Integrating Planning, Execution and Diagnosis to Enable Autonomous Mission Operations

Jeremy Frank and Gordon Aaseng and K. Michael Dalal and Charles Fry and Charles Lee and Rob McCann and Sriram Narasimhan and Lilijana Spirkovska and Keith Swanson
NASA Ames Research Center
Mail Stop N269-1
Moffett Field, CA 94035-1000
{firstname.lastname}@nasa.gov

Lui Wang and Arthur Molin and Larry Garner
NASA Johnson Space Center
Mail Code ER61
2010 NASA Parkway
Houston, TX 77085
{firstname.lastname}@nasa.gov

Abstract

NASA's Advanced Exploration Systems Autonomous Mission Operations (AMO) project conducted an empirical investigation of the impact of time delay on today's mission operations, and of the effect of processes and mission support tools designed to mitigate time-delay related impacts. Mission operation scenarios were designed for NASA's Deep Space Habitat (DSH), an analog spacecraft habitat, covering a range of activities including nominal objectives, DSH system failures, and crew medical emergencies. The scenarios were simulated at time delay values representative of Lunar (1.2-5 sec), Near Earth Object (NEO) (50 sec) and Mars (300 sec) missions. Each combination of operational scenario and time delay was tested in a Baseline configuration, designed to reflect present-day operations of the International Space Station, and a Mitigation configuration in which a variety of software tools, information displays, and crew-ground communications protocols were employed to assist both crews and Flight Control Team (FCT) members with the long-delay conditions. This paper describes the mitigation configuration, with specific attention on the plan and procedure execution tracking and fault detection, isolation and recovery software.

Introduction

NASA is now investigating a range of future human spaceflight missions that includes a variety of Martian destinations and a range of Near Earth Object (NEO) targets. These possibilities are summarized in Table 1. The table shows the approximate distance between the destination and the Earth, where the control center will be located, and the one-way light-time delay between the destination and Earth.

Destination	Earth Distance (km)	1-way Time delay (s)
Lunar	38,400,000	1.3
NEOs (close)	100Ks	10s
Mars (close)	545,000,000	181.6
Mars (opposition)	4,013,000,000	1337.6

On next-generation deep-space missions, crews will have to operate much more autonomously than they do today. A higher degree of crew autonomy represents a fundamental change to mission operations. Enabling this new operations philosophy requires a host of protocol and technology development to answer the following question: How should mission operations responsibilities be allocated between ground and the spacecraft in the presence of significant light-time delay between the spacecraft and the Earth?

Human Spaceflight Mission Operations Today

Current International Space Station (ISS) operations are conducted with significant reliance on ground monitoring, control, and planning capability; some of which is by design to maximize crew time available for onboard science. Nearly instantaneous feedback from ground commands combined with a computer architecture designed with more software control capability than previous vehicles provides Flight Control Team (FCT) personnel the ability to conduct critical mission operations while minimizing, or in some cases eliminating, the need for onboard crew intervention.

Nearly continuous communication coverage is maintained with ISS for voice, telemetry, commanding, and video transfer with the various control centers during crew wake periods. Procedures are designed for Crew, Ground, or Multi-Center execution. Crew procedures depend on existing spacecraft displays for commanding references and data telemetry checks. Ground procedures may rely on additional displays, as well as references to command instances that are not readily available on the spacecraft. There is no existing data path that can join telemetry and commanding with the procedure viewer. Further, there is no existing indication of the current step in progress transferred from crew to ground. Voice call or telemetry indications showing that equipment was affected as intended are used to view progress through a procedure by another user. Execution of a procedure by a ground Flight Controller requires approval from the Flight Director. Upon proceeding into the execution steps, the Flight Controller enables command uplink capability and executes the commands called out in the procedure steps.

Off-nominal events, such as system failures, may create a need to deviate from the original mission plan. Such deviations typically have downstream impacts to plans later in the week or even further in the future. The rest of the FCT works closely in these cases with the Ops Planner to coordinate plan impacts and reschedule events to later opportunities, while still meeting mission objectives and priorities wherever possible. Off-nominal events may also change the environment around the ISS by changing the orientation or configuration of the vehicle. These unplanned and unanalyzed changes are corrected as soon as possible, and post-event analysis is conducted to determine if damage was done to the ISS structure. Future operations may be subjected to additional constraints should analysis indicate that increased protection is necessary. In depth troubleshooting and analysis efforts are a coordinated effort between the FCT and MER in the post-event timeframe.

The Challenge of Distant Destinations

For the last 50 years, NASA's crewed missions have been confined to the Earth-Moon system, where speed-of-light communications delays between crew and ground are practically nonexistent. The close proximity of the crew to the Earth has enabled NASA to operate human space missions primarily from the ground. This "ground-centered" mode of operations has had several advantages: by having a large team of the people involved on the ground, the on-board crew could be smaller, the vehicles could be simpler and lighter, and the mission performed for a lower cost.

The roles and responsibilities of the crews of the future will differ fundamentally from those of the past. Crewmembers will be the primary "doers" for more and more activities, responsible for performing most of the procedures associated with their assigned activities, and completing troubleshooting procedures in response to system failures and medical emergencies. While FCT members are expected to play an active role in some of these procedures as well, overall their role will be more supportive, advising and guiding crewmembers as they went about their activities.

Accompanying this change in role and responsibility is a necessary change in the tools used by crews to manage the mission. With fewer crewmembers onboard spacecraft comes the need to redesign tools used for the FCT, who may have more training and more time to understand the systems. As responsibility for executing the mission shifts to the crew, the technology used to support them must evolve to suit the available time and resources, both computational and cognitive, that spacecraft and crews have to manage the tasks.

