ABSTRACT

Integrated Systems Health Management (ISHM) is a system engineering discipline that addresses the design, development, operation, and lifecycle management of components, subsystems, vehicles, and other operational systems with the purpose of maintaining nominal system behavior and function and assuring mission safety and effectiveness under off-nominal conditions.

NASA missions are often conducted in extreme, unfamiliar environments of space, using unique experimental spacecraft. In these environments, off-nominal conditions can develop with the potential to rapidly escalate into mission- or life-threatening situations. Further, the high visibility of NASA missions means they are always characterized by extraordinary attention to safety. ISHM is a critical element of risk mitigation, mission safety, and mission assurance for exploration. ISHM enables:

- Autonomous (and automated) launch abort and crew escape capability;
- Efficient testing and checkout of ground and flight systems;
- Monitoring and trending of ground and flight system operations and performance;
- Enhanced situational awareness and control for ground personnel and crew;
- Vehicle autonomy (self-sufficiency) in responding to off-nominal conditions during long-duration and distant exploration missions;
- In-space maintenance and repair;
- Efficient ground processing of reusable systems.

ISHM concepts and technologies may be applied to any complex engineered system such as transportation systems, orbital or planetary habitats, observatories, command and control systems, life support systems, safety-critical software, and even the health of flight crews. As an overarching design and operational principle implemented at the system-of-systems level, ISHM holds substantial promise in terms of affordability, safety, reliability, and effectiveness of space exploration missions.

EXPLORATION MISSION CHALLENGES

Cost, crew safety, and productivity are major challenges for exploration-class missions. A cursory review of NASA's manned space program and the recent Design Reference Missions (DRMs) developed by NASA illustrates inherent conflicts between these challenges:

Cost vs. safety: Throughout aerospace history, hardware redundancy has been considered a prudent risk mitigation and safety strategy. Another "traditionally

Serdar Uckun, M.D., Ph.D.
M/S 269-1
NASA Ames Research Center
Moffett Field, CA 94035

prudent" safety strategy is frequent inspection, overhaul, and replacement of mission-critical, life-limited components. Unfortunately, hardware redundancy and maintenance are significant contributors to escalation of total costs of ownership (TCO) for aerospace systems. Furthermore, the scope of exploration missions includes missions (e.g., long duration missions to Mars) where frequent, extensive maintenance operations or overhauls will not be an option.

Safety vs. productivity: Several recent NASA DRMs (e.g., Architecture Study #1, OASIS, and the Mars Reference Mission) propose crew escape systems as a final risk mitigation strategy when redundancy is exhausted as an option. While it serves to preserve the critical human element of the mission, crew escape is of limited utility beyond Earth orbit and it equates to a mission failure. There needs to be other alternatives to safety and reliability that do not compromise mission productivity.

Cost vs. productivity: These two goals often conflict at the design stage. The prototypical example of this conflict is the choice between a proven but relatively inefficient technology (e.g., chemical propulsion for in-space transportation) versus the prospect of a costly design, testing, and certification of a new, more effective technology (e.g., nuclear electric propulsion).

The Joint Strike Fighter (JSF) program has taken a revolutionary step to ease the conflict between cost and safety: JSF is a rare single-engine fighter jet allowed to operate on aircraft carriers. (The U.S. Navy traditionally prefers dual-engine aircraft for added safety margin on flights over water.) Furthermore, the JSF program has an ambitious goal of eliminating scheduled engine inspections entirely. The key to this bold move is Prognostic Health Management, an ISHM element focusing on scientific assessments of mission success probability based on health knowledge of mission-critical life-limited components[2].

The key to resolving the inherent conflicts between safety and productivity is yet another ISHM element referred to as fault accommodation and recovery. One of the crosscutting design principles for JSF is fault accommodation, which means that the aircraft will be designed with sufficient margins and hardware or functional redundancy to "limp back to base" following an in-flight failure or battle damage. Another principle is fault recovery, where an aircraft or spacecraft reconfigures its flight controls (autonomously or through crew intervention) in order to mitigate the impact of an in-flight failure and continue the mission. A successful example of autonomous fault recovery is the Adaptive Flight Controls research conducted by Ames Research Center (ARC) and Dryden Flight Research Center (DFRC) on a NASA C-17, allowing the aircraft to continue flying and maneuvering even after a substantial portion of flight control surfaces are lost or damaged[3]. Finally, fault

---

[2] Andrew Hess, Giulio Calvello, Thomas Dabney, "PHM a Key Enabler for the JSF Autonomic Logistics Support Concept," 2004 IEEE Aerospace Conference, Big Sky, MT.

[3] Karen Gundy-Burlet et al, "Control Reallocation Strategies for Damage Adaptation in Transport Class Aircraft." 2003 AIAA Guidance Navigation and Control Conference.

protection is a method to halt the operation of a system until the problem can be studied and remedied.

