development process.

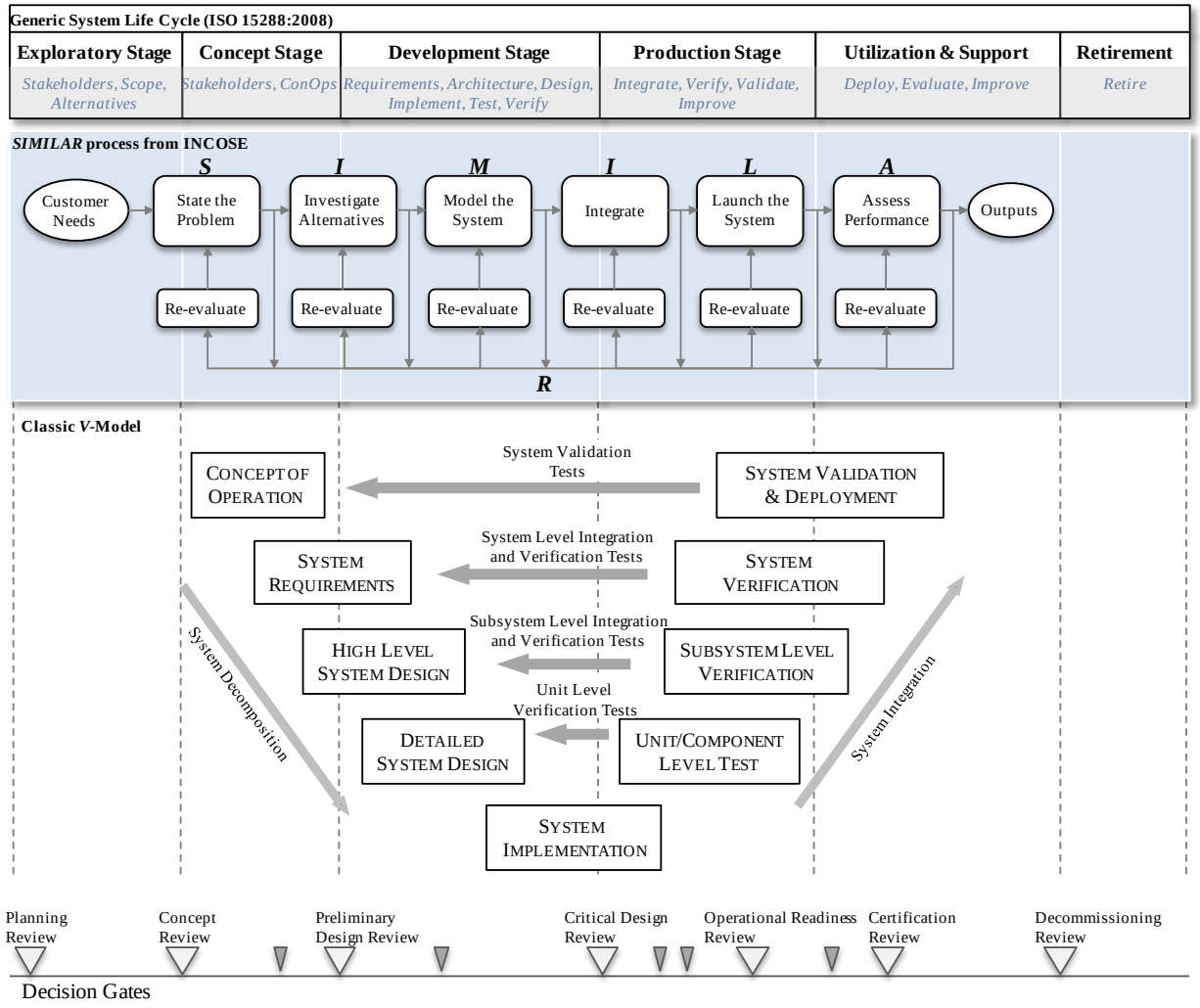

Figure 4: A generic approach to system engineering process (adapted from INCOSE[14] and ISO[15]) and a mapping to *V*-diagram depicting core systems engineering steps between the *concept* and *production* stages.

In the remainder of this section, we briefly present each stage of the SE process shown in the *V*-diagram within Figure 2 while focusing on IVHM-specific aspects. It is understood that IVHM SE process and documents will be part of overall SE process and feed into system level activities during execution of the overall project management activities such as planning, allocation, reviews, approvals, and commissioning.

Exploratory Stage: The Exploratory Stage is where programs and/or projects document the need to develop the intended IVHM system and explore possible options. This involves identifying the stakeholders and needs for IVHM; defining the scope of the IVHM system; identifying the various interfaces between components of the IVHM and with the vehicle for which the IVHM is being developed; and, understanding the available systems health data (both on-board and off-board data, as well as reference data), among others. Section III describes the key activities involved in the exploratory stage in greater detail.

