

Track Preference: Robotic Technology and Space Architecture

Presentation Title: Orion FSW V&V and Kedalion Engineering Lab Insight

Synopsis:

This presentation will outline unique aspects of the Orion FSW V&V program that is evolving, along with NASA's CxP engineering insight laboratory: Kedalion.

Abstract:

NASA, along with its prime Orion contractor and its subcontractor's are adapting an avionics system paradigm borrowed from the manned commercial aircraft industry for use in manned space flight systems.

Integrated Modular Avionics (IMA) techniques have been proven as a robust avionics solution for manned commercial aircraft (B737/777/787, MD 10/90). This presentation will outline current approaches to adapt IMA, along with its heritage FSW V&V paradigms, into NASA's manned space flight program for Orion.

NASA's Kedalion engineering analysis lab is on the forefront of validating many of these contemporary IMA based techniques. Kedalion has already validated many of the proposed Orion FSW V&V paradigms using Orion's precursory Flight Test Article (FTA) Pad Abort 1 (PA-1) program. The Kedalion lab will evolve its architectures, tools, and techniques in parallel with the evolving Orion program.

Contact Information

Name: Mark Mangieri

Title: Computer Engineer, Orion FSW V&V Facility Lead, Kedalion Lead

Company/Organization: NASA/ER6

Voice: 281-483-6126 **Fax:** 281-483-3204 **E-mail:** mark.l.mangieri@nasa.gov

Biography:

Mr. Mangieri is currently leading the NASA/JSC/ER6 Facilities and Tools group. This group is presently focused on Orion FSW engineering analysis, support, and contractor oversight/insight.

He is the Orion FSW V&V facility lead responsible for devising a robust FSW V&V program to assure that the Orion program can achieve safe manned space flight. Simultaneously, his responsibilities include build up and operation of the Kedalion laboratory for system and software engineering analysis.

His past projects include software lead on the ARED instrumentation FSW project. Software lead on several flight experiments (DTO's) oriented toward the verification of performance of critical navigation subsystems based on Global Positioning System (GPS) technology for Shuttle, ISS, and X-38 programs.

Orion Flight Software V&V and Kedalion Engineering Lab Insight

Mark L. Mangieri¹
Jason Vice²

NASA – Johnson Space Center, Houston, Texas, 77058
[e-mail: mark.l.mangieri@nasa.gov](mailto:mark.l.mangieri@nasa.gov)
[e-mail: jvice@odysseysr.com](mailto:jvice@odysseysr.com)

NASA, along with its Orion prime contractor and subcontractors are adapting an avionics system paradigm borrowed from the commercial aircraft industry for use in manned space flight systems.

Integrated Modular Avionics (IMA) techniques have been proven as a robust avionics solution for commercial aircraft (B737/777/787, MD 10/90). This presentation will outline current approaches to adapt IMA, along with its heritage Flight Software (FSW) Verification & Validation (V&V) paradigms, into NASA's manned space flight program for Orion.

NASA's Kedalion engineering analysis lab is on the forefront of validating many of these contemporary IMA based techniques, as they relate to the unique adaptation into a human space vehicle. Kedalion has already validated many of the proposed Orion FSW V&V paradigms using Orion's precursory Flight Test Article (FTA) Pad Abort 1 (PA-1) program, which was successfully flown in May, 2010 at the White Sands Test Facility (WSMR). The Kedalion lab will evolve its architectures, tools, and techniques in parallel with the evolving Orion program, to gain insight into avionics systems design and to engage in the development and test of such designs.

Orion Flight Software Project

The Orion Flight Software project is among NASA's largest FSW undertakings since the effort expended on the Space Transportation System (STS) that it is intended to replace. The STS system was developed over 30 years ago, using technologies and paradigms that were leading edge in the software industry at that time. Orion's budget and schedule constraints brought vendor responses that proposed new techniques and reliance on much COTS technology. With all of the technological advancements accrued in the past 30 years, the Orion project still required on the order of 1.3m lines of custom developed source code (or equivalent COTS) to implement its avionics software requirements. The magnitude of the software development task also brought code generation technologies

