Making Technology Ready: Integrated Systems Health Management

Jane T. Malin[1]
NASA Johnson Space Center, Houston, Texas, 77058-3696

and

Patrick J. Oliver2
Lockheed Martin Mission Services, Houston, TX, 77058

This paper identifies work needed by developers to make integrated system health management (ISHM) technology ready and by programs to make mission infrastructure ready for this technology. This paper examines perceptions of ISHM technologies and experience in legacy programs. Study methods included literature review and interviews with representatives of stakeholder groups. Recommendations address 1) development of ISHM technology, 2) development of ISHM engineering processes and methods, and 3) program organization and infrastructure for ISHM technology evolution, infusion and migration.

I. Introduction

AS the United States develops new spacecraft for missions to the Moon and Mars, new system management technologies will be needed for vehicles, habitats and robots. With longer communications delays and blackouts for interplanetary missions, most of the systems health management functions now performed by crew and flight controllers will need to be automated onboard spacecraft. Integrated Systems Health Management (ISHM) consists of the processes and activities that produce a “big picture” view of the health, state and status of spacecraft systems and components for crew, controllers, maintenance personnel and engineering. This information supports restoring functions and minimizing impacts of failures and off-nominal conditions on the mission and the reliability and safety of the spacecraft. [1]

ISHM processes and activities are performed by human teams assisted by sensors and computer systems, both in space and on the ground. ISHM functions for most current spacecraft are performed almost entirely by humans, with software handling only a limited set of functions. In Mars missions, communication delays and outages will mandate that most ISHM functions now performed by ground controllers will instead be performed onboard the spacecraft, by a combination of automation and the crew. By increasing the functionality of the software that assesses the health and status of the spacecraft, programs can support more autonomous distant crews and enable the crew and ground to focus on science and mission objectives.

ISHM technologies are being developed to aid and automate integrated fault detection and diagnosis, prognosis, impact assessment, situation assessment and prescriptive recommendation. Collecting and integrating large amounts of system health and status information and converting it into easily understood assessments should both reduce crew and ground controller workloads and handle otherwise unnoticed data. ISHM information should enhance the safety, availability and maintainability of a system.[2]

In aircraft, integrated assessments reduce unnecessary and risky troubleshooting and maintenance. Although ISHM technologies are used in some modern aircraft, there is limited operational experience in space programs. The overall impression of NASA engineers has been that ISHM technologies are too risky. The paper characterizes the sources of these perceptions and examines challenges for ISHM technologies.

For ISHM technology to be made ready for use in exploration vehicles, progress should continue both in technology maturity and development of program enablers for technology infusion and migration. ISHM technology

[1] Senior Technical Assistant, Automation, Robotics and Simulation Division, 2101 NASA Parkway./ER2
[2] Systems Engineer Staff, Requirements Definition & Management, Project Orion, 2400 NASA Parkway

maturity goes beyond Technology Readiness demonstrations.[3] It includes ISHM capabilities that address current limitations and enable compatibility and interoperation. It includes human-centered support for communication collaboration and control. It also includes supporting development of engineering processes, methods and tools for assessing and assuring ISHM system reliability and safety, and strategies and infrastructure for ISHM system evolution and upgrade during the life cycle.

Technology infusion refers to moving technology from demonstrations to routine use in systems and missions. Technology migration refers to preparing infrastructure and organization and taking the actions needed to move mature technology into a program or organization. This area includes organizational structure and processes for collaborative projects that enable ISHM infusion and migration. Technology infusion and migration factors are sometimes called Program Readiness for Transition (PRT)[4] or Advancement Degree of Difficulty (AD^2).[5] PRT measures levels of program readiness for a technology transition: customer commitment, integration into program systems engineering, and integration into program planning documentation. AD^2 measures levels of technology risks in engineering processes and tools for design, analysis, implementation, test and operations of the technology.