The Autonomous Mission Operations Experiment

NASA conducted an experiment assessing crew-ground interaction and operational performance was performed in May and June of 2012 in NASA Johnson Space Center's Deep-Space Habitat (DSH) (Kennedy, 2010; Tri, et al.,2011) an Earth-analog of a workspace and living area that might house a crew during the transport and surface phases of a deep-space crewed mission. Crews consisting of a commander and three flight engineers followed a two-hour mission timeline populated with activities representative of those that might occur during a typical day in the quiescent (cruise) phase of a long-duration space mission. Crews were supported by a small Flight Control Team (FCT) consisting of eight console positions located in the Operations Technology Facility (OTF) in the Christopher Kraft Mission Control Center at Johnson Space Center. The two-hour mission timeline was performed repeatedly under varying conditions:

- A simulated time delay between the ground and the vehicle of low (1.2 or 5 seconds), medium (50 seconds), or long (300 seconds) duration.
- Either no unexpected events (nominal), multiple spacecraft systems failures (off-nominal systems), or a crew medical emergency (off-nominal medical).
- One of two mission operations configurations. In the Baseline configuration, conducted first, the flight control team and crew performed their nominal and off-nominal tasks with support tools, interfaces, and communications protocols similar to those in use for International Space Station operations today. In the Mitigation configuration, crews and FCT members had access to an advanced suite of operations support tools and mission support technologies that we hypothesized would enable the crew to carry out nominal and off-nominal mission operations with greater autonomy and with enhanced crew-ground coordination capability under time delay.

The AMO study complements and extends previous studies (Bleacher et al. 2011; Chappelle et al. 2011; Chappelle et al. 2012; Hurst et al. 2011; Kanas et al. 2010; Kanas et al. 2011) of time delay in ground-based analog environments in a variety of ways. The AMO study is the first of the studies in NASA's Earth-analog environments to examine the effects of time delay in an operational environment that:

- Exclusively utilized highly experienced NASA flight controllers and astronauts as study participants.
- Achieved at least a medium level of mission operational fidelity (as rated by the participants).
- Exclusively employed operations products (plans and procedures) like those used in crewed missions today.

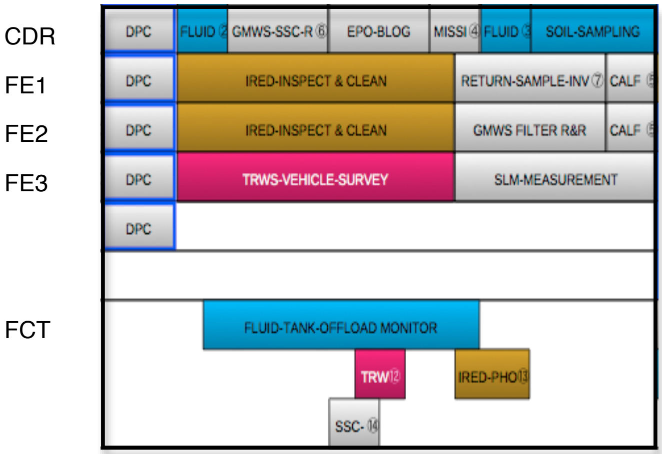


Figure 1. Mission Timeline.

Mission Timeline

The experiment employed variations of a timeline of activities that the crew needed to complete. For the simulation "initial conditions", the vehicle was returning form an asteroid and was in a "quiescent" operational mode, meaning there are no significant, complex or dynamic operations scheduled (i.e. no burns or other maneuvers were planned for the day). The vehicle was in a nominal configuration except for some designated conditions listed below, and there were no previous major systems failures. This timeline was built by hand prior to the experiments and was unchanged during the experiments (even in response to system failures).

The crew's timeline consisted of 12 activities of varying duration during a two-hour period, and is shown in Figure 1. In the Baseline configuration, these activities were preceded by a 10 minute schedule-prepwork activity and a 15 minute Daily Planning Conference (DPC) activity, in which the flight control team briefed the crew on the specifics of the day's timeline. A total of 31 procedures accompanied these activities. These procedures included both nominal and off-nominal procedures for operation of spacecraft subsystems and crew activities. The activities and simulated failures were designed so that coordination was needed between the FCT and the crew, thereby magnifying the impact of time delay.

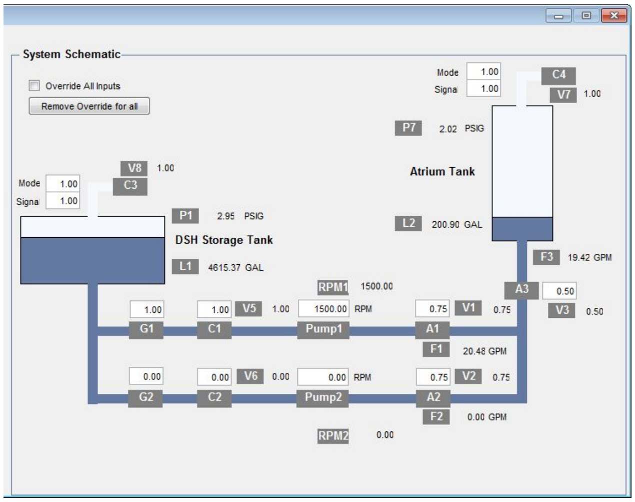


Figure 2. (Simulated) Fluid Transfer System.

The focus of this paper is on the technology used by flight controllers and crew to manage the Atrium Tank Fluid Fill activity (shown in blue), and in handling failures in the spacecraft Electrical Power System (EPS). The fluid transfer system and EPS system are described more fully in the next sections.