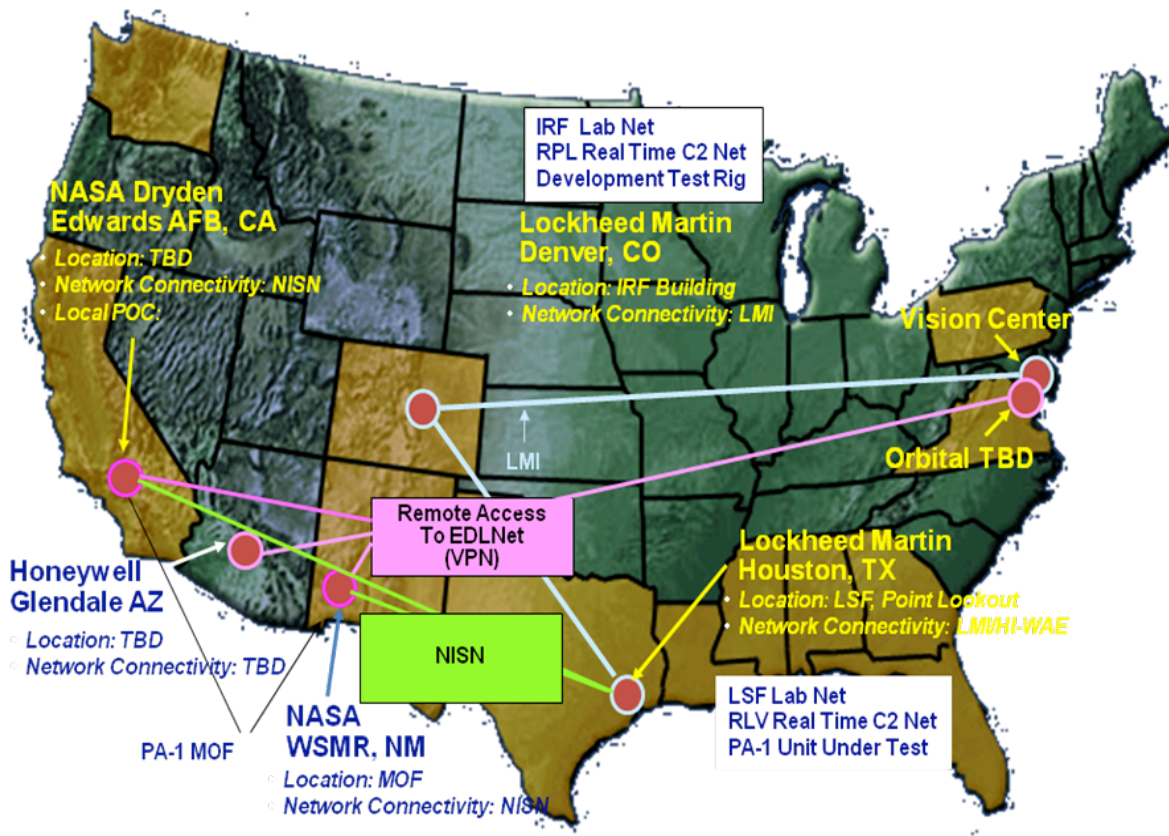
¹ Orion FSW V&V and Kedalion Lead, Spacecraft Software Engineering Branch, Houston, TX 77058/MS ER6, AIAA Member.

² Kedalion Chief Engineer, Spacecraft Software Engineering Branch, Houston, TX 77058/MS ER6, AIAA Member.

based on Unified Modeling Language (UML) design modeling (IBM/Rational Rhapsody), and Simulink for Guidance, Navigation, and Control (GN&C) intensive applications.

The magnitude of the Orion software effort, along with individual expertise from a diverse team assembled by Lockheed Martin, includes vendors from all over the country. These teams are required to coordinate, develop, and test their subsystems at dispersed locations, moving up the integration and test hierarchy toward centralized integration facilities.

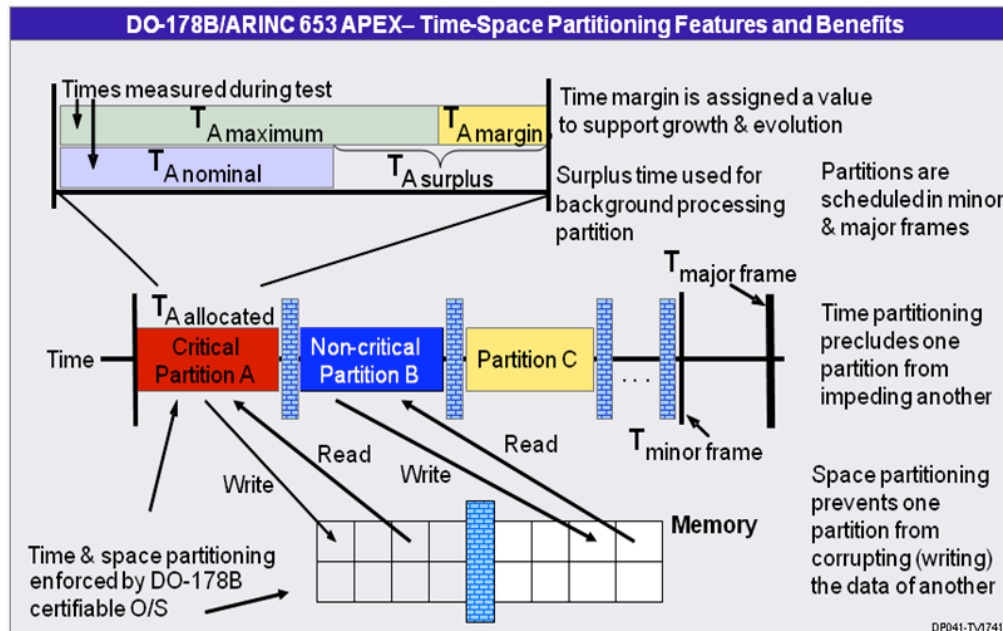
Geographical dispersion of major subsystem developers requires a paradigm unlike the methods NASA used in its STS heritage experiences. While the FAA had experiences with dispersed development and centralized system integration, NASA was accustomed to a more centralized approach. These culturally based paradigm differences proved to require significant communication, adaptation, and analogy to devise a strategy that was mutually agreeable to NASA and its contractor.



Geographically dispersed SW development

Integrated modular avionics (IMA)

IMA represents a real-time computer network airborne system. This network consists of a number of computing modules capable of supporting numerous applications of differing criticality levels, isolated from one another in partitions supported by the underlying operating system. IMA provides for an alternative hardware/software development and testing paradigm.