This paper explores the work needed by ISHM technology developers and programs in order to accomplish the technology maturation, infusion and migration needed to reduce technical risk. To gather perceptions, lessons learned, expectations and recommendations, the authors conducted interviews with twelve representatives of NASA stakeholder groups. Interviewees included individuals from the Space Shuttle, International Space Station (ISS) and Constellation Program offices, as well as the Safety and Engineering community, flight controllers and an astronaut.[6]

II. ISHM Functions

ISHM technology addresses off-nominal operational behavior in a system, including both system health determination functions and effective communication of health and status information.[7,8] ISHM technology uses models of nominal system performance, dependencies and interactions enable detection and characterization of off-nominal behaviors. The major functional capabilities usually addressed by ISHM technology are:

(1) *Fault Detection:* Integrate information to identify and communicate the current condition and symptoms of degradation, off-nominal behavior and failure in the integrated system and its components.

(2) *Fault Identification and Isolation (Diagnosis):* Integrate and analyze information about system state and symptoms, including information from built-in Fault Detection, Isolation and Recovery (FDIR) capabilities, to understand and communicate the root cause of detected problems. The fault identification and isolation function should be able to identify, down to the lowest replaceable unit, the root cause of symptoms.

(3) *Fault Prediction (Prognosis):* Determine and communicate likelihood and time when conditions, trends or causes may lead to faults or failures. Enable determination of the optimal time for proactive and preventive maintenance, enabling logistics and operations to better manage the overall system.

(4) *Situational Awareness:* Integrate condition, diagnostic, predictive and reconfiguration information from multiple subsystems to assess and communicate system health status and readiness at a glance. Support deeper investigation at the desired level of detail.

(5) *Impact Assessment:* Identify and communicate impacts of anomalous conditions on spacecraft capabilities. Impacts include lost or degraded redundancy, resources and functionality. Impact assessment capabilities can determine the “next worst thing” that could happen and when. These capabilities can also support “what if” analysis to determine impacts of possible subsequent failures. Combined with predictive degradation monitoring (“prognostics”), impact assessment identifies the next most likely failures.

(6) *Prescriptive Recommendation:* Determine, prioritize and communicate recommendations for troubleshooting or mitigation actions. Provide ISHM information that is pertinent to decision making (criticality, urgency, alternatives, and flight rules) and using applicable procedures (preparation, timing, resources, displays).

III. Technologies and Enablers

A. ISHM Technologies

1. Models

ISHM technologies use model-based state identification, comparing predicted behavior from models with observed behavior of the actual system. The models may be system configuration models, analytic state-based models, input-output transfer function models, fault propagation models, Bayesian dependency models, causal network models and qualitative or quantitative physics-based behavior models.[9] They can use fuzzy logic, case-based and statistical models and rules. Prognosis and fault modeling is typically based on empirical degradation signature models. Diagnosis is typically based on system configuration models (structure of components and connections with each component modeled as a finite-state machine) and finding configurations of the system model that are consistent with observations. The configuration indicates the likely fault location and cause of the observed symptoms. Impact assessments can also be based on such a configuration model. Recommendations are based on finding a set of operations that would transform a bad configuration to a good one. Most work on model-based ISHM systems for spacecraft has used system structure-behavior models. These models work best on discrete systems whose predicted state is based on commanding information that moves the system from steady state to steady state. Recent work is extending the scope to continuous dynamic systems.[10]

The Livingstone system (as Livingstone, L2 and HyDE) has had the most space experience. In the autonomous "Remote Agent" in the Deep Space I (DS-1) mission, Livingstone was validated along with a set of other new technologies, to reduce the cost and risk to subsequent programs. [11] The Remote Agent included the Livingstone model-based executive. The executive issued commands and used the mode identification and reconfiguration engine to assess spacecraft state and identify operations to recover from faults without ground intervention. Livingstone correctly diagnosed four simulated faults that were injected during the validation phase.

The next version, Livingstone 2 (L2) of the model-based diagnostic software,[12] was tested by simulation in the Propulsion IVHM Technology Experiment (PITEX) [13] and in the Earth Observing 1 (E0-1) mission.[13] L2 diagnostic capabilities were improved. These improvements included monitoring and diagnosis during transitions between finite states, reasoning about inconsistent diagnoses, and ranking possible diagnoses by posterior probabilities.[13] Remaining capability limitations included cumbersome models of continuous behavior, and inability to model controllers. Capability to track system state was limited by difficulties discovering initial systems state, tracking timed transitions, and tracking fault recovery from hard or intermittent faults.