Concept of Operation: In this stage, the concept of operations (ConOps) document for IVHM is developed. The ConOps document describes the characteristics of the IVHM system from the user's point of view. This document describes the quantitative and qualitative system characteristics for all the stakeholders. This document can contain use cases to describe the interactions between the user and the IVHM system to achieve the goals. The ConOps development stage is described in detail in Section IV.

Systems Requirements: Derived from the ConOps document, high-level system requirements include functional requirements (i.e., what the system must do) and also the non-functional requirements for performance (safety, availability, etc.), and cost (see Figure 3). High level system requirements then flow down to requirements for maintaining vehicle health adequate to perform the missions. They can flow from safety, cost, performance branches above and together influence HM design. From HM perspective these are still high level requirements and the exact design of HM is not yet there. Requirements at this level stay at the level of specifying reliability, maintainability, and availability without compromising safety in general. They sometimes include cost requirements pertaining to loss, incomplete missions, unscheduled maintenance, downtime, 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. Next, it is also necessary to establish the means for testing and verification that the requirements are met. This often results in *testability* requirements[19], which may flowdown to requirements for building simulation models, testbeds, built-in-test modules, and additional test assets to be used during verification step. Traditionally, IVHM requirements have not been finalized until system specification and design is complete[3]. However that takes away IVHM's ability to influence system design for a more optimal solution. Therefore, it is argued that IVHM requirements must be developed in tandem with system requirements and should participate in the system requirements review. It is expected that the requirements at this stage will be at high level to support program objectives[7]. Since detailed IVHM requirements depend upon complete specification of the vehicle design, the requirements are updated iteratively until the final system design is locked down for critical design review. Further changes in IVHM requirements should be facilitated through a predefined change management process as new needs or constraints are identified[20]. Section V discusses more details about developing requirements for IVHM systems.

High Level System Design: High level IVHM system design decomposes the IVHM system into its subsystems based on various functions that are required to carry out high level mission objectives. The decomposition is based on allocation of reliability, availability, and maintainability requirements to various subsystems such as propulsion, power, avionics, and structure. Further, it may be defined what level of HM would be appropriate to meet these requirements. Specifically, an IVHM system may be conceptualized at high level indicating what it will do – diagnosis, prognosis, real-time decision support, decision making for logistics, or all of the above, etc. While it still does not lay out exact details at software and hardware implementation level, the functional roles and interactions of the IVHM modules are well defined in the system design. This also includes the design of test platforms with fault injection capability both off-board and on-board the vehicle system, often termed as *design for testability* to increase the overall observability of the system[19].

Detailed System Design: The SE process is recursive in nature and can be applied to lower level subsystems all over again in order to come up with detailed design for the decomposed system in the previous step. It is at this level that IVHM design becomes a dedicated activity. Detailed design identifies which subsystems or components to focus on, data requirements, sensing requirements, processing requirements, interface requirements, etc. IVHM is a distributed system such that it monitors various different subsystems and components by collecting data from spatially distributed sensors and in some cases processing information in a distributed manner as well (unless implemented as a centralized system[16]). Therefore, it connects to the system through several interfaces at the subsystem and/or component levels. Often times IVHM takes advantage of synergies with other system instrumentation, but may influence the system design or add its own instrumentation if a need is determined. This requires detailed safety analyses such as failure mode and effects analysis or failure mode, effects, and criticality analysis, hazard and operability studies, reliability analysis, etc. to determine targets for health management and come up with suitable IVHM alternatives. Furthermore, the end use of IVHM output is expected to influence IVHM architecture and how it communicates with different stakeholders. IVHM design must comply with constraints arising from the overall system design and operational requirements. For instance specifications for sampling rates, model fidelity, computational complexity, sensor resolution, and power requirements, etc. should be all determined from the requirements flowed down from the higher levels.

System Implementation: This step is the core of actual product realization activity. System implementation involves implementing both hardware and software. While various low level components/systems may be developed independently they must comply with interface requirements. Representative data or prototype mockups may be

made available to each other between any two interfacing elements as outlined in the detailed system design. An IVHM system will include implementing hardware and software for accounting for relevant sensors, signal conditioning, signal processing, and health management (diagnostic and prognostic) algorithms. Each basic building block identified in the detailed design phase mentioned above are realized by either procuring it, or building it, or reusing it. The requirements and specifications flowing from the top levels are kept in consideration while making choices from among several alternatives. Therefore, it is this phase where choices are made for models, algorithms, model fidelity, time constraints, etc and where they are implemented. These choices also guide the methods to test and verify these implementations at the individual level so that the top level integrated product will likely meet the "shall" statements that were allocated, derived, or generated for it. Thus low level requirements on performance are derived and implemented here.

