Vehicle Systems Management on Orion

CreShenda Tia' Sands
Lockheed Martin: Space Systems Company
Houston, TX 77075, USA
creshenda.sands@lmco.com

Abstract – *Vehicle Systems Management is a collection of mission-level and vehicle-level functions that are necessary to control and operate the Orion spacecraft. The Vehicle Systems Management philosophy is to provide the user with basic capabilities that can be expandable over time as the experience on mission execution grows. Orion's onboard functions have two primary areas: fault management and automation control; and the remaining vehicle system management functions can be viewed as a subset or closely related to the two areas. Vehicle Systems Management has five Computer Software Configuration Items: Timeline Management, Vehicle Management, Systems Management, Abort Decision Logic, and Systems and Subsystems Test. During dynamic phases of the mission, Orion can operate under computer control (Vehicle Systems Management) presenting opportunities to transfer control to crew or ground and back again. An overview of the Vehicle Systems Management architecture, subsystem core capabilities, and flight software is presented.*

Keywords: Constellation, Orion, Vehicle Systems Management, avionics, flight software.

1 Introduction

Orion is the next-generation human space flight crew transportation system being developed to safely transfer astronauts to and from the International Space Station and other destinations beyond low Earth orbit such as the Moon and eventually Mars. Orion is the crew exploration vehicle for the NASA Constellation Program to send human explorers back to the Moon (Fig. 1) and later to Mars and beyond. As a replacement for the NASA Space Shuttle Orbiter with capability to transport crew beyond low Earth orbit, Orion will benefit from recent and more advanced technologies. The various advanced technologies to benefit Orion include avionics and software, at the core of which is a vehicle systems manager responsible for coordinating subsystems at the vehicle level and the overall mission timeline as well as vehicle phases, segments, and modes.

Vehicle Systems Management (VSM) is a cross-cutting subset of avionics functions that coordinates the flight vehicle's intersystem interactions and dependencies. This avionics and software function impacts the entire Orion mission from pre-flight through flight operations to post-flight [1]. Together with the crew and ground commanding capability, it constitutes the onboard software coordinating activities of all of the vehicle subsystems. There are opportunities for the vehicle to transmit control to crew or ground and back again. VSM provides vehicle-level management capabilities and captures system interdependencies and interactions, thus optimizing the distributions of subsystem and vehicle-level management functions while taking full advantage of the safety and operational flexibility of the spacecraft. This paper presents an overview of the Orion VSM including its architecture, subsystem core capabilities, and flight software.

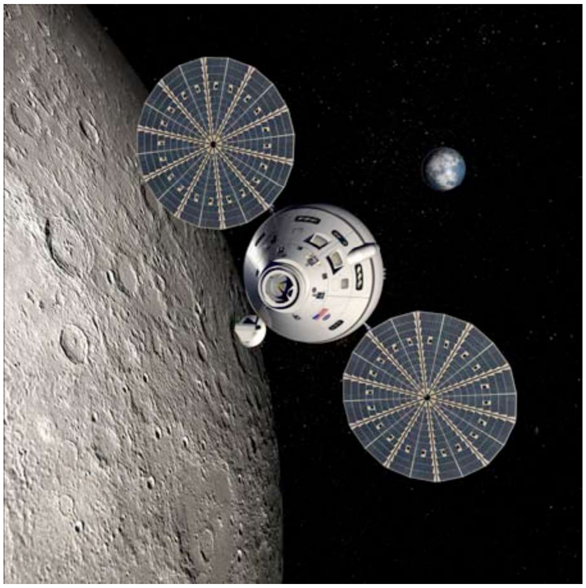

Figure 1. Orion Spacecraft (artist's conception).

2 VSM Functions

The Orion VSM encompasses nine core capabilities. These capabilities are not stand alone functions, but are coupled with each other, embodied in five software components: Timeline Management, Vehicle Management, Systems Management, ADL, and System and Subsystem Test (S&ST). Each of the five software functions is supported with risk mitigation activities: script development and verification, and VSM Data Reconfiguration. The VSM flight software is designed to use parameterized data and sequences of scripted commands to accommodate mission-unique and vehicle-unique functionality. The VSM core capabilities are briefly described as follows:

1. *Fault Detection, Isolation, and Recovery (FDIR)* determines vehicle faults and the source of their location; it protects critical vehicle capabilities, and restores the vehicle to an operational state by justifying these faults. At a minimum, FDIR provides fault detection at the subsystems and vehicle level.