PITEX demonstrated health assessment of a rocket propulsion system through the use of flight-like data in simulation environment that took into account noise, sensor resolution and hardware uncertainties, realistic nominal and failure modes.[14] During the EO-1 mission, L2 was tested in 17 diagnostic scenarios, and 16 of them were successful. Cumulative operations in space increased from 20 hours on DS-1 to 143 days on EO-1, including an extended run of 55 days without a false positive.[13]

Integration of L2 in these experiments required changes that contributed to technology readiness: 1) porting to the VxWorks operating system; 2) binary representations of the models to avoid using an XML parser in flight; 3) conversion to C++ and no longer using dynamic memory allocations and recursion, 4) new interfaces for communicating with the vehicle management system, and 5) accommodation to constrained telemetry bandwidth and capacity of the CPU and memory.[15] These constraints affected L2's ability to perform hard real-time diagnosis and provide timely guidance on failures and appropriate recovery. Reuse of L2 would have been simplified if Livingstone developers had developed a version of the engine that met typical flight system safety requirements and was able to operate on a typical avionics platform within typical resource limitations.

L2 on EO-1 successfully demonstrated separation of the diagnostic engine from the data and models.[13] L2 demonstrates how ISHM model-based technologies separate data and models from the application engine. This simplifies test, verification and validation. The engine can be independently verified. Test procedures are only needed to verify the changes to the data set or model and integration with the already verified engine. Separating the application from the data also simplifies reuse and lowers development cost. An application framework that manipulates changeable objects encourages development of reusable code for multiple missions. [16]

2. *Adjustable Autonomy and Collaborative Systems*

Adjustable autonomy capabilities allow the level of automation to be adjusted based on mission requirements or crew desires. Adjustable autonomy requires not only control mechanisms, but also modularity and restart features. Levels can be adjusted from fully automated operations when human intervention is unwanted or impossible, to fully manual operations, where operators vigilantly monitor and control at a low level. Generally crew prefer to perform health management themselves, to better maintain their situational awareness of spacecraft state and configuration. However, over time crew may tire of the routine work and adjust ISHM automation so that they can spend more time in exploration and scientific studies. ISHM assessment can make it easy for human operators to determine the operational state of the system, including the level of automation, and then adjust the level of automation or operational state with minimal effort.

Collaborative autonomy allows automated systems to function more like members of a team. Collaborative systems are designed with mixed-initiative capabilities that facilitate give-and-take collaboration and use of volunteered information. Two-way communication is used to support incremental understanding and problem solving. In a well designed system, the human-computer interaction time is minimized while the time between human-computer interactions is maximized.[17]

B. Technical Enablers – Sensors and Architecture

1. Sensors and Sampling

Better instrumentation can provide humans and software greater insight into system, subsystem and component health and can provide redundant sensors for error correction. Sensor technology advances are producing smaller, lighter self-calibrating and self-testing sensors that consume minimal amounts of power. More fully instrumented experimental spacecraft enable engineers to validate models and identify modifications that are needed to increase reliability. Capacities for transmitting and storing vehicle data are also important enablers of ISHM. Adequate sampling rates and bandwidth are needed.

The right number sensors at the right locations can simplify diagnosis and reduce ISHM code complexity. The optimal design goal would be the minimum number of sensors placed in the appropriate locations such that every identified critical failure mode or combination would have a unique failure signature. This capability will be needed on interplanetary missions where communication delays and blackouts hamper the ability of the ground to render timely aid in troubleshooting problems.

2. Information Architecture for Update and Evolution

There are several reasons to expect adaptation, update or evolution of ISHM software in exploration missions. They include: 1) discovery of novel system health problems; 2) migration of ISHM functions from ground to onboard during a long duration mission or between missions, 3) adjustments to the automation level during a mission or operation, and 4) technology advances during a multi-mission campaign. As exploration missions become more remote, ISHM capabilities on earth will need to migrate from ground-based systems into onboard systems. Likewise, as ISHM technologies mature and missions become more remote, systems management capabilities will need to be upgraded.

The architecture and systems in the Space Shuttle have proven inflexible, making development and integration of ISHM technologies into the vehicle prohibitively expensive. Information and data architectures in future spacecraft must support the adaptation and update of ISHM models and data as well as upgrade to use more advanced mature technologies. The architecture must also accommodate adjustable levels of automation during or between missions.