Unit/Component Level Test: Testing or verification is performed for each of the low level components or IVHM subsystem implementations. Verification consists of implementing a set of processes that assure the designer that the system is designed correctly, i.e. that it functions according to the requirements. Note that unit/component level verification is not the verification of the final IVHM system. However, using analysis, simulation, models or other means to test products at this level shows that they are implemented correctly, meet requirements, and are likely to integrate into a successful system. This also allows identifying important areas and drafting verification procedures for them to be used during overall system verification. Low level performance tests developed during detailed system design step are carried out for corresponding components and/or subsystems. Simulated or experimental data may be obtained to build test scenarios. For instance, for a contingency management based IVHM system fault detection and failure prediction algorithms may be tested using experimental testbeds equipped with a fault injection capability using appropriate metrics[21-23]. Fault injection must be designed to represent actual faults encountered during operation that were also determined during detailed design phase through FMECA and other fault analyses. Separate algorithms, sensors, and data processing approaches may be used for different type of components that will be tested separately at this stage. Likewise, if there are hardware implementations such as sensor selection and placement, signal conditioning, data processing, etc they should be tested for desired specifications. While verification at the lowest level is not sufficient for the verification at the next level it is a necessary step before individual parts can be integrated.

Subsystem Level Verification: Components and modules verified at the previous level are now integrated and tested to carry out verification at the subsystem level. This is an iterative step and is repeated whenever two or more subsystems are integrated together[24]. During this step major subsystems of a system are incrementally tested and verified. All major subsystems as identified in the high level design must be verified against requirements at that level. In the IVHM context algorithms may be integrated with respective hardware, data acquisition, and display interfaces. Verification at this level requires correct sequence of information flow as well in correct temporal order. It is tested whether health management algorithms implemented for different subsystems and components are performing their functions independently. For instance it is desired that a health management module for a specific component does not get affected by faults in other subsystem. Therefore, interference due to other subsystems is also determined and corrected for during the integration testing. Further, the process for fusing subsystem level health information to come up with overall system health is tested along with decision making routines.

System Verification: During this step the IVHM is tested within the integrated system based on the verification plan that lists what requirements are to be tested at what level of integration. Verification methods, as noted earlier, are determined upfront to include development/procurement of supporting test platforms and tools that must be built to carry out testing. Tests are carried out by simulating a relevant environment at the system level to ensure proper functioning of the integrated system during off-nominal operation. Key steps involve inclusion of fault injection capability to test IVHM functionality without breaking the system itself. There are many scenarios where verification metrics based on offline tests do not suffice. In such cases verification through deployment, such as *test-as-you-fly* approach, may be needed. These methods have inherent risks of loss due to unforeseen outcomes from untested scenarios. To minimize losses, policies like that of *controlled introduction* into service may be used where more authority is granted to IVHM system in an incremental fashion as more trust is gained through controlled usage over some desired period of time[25].

System Validation and Deployment: The system is now deployed and tested in realistic environments under various scenarios as described in the ConOps. Validation is the process by which one proves that the system indeed performs to satisfy the needs of the customers, for example as codified in ConOps. Validating IVHM functions can be somewhat difficult. For example, if one of the requirements of an IVHM system is to increase the maintenance interval from 4 to 5 years, one has to find a way of validating this without having to wait five years. As another example, if an IVHM system is designed to monitor for a fault with a certain detection and false alarm rate, it will be

difficult to test this in the real world without seeding the system with actual faults. The validation, therefore, in this case relies heavily on simulations based testing. Other approaches such as *in-service-validation* for IVHM have been suggested that primarily take an incremental approach for trust building by allowing IVHM to participate in the control loop in a controlled manner[25].

Operations and Maintenance: An IVHM system is unique and different from other capabilities in the sense that its performance and correct functioning may not be determined for a long time. However, there should be assessment metrics in place that measure IVHM performance over time and in the context of IVHM it is often referred to as IVHM *maturation* phase[17]. IVHM parameters and thresholds may need to be fine tuned as operations begin and there is more information available about how the system is reacting to the operational environments. IVHM models may need to be updated as the system parameters change over time (due to normal wear, change in operational environments, etc.) or some modifications (such as due to maintenance and repair) are applied. The components used specifically for implementing IVHM capabilities are themselves subject to failure and, therefore, may require maintenance. Finally, as improved technologies become available there may be a desire to apply updates to the IVHM system as time goes by.

III. Exploratory and Concept Stage

The Exploratory and Concept of Operation involves identifying user needs, exploring various concepts that meet those needs, and selecting a concept solution that can be developed and tested. To describe the situation of the past most of the time it is not clear to the subsystem designers how these IVHM system or resulting data will be used during operations and they often interpret the needs differently. This indicates that stakeholders are not always clearly identified, ConOps for IVHM are not crystallized, and consequently the requirements never flowdown adequately enough for a useful system to be developed.

This section addresses this initial step that sets the stage for the success or failure of a useful IVHM system. It is for this stage that the HM community needs to instill a culture of thinking about IVHM from the design phase. In order to determine what may be needed, the key issues to understand are:

- What are the mission or program needs that IVHM can address or help in reducing programmatic and/or technical risks?
- What are the relevant figures of merit for the intended mission or program and how can IVHM contribute to meeting those metrics?
- Will it be possible to realize a quantifiable 'benefit' within the mission/program's duration despite additional costs of implementing IVHM, and how?