Fluid Transfer Activity

The Atrium Tank Fluid Fill activity employed a software simulation of a spacecraft water tank and valve system; the schematic of the system is shown in Figure 2. It consists of a DSH storage tank on the left and Atrium tank on the right. The fluid transfer activity involves transferring fluid from the storage tank to the atrium tank. This is achieved by using redundant transfer lines through a combination of valves and pumps. The G valves represent gate valves that can only be opened or closed manually and can only be controlled to be fully open or fully closed. The C valves represent control valves that can be commanded remotely and can also only be fully open or fully closed. The A valves represent annin valves that can be remotely controlled to any partially open status between 25% and 100%. The pumps can be operated at different RPMs ranging from 0 to 3000. For a nominal fluid transfer operation the main transfer line on the top will be used while the auxiliary transfer line in the bottom is only used in case of contingencies. This activity was planned to take roughly an hour and a half in total.

The Fluids system had associated thresholds, which if exceeded, would produce Caution and Warning messages:

C&W	Threshold
FLOW_HIGH	> 26 GPM
FLOW_LOW	< 10 GPM
FLOW_CHECK	< 12 GPM or > 24GPM
TANK_FULL	>= 100%
TANK_HIGH	> 93%
TANK_LOW	< 10%
TANK_EMPTY	< 3%

Only the flows at the outlet of annin valves and tank levels are measured and simulation is configured to publish only these values to the HDU communication infrastructure. These subsets of sensor locations were chosen to increase the diagnosis ambiguity, which was driven by the experiment design to increase ground/crew interaction. The simulation includes the capability to inject faults. The faults considered were valves stuck in fixed positions, pumps failed or operating at lower efficiency, and sensor faults. Only one fault was introduced in the system at any point in time.

A total of 8 procedures were developed, including both nominal and off-nominal procedures.

Electrical Power System and Wireless Sensors

The DSH EPS system consists of an interconnection of 120Vac, 28Vdc and 24Vdc power sources. These power sources are distributed throughout the inside of the DSH through six Power Distribution Units (PDUs), each of which has 16 outlets. These can be remotely commanded on and off.

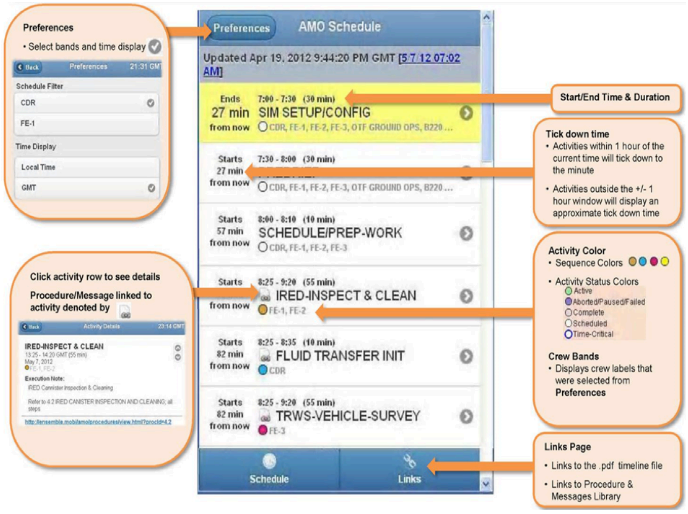
DSH data (temperature and humidity) was collected through a network of Wireless Sensor Nodes (WSNs); these sensors were powered via the DSH power system. They reported data via a Compact Remote I/O (cRIO) card, also powered by the DSH power system.

Failure injection included the ability to fail the 24V converter or part of the cRIO. These failures would also eliminate data delivery via the WSNs, leading to a typical 'C&W storm' for both loss of sensor data as well as loss of power on the various power channels, requiring diagnosis. Individual WSNs also proved unreliable and caused unplanned failures. In the event the cRIO needed to be rebooted, this would take between 15 and 25 minutes, during which no WSN data is available.

A total of 7 EPS procedures were developed, all of which were off-nominal procedures.

Technology Enabling Crew Autonomy

The AMO experiment included a wide range of technologies enabling autonomy; see (Frank et al. 2013) for a more complete discussion. In this paper we focus attention on three key technologies that aided the FCT and crew in executing the plan: Mobile Score, WebPD, and Advanced Caution and Warning (ACAWS). These tools are described in the next section.



Preferences
- Select bands and time display

Click activity row to see details

Procedure/Message linked to activity denoted by

IRED-INSPECT & CLEAN
13:25 - 14:20 GMT (55 min)
May 7, 2012
FE-1, FE-2
Execution Note:
IRED Cannister Inspection & Cleaning
Refer to 4.2 IRED CANISTER INSPECTION AND CLEANING; all steps
http://ensemble.mobi/amo/procedures/view.html?procid=4.2

Updated Apr 19, 2012 9:44:20 PM GMT [5/7/12 07:02 AM]

Ends 27 min from now 7:00 - 7:30 (30 min) SIM SETUP/CONFIG
CDR, FE-1, FE-2, FE-3, OTF GROUND OPS, B220 ...

Starts 27 min from now 7:30 - 8:00 (30 min)
CDR, FE-1, FE-2, FE-3, OTF GROUND OPS, B220 ...

Starts 57 min from now 8:00 - 8:10 (10 min) SCHEDULE/PREP-WORK
CDR, FE-1, FE-2, FE-3

Starts from now 8:25 - 9:20 (55 min) IRED-INSPECT & CLEAN
FE-1, FE-2

Starts 82 min from now 8:25 - 8:35 (10 min) FLUID TRANSFER INIT
CDR

Starts 82 min from now 8:25 - 9:20 (55 min) TRWS-VEHICLE-SURVEY
FE-3

Tick down time
- Activities within 1 hour of the current time will tick down to the minute
- Activities outside the +/- 1 hour window will display an approximate tick down time

Activity Color
- Sequence Colors
- Activity Status Colors
  - Active
  - Aborted/Paused/Failed
  - Complete
  - Scheduled
  - Time-Critical

Crew Bands
- Displays crew labels that were selected from **Preferences**

Links Page
- Links to the .pdf timeline file
- Links to Procedure & Messages Library

Figure 3. Mobile Score.