ISHM methods do not address design trade studies directly and as such cannot help resolve conflicts between affordability and effectiveness. However, implementation of a comprehensive ISHM strategy makes revolutionary technologies (e.g., novel propulsion systems) feasible for NASA's exploration missions by increasing reliability and safety. The key is to understand the physics of failure in these novel systems and to design spacecraft so that all such mission-critical faults may be sensed well before they lead to system failures, diagnosed accurately, repaired in time, or accommodated without mission impact. All the base technologies required for this scenario are available or in development today at NASA or elsewhere.

Cost control is a critical requirement for mission operations. Today, NASA missions are typically managed from the ground and mission success depends on literally thousands of ground support staff including mission controllers, trainers, procedure writers, technicians, and maintenance personnel. Keys to reducing ground staffing costs include more efficient maintenance processes, increased automation in mission operations, and more supportable spacecraft designs; these are some of the benefits of a comprehensive ISHM strategy.

SPECIFIC MISSION CHALLENGES AND SOLUTIONS

In addition to the overarching strategic mission challenges, there are a number of specific challenges within the envisioned scope of NASA's robotic and crewed exploration missions. We address a number of such challenges below and discuss how ISHM might play a role in addressing these challenges.

Phased Development: Since many of the requirements 20-30 years down the road cannot be envisioned with certainty. However, redesigning each new generation from scratch is not an option. The affordability of successive generations of the planned Crew Exploration Vehicle (CEV) will largely depend on our ability to identify modular design elements that contribute to mission success and eliminate elements that increase risk and decrease overall reliability. An ISHM infrastructure will be critical in collecting operational data on all critical design elements and making design persistence determinations early on. Such data collection needs apply to reusable as well as expandable elements.

Knowledge Management and Retention of "Institutional Memory:" For the Apollo or the Space Shuttle programs, the same prime contractor workforce was retained throughout the program (despite the sale of Rockwell's aerospace businesses to Boeing and the subsequent formation of United Space Alliance). NASA's new exploration vision is envisioned to continue for several decades, and it is quite probable that the development contracts for successive stages will be awarded to a variety of prime contractors. Thus, it is essential that NASA take the initiative in retaining the "institutional memory" required for sustained development, including

design trade studies, assumptions, operational information, and lessons learned. This is not an ISHM-specific issue; however, the capture and retention of ISHM-related operational information will be essential for the evolution of ISHM elements as the development programs mature.

Adequate Sensing Infrastructure: In current spacecraft designs, sensor selection and installation is typically guided by the needs of control avionics. Due to cost, reliability, and complexity constraints, systems are often designed with the minimal complement of sensors necessary to accomplish control and fault detection, isolation, and recovery (FDIR) requirements. Such sensor selection processes often result in inadequate sensing for health management purposes, limiting health management to only those sensors that were already designed into the system for control purposes. As a result, it is often impossible to detect and isolate signals (e.g., vibration data from individual components) that relate to in-flight component failure. Furthermore, there is often very little sensor information on spacecraft structural components and thermal protection systems (lack of sensor coverage on the Space Shuttle thermal protection system was extensively discussed subsequent to the Columbia accident).

Data Glut: Even with relatively modest telemetry streams, the Space Shuttle and International Space Station programs overwhelm mission controllers with telemetry data. The same goes for robotic spacecraft – for example, it is expected that the data collected by the Deep Impact spacecraft during its brief encounter with an asteroid will take years to analyze. Our existing data monitoring and analysis methods are not scalable to next-generation vehicles that will have substantially larger sensor suites. Thus, we need to develop effective methods for onboard data compression, data interpretation, and summarization. Furthermore, we need to automate methods to derive useful operational knowledge from data (such as the safe operating margins or fault progression characteristics of a certain component). The data mining and intelligent data understanding methods critical to the success of future missions are significant elements of a comprehensive ISHM strategy.

Logistics and Maintenance for Long-Duration Crewed Missions: Although NASA develops exceptionally reliable space systems, all materials, structures, and electronics eventually do fail. This is often the result of a slow fault progression over a long period. Material imperfections and weaknesses (e.g., cracks, fatigue, etc.) may begin early in the operational life of a component, often at microscopic levels. As operational loads (e.g., thermal, vibration, acceleration, etc.) continue to stress the material, incipient faults appear. Eventually, damage patterns develop with overt manifestations that can be identified with signal detection and fault isolation technology. ISHM provides the prognostic framework by which incipient faults can be detected before they progress to the point of failure, triggering condition-based maintenance actions or fault accommodation/recovery mechanisms. Design of transportation systems for maintainability by crews during flight (or during surface operations) should be an overarching design and engineering principle for future exploration missions.

