

INTEGRATED SYSTEM HEALTH MANAGEMENT FOR REUSABLE, IN-SPACE TRANSPORTATION SYSTEMS

By

Anthony R. Gross, Associate Director (anthony.r.gross@nasa.gov),
Ann Patterson-Hine, Senior Research Scientist (ann.patterson-hine@nasa.gov),
Brian J. Glass, Senior Research Scientist (brian.j.glass@nasa.gov), and
Joan Pallix, Senior Research Scientist (joan.b.pallix@nasa.gov)

Information Sciences & Technology Directorate
NASA Ames Research Center, Moffett Field, CA, USA

Abstract

New missions of exploration and space operations envision architectures that are based on powerful new in-space transportation systems. Such missions as the development of human-tended operations nodes at the L1 or L2 Lagrange points, very large telescope assemblies, and planetary missions developed and operated from such points, will all require highly capable space transportation systems to transfer cargo and humans crews from low Earth orbit (LEO) to these locations. Such missions could involve a complex transportation infrastructure, containing a few elements or many “independent agents”, i.e., space tugs, refueling stations, and an overall control and communication system. New information technologies, which take advantage of knowledge-based software, model-based reasoning, and high performance computer systems, will enable the development of new generations of planner/schedulers, and autonomous control systems with diagnosis and recovery capabilities. Integrated system health management (ISHM) frameworks use these technologies to increase the reliability and robustness of vehicles. This paper will describe design considerations for implementing the ISHM concept on reusable, in-space transportation systems. Topics to be presented will include a mission description and needs assessment, brief description of key ISHM concepts, potential architectures for ISHM as applied to in-space transportation systems, and how ISHM concepts will be implemented for the system-of-systems of “independent agents” mentioned above.

Introduction

New generations of space exploration missions will inevitably evolve from current capabilities to new levels of complexity and longer duration. As we reach out to explore planets further out in the solar system, the architectures necessary to support such missions will require spacecraft that will spend their entire working lifetimes in the space environment, without returning to Earth. Such in-space systems will perform a wide range of functions, including crew transfer, ferrying supplies and scientific instruments systems, and as refueling tankers for long duration missions. Each will embody its own propulsion system, and will require a high degree of autonomy and the ability to manage its operational status.

Such intelligent modular systems will signal a new approach to space exploration and, in this paper, the systems and technology necessary to assure the reliable operation of in-space vehicle systems will be discussed. The capability for such reliable operation is known as Integrated System Health Management (ISHM) and will be described in general terms first, then in specific detail as it is applied to intelligent, modular, in-space propulsion systems. The discussion will begin by describing potential exploration scenarios that involves many independent spacecraft systems, all required to work together to achieve the complex goals of the mission. ISHM capability will be a required part of such systems in order to assure their success. Some of the technologies required for the implementation of such systems include: automated reasoning, data mining and fusion, human-

Copyright ©2003 by the American Institute of Aeronautics and Astronautics, Inc. No copyright is asserted in the United States under Title 17, U.S. Code. The U.S. Government has a royalty-free license to exercise all rights under the copyright claimed herein for Governmental purposes. All other rights are reserved by the copyright owner. Presented at the 54th International Astronautical Congress, Bremen, Germany, September 29 - October 4, 2003.

system computing, and advanced decision systems. The following sections discuss where these technologies will be required, and how they might be implemented.

Mission and Problem Description

Gateway-like Mission Concepts

Some concepts for future remote exploration envision one or more “gateway” stations – located at a libration point – as human logistics and resupply outposts. Unlike lunar or Martian-orbiting space stations, relatively low-energy transfer trajectories may be used.