To aid in answering these questions some key steps are defined next that must be carried out and used to document the findings into reports that will be used to get a buy in from the program management.

1. Identify Stakeholders and Needs for the IVHM system

The key to the development of good requirements is to identify the stakeholders early, and officially document their needs. This is one aspect in which IVHM-enabled systems differ from other systems on the aircraft, because just about everybody has a stake in the IVHM functions. As mentioned in the introduction, examples of IVHM stakeholders can be line maintenance, maintenance management, owner, operator, customer, original equipment manufacturer (OEM), regulatory authorities, which can be categorized from requirements perspective in the following manner:

- Maintenance personnel and management (e.g. line, overhaul, MRO personnel)
- Operator (e.g. pilot)
- Fleet manager (e.g. mission commander)
- Owner (e.g. airline / lease company / USAF)
- Regulatory authorities (e.g. Airworthiness, certification)
- General public
- HM system integrator (e.g. Third party IVHM provider)
- 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 incidences, reducing parts inventory, reducing maintenance cost, etc. If

the maintainer has a long-term service agreement with the customer his needs are very different from an IVHM system than if he only has a time & material contract with the operator or owner. The OEM and the ultimate customer also have stakes in the recommendations of the IVHM system. All these things have to be considered 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 requirements. Once analyzed, these can be translated to low level (LL) requirements that are more specific and verifiable.

Specifically the activities during this step should try to answer the following questions:

- Who are the *users* of the system?
- What functions of the system will be improved or feel an impact due to IVHM, and how?
- Choice between autonomy versus human-in-the-loop and onboard versus off-board functions.
  - Will IVHM be used for automated or autonomous systems or will be of the man – machine variety such as engineering analysis, traditional hands on maintenance, planning and scheduling?
- Are there potential conflicts arising from the needs of different stakeholders?
- How are these needs prioritized to resolve such conflicts?

2. Defining Scope of the IVHM Functions:

Defining scope for IVHM functions is key to satisfying all relevant stakeholders and set expectations, narrow down and focus on prioritized fault modes, and bound the development effort. Complex systems consist of multiple subsystems comprising numerous components that can all develop fault modes that cannot be all feasibly or practically tackled by IVHM. It is therefore important to narrow down on those that are more critical from overall system's point of view while writing scope statement. A Scope Statement should include the following information:

a) *Justification:* Provide a justification of why IVHM is necessary in meeting system level objectives.
- What is the intent of the system being considered?
- What is its main purpose (priorities among safety, cost, or both)?

b) *Objectives:* Define the IVHM functions – specifically the IVHM outputs and/or the IVHM action. These outputs can be a set of implemented actions based on prognostic estimates (autonomous functions), proposed alternatives, prognostic outlook, or just the current state estimate depending on the scope of IVHM's role.
- How will the IVHM output be used?
- How will IVHM affect, and/or be affected by, other related system development activities?
- Are there legacy systems with IVHM with success stories and/or lessons learned?

c) *Product scope description:* Describe the features and functions of the products, services, and/or results the project will produce.
- What is the Scope of the system being considered?
- What are critical scenarios under which IVHM will be used to extend systems safety and availability?
- Is it a real-time on-board decision support system capable of learning and adaptation or an enhancement to the supply chain for maintenance or logistics?
- Will the IVHM system be mission, safety, or flight critical and how will that impact specific and general system requirements?
  - In addition to the reliability of the system and its components, is the criticality analysis also considered for any on-board development?
  - What is needed (diagnostics, prognostics, decision support, or decision making (correction, mitigation, or isolation), etc.)?
- What are the budget constraints for the system within which IVHM should be developed?
- Are IVHM requirements technically feasible within programs budget, schedule, and risk posture?

d) *Product acceptance criteria:* Describe the process and criteria for accepting completed products, services, or results. Acceptance criteria can be defined in terms of product specifications validated by certain tests, demonstrations, and/or documented reports. For an IVHM-enabled system such criteria may be specified in terms of false positives, false negatives, timeliness, prediction horizon or similar type of metrics. These criteria must additionally specify the environments in which these tests would run, i.e. simulation, lab, flight, etc. Relevant tolerances in test results, number of tests for statistical significance, safe modes, etc. must be defined under acceptance criteria.

e) *Constraints:* Restrictions that limit the scope of IVHM development or that limit the access to data and required resources. Some typical system development constraints include time and budget limits. In aerospace

applications, constraints also include limits on weight, volume, computational power, communication delay, communication protocols, data and physical access to system, etc. These system constraints have a direct influence on IVHM capabilities and scope. All such constraints must be identified and enumerated in the scope document. In general, constraints identification will try to answer the following question:

- How does *accessibility* to the target subsystem/component influence the requirement development process?
- What other systems and data access will have to be considered?
- Will there be single or multiple users with read/write access and the necessity to establish publish/subscribe protocols?
- Another consideration similar to access is *availability*. How often and for how long will access be required to the host subsystems?

f) *Assumptions:* Assumptions need to be listed to communicate expectations and limitations to other stakeholders. Consider the situation when IVHM development is carried out as a parallel activity with inputs from system development and access to a fully functional system is not yet possible. In such cases IVHM development will be based on an understanding of how a system would operate nominally and under various faults that are candidates for HM. All assumptions should be listed that describe the model of the system as seen by IVHM, interactions, availability of data, noise levels, communications, operational conditions (for functions active during operation), hardware capabilities, assurance of software and hardware integrity, etc. The other source of assumptions is in estimating uncertainties in future operating conditions, changes in system and/or system ConOps, changes in intended use of IVHM output or operational procedures, etc. Assumptions that deal with such uncertainties should be identified and documented.

3. Identify interfaces for IVHM system

Interfaces identify various interactions that would take place in an IVHM equipped system. This would include interfaces between the system and the various elements of IVHM such as sensors, communications, control system, displays, etc. Typical interfaces are data interfaces between software modules, between data acquisition and state estimations algorithms, and further between state estimation and decision/planning modules. Interfaces identification relevant to IVHM systems should try to answer the following questions:

- What Interfaces are encompassed by the scope of IVHM?
- Does the system operate with on-board hardware, pass data to off-board systems, link to sustainment and finance databases, or other logistic and supply chain data collection systems?
- Can IVHM access data from bus supporting core system functions?
- Are system related sensing and operational environment data available to IVHM?
- What are the compatibility considerations?
- Is the system updateable and will contemplated future systems be accommodated?
- What standards have to be met and what means and methods will be used to link to other data systems?
- Which subsystems or components IVHM will monitor?
- Will IVHM system be a part of a control loop?
- Who will be the users of IVHM output and how will this output be made available to them (displays, alarms, databases, etc.)?

When considering interfaces, one must strive to use the interface to improve access to data through a common universal format which is scalable and enables multi-disciplinary users to analyze data to discover invaluable information.

- Interface Examples – On-board systems, off-board systems, maintenance systems, planning systems, data warehouse, logistics, finance systems, OEMs, acquisition, HR, research environments, and other services.
- Interface Documentation – Documentation of interfaces should be done via interface control documents / specifications, architecture drawings, data flow diagrams, sequence diagrams, data mapping diagrams, and example data.

4. Data Inventory

Current inventory health management system developers must first understand the available systems health data and interfaces. Vehicle health management data come, in general, from on-board and off-board sources. Reference data are also essential.

- On-board Data Sources - Operational data (e.g. flight phase, status, or other discrete signals), parametric data (e.g. air speed, angle of attack, timing, etc.), and fault data (e.g. fault and maintenance codes, BIT codes, etc.)

- Off-board Data Sources - Maintenance data (e.g. maintenance actions, pilot or crew reports, part installation and removal information, etc.), test stand data (e.g. test stand test limit reference data, test summary reports, etc.), and unstructured data (e.g. bore scope or other hand-held inspection system data).
- Reference Data - System and subsystem organizational structure (e.g. Work Unit Code, ATA), engineering units (e.g. knots, psi, degrees F), on-board and off-board data recorder configurations, hardware and software versions, calibration / correction / conversion other metadata info and a data dictionary including domain-specific semantic information.

IV. Concept of Operations and Use Cases for IVHM

A Concept of Operations (ConOps) is a document that describes the characteristics of a system from the user's point of view[26]. This document describes the quantitative and qualitative system characteristics to all the stakeholders. This document can contain use cases to describe the interactions between the user and the system to achieve the goals. The concept of "use cases" forms a strong basis for developing requirements.

The ConOps begin as a thought exercise, where utility of novel ideas are explored though various scenarios in which a system would operate and benefit from the new concepts. The level of details in the scenario should be just enough to come up with need statements. The ConOps document can be iteratively revised as more insights are gained in the development phase. The ConOps are a means to communicate our understanding of the needs with all stakeholders. An overall system ConOps document is expected to include ConOps for IVHM module, which describes the functions of IVHM in situations with/without fault conditions in the system. The ConOps document should describe both normal and abnormal operations of the system

Use Cases are also the results of thought experiments. However, they are somewhat more detailed than the ConOps document. They describe, in specific detail, how the system is going to be used by the users. The key to developing a useful use case is to identify the user (or the actor) and his or her actions on the system. They describe the nominal operating case as well as the abnormal (or alternate) operating cases.