Mobile Score

Mobile Score is a browser and server based application to provide lightweight display of timeline information, and to provide easy access to procedures and other experiment documentation; an overview of Mobile Score is provided in Figure 3. The FCT and crew used Mobile Score to display the plan, filter plan activities based on assigned crew performing the activity or activity time, show which activities were slated to occur soon, and quickly access procedure references, messages, and other information needed to perform activities. The Mobile Score UI was accessible via modern versions of web browsers like Firefox, or Google Chrome on desktop machines, and using Mobile Safari on the Apple iPads used by the AMO crew members in the DSH.

As mentioned, previously, the timeline was not altered during the experiment; no activities were reordered, added or removed. This was driven by the shortness and simplicity of our experiment timeline, and typical practice for ISS operations today is to limit plan updates to once per day.

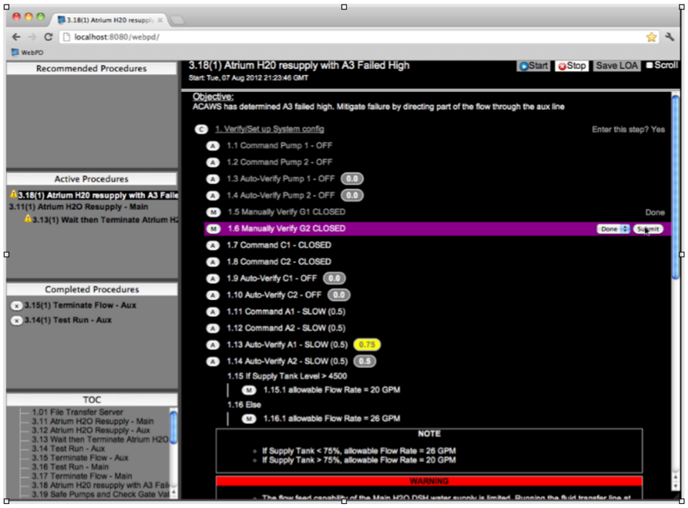
Easy access to procedures, and the AMO Message Library, was available via Mobile Score by selecting Links in the lower right corner. Mobile Score was used by the crew members while they were performing procedures that were being viewed on one of the four crew iPads. During Baseline experiments, crew members would use Mobile Score to navigate to PDF versions of their procedures. During Mitigation, they would use Mobile Score to provide convenient access to the desired procedures within WebPD (see the next section). After selecting a procedure from the index, the crew member could select either the PDF or WebPD version of the procedure. Note also that two separate procedure table-of-content (TOC) lists were available – one accessible from Mobile Score, and another available directly within WebPD. This is because the WebPD TOC also contained engineering procedures that were only intended for the DSH engineering team.

WebPD

The procedures for operating spacecraft systems and performing tasks were presented using an electronic interface called WebPD, shown in Figure 4. These resources were accessible to all team members from their browser, and from the DSH iPads. WebPD incorporated a focus bar, allowing the crew to track their place in a procedure. The crew could issue commands to spacecraft systems from WebPD. Procedure instructions that verify telemetry readings display the current reading along with an indication of whether or not it is in range of the desired value(s). Procedure steps often required reading system data values or checking limits; WebPD receives system data, and these are incorporated in the WebPD interface.

The WebPD allows many users to monitor the execution of all procedures simultaneously. However, only one client, the one that started the procedure, has control of the procedure's execution (e.g. takes input from the user); the others simply track execution and do not allow interaction.

The WebPD presents a list of all available procedures, any of which can be selected for execution at any time, by any user. When a procedure from the list is selected, it is displayed, and can be started with the mouse-click (or finger touch on the iPad) of a button. The WebPD also maintains lists of procedures that are active, completed, and those that have been recommended by the AMO diagnostic tools (described further in a later section). Any number of procedures can be running concurrently and monitored by the WebPD. However, only one procedure can be viewed a time; a single click switches the view to the desired procedure.



3.18(1) Atrium H20 resupply with A3 Failed High
Start: Tue, 07 Aug 2012 21:23:46 GMT

Objective:
ACAWS has determined A3 failed high. Mitigate failure by directing part of the flow through the aux line

C 1. Verify/Set up System config
A 1.1 Command Pump 1 - OFF
A 1.2 Command Pump 2 - OFF
A 1.3 Auto-Verify Pump 1 - OFF 0.0
A 1.4 Auto-Verify Pump 2 - OFF 0.0
M 1.5 Manually Verify G1 CLOSED
M 1.6 Manually Verify G2 CLOSED
A 1.7 Command C1 - CLOSED
A 1.8 Command C2 - CLOSED
A 1.9 Auto-Verify C1 - OFF 0.0
A 1.10 Auto-Verify C2 - OFF 0.0
A 1.11 Command A1 - SLOW (0.5)
A 1.12 Command A2 - SLOW (0.5)
A 1.13 Auto-Verify A1 - SLOW (0.5) 0.75
A 1.14 Auto-Verify A2 - SLOW (0.5) 0.5
1.15 If Supply Tank Level > 4500
M 1.15.1 allowable Flow Rate = 20 GPM
1.16 Else
M 1.16.1 allowable Flow Rate = 26 GPM

NOTE
- If Supply Tank < 75%, allowable Flow Rate = 26 GPM
- If Supply Tank > 75%, allowable Flow Rate = 20 GPM

WARNING

Active Procedures:
3.18(1) Atrium H20 resupply with A3 Faile
3.11(1) Atrium H2O Resupply - Main
3.13(1) Wait then Terminate Atrium H2

Completed Procedures:
3.15(1) Terminate Flow - Aux
3.14(1) Test Run - Aux

TOC:
1.01 File Transfer Server
3.11 Atrium H2O Resupply - Main
3.12 Atrium H2O Resupply - Aux
3.13 Wait then Terminate Atrium H2O
3.14 Test Run - Aux
3.15 Terminate Flow - Aux
3.16 Test Run - Main
3.17 Terminate Flow - Main
3.18 Atrium H20 resupply with A3 Fail
3.19 Safe Pumps and Check Gate Val

Figure 4. WebPD.