These low-energy trajectories allow bulk transfer and resupply with modest velocity changes (Δv). Given radiation concerns, their long flight durations will make them unsuitable for human crew transfer, so a separate class of smaller, high- Δv crew transfer vehicles will be necessary, as shown by the notional vehicle in Figure 1. Logistics resupply transport vehicles can then be expected to be both automated and

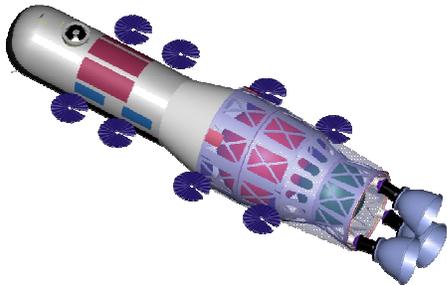


Figure 1. Notional LEO-Gateway crew transfer vehicle.

in long-duration transfers. Minimal deep-space bandwidth can be expected to be made available for real-time monitoring of these cargo carriers.

While LEO-to-gateway crew transfer vehicles will have on-board crew available for systems management, the vehicles will have additional safety and certification burdens and can be expected to have greater systems redundancy. Operations will be both ongoing in space (like the Space Station) and will include frequent high-energy propulsive segments (like the Space Shuttle). Unlike the latter, there can be no teardown or intrusive manual inspection between flights.

SHM Requirements Drivers

The logistics transfer vehicle will be expected to likewise support multiple flights – with different payloads –

without extensive maintenance or reconditioning. A 30-50 metric ton capability is necessary to place a gateway station. Candidate propulsion technologies include solar-electric, nuclear-electric or nuclear-thermal systems, with a design lifetime of five years with only periodic LEO maintenance at the ISS. Deep-space cruise would either operate autonomously, or with minutes of time lag if controlled from Earth.

By comparison, Earth-to-Orbit (ETO) and low-Earth-orbiting systems operate within milliseconds to seconds of the Earth’s surface, in terms of monitoring and control lags. Minimal lag makes stable and safe control possible for these systems, as has been performed historically from ground-based mission control centers.

ETO systems have another advantage, in that human inspection and maintenance is possible, and currently required, between flights of reusable systems. These operations take place under convenient shirtsleeve conditions, with effectively-unlimited supplies of power, labor and spares, and under uniform 1-g conditions.

Needs for automated health management

Given that deep-space transfer vehicles (crewed or cargo transfer) will necessarily function out of communication with Earth control for long periods of time, safety requires active monitoring and control (rather than a “fire and forget” approach). Due to the transmission time lags, traditional Earth-centralized mission operations will not be feasible in deep-space exploration architectures. Single-string lunar exploration can be done, given just a few seconds lag, but not multiple ongoing missions and exploration at distances beyond the Moon. Large dynamic solar-electric array or nuclear reactor control both require real-time responses – in terms of seconds or faster – without large gaps in coverage.

There are a number of partial solutions to address the problem of remote operations. One of them, discussed in this paper, is the use of automation to implement on-board system health management. Another complementary strategy is the eventual decentralization of mission control authority, moving the locus of responsibility for vehicles to the humans on the nearest gateway station.

Crew transfer vehicles have perhaps an option of limited in-flight Line Replaceable Unit (LRU) replacement by their passengers or by integral robotics, but otherwise they and bulk cargo transfer vehicles will have to wait for maintenance or repair until their next station docking.

In ETO systems, ISHM is enhancing, rather than required – for increased safety, faster ground turnarounds, and lower operations costs. But in deep space transfer applications, ISHM is essential. Complex, high-energy, quick-responding, robotic systems deployed to regions beyond the timely reach of terrestrial control require ISHM and other automation in order to safely operate. Given the difficulty of intrusive inspections on-orbit – even while docked to a station – transfer vehicles must have adequate built-in sensors and instrumentation to observe all high-criticality failure modes and predict required maintenance actions prior to failure.

Overview of Integrated System Health Management

Exploration missions such as those described in the previous section require many system elements coordinating their activities to achieve the goal of the mission. It is important to determine the health status of the individual elements, but often it is essential to understand the relationships of the elements to one another. System designers study the propagation of failures throughout subsystems and systems. Mission developers analyze the effects of the element failures on mission scenarios. During operation, the intelligent system health manager must have access to all of this information in order to effectively manage the health of the entire system of systems.

