Sustainable, Reliable Mission-Systems Architecture

Graham O'Neil,[*] James K. Orr, [†] and Steve Watson[‡]
United Space Alliance, Houston, TX, 77058

A mission-systems architecture, based on a highly modular infrastructure utilizing open-standards hardware and software interfaces as the enabling technology is essential for affordable and sustainable space exploration programs. This mission-systems architecture requires (a) robust communication between heterogeneous systems, (b) high reliability, (c) minimal mission-to-mission reconfiguration, (d) affordable development, system integration, and verification of systems, and (e) minimal sustaining engineering. This paper proposes such an architecture. Lessons learned from the Space Shuttle program and Earthbound complex engineered systems are applied to define the model. Technology projections reaching out 5 years are made to refine model details.

I. Introduction

The mission systems architecture to support ambitious space exploration activities will be challenged at the physical level by large scale distances and hostile environements, at the local level by allocation constraints, and at the support level by organizational, social and cultural divides. Each of these except for the long distances and hostile environement will change on a periodic basis several times over the decades of space exploration envisoned by the NASA Roadmap [1]

The paper will present four operationally significant criteria that will be used in defining the systems and in allocating functions for local or remote performance. Three major components to be examined for their contribution to deploying a successful mission systems architecture are:

- A hardware layer based on a node-based network with tunable redundancy, automated fail-over based on intelligent agents, and plug and play interaction that includes automatic reconfiguration based on detection and recognition of new components.
- A software architecture applicable from the lowest level subsystem to the integrated mission system based on open-standards middleware, eg IEEE 1516.
- A transparent switching framework of flight hardware, flight equivalent hardware, emulation of flight hardware, and network-connected computers containing high-fidelity software models as well as stubs and harnesses necessary for system testing.

II. The Four Keys to Success of Mission System Architecture

"A central concept of the new U.S. National Vision for Space Exploration is that space exploration activities must be 'Sustainable'" (NASA's 2004 H&RT Formulation Plan). Sustainability encompasses the following four key areas that are critical to successful deployment and operations of the conceptual mission systems architecture. Each of these criteria has built-in trades that if carried out consistently and systematically will lead to an implementation that supports human space exploration for decades to come.

- Affordable: Life cycle costs at each stage must be consistent with NASA budgets. Unplanned spikes must be minimized. Future costs resulting from decisions made today should be well grounded with relevant validation and historical basis. The primary trade is when will a system or capability be available and in what quantity.

[*] Computer Scientist, Shuttle Flight Software, 600 Gemini M/C USH-632L, AIAA Senior Member.
[†] Chief Engineer, Shuttle Flight Software, 600 Gemini M/C USH-631A, Member
[‡] Computer Scientist, Shuttle Flight Software, 600 Gemini M/C USH-635L

- Reliable and safe: Future space exploration systems, infrastructures and missions must be safe and reliable. Safety will be defined as "As Safe As Reasonably Achievable" (ASARA); analogous to the nuclear industries "As Low As Reasonably Achievable" (ALARA) when deciding on alternatives involving human exposure to radiation.

- Effective: The capabilities of a new system or infrastructure must be worth the costs of developing, building, and owning them. The goals and objectives achieved by missions using those systems and infrastructure components must be worth the costs and risks of owning them.

- Flexible: The families of new systems, infrastructures, and technologies should be capable of adapating to changing policy objectives, requirements, interfaces, and operational scenarios. The systems and infrastructures whould be capable of extension to support new missions. The principal focus of trades in this area is how much flexibility is desired in each component of the MSA.

The three MSA Components treated in this paper support the four operations criteria as explained below:

Affordability

- Transparent switching significantly reduces costs by supporting new systems concept validations earlier without real hardware, by reducing hardware requirements for training scenarios, and by reducing systems ~~integration efforts.~~
- ~~Reliable automatic reconfiguration required in long distance missions, virtually eliminates expensive~~ ground-based reconfiguration applications and reduces human-in-the-loop interaction requirements for shorter range missions.
- Incremental building block approach simplifies integration of new systems into existing flight systems.

Reliability/Safety

- Redundancy tuned to the level required, whether N+1, N+M or full duplication where necessary, to give quantifiable probability of mission success.

Effectiveness

- Building upon recognized industry/space standards significantly reduces costs and the risk of development while offering a highly effective combination of real-time performance, scalability, and fault-tolerance.

Flexibility

- Open-standards interfaces allow for technology evolution.
- Plug and Play supports the building block approach.
- Automated reconfiguration driven by intelligent agents provides fast responses with minimal human demand.