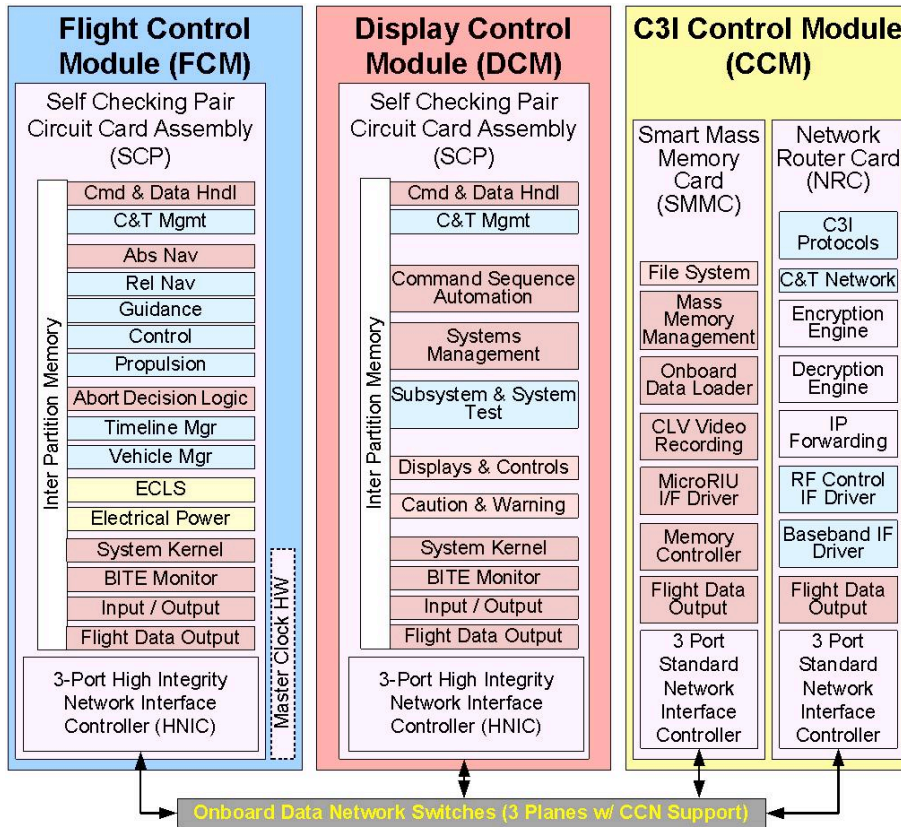
³ IMA Time & Space Partitioning

Orion's prime contractor, Lockheed Martin, has subcontracted Honeywell's vast experiences in its aircraft avionics heritage. Honeywell's paradigm is an Aeronautical Radio, Incorporated (ARINC) compliant adaptation of IMA, which Honeywell had successfully deployed on several Boeing and McDonnell Douglas aircraft designs (B737/777/787, MD 10/90). These techniques are mature enough to have been certified as DO-178b compliant by the FAA, and also have the support of major COTS Real-time Operating System (RTOS) vendors with mature products.

While there are significant similarities between aircraft avionics system requirements and space vehicle avionics system design, an augmentation was required to achieve the Orion avionics system design. Aircraft do not have flight dynamic phases as intense as a space vehicles ascent and decent phases, which require near instantaneous reaction with multiple failover scenarios to avert catastrophic failure. Additionally, aircraft do not generally sustain missions as long as typical spacecraft, which could last weeks or months.

FAA Heritage integration and test processes

The FAA has successfully used IMA techniques, primarily via Honeywell technology, to independently develop and test partitioned modules of flight SW across vendors at dispersed locations. This paradigm underwent significant analysis by NASA, as it was an unusual form of conducting a software development program since NASA's earlier STS experience base and culture.



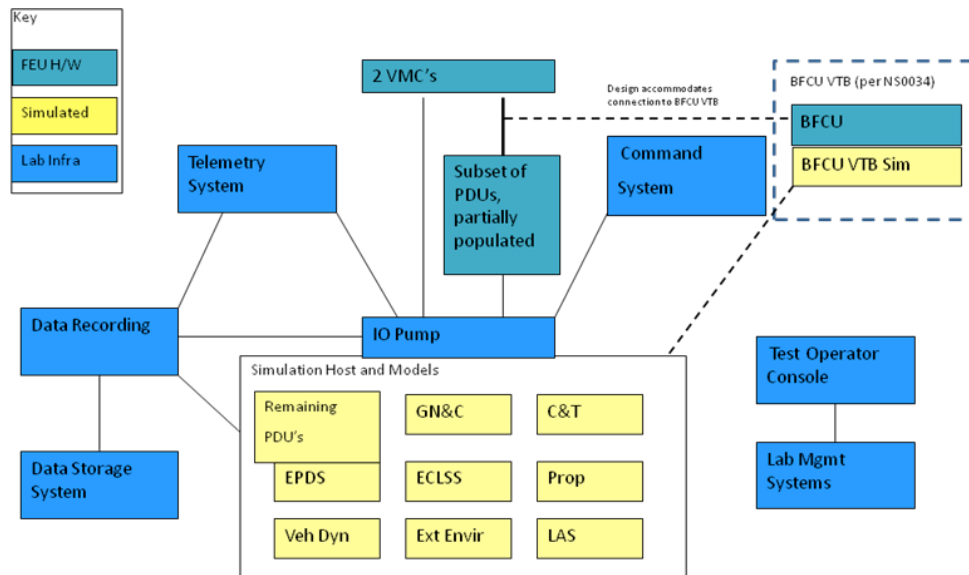
Orion IMA Architecture

Multiple fidelity test platforms

The first platform that a software module is subject to test on the Orion program is the desktop software development platform that every programmer has access to. This platform includes all of the tools to design and develop software algorithms, and a suite of simulation tools (SoftSim) capable of executing low fidelity executions of newly developed algorithms. SoftSim is an approach to bring target hardware simulation to the developer's desktop SW development platform, based on contemporary advances in simulation technology.

Commercially known as the Honeywell (HI) Valfac Test Bench (VTB), the VTB platform was adapted first to successfully support the integration and testing of major SW subsystems on the FTA/PA-1 program. The Orion instantiation of the VTB is a modification of HI's commercial VTB concept to include support for Orion unique interfaces and target HW, including Time Triggered Gigabit Ethernet (TTGbE) and VMC flight computers to support medium fidelity testing and integration.