   Health and Status (H&S) manages the data and onboard measurements to allow for an assessment of the condition of the vehicle. H&S is essential for the crew and other vehicle components to maintain spacecraft situational awareness, providing critical decision support information to trigger or identify nominal or off-nominal actions in response to the dynamic health and status of the system.

2. *Caution and Warning (C&W) Logic* uses health test results and associated root causes to determine correct messages and any other significant information required for display to the crew. Audio cues and lights are used appropriately.

3. *Resource Management* provides knowledge of the remaining resources (which are defined as power, thermal, and computer processing) on the vehicle based on the cross-strapped vehicle architecture. VSM collects, sorts, and analyzes this data so that resource information can be accurately displayed to the crew and ground.

4. *Vehicle Configuration/Reconfiguration* detects events or commands that trigger the transition to a vehicle operational configuration.

5. *Mission Time and Event* is used to maintain or manage the mission in automatic and/or autonomous situations and is controlled by data-driven events and/or the vehicle clock. The Mission Time and Event scheduling function is focused on decomposing and executing the mission phase and mode transitions required to perform the mission plan.

6. *Abort Decision Logic (ADL)* contains the flight software (FSW) associated with the identification and evaluation of mission critical safety parameters. It recognizes conditions that jeopardize the crew or mission objectives, and commences actions based upon recognition of those conditions.

7. *Onboard Checkout (OBCO)* asses the functionality of a particular vehicle capability prior to operational use.

8. *Re-initialization/Checkpoint/Restart* initializes the flight processors to a predefined operating configuration and can snapshot, export, and load (to/from external systems) predefined flight processor computational execution states (checkpoint).

9. *Command Script Automation (CSA)* provides infrastructure for vehicle automation including automated fault recovery, OBCO, and flexible command scripting.

H&S has been described as a data function used to detect faults in components and subsystems; as a result, H&S is an input to the vehicle-level FDIR. Upon fault(s) being detected or isolated, the information is sent to the C&W system for display to the ground and crew. Orion has the choice to recover from a fault with the use of recovery scripts. Built-in-Test (BIT) is not a VSM function but is required to detect faults and anomalies [2]. The H&S subsystem data obtains messages that include subsystem identification, software configuration, hardware configuration, health reports that contain faults, and status information (i.e., state and redundancy).

Abort of the mission during ascent phase of a mission and re-initialization of the flight processors in the event that vehicle management computers (VMCs) hit failure modes are two specialized fault cases. An out of plan situation is reported to the crew and ground with the C&W system.

Vehicle Configuration functions and Mission Time and Event Scheduling are closely linked. Mission Time and Event Scheduling allows the Orion vehicle to execute the mission plan while vehicle reconfiguration keeps running a tally of the state of the hardware at all times. Both functions are used to identify the subsystem H&S message as shown in Figure 2.

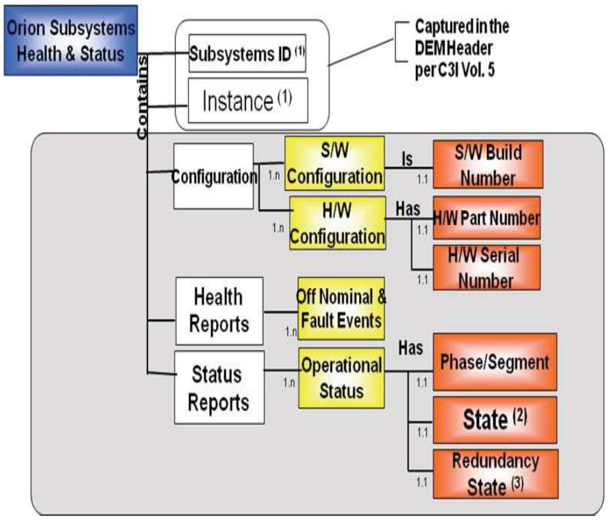

Figure 2. Example of Health & Status Message.

3 VSM Architecture

VSM will also interface with the majority of the onboard subsystems and presents an integrated and systematic view of the spacecraft to the crew and pilot. These activities include the instrumentation assessment, abort decision and execution, phase/segment definition (apart of Mission and Event sequencing), FDIR Integration, C&W Integration, and VSM Concept of Operations.