WebPD procedures are stored in Procedure Representation Language (PRL), a derivative of XML (Kortenkamp et al. 2008) and developed in a graphical environment called the Procedure Integrated Development Environment (PRIDE) (Izygon et al. 2008). PRL and a predecessor of WebPD have been used in previous simulations of mission operations environments. PRIDE is a graphical tool that allows easy drag-and-drop construction of procedures, in a fashion that only permits procedures with valid structure and content. In particular, the most system-specific procedure content – telemetry and commands – are provided in a system menu and do not need be looked up manually in documents, as was the prior approach. In addition, PRIDE provides a host of GUI features that make procedure authoring convenient. Procedures in PRL can be automatically translated to the Plan Execution Interchange

Language (PLEXIL), which allows instruction-by-instruction automated execution of procedures according to the operator's wishes (Frank 2010).

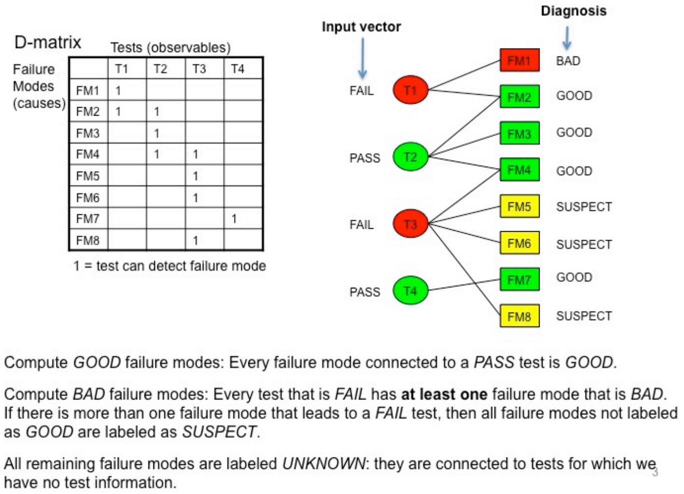
Advanced Caution and Warning

The Advanced Caution & Warning System (ACAWS) for both the fluid transfer simulation and EPS system consists of three main components. A diagnostics engine is responsible for diagnosis of any faults. This includes detection of off nominal behavior, isolating the cause for the off-nominal behavior, and determining the magnitude of the deviation from nominal behavior. A diagnosis to recommended procedure mapper is responsible for recommending disambiguation and/or mitigation procedures to be executed based on the current diagnosis provided. Finally, the ACAWS GUI is responsible for presenting the results from diagnosis and the procedure mapper to the user. Procedure recommendations are also displayed by WebPD. In the following sections we describe the diagnosis engine used to handle failures in that subsystem.

TEAMS

The diagnostics engine for EPS failure utilizes the Qualtech Inc. Testability Engineering and Maintenance System (TEAMS) tool (Mathur et al. 1998). TEAMS determines the root cause (failed components and their failure modes, the "bad" components in the TEAMS vernacular). When the sensor signature is ambiguous, TEAMS provides a list of possibly failed components (the "suspect" set). A companion tool, TEAMATE, provides the operator recommendations on additional observations to perform the most effectively reduce the ambiguity.

TEAMS is a model-based system. The model captures a system's structure, interconnections, tests, procedures, and failures. This dependency model captures the relationships between various system failure modes and system instrumentation.



	T1	T2	T3	T4
FM1	1			
FM2	1	1		
FM3		1		
FM4		1	1	
FM5			1	
FM6			1	
FM7				1
FM8			1	

1 = test can detect failure mode

Compute *GOOD* failure modes: Every failure mode connected to a *PASS* test is *GOOD*.

Compute *BAD* failure modes: Every test that is *FAIL* has **at least one** failure mode that is *BAD*. If there is more than one failure mode that leads to a *FAIL* test, then all failure modes not labeled as *GOOD* are labeled as *SUSPECT*.

All remaining failure modes are labeled *UNKNOWN*: they are connected to tests for which we have no test information.

Figure 5. TEAMS algorithm.

For real-time diagnosis, a dependency matrix (D-matrix) is generated from the model. The D-matrix is a two-dimensional matrix of failure modes and effects ("tests"; things that can be observed). The values are binary with 1 meaning a test can detect a failure mode and 0 meaning that a test cannot detect that failure mode.

Input to TEAMS is a vector of binary health status tests as computed by the DSH software and supplemented by the ACAWS-EPS system. DSH software provides observations on whether certain telemetry parameters are valid and whether they are in bounds. The EPS system input used validity bits for a parameter rather than its actual value, since that provides the information necessary to determine whether an EPS component is being powered. ACAWS-EPS supplements these observations with heartbeat data providing observations on when the last time a component was heard from.