The VTB platform is conceived as a highly adaptable and reconfigurable rig to support the many variations of tests required by the Orion SW project. The ultimate variation is the highest fidelity SW test platform known as the Super VTB. This test platform includes a dual string set of bus and target processors for testing redundancy and failover scenario's, as well as robust interface capability to access sensors/actuators allowing for first stages of subsystem vertical integration and test.



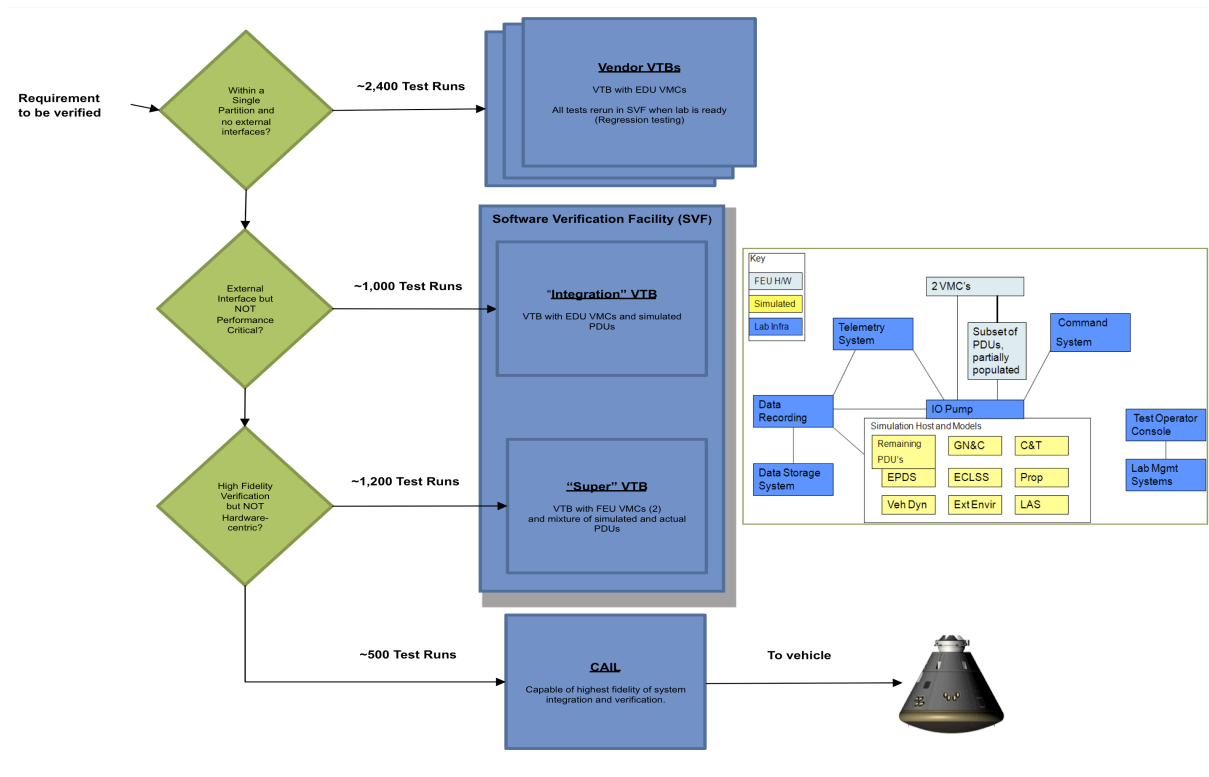
Super VTB Schematic

Hierarchical Distributed Testing on Orion

To achieve maximum schedule development and test parallelism, Orion SW teams recognized that a majority of lower level requirements were isolated to Computer Software Configuration Item's (CSCI's) and/or IMA partitions. NASA and LM teams analyzed the Orion SW requirement set and allocated specific requirements for eligibility for testing on the appropriate test platform, maximizing the usage of lesser fidelity platforms as appropriate, and minimizing usage of the highest fidelity platforms. This test allocation strategy accommodated for the fact that many VTB's would be distributed and used by subsystem managers ¹, while only a few Super VTB's would be available at a centralized integration and test facility.

The Super VTB's scarce resources are reserved for the ~10% subset of overall FSW requirements that have been analytically shown to only be testable on a platform with the Super VTB's resources. It was also designated, as a strategic regression test platforms to re-test a subset of VTB "corner case" test cases to bolster confidence that lower fidelity tests were accurate.

The Super VTB is also the platform to conduct "test as you fly" validation test cases of the integrated flight load. These specialized validation test cases are to be derived from Orion ConOps based on anticipated mission profiles, both nominal and off nominal. The "test as you fly" concept is common to both NASA and the aviation avionics industry, and stresses the notion to create test beds as close to a flight configuration as possible.