Functions managed by VSM are distributed across the subsystems in both hardware and software. Thirteen subsystems make up VSM. Five subsystems are self-managed subsystems and the remaining eight are managed subsystems. The VSM software integrates output from the subsystems and vehicle instrumentation to coordinate vehicle functions and provide crew situational awareness. The subsystems are responsible for design and implementation of their components including: subsystem reporting of conditions that could lead to an abort, FDIR recovery of local faults, and C&W reporting of health and status data to vehicle FDIR and C&W. Figure 3 illustrates the interactions of the VSM architecture.

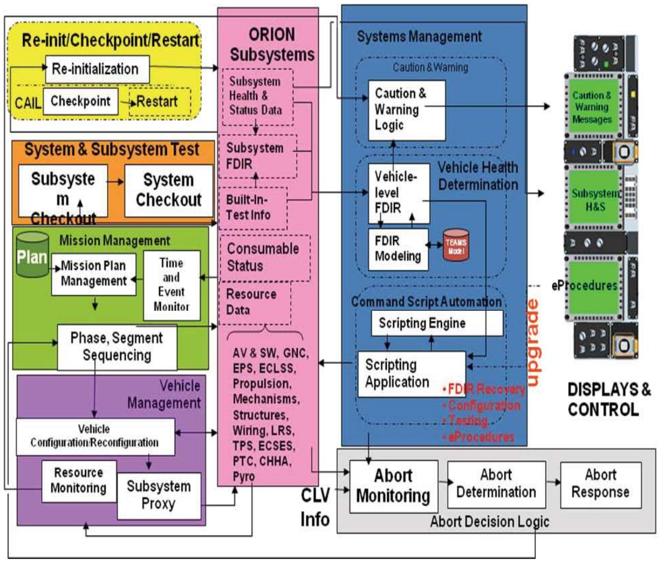

Figure 3. VSM Functional Architecture.

The VSM architecture has a two layer distributed structure, the lower level subsystem layer and the upper VSM layer. Re-initialization and Checkpoint/Restart are distributed functions and implemented in multiple software domains. All five Computer Software Configuration Items (CSCI's) interface with the Orion subsystems. S&ST permits the testing of individual components on the entire vehicle and on the entire subsystem to complete a thorough checkout.

An event plan is loaded into the Timeline management (TM) CSCI prior to launch. Orion is controlled by the sequencing of phase and segments as laid out by the event plan. Once this information is published, the remainder of the vehicle subscribes to the phase and segment portion. There are specific transition criteria built into the plan that can be triggered by time or specific events taking place. There is an electronic procedure (eProc) for every segment transition and the critical action alert (CAA) has the capability to prompt the crew to the appropriate electronic procedure when all other transition conditions necessary for the segment transition have been satisfied [2].

Orion has two types of subsystems: self managed (smart) or managed. The five self-managed subsystems are: 1. Avionics and Software, 2. Electrical Power System (EPS), 3. Propulsion, 4. Guidance, Navigation, and Control (GN&C) and 5. Environmental Control and Life Support System (ECLSS). TM publishes the phase and segment of the mission and the self-managed subsystems reconfigure themselves based on the transition logic. For the managed subsystems, Vehicle Management (VM) acts as a proxy coordinating and executing the hardware reconfigurations of vehicle subsystems as specified by configuration activities required in the current mission segment. It also performs ordnance control to execute abort sequences [3]. The Resource Management function collects consumable status and resource data from the subsystems, compares usage against a plan, and is a trigger for caution and warning when resources deviate high or low from the plan.

ADL is the logic required to initiate abort during ascent and potentially a contingency such as early returns. During ascent, ADL analyzes and monitors conditions from both Orion and the launch vehicle for an abort and if triggered, starts the abort process. It takes guidance information from the GN&C subsystem to insure the crew is returned safely to Earth or orbit depending on its phase of ascent. An automatic abort is required in time critical situations. When this happens, the abort signal is sent to the TM CSCI which switches the phase and segment to a contingency plan for an abort mode. Figures 4 and 5 illustrate a scenario where an abort is initiated in the Second Stage Ascent with the Launch Abort System (LAS). They also illustrate the execution of a nominal event plan predefined by mission segments in a particular portion of the mission from pre-launch to when the vehicle is in orbit.