Intelligent system health management (ISHM) architectures have been developed under NASA's Space Launch Initiative. Since the goal of this program is launch vehicle development, the health management task is called IVHM, and that nomenclature will be used in this section for consistency with the referenced architectures. One of these architectures, developed by Honeywell Space Systems, is illustrated below in Figures 2 and 3¹. Its inherent modularity and ability to represent large, distributed systems makes it a candidate for application in the exploration area. The architecture is developed hierarchically to provide expansion capability. For the present application, the elements could include the crew transfer vehicle (CTV), the gateway, a lander, and a habitat. Each of these elements would be decomposed into sub-elements. In the case of the crew transfer vehicle, the elements would include the boosters, the CTV and perhaps a payload module. As shown in Figure 2, each element consists of components in which an IVHM kernel would reside. The subsystem interface provides the mechanism by which information is distributed among the various subsystems. During design, a subsystem interface specification can be used to control the information flow at the subsystem interfaces. If a component complies with the specification, it is called a Member Subsystem and it will supply its health status in well-defined parameters and formats. If a component is not able to

comply with the Subsystem interface specification, its health can still be integrated into the architecture. An adaptor is custom-designed to provide an interface to a Non-member Subsystem. The IVHM kernel provides reasoning across the subsystem and also across subsystems at the system level. Issues arise such as how to provide communication of health status among subsystems as well as up and down the hierarchy in a timely manner. These issues must be addressed early in the design of the health management architecture. Another challenging issue is the incremental construction of space systems such as these and how that impacts the health assessment, monitoring, and reconfiguration of systems which are changing periodically due construction. Strict model specifications, updating, and configuration management will be essential to the successful application of IVHM strategies.

Figure 3 contains the functions provided in the IVHM Kernel. The System Level IVHM Manager coordinates IVHM operations across multiple elements. The Mission Readiness Manager assesses the capability of specific subsystems to perform a mission profile. Maintenance and Troubleshooting Support can coordinate the maintenance activities among the available maintenance depots. For instance, there could be maintenance performed during flight of the CTV or it could be performed while the CTV is docked to a Gateway station, with all of the information archived to support further health management activities. The Event Manager manages events such as crew caution and warnings, information directing the System Level IVHM Manager to reallocate management responsibility, and events identifying diagnostic or prognostic results from subsystems. The architecture is designed to accommodate various reasoners and knowledge fusion tools. These tools, located in each element, perform diagnostics and prognostics across all subsystems within the element. They can also be used to perform these functions at higher system levels. Reference 1 describes several tools well-suited for application to larger systems. Model-based reasoning capability has been demonstrated for space applications on the Deep Space 1 mission in 1999². A heterogenous architecture utilizing multiple, disparate reasoners was demonstrated under the SLI program and is described in Reference 3. Because this IVHM architecture was designed to be open and scalable, its structure and functionality can be used for the broader System Health Management function required by Gateway-like Missions.

Applications to In-Space Transportation Systems

New space exploration missions will be increasingly complex and of longer duration. Increased functional goals often result in increased implementation

complexity, making it much more challenging to achieve both reliability and affordability. In order to meet the challenges of future mission complexity, NASA will need to make use of all of the recent advances in communications, computers, software, sensors, design, and engineering technologies. Despite significant technological advances, all mission risks will not be

mitigated during the mission design phase: software and components will fail or degrade; operators will make mistakes; and operating environments may be uncertain. Implementation of critical future mission systems to recover from these unanticipated problems and will significantly reduce the cost of system operations.