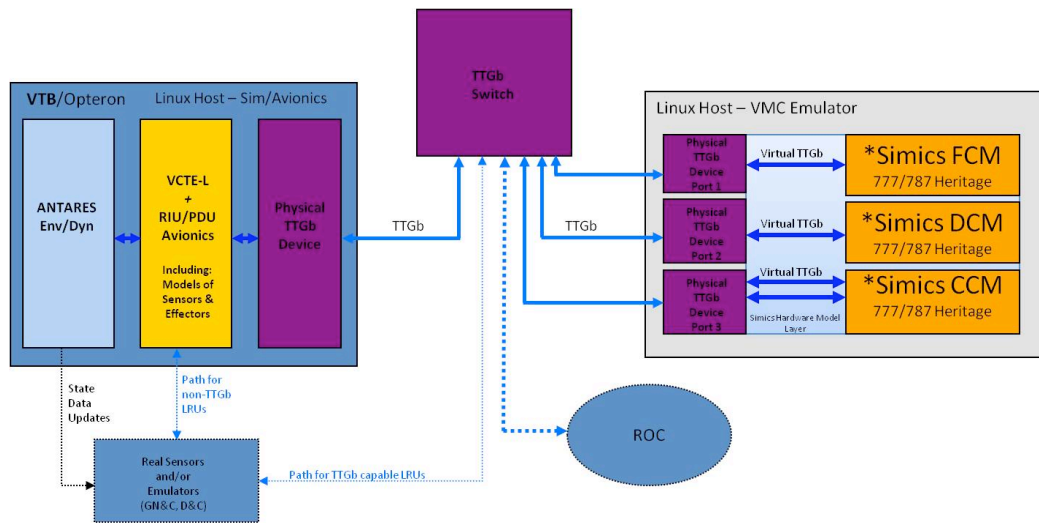
Hierarchical Distributed Testing

Kedalion – NASA’s insight and software analysis lab

Since Orion’s inception, NASA has conducted a risk mitigation strategy by implementing an in-house lab resource for targeted analysis and experimentation of FTA and Orion concepts. Largely used for analysis and validation of PA-1 flight loads, and GN&C mode team support, Kedalion developed into a significant program resource recognized by Orion program management as an integral part of Orion’s overall success.

Integration Synch Points (ISP's) are developed as interim demonstrations of Orion developmental technology at strategic points mutually agreed to by NASA and LM. These ISP's accomplish both milestones of progress and confidence building, especially in the area of inherently risky program technologies. ISP schedules and capabilities are coordinated with the Kedalion lab for purposes of technology sharing between NASA and LM, as well as validation of ISP content after it has been installed in the Kedalion lab.

Orion flight software loads will be delivered to the Kedalion lab for validation runs, much like PA-1, to further mitigate risk as the FSW loads are prepared for formal testing on the programs scarce VTB test platforms.



Early Kedalion Test Bed Concept with Simulated VMC

Lab heritage (JAEL, GITF)

NASA's Kedalion lab is the latest implementation in a rich history of analysis, prototyping and integration facilities. Understanding the complex interactions between spacecraft avionics has always required hands-on engineering analysis and testing. Experience gained on previous NASA programs has shown that the use of an agile analysis and integration facility can greatly benefit a program by allowing for risk mitigation very early in the program development as well as throughout the life cycle of the program.

NASA facilities such as the Shuttle Program's JAEL (JSC Avionics Engineering Lab) and the ISS Program's GITF (GN&C Integration Test Facility) have brought many years of value to those programs by providing more efficient and productive facilities for early integration testing, risk mitigation, avionics burn-in, problem resolution and other critical program tasks best done in an agile process oriented facility. While not always initially implemented as an inline testing facility, these types of NASA facilities have typically become early in-line testing facilities that allow for pre-formal testing in advance of the more expensive formal V&V facilities.

Kedalion was born from this heritage of agile and quickly reconfigurable integration and test facilities. In fact, the Kedalion facility is housed in the same room as GITF was for many years and even uses some of the same facility assets as were used by GITF.

Kedalion's purpose

The Kedalion lab's fundamental mission is to provide a facility for risk mitigation throughout the life cycle of a space vehicle's development and operation. To achieve success the lab is oriented toward hands-on engineering analysis that allows NASA engineers to achieve a deeper understanding of the avionics software and hardware than could be achieved by only reviewing documentation. It is not, however, a formal oversight or verification facility but rather a flexible facility that welcomes collaboration with the vehicle contractors as well as personnel from other facilities to establish the best possible solutions to design issues, operational constraints and problem resolution as early in the life cycle of a vehicle as possible. It is this approach that allows NASA to blend years of experience on past programs with new ideas from industry and from within NASA to produce solutions that can guide a vehicle's development toward ultimate success.

Lab architecture and components

The architecture of the Kedalion lab emphasizes flexibility, modularity and reconfiguration. The lab is populated with a variety of COTS hardware and software as well as some custom items and legacy assets from previous programs.

To establish a robust prototyping and development environment the lab was populated with a mix of development workstations that are powered by a variety of commercial computing operating systems including Microsoft Windows, Linux, IRIX and Solaris. By employing modern and legacy operating systems in the development environment engineers are able to maximize the use of modern tools as well as legacy software proven on prior programs.

More capable computing platforms are used to host simulation environments and emulation platforms. Embedded systems running real-time operating systems such as Green Hills Integrity and Windriver's VxWorks are used as needed to establish more robust real-time computing platforms. Non-real-time Linux platforms are also used for simulation and emulation but through careful software design these systems can be used in integrated configurations with real-time hardware.

A variety of data bus configurations are also used to allow integration of a wide range of devices. These data bus types include MIL-STD-1553, commercial Ethernet, Time Triggered Ethernet, various serial interfaces and others as required. The concept of "bus adapters" is also used to allow legacy equipment to be mixed into configurations with more modern data busses.

The overall emphasis of this mixed bag of equipment is to allow all of these diverse lab configuration pieces to be integrated together into any as needed architecture to support prototyping and testing. The same equipment can then be easily and quickly reconfigured to implement some other configuration as required. Computing platforms can be repurposed and data busses can be reconfigured to produce the necessary configurations to support the engineers needs.