A simple example of how TEAMS uses the D-matrix and tests vector is shown in Figure 5. The D-matrix is shown on the left. The same matrix can be represented by the graph on the right. The input vector is the observed state of the tests. The right column shows the output from TEAMS – a diagnosis that explains the input vector given the D-matrix as generated by the model (not shown). In this case, given the two failed tests and two passed tests, TEAMS has determined that failure-mode-1 is definitely failed ("bad"), failure-modes 2, 3, 4, and 7 are all healthy ("good"), and failure-modes 5, 6, and 8 can each explain failed test T3, hence those three failure modes are placed into an ambiguity group of "suspects." In cases where the

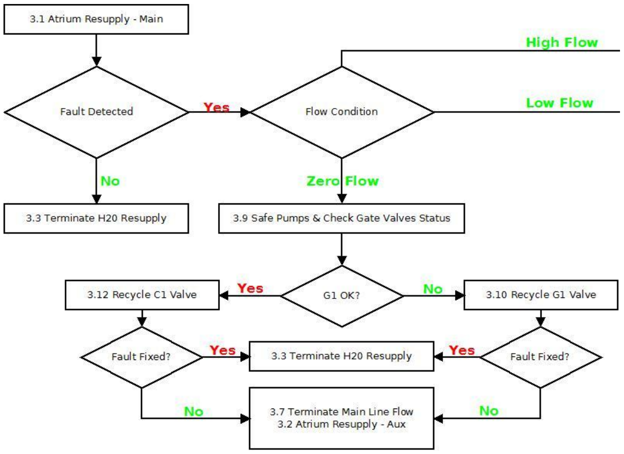


Figure 6. Subset of Fluid ACAWS model Diagnosis to Procedure Mapper.

input vector leads to an ambiguity group, TEAMMATE recommends a procedure that can help disambiguate the suspects. For the DSH system, this was exclusively a request for crew observation of data not available via telemetry, such as the status of an indicator light, the operation of an overhead light, etc. In the D-matrix above, these "manual tests" would be additional columns of the matrix, with mapping from those tests back to the failure modes they can observe or detect.

HyDE

HyDE (Narasimhan and Brownston, 2007) was used for fault detection and isolation of the fluids system. A model in HyDE is a hybrid, consisting of a finite set of states and transitions between those states (a discrete model), as well as sets equations over real-valued quantities that either hold within a state, or can trigger transitions between states (a continuous model). The models describe the behavior of the system under nominal and faulty conditions. HyDE uses commands sent to actual system to drive these models to predict the behavior of the system as it evolves over time. These predictions are checked for consistency with the observations available from the sensors. Any inconsistencies indicate presence of faults in the system. These inconsistencies, if any, are then used in a search to identify cause for the inconsistencies. This is achieved back propagating through the model to identify components in the model contributing to the inconsistency.

For the fluid transfer system HyDE was used to serve two purposes. First a hybrid quantitative model was used as an observer to track the behavior of the system. This observer used the same commands that were being sent to the simulation through the communication interface to predict the expected values for the flows and tank levels. These predictions were compared against sensor observations (available through the communications infrastructure) to generate qualitative symbols indicating low, high and no flow.

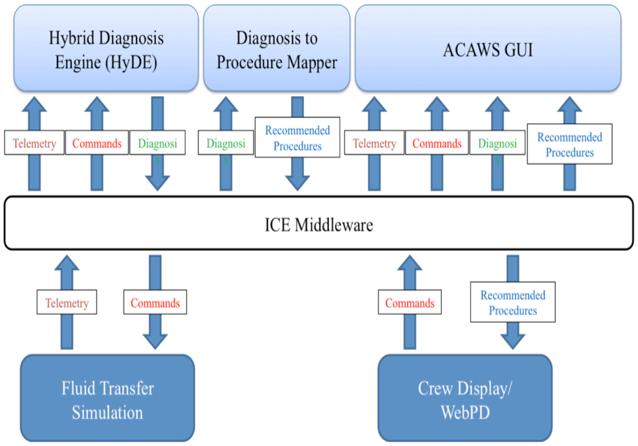


Figure 7. Fluids System ACAWS architecture.

These qualitative symbols are then fed into the qualitative part of the HyDE model which then determines the state of the components and sensors. Once an initial diagnosis has been established HyDE uses a fault disambiguation and mitigation treeto recommend procedures to isolate the fault and mitigate the effects of fault so that the fluid transfer activity can be completed as planned. This tree is generated manually based on the set of faults and ambiguity groups that would be generated by HyDE; a portion of which is illustrated in Figure 6.

Figure 7 shows the architecture of the ACAWS-Fluids system as built for the Atrium fluid transfer system incorporating HyDE. The ACAWS-EPS architecture differs from this in only minor ways (test result input and invocation of TEAMMATE).

Technology Integration

Figure 8 shows how all of these components were integrated for use by the crew and the FCT for the AMO Mitigation Configuration. A crewperson examining the timeline in Mobile Score can automatically invoke WebPD, which would display the procedure corresponding to the activity. The procedure (as written with PRIDE) has all necessary commands and telemetry elements embedded in it; using WebPD, the crew can send commands, check relevant telemetry values, step through the procedure and track the current instruction. Using shared situational awareness between crew and ground, the FCT could monitor procedure progress without the need to bother the crew. In the event of faults, ACAWS would send procedure recommendation messages to the WebPD, prompting the crew to perform a procedure. In cases where a further piece of information was needed (e.g. the crew had to examine a system and manually enter data) the procedure recommendation function was performed by TEAMMATE; in cases where a unique fault diagnosis

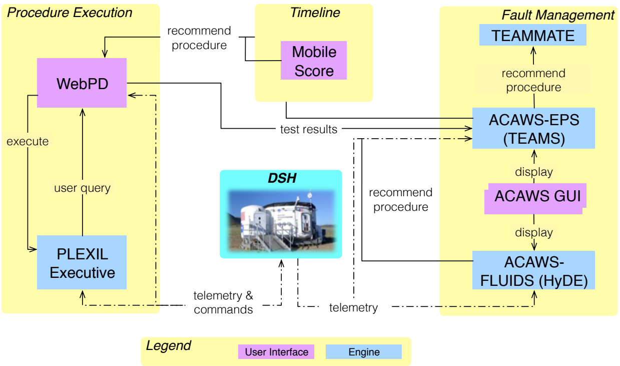


Figure 8. Mitigation Software Integration Architecture.

required a recovery action, this was accomplished by the more generic diagnosis to procedure mapper.