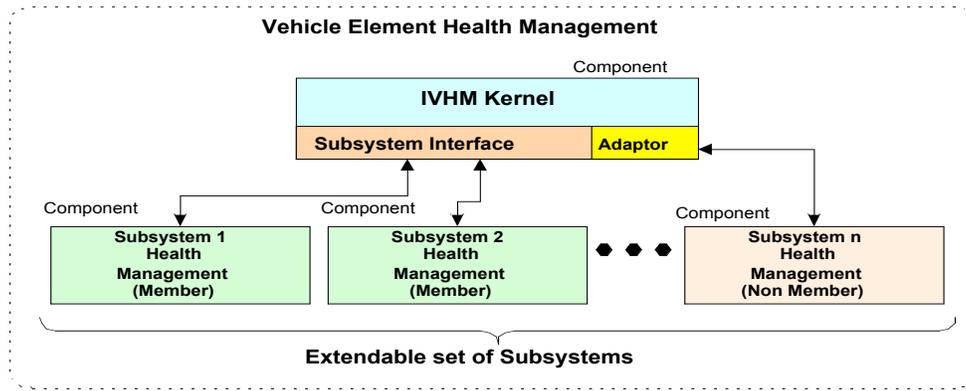


Figure 2 Vehicle Element Health Management

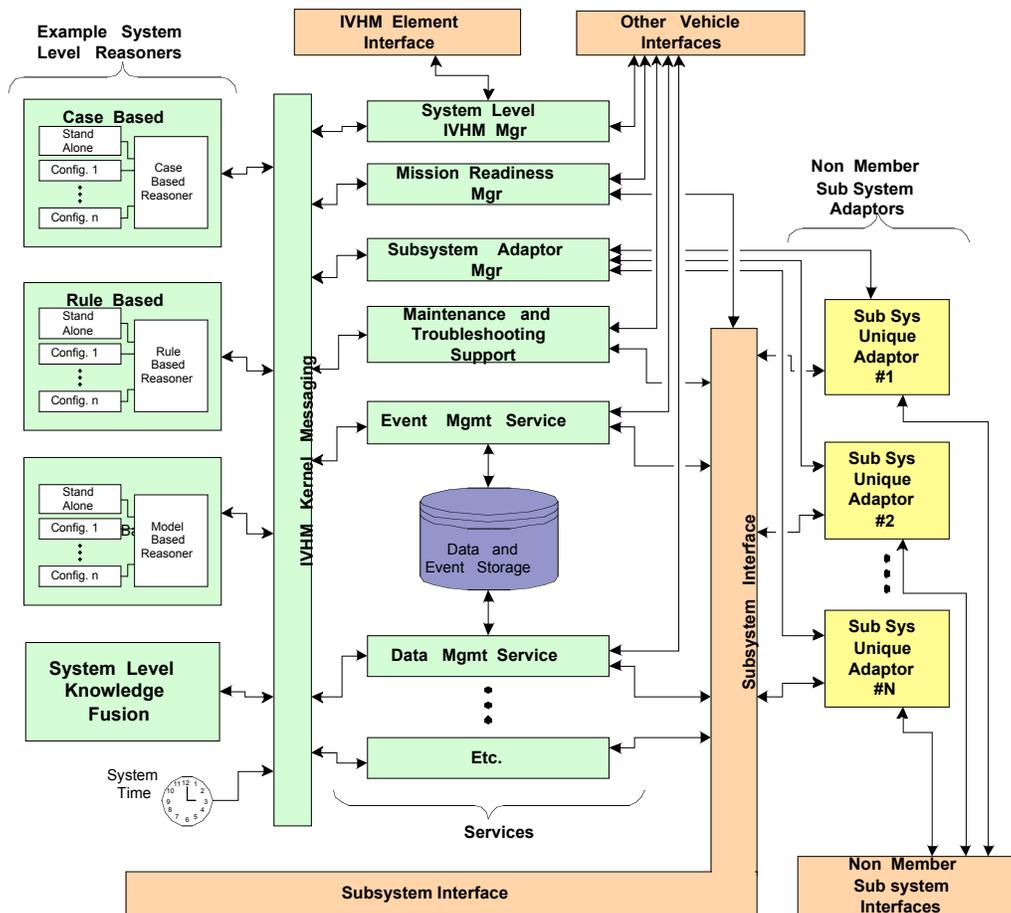


Figure 3 IVHM Kernel Component

The mission described in this paper will require ISHM technologies to be integrated with all mission systems. Studies of past mission failures can be used to establish ISHM technology application priorities that address cost and risk reduction for this mission⁴. Studies indicate that current mission technologies are not optimal for carrying out effective risk mitigation strategies as they lack significant capability to assess system condition or to validate system performance. System robustness, redundancy and capability for rapid recovery are currently inadequate. In addition, incorporation of information technology in the maintenance process is insufficient for the required reduction in life-cycle costs for the future.