For example, the ConOps document might state that: "*The system will be able to take off in normal and abnormal environmental conditions. It will also be able to take off if a single engine fails during takeoff.*" The use cases associated with this ConOps might be far more detailed. It would describe exactly what normal conditions are. It will describe a set of abnormal conditions including temperature, altitude, rain and ice, and head and cross wind parameters. It might go into all the possible faults that can occur during take off that need to be designed for, etc. Since the general concepts are similar, we will use these terms interchangeably in the course of this paper. The key is to make sure that the set of requirements that result from these thought experiments are correct and complete.

As we stated earlier, the overall ConOps document for systems equipped with IVHM, can be divided into two main parts.

1. The first part of the system ConOps document describes a typical nominal system operational scenario. Since no health concerns are present for the system the IVHM is expected to continue monitoring the system and make sure no interference is caused in the nominal system functions. Therefore, this describes system operations when no health concerns are present. This would include IVHM output that would be considered indicative of healthy system and no false positives resulting in unnecessary concerns and/or actions.
2. The second part of ConOps/Use Cases should describe the IVHM function when the system experiences a fault or abnormal condition. The IVHM output, corresponding set of actions, its interactions with the system, and expected consequences should be described at a generalized level. If the IVHM response is expected to be similar for all possible fault modes a single scenario description would suffice, otherwise, ConOps/Use Cases should include description for each category of contingencies. If it is expected that IVHM function evolves with system life cycle or is different in different modes of operation, all such scenarios should be described. Various different stages to be considered could be system development, integration, test and verification, operations, training, maintenance, upgrades, etc. However, the most important stage that needs description is operations[19]. Furthermore, ConOps/Use Cases should describe scenarios from all key stakeholders' point of view to make use all IVHM users are satisfied with its functionality. For IVHM such users are typically maintainers, managers, operators, and regulatory bodies, etc.

ConOps relevant to IVHM will try to answer the following questions:

- Who are IVHM stakeholders and what are their viewpoints?
- How would these stakeholders use IVHM output in their actionable decisions?

- What are the operational modes (both nominal and off-nominal) of the system under which IVHM will operate?
- What are the IVHM nominal (and off-nominal) operational modes and how they affect system safety?
- How would IVHM function in presence of system fault?
- How is IVHM expected to interact with the system (i.e. inflow & outflow of information)?
- Will the IVHM system control hazards, and/or maintain safety, and/or protect assets?

Ultimately, ConOps and Use Cases are used to derive system requirements. When considering intent and scope, the details of the Concepts of Operation are a significant element and affect much of the preparation for requirement development. Therefore the more details are added in ConOps/Use Cases, the more coverage of requirements can be achieved. All assumptions should be clearly stated. If during the development stage any assumption is found to be incorrect, then the ConOps/Use Cases may need to change; and, therefore, corresponding requirements may change as well.

Another important aspect of requirement development is that is it essentially a collaborative process. Consequently many organizations and information sources must be prepared to participate in requirements generation and it is extremely important to establish the procedures for coordination upfront. Following categories must be considered.

- Resource availability – The supporting resources for the program must be taken into account and vetted through the responsible organization and all support functions as well. Resources include in some cases, facilities, finances and equipment. Additional considerations that may come from support elements include computation and data resources.
- Schedule – As health management is often a multi-disciplinary enterprise, it also tends to be multi-organizational. As a result, independent scheduling and tasking need coordination and an upfront understanding of program resources.
- Coordination – The primary element of coordination is frequent and unambiguous communications. But in addition, contributing elements are: a clear statement of work and schedules, well understood and mutually agreeable contract terms and conditions, well-understood roles and responsibilities, working sessions and technical interchanges, collaborative tools, information exchange processes, and a common technical and systems domain knowledge.

V. Systems Requirements

It is after the *concept* phase when a complete set of system requirements including those of an IVHM system should be derived from the ConOps already established. These requirements, if done well, allow an effective IVHM development management with assurance of meeting customer needs and expectation. In addition to product requirements some of the requirements are associated with management and administration of the system development, where budget and schedules are developed, the management team is created, and legal and reporting requirements are identified[17]. Such requirements are referred to as process or program requirements in this paper and discussed briefly later.

A. Product Requirements

Product requirements define what the IVHM system will do. Based on the ConOps document high level system requirements are usually functional requirements (i.e., what the system must do). These requirements also include performance requirements (safety, availability, etc.), and cost. High level system requirements then flow down to requirements for maintaining vehicle health adequate to perform the missions. They can flow from safety, cost, performance branches above and together influence HM. From HM perspective these are still high level since exact design of HM is not yet there. From an IVHM point of view, system requirements at this level stay at the level of specifying reliability, maintainability, and availability requirements without compromising safety in general and sometimes include cost requirements (pertaining to loss, incomplete missions, unscheduled maintenance, downtime, etc.). Industry experience reveals that lack of a systematic methodology to come up with IVHM requirements upfront has led to vague and incomplete requirements. This forces the lower level subsystems to make assumptions in interpreting those requirements and pose system level risks of cost, schedule, safety, and robustness.

This step will try to answer the following questions relevant to IVHM:

- Which components and fault/failure modes will be addressed by IVHM?
- Are IVHM functions defined for each of the candidate subsystems/components?