III. Where Are The Challenges?

Technical challenges are expected in providing the scalability required for increasingly more ambitious space missions. Advancing technology can be counted on up to a point. Robust margins are helpful, but must be paid for in advance with no guarantee thay will be used.

Automatic reconfiguration and the plug and play implementation require strict adherence to standards. Making the standard interface infrastructure robust enough to minimize the need for unique interfaces is a technical challenge to be addressed. But much of the risk has been reduced by DOD and industry initiatives in High Level Architecures (HLA) . Re-use of these HLAs eliminates major overhead of developing such an infrastructure from scratch. So work can be focused on interfacing with common HLA interfaces rather than painful iterative refinement of another standard exclusive to the space community.

Reconfiguration work must begin early so that major cost drivers such as number of modes and states, interfaces, and size of the data and information base will be accurate. Addition of a mojor mode late in the development cycle will have adverse effects on cost and scheduel while increasing program risk. Early definition of these features provides a solid foundation for mission system planners and analysts to begin scenario development and analysis.

This early start can be leveraged to gain much experience in safety related issues while there is still time to accommodate changes.

Each generation of aerospace modeling and simulation faces new challenges since data becomes more refined, CPUs run faster, and smaller details become important in second order interactions. Other difficulties cease to be a problem. No one develops Six Degree of Freedom simulations in Assembly language to fit CPU provisions anymore. But no one has a solid answer to automated reconfiguration requirements for life critical functions on very long term space missions.

Based on recent experience, modeling and simulation approaches should utilize:

A. Tight coupling between the operational software, and that used for test, and training.
B. Tight coupling of the simulators with the operational software.

Based on need projections for long duration space missions, new start modeling and simulation approaches should include:

A. Use of mirrored networks for operational and simulations.
B. On-board versions of the simulations for checkout, training, test, and procedures development.

IV. Future Vision

Modeling and simulation will play an important role in the development of new space systems. The development and use of the models and simulations will have significant impact on cost and schedule, so it is important to provide the best framework and tools. Models will be used for early prototype validation, for flight and support software development, for hardware checkout, and for crew and ground support training. A continuing challenge is the accurate emulation of hardware by the models. To minimize cost, the models should be developed once and reused, as required, throughout the various mission phases: planning, preparation, flight, and post-mission analysis.

One way to reduce simulation costs is to factor the need for models into the hardware architecture for the envisioned space vehicle. Considering the operational aspects during hardware design will avoid the need for the parallel modeling systems and additional overhead prevalent in today's operations using custom models or simulations at each facility or lab. An architecture that supports generic hardware executing models and using the same interfaces as the real hardware allows the models to be used earlier and more effectively in the development and operational support of the next generation space vehicles. For example, a model of a proposed hardware upgrade can be developed and used within the existing vehicle architecture to better determine the impacts to the overall system before the actual hardware specifications are released.

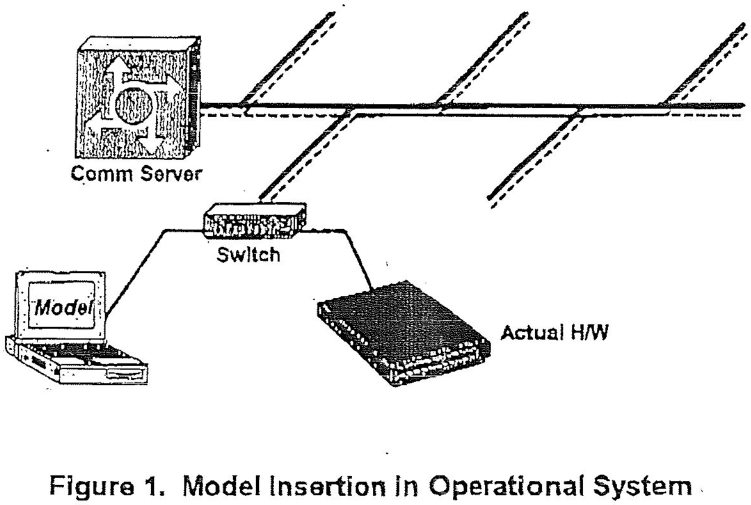

Figure 1. Model Insertion in Operational System

The entire space vehicle's systems would be set up as a high-speed interconnected system of networks. Each system (engines, environmental, maneuvering, landing gear, displays, flight control computer, mass memory, telemetry, etc) would have its own logical computer resources. The redundant network would provide communications, centralized timing, and power capability for each system. All flight hardware would be designed