Shared Situational Awareness

WebPD status was shared over the air-ground link, so that the flight control team could see what procedures were executing, and what procedure step the crewperson running a procedure was presently executing. This information was rendered on the same WebPD UI the crew used, albeit after a delay. This is accomplished via a publish-subscribe paradigm, in which the WebPD software on one end of the time delay publishes any change of status (e.g. the execution of a procedure step), which is then received by the WebPD and causes the update of the receiver side. ACAWS was run both onboard and on ground; the same data was ingested and used to perform diagnosis, thereby also providing shared situational awareness.

Failure Scenarios

In this section we describe the specific scenarios during which the plan execution and fault management technology were used during the AMO experiments.

Fluid Transfer System Failures

This is the first activity on the timeline. The crew browses the activity with Mobile Score, and can either bring up the procedure as a PDF file (in Baseline) or navigate to the WebPD (in Mitigation) to initiate the activity.

The fluid transfer activity is initiated through a procedure which first verifies that all components are closed/off and then sets all the annin valves to desired values (based on level in the storage tank) and then opens the main transfer line by opening valves G1 and C1 and setting Pump1 speed to 1500 rpm. Initially while the flow stabilizes a low flow C&W is received, but ignored as per recommendation of the procedure.

After the flow has stabilized, an A1 Valve stuck at 25% fault is injected. This results in a low flow C&W message, which directs the crew to check consistency between the flow sensors. At this point all components in the main transfer line (G1, C1, Pump1, A1, and A3) are suspected to be faulty. The first step of the troubleshooting focuses on the G1 valve. The crew is asked to manually inspect the Gate Valve and report the status. When the G1 status indicates that it is open, the next step is to cycle the C1 valve (in case this gets the C Valve unstuck). When that does not resolve the problem, a test run using the auxiliary line is proposed. The main line components are closed or turned off and the auxiliary line components are opened or turned on. After the flow has stabilized the flow values are checked and indicate that the problem has been resolved. The crew records that one of C1, Pump1 or A1 is faulty and continues the fluid transfer activity using the auxiliary line. Recall that in Baseline, all of this activity is managed by the crew reading the PDF version of the procedure, and using other tools to monitor the status of the fluid system, or command, as needed.

By contrast, in the Mitigation configuration, HyDE is able to use the quantitative and dynamic information from the changes in the flow to determine that Pump1, A1 or A3 is causing the low flow. In addition HyDE is also able to provide estimates for the fault magnitude. The crew can see the fault candidates on the Fluids ACAWS system animated schematic of the Fluid system. Based on this diagnosis HyDE recommends a procedure to perform Test Run using Aux procedure. This recommendation is received by WebPD. All commands and data are fully integrated, so the crew can execute this procedure from WebPD, without referring to other tools. When this procedure is executed all the flows get back to normal and so HyDE does not recommend any more procedures. Steps involving troubleshooting G1 and C1 valves can be completely skipped because of the additional information available. This configuration was not completed in time for the AMO experiments, was implemented later (along with fully automated procedure execution) and is described further in [20].

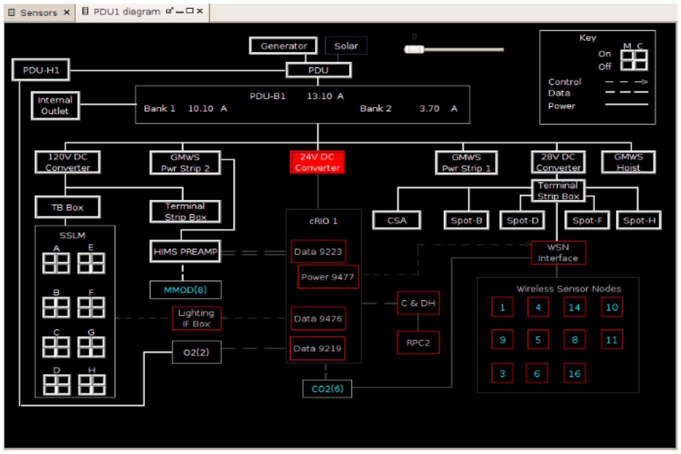


Figure 9. ACAWS EPS UI.

EPS System Failures

The EPS system and WSNs are organized in such a way that, initially, a 24Vdc converter failure and a cRIO card failure all exhibit the same symptoms, namely, loss of data from all of the WSNs. This is distinguished from individual WSN failures. The 24Vdc converter has an LED that the crew can inspect manually, which disambiguates a 24Vdc failure from a cRIO card failure.

In the Baseline configuration, the crew's indication of a problem is loss of data from some or all of the WSNs and the accompanying 'C&W' storm. The 28Vdc failure has a similar flavor to the 24Vdc failure. The crew had procedures available to handle this problem, but it was not actually introduced in simulation. The crew was trained on the EPS procedures, and would then have to call up the relevant EPS procedures and determine whether the problem was one or more WSN failures, a failure of the 24Vdc, the 28Vdc, or the cRIO card.