- Are requirements between flight (airborne) and ground operations distinguished and specified for vehicle (launch and flight) and payload separately?
- Are requirements for portable maintenance aids and maintenance management covered?
- Are performance specifications for all IVHM functions specified with margins?
- What are the tolerances around IVHM function outputs? Are these flowed down from top level mission objectives and properly specified at the lower level?
- Are all interfaces, identified earlier, covered?
  - Are all hardware and software interfaces defined?
  - Are communication, command, and control interfaces defined?
  - Are test and operational interfaces such as GUIs, data reports, alarms, warnings, etc. defined?
- Are IVHM function maintainability requirements included?
  - Calibration, updates, upgrades, etc.
- What are the requirements for IVHM test capabilities to enable fault injection for verification and validation?
- Are non-functional system requirements considered in the IVHM requirements?
  - Are requirements related to aspects like *security* considered?
  - Specifically, are topics like information sensitivity, data rights and proprietary information, and the requirements and procedures of classification included?
- Are all requirements allocated?

B. Process/Program Requirements

In addition to developing product requirements that define '*what is needed'* it is also critical to define the set of milestones, roles and responsibilities, mode of interaction between different subsystem teams, timeline, deliverables, reviews, and acceptance procedures. IVHM is developed by multi-organizational teams including external contractors, and therefore, development of a cross-functional and inter-organizational program management plan is extremely important to support the execution of an effective IVHM development[17]. Specifically, these requirements will determine the IVHM project management structure and answer the following questions:

- Do all IVHM product requirements trace back to the mission concept and risk assumptions outlined in the ConOps?
- Is there an IVHM design and development team in place? What is the structure of the team?
- How does the lead IVHM engineer interface with the lead systems engineer and other subsystem leads?
- Are IVHM requirements allocated properly to respective subsystems/components?
- What is the timeline for IVHM requirements, design, and development and respective decision gates and reviews?
- What are various formal documents that need to be maintained and produced?
  - For reference (e.g. ConOps document, requirements document, design document, etc.),
  - For analysis (e.g. FMECA, hazard analysis, risk analysis, fault tree analysis, etc.),
  - For evaluation (fault/failure scenario tests and test procedures, incompressible test list, verification and validation reports, acceptance criteria, etc.),
  - Approvals (verification and validation checklists, design change document, requirement waivers, etc.).
- What is the process for making changes in IVHM requirements?
  - As system design takes shape exposing additional needs (such as when new failure modes are discovered or if new constraints arise due to implementation choices) how can the changes be made and tracked?
  - How are the changes due to scope, budget, and schedule adjustments accommodated?
- Are the IVHM product requirements inclusive of requirements for system operation and maintenance and not just product development, i.e. how well are the end user (stakeholder) objectives addressed?

While answers to these questions depend on the project management, team structure, and specific mission types[27], it is recommended that IVHM design reviews be conducted as part of overall system design reviews[4]. From costing perspectives, recent industry experience calls for a separate work breakdown structure and resource allocation for IVHM activities starting from the concept phase[11]. An important process in developing good requirements is that requirements are flowed down, and bi-directionally traced[8, 10] – this ensures that all needs are considered and nothing is built without a need.

At the end of the requirements stage, the outputs should be clearly defined product requirements with an understanding of mutual goals, a program management structure, and well defined and documented processes and tools to help successful system development and deployment. This process is explained with an example in another paper that discusses development of an IVHM system for an aircraft Landing Gear System (LGS)[10].

VI. Conclusion

This paper examined the various stages in the SE process and identified activities specific to IVHM design and development. Important aspects of the SE process for IVHM are highlighted by asking several relevant questions that system engineers must address at various design and development stages. Addressing these questions should provide some guidance to systems engineers towards writing IVHM related requirements to ensure that appropriate IVHM functions are built into the system design. A discussion on programmatic requirements and management structure emphasizes the uniqueness and importance of IVHM system within overall system development. As such this paper strives to contribute to the general discussion on developing IVHM requirements and systems engineering process for a truly integrated health management into a systems design.

Acknowledgments

The funding of this work was provided by the NASA System-wide Safety and Assurance Technologies (SSAT) Project under NASA Aeronautics Research Mission Directorate's (ARMD) Aviation Safety program. Authors acknowledge the support and contributing discussions from several industry experts including Dr. Ravi Rajamani, Mr. Frank Kramer, Mr. Mike Augustin, Mr. John B. Schroeder, and Ms. Ginger Shao. Authors would also like to thank several members of the Discovery and Systems Health (DaSH) area within the Intelligent Systems Division at NASA Ames Research Center for very insightful discussions.

References

[1]Muirhead, B.K. and L. Fesq, *Coalescing NASA's Views of Fault and Health Management*, in *NASA Spacecraft Fault Management Workshop*2012: New Orleans LA.