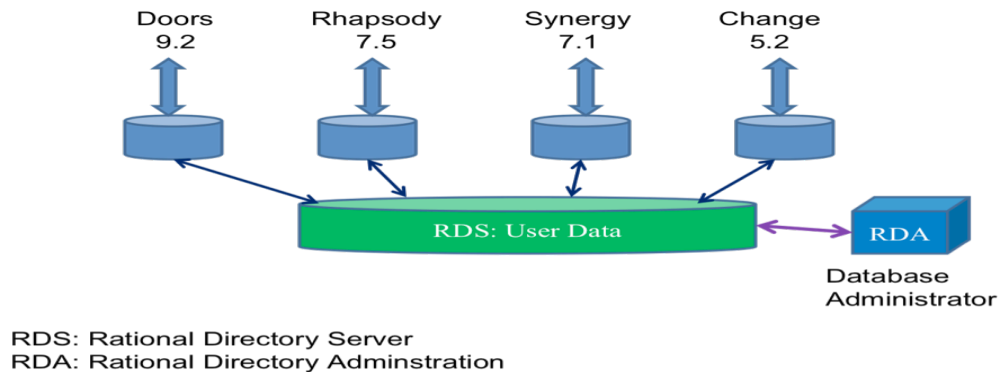
- **Heavy use of COTS software tools**
 - IBM Rational Tool Suite
 - Mathworks Model Based Development – Simulink
 - NI Labview
 - Windriver Simics & VxWorks RTOS
 - Green Hills Software – Multi, Integrity RTOS
- **Reuse of common NASA developed tools**
 - Trick Simulation Framework
 - EDGE – Graphics visualization package
- **Multipurpose workstations and servers**
 - Multiple OS environment
 - Linux, Windows, IRIX, Sun
- **Diverse hardware platforms**
 - Orion flight computers
 - Vehicle test bench
 - Multiple I/O interfaces available
 - Emulators and simulators used in place of unavailable hardware
 - Sensor integration platforms
 - Rate Table for inertial sensors
 - Star Field Stimulator for star trackers
 - GPS signal generator for GPS
 - Cockpit prototyping hardware
 - Engineering quality Display Units – low cost
 - Touch screen to virtualize display units
 - Hand controllers
 - “Out the window” views



Software Tool Chain (integrated SW development tool set)

Critical to understanding, designing and analyzing the avionics systems of a space vehicle is an understanding of the software tools used to build the vehicle’s software products. For this purpose, the Kedalion lab has instantiated a modern and fully capable software development environment. While not limited to these tools the core of this development environment was based on the software tool chain selected by the prime contractor for the Orion program. For this reason, the IBM Rational Tool Suite was implemented as the foundation of the tool chain for the Kedalion lab. In addition, tools such as Mathworks’ Matlab/Simulink, National Instruments Labview, Green Hills Multi, Microsoft Visual Studio, DiSTI’s GL Studio as well as a variety of commercial software testing tools were added to the development environment to enhance the lab’s tool chain.

IBM Rational Tool Suite



⁵ Rational™ Tool Suite

Many of these tools serve a dual purpose. First, they allow NASA engineers to have a rich set of development tools for use in a variety of development projects. But in addition, by implementing the tools used by the vehicle contractor, NASA engineers are able to become knowledgeable about and technically proficient in the use and applicability of these tools. The use of commercial tools can positively impact a program but this is dependent upon the selection of the most fitting tools. By taking a hands-on approach to understand these tools, NASA engineers are able to guide the vehicle development teams toward the most appropriate tools and away from tools that could negatively impact the progress of a vehicle's development.

Simulators/Emulators/Hardware/Software

Another key feature of the Kedalion lab is the use of high fidelity simulations to add realism to test configurations. Vehicle avionics components are integrated with complex high fidelity simulations to produce a realistic configuration that can produce the same environmental and dynamic data as would be experienced in actual flight. Interactions with the natural environment and full vehicle dynamics as well as subsystem behaviors are produced through these complex high fidelity simulations.

Many of the models used in these simulations are reused common models and legacy models developed in other programs. This model reuse is enabled by the use of a NASA developed simulation framework known as TRICK. The TRICK framework is used extensively in the Kedalion lab as the basis of most simulations and emulators. TRICK provides an extensive suite of simulation development, execution, monitoring and post execution analysis tools. In addition, it provides a full-featured executive framework that can be configured and built into a variety of simulation architectures. It provides auto-coding services that allow model developers to focus on their domain expertise rather than on the development of a simulation structure. This combined with the easy reuse and reconfiguration of models allows for very rapid development of complex simulations.

TRICK also provides simple options for integration with hardware interfaces and, therefore, provides an ideal framework for implementing emulators. If actual hardware elements are too expensive or simply not available an emulation of the device can quickly be developed through the use of TRICK.