It is reported that flight control subsystem failures rank among the highest as initiators of mishaps. Major contributing factors in past accidents included component failures, lack of proper human-machine interactions, operator error on-board or on the ground (often due to an uninformed operator) and unanticipated operating environments. Reference 4 contains data from a number of mishaps described in several important agency reports including the NASA Integrated Action Team Report, the Shuttle Independent Assessment Team Report, the Faster, Better, Cheaper Task Report and the USAF Broad Area Review of 1999. All of the factors outlined in the reports can be addressed by future implementation of ISHM Technology.

The human-machine interaction will be extremely important for the gateway mission because there will be a significant robotic component of the mission. Humans will need to effectively interact with robots and other autonomous systems. Today, the primary responsibility for fault management lies with the crew or ground personnel. In fact, pilots have pointed out the demand for real-time, on-board integrated diagnostics that provide “answers not just clues” to the causes of multiple anomalous conditions occurring during all phases of flight operations. Nonintegrated caution warnings are not sufficient because pilots and controllers are responsible for cognitive integration that consumes valuable time. Pilots are often required to refer to on-board manuals to determine the cause of an anomalous event.

As was described in the previous section, next generation intelligent systems are expected to automate much of the fault management process and enable real-time fault management for remotely operated or autonomous vehicles. The incorporation of these advanced technologies into the fault management process carries human factors risks, including over-reliance on automation, information overload, poorly designed user interfaces, and mode confusion: insufficient understanding of automated activity and/or insufficient awareness of the effects of automated actions on systems

functioning. ISHM will be essential to inform both humans and autonomous systems of component failures as well as failures induced by the human-machine interaction itself. This will inform humans and be enabling to autonomous operations. Numerous mishaps have been reported that were due to the human’s lack of awareness of the function of the autonomous system. The autonomous system must also be aware of the goals of the humans and any obstacles to meeting those goals. A human centered approach to design of these complex systems will be pursued.

For unmanned, long duration or distant missions the autonomous systems will need to be self-aware. For example, the Mars Polar Lander⁴ could have benefited from a simple integrated health management system. There is evidence to suggest that the lander crashed into the surface of Mars as a result of misinformation relayed to the landing control system resulting in shut off of the engines at 40 meters above the ground. There were other sensors on board that could have clarified the ambiguous data but there was no system integration and no intelligent reasoner available to evaluate the overall state of the system and take the appropriate course of action. The communication delay between the Earth and Mars is too long for ground controllers to have had any impact on this critical real-time control issue.

For in-space vehicles involved in the Gateway mission, other critical control capabilities may be shared by humans and autonomous systems such as docking, launch and landing on the moon, aerocapture maneuvers, and control of multiple coordinated micro-spacecraft. For the manned portions of the mission, reliable control of life support systems (including human habitats) will be critical. The control systems will consist of a network of intelligent agents that work with the ISHM system (Figure 4) to sense the environment and reason based on internal state (stored information that may include sensory data and goals). Predetermined procedures, constraints, and domain models allow the determination of the internal state.

These agents will maintain stability or recover in the presence of subsystem or system level anomalies and environmental uncertainties. They will reconfigure the control system to compensate for damage/failure to control effectors or will gracefully degrade performance, while maintaining functionality to the greatest extent possible, if unable to fully recover from damage/failure. They will also optimize achievable control performance through integration of motion control, power, propulsion, and structural subsystems.

Figure 4, shows how the ISHM architecture may be integrate with a general purpose integrated reasoning framework for an intelligent agent controlling a vehicle.