[2]Johnson, S.B., et al., eds. *System Health Management with Aerospace Applications*. 1st ed. 2011, John Wiley & Sons Ltd. 664.

[3]Fesq, L.M. and D. Oberhettinger, *Fault Management Practice: A Roadmap for Improvement*, in *AIAA Infotech@Aerospace*2010: Atlanta GA. p. 13.

[4]Fesq, L.M., et al., *V&V of Fault Management: Challenges and Successes*, in *AIAA Infotech@Aerospace*2013: Boston MA. p. 7.

[5]Jennions, I.K., *Perspectives on an Emerging Field*. Integrated Vehicle Health Management: , ed. I. Jennions. Vol. 1. 2011: SAE International. 188.

[6]*NASA Spacecraft Fault Management Workshop*. 2012 [cited 2013 July 27]; Available from: http://www.nasa.gov/offices/oce/documents/2012_fm_workshop.html.

[7]NASA, *Fault Management Handbook (Draft)*, 2012, NASA.

[8]Rajamani, R., et al., *Developing IVHM Requirements for Aerospace Systems*, in *SAE 2013 AeroTech Congress & Exhibition* 2013, SAE: Montreal Canada.

[9]Saxena, A., et al., *Requirements Specification for Prognostics Performance – An Overview*, in *AIAA Infotech @ Aerospace*2010: Atlanta.

[10]Saxena, A., et al. *Requirements Flowdown for Prognostics and Health Management*. in *AIAA Infotech @ Aerospace*. 2012. Garden Grove CA.

[11]Fretz, K. and A. Hill, *Recent Progress in the APL Fault Management Process*, in *NASA Spacecraft Fault Management Workshop*2012: New Orleans LA.

[12]Ingham, M., *No more Band-Aids: Integrating FM into the Onboard Execution Architecture*, in *NASA Spacecraft Fault Management Workshop* 2012: New Orleans LA.

[13]Forsberg, K., H. Mooz, and H. Cotterman, *Visualizing Project Management*. 3rd ed2005, New York, NY, USA: J. Wiley & Sons.

[14]INCOSE, *Systems Engineering Handbook*, in *A Guide for System Life Cycle Processes and Activities*2012, International Council on Systems Engineering (INCOSE): San Diego, CA, USA.

[15]ISO/IEC, *Systems and Software Engineering*, in *System Life Cycle Processes*2008, International Organisation for Standardisation / International Electrotechnical Commissions: Geneva, Switzerland.

[16]Deal, R.W. and S.S. Kessler, *Architecture*, in *System Health Management with Aerospace Applications*, S.B. Johnson, et al., Editors. 2011, John Wiley & Sons Ltd. p. 115-127.

[17]Wilmering, T.J. and C.D. Mott, *Health Management Systems Engineering and Integration*, in *System Health Management with Aerospace Applications*, S.B. Johnson, et al., Editors. 2011, John Wiley & Sons Ltd. p. 95-113.

[18]Johnson, S.B., *The theory of System Health Management*, in *System Health Management with Aerospace Applications*, S.B. Johnson, et al., Editors. 2011, John Wiley & Sons Ltd. p. 3 - 27.

[19]Tumer, I.Y., *System Design and Analysis Methods*, in *System Health Management with Aerospace Applications*, S.B. Johnson, et al., Editors. 2011, John Wiley & Sons Ltd. p. 129-143.

[20]Hooks, I.F. and K.A. Farry, *Customer Centered Products: Creating Successful Products Through Smart Requirements Management*, in *AMACOM American Management Association*2000.

[21]Kevin R. Wheeler, T. Kurtoglu, and S.D. Poll, *A Survey of Health Management User Objectives Related to Diagnostic and Prognostic Metrics.* International Journal of Prognostics and Health Management, 2010. **1**(1): p. 20.

[22]Saxena, A., et al., *Metrics for Offline Evaluation of Prognostic Performance.* International Journal of Prognostics and Health Management, 2010. **1**(1): p. 21.

[23]Kurtoglu, T., O.J. Mengshoel, and S. Poll. *A framework for Systematic Benchmarking of Monitoring and Diagnostic Systems*. in *International Conference on Prognostics and Health Management*. 2008. Denver, CO: IEEE.

[24]Roychoudhury, I., et al., *Verification of Prognostic Algorithms*, 2013, to appear in Annual Conference of the PHM Society: New Orleans.

[25]Augustine, M., et al., *CBM Maintenance Credit Verification and Validation Process*, in *National Rotorcraft Technology Center Research Program*2011, Verical Lift Consortium: Glen Mills, PA. p. 130.

[26]Shishko, R., et al., *NASA Systems Engineering Handbook*, 2007, NASA.

[27]Shenhar, A. and Z. Bonen, *The New Taxonomy of Systems: Toward and Adaptive System Engineering Framework.* IEEE transcations on System, man, and Cybernatics - Part A: Systems and Humans, 1997. **27**(2): p. 137-145.