Kedalion lab extensibility – ROC/Optics/MCC

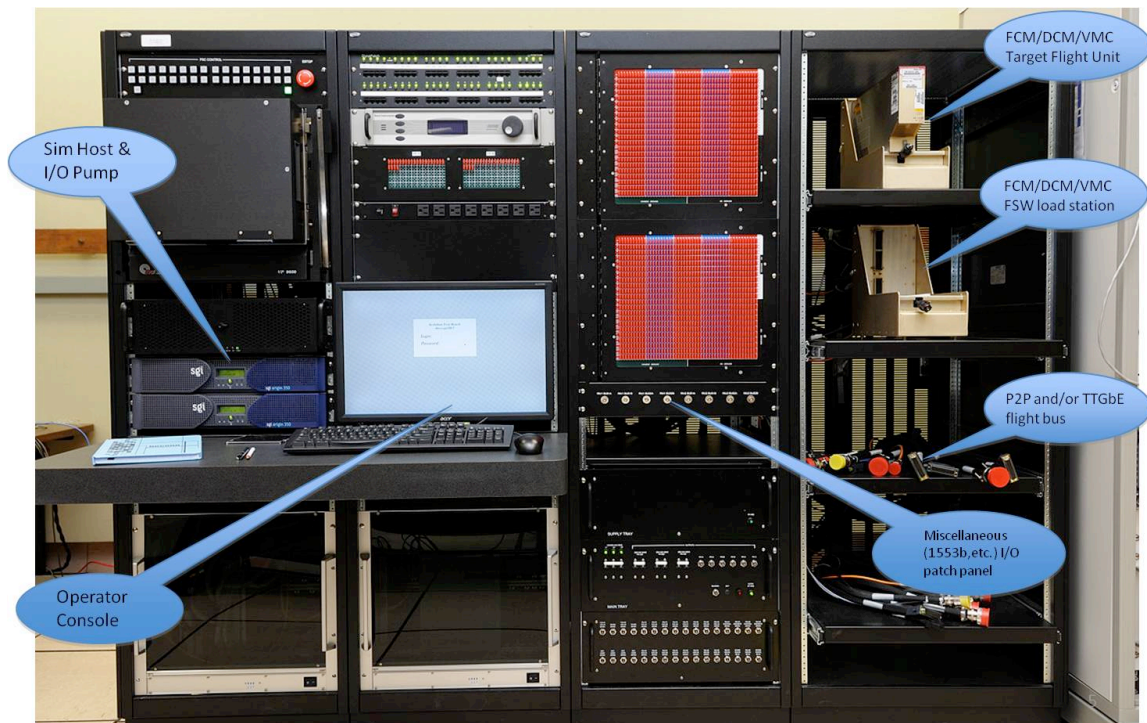
Since its establishment, the Kedalion lab has experienced steady increases in capability and capacity. The initial implementation of the lab began in the early stages of the Orion program and was largely based on the need to analyze early program options. Software tool selections, development and test methodologies, integration approaches and system architectural investigations all drove the need to implement various capabilities in the lab. These lab building blocks were matured through use and helped to mature the NASA engineering community's understanding of how the Orion vehicle would be developed.

As the lab matured and its capabilities became more stable the opportunity to expand beyond the lab walls became available. One of the strengths of the Kedalion's location is its proximity to other JSC lab facilities. Cooperative efforts and integrated configurations with several other facilities have greatly enhanced the capabilities of the lab. For example, JSC's ROC (Reconfigurable Operational Cockpit) is located a short distance from the Kedalion lab. The ROC is a human-in-the-loop engineering facility with medium fidelity cockpit configurations combined with a dome projection system for accurate out-the-window visualizations. Dedicated data lines have been connected between the ROC and Kedalion, which increases the capabilities of both labs by adding the human-in-the-loop cockpit capabilities to the vehicle avionics configuration. This combination of labs produces a joint configuration that normally would only be found in a more formal and complex iron-bird style lab.

Other facilities and labs have similarly been connected with the Kedalion to produce several cooperative mutually beneficial configurations. A space vehicle optics lab, avionics hardware focused lab and the JSC Mission Control Center (MCC) have all been connected to the Kedalion lab to augment its capability. Cooperative configurations like these have added value to the program without incurring much additional cost.

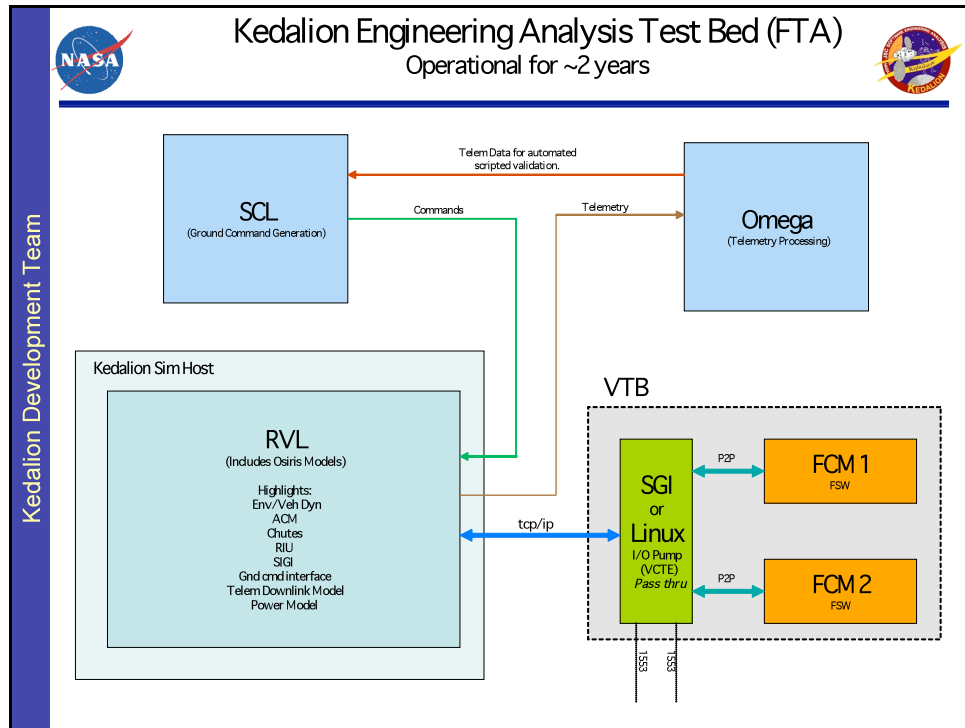
PA-1 test bed architecture

An early focus of the Kedalion lab and a key feature is the FTA PA-1 Test Bench hosted in the lab. This test bench, known as the FTA VTB (Vehicle Test Bench), was procured early in the lab's build-up to serve as a platform for evaluating the Orion contractor's plans for testing flight software.