C. Engineering Enablers

1. ISHM System Engineering

Models and sensors are critical to the success of ISHM technology. Processes and methods are needed to allow designers of subsystems and components to work jointly with ISHM software designers to determine the quantity, type and location of sensors, with a focus on detectability and unambiguous diagnosability. One of the primary enablers of ISHM is knowledge of design, interactions and performance (design data and models). ISHM engineering includes acquiring and accessing that knowledge. Processes and technologies are needed for capturing, organizing and mining knowledge used for ISHM system models.

2. Assessment Tools

Allocating ISHM functions between software and humans is a task that must be performed in order to maximize the investment in ISHM technologies. Johnson Space Center (JSC) engineers have developed the Function-specific Level of Autonomy and Automation Tool (FLOAAT).[18,19] The tool uses a questionnaire to get agreement on a level of autonomy and automation for each functional capability and produces an analytical summary of the results. The FLOAAT tool was used to generate autonomy and automation-related Exploration Level 2 architecture independent requirements for the Rendezvous, Proximity Operation and Docking (RPOD) system for Orion. This Delphi-like rating technique may be useful for ISHM automation allocations. Currently the tool is designed for fixed allocations and should take account of adjustable autonomy and changing allocations.

3. Test Capabilities

One difficulty that ISHM technology developers face is the lack of testing environments that are relevant to the maturity level of the technology. For low maturity technologies, a test environment that operates on a low-cost desktop computer may be sufficient. More realistic test environments with increasing fidelity, such as the PITEX simulation, are needed to ready technologies for operations. For operational testing, environments such as terrestrial analog sites or even space-based assets can provide low cost alternatives to expensive dedicated test missions. The lack appropriate and accessible test facilities increases the risk that the technology will not be ready because the test and demonstration environment is inadequate.

IV. Maturity Challenges and Recommendations

ISHM technologists are likely to be aware of research and development that is needed to increase capability of ISHM software and supporting sensors and data architecture. However, most technology development to advance technology readiness is in the areas of engineering and integration. Technologists are less likely to be aware of these needs. Advancement Degree of Difficulty (AD^2), details types of engineering requirements needed to make technology ready, beyond Technology Readiness Level demonstrations. [5] AD^2 dimensions include 1) Design and Analysis; 2) Manufacturing/Implementation; 3) Operations; and 4) Test and Evaluation. Finally, compatible program infrastructure is needed.

A. ISHM Capabilities, Sensors and Data

Much ISHM technology development has focused on model-based detection and diagnosis. Additional work is needed to integrate multiple technical approaches and diverse information sources. An integrated approach will enable diagnosis of more complex failure scenarios, and increase model expressiveness and engine capability. More strategies and capabilities are needed for interacting with embedded systems for control, fault detection, identification and reconfiguration (FDIR) and caution and warning. ISHM technology complexity is perceived as a major risk. Separation of ISHM engines from models and data reduces complexity and increases reusability, understandability and ease of software maintenance. Work is needed to characterize complexity and further reduce it as needed. Technology development is also needed in some neglected high-value areas: impact assessment, situation assessment and evaluation of “what if” scenarios, including worst case next failure analysis.

Advancements are needed in sensors, data storage and communication to support increased sampling rates and bandwidth. Software systems face the same limitations as humans when needed information is not available. Sufficient high quality data is needed for any ISHM system, automated or manual, to operate effectively.

B. ISHM Engineering Advancement

Much of the technology maturation activity for advanced software should focus on engineering and integration methods and tools. The interviews yielded numerous requirements for mature-enough ISHM technology. There was a common theme: the need for an intermediate development phase, to reduce risk. During this phase, the technology previously demonstrated at the TRL 6 or 7 levels would be redeveloped as critical flight software, using the engineering processes and procedures for developing, implementing, testing and certifying flight critical software.

1. *Process and Operations*

ISHM technology must enhance safety and be more reliable than the systems being managed. Work on design and evaluation of dependable ISHM software systems should be accelerated.