Software Health: Traditionally, health management efforts often focus on propulsion systems or other mechanical vehicle subsystems. An increasing trend in engineering systems is software complexity accompanied by software faults. In recent years, two missions to Mars (Mars Polar Lander and Mars Climate Orbiter) ended in failures caused by software design flaws, and the MER Spirit Rover was almost disabled by another software flaw which, fortunately, was diagnosed and repaired by humans hundreds of millions of miles away. The trend is disturbing: Average software flaw densities remain approximately constant (0.5 flaws per thousand lines of commercial software code, according to Reasoning, Inc.) while the number of lines of code in each new generation of spacecraft increases drastically. The only way to reverse the onslaught of software flaws is through emerging software health management technologies such as verification and validation, model checking, static analysis, and automated software generation.

Software Certification: Avionics software for human-rated space flight goes through an extensive certification process that requires verification and validation of every execution path in the software, including every possible command input and possible range of state variables. This is an expensive and complex task for even the simplest avionics software code. True ISHM requires large-scale models of the spacecraft and the environment it interacts with. Furthermore, these models are executed on "inference engines" that can cover a vast number of possible states and state transitions. Cost-effective verification and validation of large models and complex inference engines is an open issue. Thus, deployment of complex ISHM software is likely to run into cost and complexity barriers with respect to certification.

IMPLEMENTATION APPROACH

Although several health management elements have been deployed in flight demonstrations and actual missions, system-wide integration of health management technologies is a brand new frontier for NASA. Until the value of the ISHM practice is firmly established, investments need to be made selectively and the return on investment (ROI) assessed rigorously. This is where system engineering plays a critical role. Health management hardware (processors, sensors, wiring, etc.) and software must be incorporated selectively and optimally into a new platform to provide maximum benefits at a minimum cost.

NASA's past efforts in spacecraft autonomy as well as vehicle health management have shown that optimal system designs result when structured design techniques are utilized starting with the conceptual design phase and throughout the development and testing phases. Thus, certain investments must be made upfront to lay the groundwork for advanced exploration missions. Such upfront ISHM investments include standards-based implementation, design for diagnosability and testability, and a robust sensor infrastructure (even if all the downstream data processing and information management architecture is not implemented at once).

The initial CEV design should include mature ISHM methods and technologies to contain the technology risk and to demonstrate ROI on "low-hanging fruit." Candidate methods and technologies for early deployment include propulsion monitoring, caution and warning systems with root cause identification capability, rapid-acting propulsion safing and crew escape technologies, and onboard data analysis and reduction methods. The initial design should also lay the groundwork for a comprehensive prognostics infrastructure on flight-critical hardware. Operational data should be collected via the prognostics infrastructure during all test firings, test flights, and actual missions. During the life span of the initial CEV, physics-based and data-driven prognostic models should be developed for major flight-critical life-limited components, and model predictions should be compared to inspection findings. Finally, the knowledge management and retention infrastructure should be established upfront.

The CEV for lunar exploration should incorporate lessons learned from the CEV designed for earlier orbital missions (mainly in the areas of prognostics). Candidate technologies and practices include advanced diagnostics for a larger set of subsystems and more sophisticated human-system interfaces such as sophisticated fault identification and management interfaces. We can also expect moderate improvements in maintenance practices based on limited prognostics and more advanced automated recovery capabilities for spacecraft. Robotic craft introduced for lunar exploration should have more sophisticated autonomous navigation capabilities and exhibit limited goal-directed behavior. Finally, a human outpost on the moon will require significant investments in structural health for the habitat and other crew shelters.

Looking forward toward Mars exploration, we can anticipate a fully-integrated systems health management architecture. This architecture would cover all subsystems of the craft and integrate information from these systems into an autonomous mission management capability. Exchange of control authority between crew and systems would be seamless and accomplished as mission demands dictate, and mission command duties would be largely limited to oversight of systems (not unlike the duties of commercial air transport crews today). "Fault protection" would yield to "fault anticipation" as accurate prognostic models become available for all mission-critical life-limited components. Significant savings in maintenance will be coupled with increased availability of system-of-systems elements. Robotic craft will be goal-directed and able to conduct autonomous science missions with limited human oversight. Self-sustaining robotic "ecologies" will become a reality in later spirals.

CONCLUSION

Literally all systems in a system-of-systems framework are potentially impacted by ISHM investments:

- For example, ISHM will impact the affordability of an entire system-of-systems by reducing the need for hardware redundancy (and thus reducing

system acquisition as well as launch costs) and by allowing maintenance policies to be driven by scientific observations rather than "fear of failure."

- A broad ISHM implementation will impact the overall reliability and safety of an entire space transportation and exploration system by ensuring the health and continued effectiveness of all its constituent systems.
- Finally, investments in ISHM will increase the productivity of the entire system-of-systems by increasing mission availability across the board.

As with many other non-traditional concepts, ISHM will have to buy its way into exploration missions with demonstrated success and return on investment. Staged development and implementation of ISHM over the CEV lifecycle is a safe, effective, and affordable way to implement a crosscutting ISHM strategy for exploration.