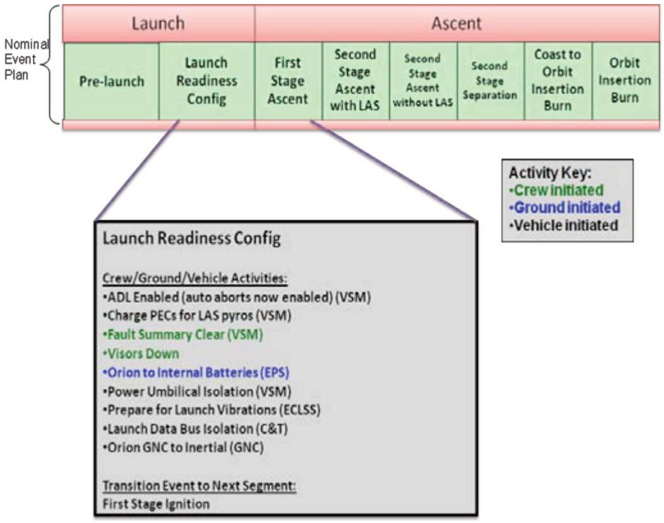
Nominal Event Plan
Launch
Ascent
Pre-launch
Launch Readiness Config
First Stage Ascent
Second Stage Ascent with LAS
Second Stage Ascent without LAS
Second Stage Separation
Coast to Orbit Insertion Burn
Orbit Insertion Burn
Activity Key:
•Crew initiated
•Ground initiated
•Vehicle initiated
Launch Readiness Config
Crew/Ground/Vehicle Activities:
•ADL Enabled (auto aborts now enabled) (VSM)
•Charge PECs for LAS pyros (VSM)
•Fault Summary Clear (VSM)
•Visors Down
•Orion to Internal Batteries (EPS)
•Power Umbilical Isolation (VSM)
•Prepare for Launch Vibrations (ECLSS)
•Launch Data Bus Isolation (C&T)
•Orion GNC to Inertial (GNC)
Transition Event to Next Segment:
First Stage Ignition

Figure 4. Example of Nominal Mission Event Plan Execution.

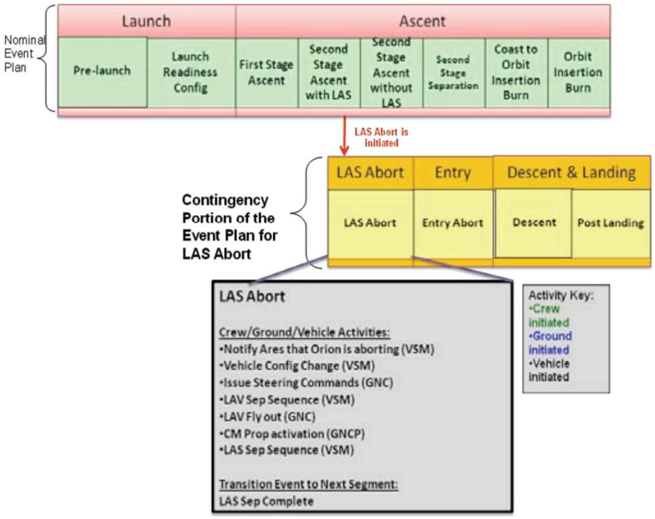

Figure 5. Example of LAS Abort Scenario in Mission Event Sequencing.

The subsystems are responsible for their individual FDIR and develop respective Health and Status messages. FDIR is the critical activity in VSM and exists on two levels; each subsystem has its own FDIR function on various critical components and a vehicle-level FDIR that works across the subsystems. Built-in-Test is a key component that drives that ability to determine off-nominal and fault events. The subsystem FDIR that cannot be isolated or resolved is sent to the Vehicle Health Determination (VHD) domain within the Systems Management CSCI. VHD also addresses vehicle-level fault isolation with root cause determination. Vehicle-level faults are faults that crossed multiple subsystems such as those associated with data, power, and possibly thermal abnormalities. Output VHD consists of caution and warning messages displayed to the ground and crew for situational awareness. In events that are time critical, scripts can be used to automatically recover from selected vehicle-level faults.

4 Flight Software

As mentioned above, VSM flight software is designed to use parameterized data and sequences of commands or scripts to accommodate mission-unique and vehicle-unique functionality. Figure 6 demonstrates the nine VSM functions mapped into the five VSM CSCIs.