Technology demonstrations should include rigorous development plans and demonstrate supportable and upgradeable technology with low operational costs. Operations personnel have historically been skeptical of ISHM technology demonstrations. Capable technologies look bad when a technologist cannot demonstrate use of the processes necessary to keep an application functioning during operations. Capable technologies can also look bad when dated information is used to construct the models and application, even if this was the best information available for the demonstration. Technology demonstrations gain credibility by using current data and an operations change process to upgrade the data, models and application. By using a change process, technologists can also assess cost and schedule impacts of changes that impact ISHM applications.

2. *Model Capture and Updating*

The cost of capturing models is a general problem in space programs. Processes and methods are needed to facilitate the reuse of models throughout the life cycle, and to reduce the risks of developing duplicate models for multiple organizations. ISHM development will benefit from the same improvements in model capture and reuse. Technologists should also demonstrate upgradeable ISHM system models and methods for updating and verifying as configurations change.

3. *Testing*

Test beds and test facilities are needed for ISHM technologies, to provide flight-like architectures and data that enable testing in environments that closely mimic the expected operational environment. A scalable test system is needed to provide spacecraft telemetry for test and verification. Advanced model-based and rule-based ISHM software should be tested in “nondestructive” virtual environments that challenge the software with processor failures, environment failures, complex failure cascades and erroneous or uncertain data. The use of terrestrial analog sites as test beds will help validate ISHM systems during long duration tests.

C. Program Organization and Infrastructure

1. *Compatible Mission and Spacecraft Infrastructure*

For ISHM technology to be incorporated successfully into future spacecraft, these designs must accommodate integration and evolution of software and hardware. Systems, infrastructure and processes must be designed so that models and data used by software can be routinely updated as novel anomalous conditions are analyzed and understood.

2. *Cross-Organization Human Support*

ISHM systems can aid and automate complex assessment functions that are currently being performed by distributed mission personnel in space and on Earth. Programs need to address the organizational complexities that have made cross-organization system health management difficult. These difficulties have also contributed to the cost and difficulty of ISHM technology maturation. Further work is needed on methods and technologies for maximizing the combined performance of the software and human systems that cross organizational boundaries. These include adjustable automation capabilities, collaborative capabilities, data fusion and presentation of situational awareness information.

VI. Conclusion

For any technology, there is a significant amount of engineering development required beyond achieving mature core capabilities. Sponsors of technology development programs should emphasize risk reduction projects, using a checklist like AD^2. AD^2 measures technology risks in design, analysis, implementation, test and operations. These are the risks that will be assessed by space programs as they make technology development decisions. Technology development programs should perform early AD^2 assessments. This will help the programs identify appropriate scope and funding for development of engineering methods and tools that will decrease both Advancement Degree of Difficulty and technology risk. In relatively young fields like software technology, it can take significant sustained effort to reduce technology risk in these engineering areas. In these fields, a sustained effort in risk identification and reduction should be institutionalized and emphasized in pre-Phase-A technology development. This paper serves to summarize progress in ISHM technology development, and identifies some engineering development areas where work is needed. Resources spent in these areas will make it easier to prepare for TRL 6-7 demonstrations and make it easier for programs to find technology that is really ready. The likelihood of use of new technology in space missions will increase. Programs, systems engineers and technologists will benefit.

Acknowledgments

This paper is based on work performed for the Integrated System Health Management Project, funded by the NASA Exploration Technology Development Program.

References

[1]Aaseng, G. B. "Blueprint for an Integrated Vehicle Health Management System," *Proceedings of the 20th Digital Avionics Systems Conference*, Vol. 1, 2001, pp. 3C1/1-3C1/11.

[2]Zuniga, F., Maclise, D., Romano D., Jize, N., Wysocki P., and Lawrence, D. "Integrated Systems Health Management for Exploration Systems," *1st Space Exploration Conference: Continuing the Voyage of Discovery*, AIAA-2005-2586, Washington, DC, 2005.

[3]Mankins, J. C. "Technology Readiness Levels," A White Paper, NASA, Office of Space Access and Technology, Advanced Concepts Office, 1995.

[4]Nolte, W. L., Kennedy, B. C. and Dziegiel, Jr., R. J. "Technology Readiness Level Calculator." *NDIA 6th Annual System Engineering Conference*, 2003.