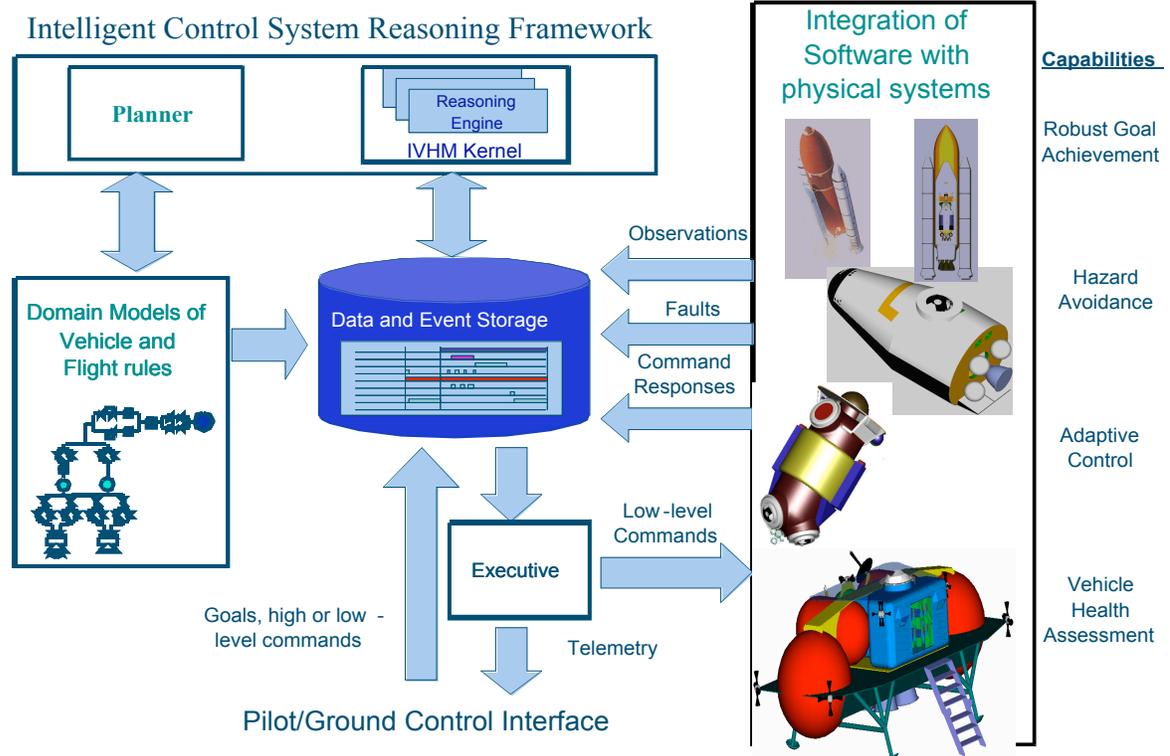


Figure 4. Intelligent Control System Reasoning Framework

This framework is similar to that used in the Remote Agent Demonstration that autonomously controlled the ion-engine propelled Deep Space One spacecraft in 1999².

Goals or commands are input to the system from a crew member, remote operator, or another system and are entered into a data and event storage database where they are sequenced and decomposed by various reasoning engines into primitive commands. Sensory information and subsystem feedback from previous commands, which may be fused or used by the reasoning engines to determine states that are not directly sensed, (e.g., a diagnosis) are also entered into the database. The reasoning engines and the temporal database use the flight models, rules, etc..., to insure that any command sequence in the database does not violate a constraint. This will enable the command sequences to adapt to changes in the system and environment. The executive sends the primitive commands to the specified control system at the appropriate time. As shown in Fig. 4, the system also contains a planner, which plays a key role in goal decomposition, scheduling, and planning repairs required from command failures, new or altered goals, or other unexpected information.

Using this approach, plans can be dynamically updated at execution time. This allows the agent to respond to change in the system or environment, e.g., reconfiguring itself due to the failure of a component, and achieve the system goals or a subset of them. With such a closed loop system, commanding and sensing are unified so that conflicts are resolved prior to execution and decisions are made based on a consistent state of the system and its environment. An agent may make use of several of different reasoning engines and be flexible so that it can dynamically generate plans to achieve complex goals. The system also enables prognostics through analysis of historical data related to faults/failures, observations, successful response strategies, and trending.

The modular architectures of the systems shown in Figures 3 and 4 have many advantages in the development, cost and function of complex space systems. They allow components to be exchanged without redesigning the entire system. This is of particular value since it facilitates the integration of specific intelligent system and ISHM technologies without requiring them to meet all the requirements of the vehicle that it will be used to control.