FTA VTB (Valfac/Vehicle Test Bench)

The VTB provides integration capabilities that allow flight software to be executed on actual flight processors while integrated with a full-featured simulation. This allows scenario based testing to be performed where the flight software is executed in a “test like you fly” approach. Since the flight computers for Orion are based on IMA architecture, this type of test configuration is able to produce the fidelity necessary to simulate actual flight conditions, as the flight computer would perceive them. The high fidelity simulation combined with a flight data bus capable I/O pump makes this type of test configuration possible. The simulation feeds the I/O pump with all of the inputs necessary to fully populate the flight data bus. This allows all of the elements of the IMA architecture on the flight computer to interact with the same interfaces as they would in actual flight.

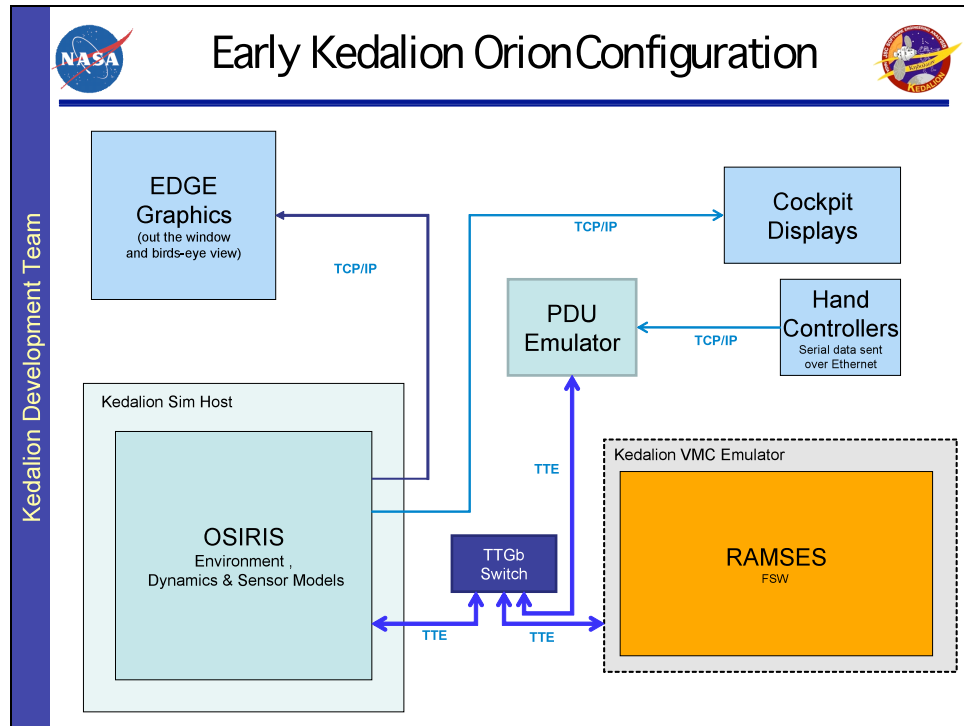


PA-1 Kedalion Test Bed with Honeywell Flight Computer Modules (FCM)

Hybrid PA-1/Orion test bed architecture

After achieving success with the FTA VTB in the Kedalion lab it was necessary to begin modifying the lab configurations to support the Orion test bed architecture. Because Orion is still in the early stages of development many of the avionics elements are only available in prototype or very early form. Due to this early level of project maturity substitutes for avionics elements had to be selected or developed to provide the necessary functionality to instantiate the Orion avionics architecture.

Since the IMA architecture partitions individual functional areas into discrete modular elements it was possible to move early version of some of these elements to different platforms. For example, instead of executing early GN&C flight software on actual flight computers (which were not available), a platform was developed that allowed this same software to be encapsulated inside a simulation environment, provided by TRICK, and executed with an actual flight data bus to produce hybrid avionics architectures.



Adaptation of IMA architecture to early hybrid prototype configuration.

The FTA VTB was modified to implement this configuration. Modular pieces of the test bench were upgraded or enhanced to include both FTA and Orion data bus interfaces. This allows for reuse of lab assets and also allows for a much easier transition to the new avionics architecture as it is being developed. With interfaces already in place, newly available hardware elements can be added as they become available.

Orion test bed architecture – adding hardware as it matures

Early versions of Orion hardware are now becoming available to the project. Flight software will be moved off the simulated or emulated platforms and onto these early flight computers. Since the changes to the configuration will happen at the hardware interface points the disruption to the operation of the test configuration will be minimal. As additional hardware becomes available it will be added to the configuration in a similar way.

The Kedalion test configuration will continue to be modified and upgraded as the Orion program matures. Hardware and software will be integrated with the other elements as it becomes available in an effort to keep the Kedalion configuration for continued support of program needs.

Acknowledgements

The authors thank the Orion project management team including Mike Brieden and Chad Rowe for their guidance, collaboration, and support. The authors further thank the Spacecraft Software Engineering Branch management leads Steven Frederickson and Pedro Martinez for encouragement and technical support in producing this paper. For support in sharing this information at the AIAA Space 2010 conference, the authors thank Rob Ambrose and Cliff Farmer, as well as the overall Orion project management team.

References

¹ "Modular Verification: Testing a Subset of Integrated Modular Avionics in Isolation", Christopher B. Watkins, 25th Digital Avionics Systems Conference (DASC), Portland, Oregon, October 2006.

² Feiler, Peter H. "Challenges in Validating Safety-Critical Embedded Systems." *Proceedings of SAE International AeroTech Congress*. Seattle, WA (USA), November 2009.

³ "ARINC 653 - An Avionics Standard for Safe, Partitioned Systems". WindRiver Systems/IEEE Seminar. August 2008. http://www.computersociety.it/wp-content/uploads/2008/08/ieee-cc-arinc653_final.pdf. Retrieved 2009-05-30.

⁴ RTCA, Incorporated, document RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," December 1, 1992.

⁵ "How the IBM Rational Team Unifying Platform integrates with IBM Development Tools", IBM Corporation, Document G507-0962-00, July 2005