[5]Bilbro, J. W., "Systematic Assessment of the Program/Project Impacts of Technological Advancement and Insertion", A White Paper, NASA Marshall Spaceflight Center, 2006.

[6]Oliver, P., and Malin, J. "Making Ready: Integrated Systems Health Management for Exploration Operations." NASA Johnson Space Center, 2006.

[7]Hadden, G. D., Bergstrom, P., Samad, T., Bennett, B.H., Vachtsevanos G.J., and Van Dyke, J. "Application Challenges: System Health Management for Complex Systems," *5th International Workshop on Embedded/Distributed HPC Systems and Applications (EHPC 2000)*, 2000.

[8]Wade, R. A. "A Need-focused Approach to Air Force Engine Health Management Research," *Proceedings of the 2005 IEEE Aerospace Conference* [CD-ROM], IEEE, Manhattan Beach, CA, 2005.

[9]Patterson-Hine, A., Aaseng, G., Biswas, G., Narasimhan, S., and Pattipati, K. "A Review of Diagnostic Techniques for ISHM Applications," *1st International Forum on Integrated System Health Engineering and Management in Aerospace (ISHEM 2005*), NASA, 2005.

[10]Mosterman, P. J., and Biswas, G. “Diagnosis of Continuous Valued Systems in Transient Operating Regions,” *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, Vol. 29, No. 6, Nov. 1999.

[11]Rayman, M. D., Varghese, P., Lehman, D. H., and Livesay, L. L. “Results from the Deep Space 1 Technology Validation Mission,”50th *International Astronautical Congress*, Amsterdam, The Netherlands, 1999.

[12]“Virtual Propulsion System Meets Real-Time Diagnostic System,” *Aerospace Technology Innovation* [online journal], Vol. 10, No. 5, Sept./Oct. 2002. URL: http://www.nctn.hq.nasa.gov/innovation/innovation105/index.html

[13]Hayden, S. C., Sweet, A. J., Christa, S. E., Tran, D., and Shulman, S. “Advanced Diagnostic System of Earth Observing One.” *Space 2004 Conference and Exhibit*, AIAA-2004-6108, 2004.

[14]Maul, W., Chicatelli, A., Fulton, C., Balaban, E., Sweet, A., and Hayden, S. “Addressing the Real-World Challenges in the Development of Propulsion IVHM Technology Experiment (PITEX),” *AIAA 1st Intelligent Systems Technical Conference*, AIAA-2004-6361, 2004.

[15]Schwabacher, M., Samuels, J., and Brownston, L. “The NASA Integrated Vehicle Health Management Technology Experiment for X-37”, *Proceedings of the SPIE AeroSense 2002 Symposium*, 2002.

[16]Garlan, D., Reinholtz, W. K., Schmerl, B., Sherman, N. D., and Tseng, T. “Bridging the Gap between Systems Design and Space Systems Software.” *29th Annual IEEE/NASA Software Engineering Workshop (SEW-29)*, 2005, pp. 34-46.

[17]Bradshaw, J. M., Acquisti, A., Allen, J., Breedy, M., Bunch, L., Chambers, N., Galescu, L., Goodrich, Jeffers, M. R., Johnson, M., Jung, H., Kulkarni, S., Lott, J., Olsen, D., Sierhuis, M., Suri, N., Taysom, W., Tonti, G., Uszok, A., and van Hoof, R. “Teamwork-Centered Autonomy for Extended Human-Agent Interaction in Space Applications,” *Proceedings of the AAAI Spring Symposium, Interactions between Humans and Autonomous Systems over Extended Operation*, AAAI Press, 2004, pp. 136-140.

[18]Proud, R. W., and Hart., J. J. “FLOAAT, A Tool for Determining Levels of Autonomy and Automation, Applied to Human-Rated Space Systems,” *AIAA Infotech@Aerospace 2005 Conference and Exhibit*, AIAA-2005-7061, 2005.

[19]Proud, R. W., Hart., J. J., and Mrozinski, R. B. “Methods for Determining the Level of Autonomy to Design into a Human Spaceflight Vehicle: A Function Specific Approach,” *Proceedings of the 2003 Performance Metrics for Intelligent Systems (PerMIS) Workshop*, 2003.