The architectures are also amenable to being distributed over multiple computers and controlling multiple vehicles. In order to achieve low latencies between sensing and acting, particularly when this may involve computationally intensive activities such as planning and image recognition, it is helpful to distribute the computational load over multiple processors in a straightforward manner. Moreover, the framework can be used to control multiple vehicles in a manner similar to how it would control a single vehicle with multiple subsystems. Thus one vehicle could be used to repair another vehicle.

Modular system software designs allow for information to be used not only for safe control but for cost effective maintenance operations. A properly instrumented ISHM system will be able to report maintenance requirements autonomously. Many hours of routine system inspection can be avoided and costly scheduled maintenance operations will be replaced with conditioned-based maintenance. ISHM will ultimately reduce system life cycle costs by many orders of magnitude. Significantly less human interaction will be required for system diagnostics and maintenance. This will be essential to the success of the Gateway Mission.

Mission and Technology Challenges

It is possible that the current state of automation could be used to begin development of remote ISHM. However, there are several unresolved issues requiring further definition, or in some cases, future research. In remote operations beyond terrestrial mission control, critical control capabilities may be shared by humans and an autonomous agent-based ISHM system. How will humans and automation execute “shift changes”, either with onboard crew or when a transfer vehicle comes into range or leaves the vicinity of a gateway station?

Current onboard ISHM in space and aircraft is centralized, while supporting scale-up and increased complexity is leading the field towards decentralized agent-based architectures. Given networks of automation, who/what intermediates? And how can a critical safety system dependent on ad-hoc agent network interactions be verified and eventually certified?

Just as in hardware standardization, a wide variety of disparate ISHM software approaches across future space systems will lead to unnecessary development cost, high recurring software maintenance and a greater possibility of induced errors. Some process must define a modular software approach that can be consistent across a broad base of vehicles and systems.

Given transmission delays, it will be unreasonable to treat the Deep Space Network as a star architecture for future vehicle-to-gateway station communications. Some independent point-to-point in-space communications capability will be necessary.

Directions for the Future

Many advances have occurred over the past decade in the software and sensor technologies required for integrated system health management. The actual integration of these components has not been explored as rigorously. It is difficult to find testbeds that enable the exploration of system-level architectures to any detail. It is very difficult to find testbeds which are robust enough, and with sufficient fidelity to thoroughly validate all modes of operation and the performance of the health management system under failure or degraded conditions.

The modularity required by in-space transportation systems must be leveraged by the health management architecture for these systems. The process for incremental, staged construction required to build outposts, for example, is only now being explored during the construction of International Space Station. Many challenges have arisen in the staged construction of the data and power management systems for ISS; most of the troubleshooting has been carried out by ground support teams. The systems needed for future missions must be able to operate autonomously and must be robust enough to withstand a variety of failures and still provide the functionality required by the mission.

The technologies and processes developed thus far are capable of supporting the exploration missions of the future given proper attention to the final, and perhaps most difficult, step – the *integration*.

Acknowledgements

The authors would like to thank the reviewers, Gregory Dorais (ARC), Claudia Meyer (GRC), Lui Wang (JSC), Amir Fanjay (JPL), and Anupa Bajwa (ARC), for valuable input to ISHM planning for this and many other missions.

References

1. Preliminary Software Design Document (SDD), 2nd Generation Reusable Launch Vehicle (RLV), Integrated Vehicle Health Management (IVHM), SDD8270370 Rev B, Honeywell Space Systems, Contract No. NAS2-01060, October 4, 2002.

2. Remote Agent Final Report; http://nmp-techval-reports.jpl.nasa.gov/DS1/Remote_Integrated_Report.pdf
3. R. Wayne Dixon, et al, "Demonstration of an SLI Vehicle Health Management System with In-flight and Ground-based Subsystem Interfaces," 2003 IEEE Aerospace Conference, Big Sky, Montana, March 9-14, 2003.
4. Mishap Cause Classification Report, T. Panontin et al (To be Published)