Timeline Management provides on-board automated sequencing of software activities at the mission level acting as the central coordinator of vehicle- and subsystem-level activities through the broadcast of phase, segment, events and other vital timeline related information. TM interfaces with subsystems computer software configuration items or CSCIs and other VSM components to exchange data across the vehicle. It serves to execute the sequence of mission phases and segments or the onboard event plan. With these actions, TM automatically monitors parameterized event criteria accepting commands from the crew and ground for segment transition and for inhibit of segment transition as well. On the Orion vehicle, the mission planning function is mainly the responsibility of the mission operatives' personnel, developing pre-flight plans, and performing real-time re-planning. VSM TM is focused on mode transitions required to perform the mission plan.

Vehicle Management is securely united with Timeline Management and is responsible for the hardware configuration of the vehicle and is also the executor of the vehicle plan (which is derived from the mission plan). It configures vehicle subsystems to execute the vehicle plan for nominal and contingency scenarios. Resource management is shared with vehicle management and it administers the real-time allocation and real-time utilization of shared resources based on predetermined allocations that are part of the vehicle plan. Vehicle management also serves as the proxy application software for onboard heater control, the Low Impact Docking System (LIDS), the Vision Processing Unit (VPU), and the Crew Health and Habitation Accommodation (CHHA) system.

Systems Management (SM) provides vehicle-level health monitoring and assessment of the circumstances of the vehicle, command sequence and automation, caution and warning, and vehicle-level FDIR. It monitors subsystem level FDIR to provide system-level response when the subsystem has exhausted its fault response capability. SM also provides automated command sequencing through the implementation of onboard scripts and correlates subsystem-level fault information to determine vehicle-level faults, and provides fault improvement through predefined responses to identified vehicle-level faults. These scripts can be initiated by vehicle-level FDIR (automated recovery) or commanded by the crew, mission systems, or other subsystems.

Abort Decision Logic distinguishes conditions that endanger the crew or mission objectives, initiates actions based upon recognition of those conditions, and interacts with timeline management during the ascent portion of the mission. ADL monitors vehicle-level performance and detects pre-determined abort conditions to respond to conditions that jeopardize the crew or the vehicle. ADL is most prominent during the ascent phase of the mission due to its dynamic change and is available during other phases. ADL responses will ensure the safety and recovery of the crew, the safety of ground personnel and equipment, and the recovery of flight articles. When abort conditions have been detected, ADL will select one of the available abort modes, which are determined by the GN&C subsystem. Available modes are based on phase and segment and achievable modes are based on G&NC input. The vehicle manager will receive abort plan information from the timeline manager and will coordinate events and execution of commands for the Launch Abort System initiation. The vehicle manager is also responsible for issuing the ordinance commands associated with the abort mode, which is a critical part of the abort execution sequencing. ADL provides the crew with a time to veto before automatically proceeding with an abort. During an autonomous abort, ADL prompts the crew with an abort recommendation and allows the crew to make another decision or an authority to proceed (ATP) with an abort [3]. These two functions allow the crew to evaluate the situation while allowing the ADL to initiate the abort if the crew does not respond before the timer expires.

System and Subsystem Testing reports the capability and test of the integrated vehicle. Within this system, subsystems are competent of performing tests on their individual components, which then reposts the results of any subsystem test as well as integrates subsystem tests into larger vehicle tests. The test command integration is performed using scripts and is modified through uplink. Onboard checkout includes the systems and subsystems test software component and other onboard test functions including Built-in-Test. S&ST thus provides a capability to perform and report results of any subsystem test and integrates the subsystem tests into larger vehicle tests. The tests will perform three functions: exercise systems and subsystems, confirm the available capabilities, and report on the availability of the capabilities. These tests will use S&ST to issue commands with normal operations and with appropriate safety limitations allowing for system checkout as it is used to operate the system. Figures 3 and 6 show how these core components flow together in a normal operation.

With a data driven and script-based approach, the executable code remains unchanged from flight-to-flight and only the parameterized data changes before or during the flight. The VSM viewpoint provides the user with basic capabilities that can be expandable over time as the experience on mission execution grows. During vigorous phases of the mission, the vehicle can be under VSM control (computer control) and have opportunities for the vehicle to transfer control to crew or ground. This flexibility allows the precision and mathematical logic of the computer and software to merge with the interpretation and conclusion capability inherent in the human intellect.

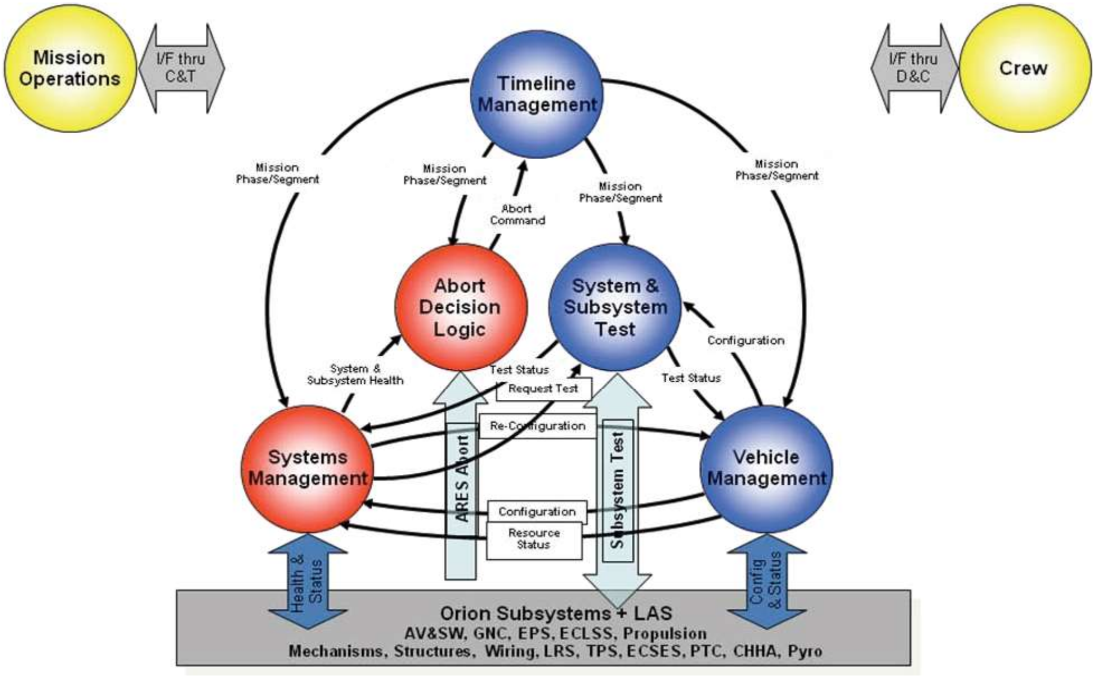

Figure 6. VSM Software Architecture.

5 Conclusions

The Orion contract was awarded to Lockheed Martin in September 2006, and the VSM team has been working since the end of the 2006 calendar year. The design of the Orion spacecraft intends to optimize the distribution of subsystem- and vehicle-level management functions while maximizing the safety and operational flexibility of the spacecraft. For this reason, the VSM function will integrate subsystem- and vehicle-level functions to optimize the management and control of the spacecraft. Forward work includes development of the transition criteria for the lunar segments and VSM will be developing the abort timeline in support of Abort Decision and Execution integration. The VSM Concept of Operations will be evaluated with the subsystem specifications to insure the VSM design satisfies the requirements and its intended use. The Critical Design Review for the program is scheduled for early 2011 and the first flight is planned for 2015.

Acknowledgment

The author acknowledges contributions of the following individuals working on VSM at NASA: Steve Mueller, James Carvajal, Darrel Raines, Grace Hua, Charlie Riall, Kenneth Chevalier, Jennifer Ha, Theresa Spaeth, Kevin Butler, and Gretchen England. The author also acknowledges contributions of the following individuals at Lockheed Martin: Wendell Chun, Karen Gandy, John Peterson, Chris Weber, and Alan Bishop. Finally, the author acknowledges contributions of the following teammates at Honeywell: Erv Baumann, Steven Bradford, Brenda Weber, Joe Breno, Mike Berning, Chris Couch, Thomas Gates, Khanh Hoang, John Hoffman, Melissa Kirkland, Louise Li, Robert Sterner, Kelly Tuttle, Shawn White, and Kim Topps.

References

[1] W. Chun, "Paradigm shift to autonomous operations," Proc. AIAA/ICAS International Air & Space Symposium and Exposition, Dayton, OH, July 2003.

[2] G. Bird, M. Christensen, D. Lutz and P. Scandura, "Use of integrated health management in the field of commercial aviation," Proc. First International Forum on Integrated System Health Engineering and Management in Aerospace, Napa, CA, November 7-10, 2005.

[3] P. Scandura and C. Garcia-Golan, "A unified system to provide crew alerting, electronic checklists and maintenance using IVHM," Proc. IEEE 23rd Digital Avionics Systems Conference, October 2004.