By contrast, in the Mitigation configuration, the crew had access via the ACAWS-EPS system to an animated schematic of the EPS system that was informed by the TEAMS model. This UI rendered the diagnoses produced by TEAMS. In addition, the procedure mapper would send recommended procedures to WebPD, which reduced the amount of time needed for the crew to bring up relevant procedures to run. As the crew executed steps and provided the answers to the diagnostics questions, ACAWS would automatically refine its diagnosis, render this on the UI, and then produce new procedure recommendations, which would appear in WebPD. Finally, with commands and data integrated into the WebPD, the crew could issue commands and read telemetry directly in WebPD instead of turning to other software tools to command the EPS system. The ACAWS-EPS UI is shown in Figure 9.

Measuring the Impact

The AMO experiment incorporated both qualitative and quantitative measurements to assess the impact of time delay and the impact of the Baseline vs Mitigation configuration on operator performance. Since this paper is focused on a subset of all of the protocols and technologies used in the Mitigation configuration we focus attention on a subset of the performance impact story; a more complete description of the experiment and the results can be found in (Frank et al. 2013).

Quantitative Impact

Quantitative performance measures for the experiment included task completion rates, crew and flight controller workload, and crew-flight controller coordination difficulty; discussions of how these metrics are collected can be found in (McCandless et al. 2005, McCann et al. 2006). Task completion rates, surprisingly, did not vary significantly between Baseline and Mitigation configuration. However, FCT and crew measurements of workload and coordination difficulty were positively impacted:

- Workload and coordination difficulty *decreased* at every time delay as a result of the Mitigation configuration.
- Communications acts *decreased* in the Mitigation configuration.

It is notable that ACAWS also rendered some procedure steps and some procedures performed in the Baseline tests unnecessary. For example, because of HyDE's capability to maintain the current state of the system and the ability to fuse multiple sensors, steps associated with checking for consistency among sensors can be eliminated. This also enabled revision of the set of procedures to a simpler and more concise set. Similarly, TEAMS replaced procedure steps to both determine the likely EPS failure causes, and the TEAMMATE component automatically recommended both fault isolation and recovery procedures.

Qualitative Impact

Along with the quantitative measurements described above, experiment participants provided subjective comments on their experiences with the technology.

ACAWS technology provided two different forms of automated assistance with FDIR activities: Automated fault diagnosis, and automated recommendation of fault isolation or recovery procedures. Comments indicate both workload reduction and a reduction in the need for coordination followed from these capabilities:

"ACAWS provided useful direction for the crew, so there was little need for us to do anything other than concur"

"ACAWS told me which procedure to work which the ground later confirmed but I had already completed the procedure."

The last quote speaks to both the situation awareness and autonomy issues, and also notes the benefits of greater autonomy for mitigating the effects of time delay:

"The time delay had little impact because ACAWS ran most of the procedure. Since the ground and crew can follow ACAWS, it was pretty seamless. MCC and DSH were able to come to common agreement with ACAWS. MCC and DSH statused each other via voice calls and texting."

The following are two highly representative comments about the benefits of WebPD from FCT members:

"WebPD made it very easy to follow along in the procedures even with the time delay"

"Very easy to see where the crew should go from the line they were on as well as where they were going".

"The ability to track procedures and where the crew was in each step was awesome".

Not only did WebPD help the ground keep track of where the crew with within a procedure, but several mentions were made of the usefulness of the windows that showed what procedures were currently active, and which procedures had been completed:

"[I liked] [Ability to] see when crew brings up and starts a procedure, can see when they are done with a procedure."

Conclusions and Future Work

Human spaceflight missions to distant destinations impose significant added burdens on the FCT and the crew. The AMO experiment quantified these burdens, and showed that a tight integration of plan execution tracking (Timeline and procedures) and ACAWS provided both qualitative and quantitative benefits to both the FCT and crew during quiescent mission phases.

Extending these benefits to more systems, increasing automation, and conducting experiments in higher fidelity settings are the subject of future work.

Acknowledgements

The AMO experiment could not have been conducted without the dedication of dozens of people at NASA ARC, JSC and KSC. The AMO project was funded by the NASA Advanced Exploration Systems (AES) Program.

References

J.E. Bleacher, J.M. Hurtado, Jr., K.E. Young J. Rice, W.B. Garry, and D. Eppler. Desert Rats 2010 Operations Tests: Insights from the Geology Crew Members. Proceedings of the 42d Lunar and Planetary Sciences Conference, 2011.

Chappelle, S. Andrew F. Abercromby, Ph.D., Michael L. Gernhardt, Ph.D. NEEMO 15: Evaluation of Human Exploration Systems for Near Earth Asteroids. Proceedings of the Global Space Exploration Conference, 2012.

Steven P. Chappell, Andrew F. Abercromby, William L. Todd, Michael L. Gernhardt. Final Report of NEEMO 14: Evaluation of a Space Exploration Vehicle, Cargo Lander, and Crew Lander during Simulated Partial-gravity Exploration and Construction Task. NASA Technical Report 2011-216152, 2011.

Frank, J. When Plans are Executed by Mice and Men. Proceedings of the IEEE Aerospace conference, Big Sky, MT. 2010.

Izygon, M., Kortenkamp, D., Molin, A., A Procedure Integrated Development Environment for Future Spacecraft and Habitats. Space Technology and Applications International Forum, Albuquerque, NM, 2008.

V. W. Hurst IV, S. Peterson, M.D. K. Garcia, A. Sargsyan, D. Ebert, D. Ham, B.S. D. Amponsah. S. Dulchavsky, Smart Ultrasound Remote Guidance Experiment (SURGE) –Ultrasound Image Collection during Lunar and Near Earth Orbit Space Missions. 82nd Annual Scientific Meeting of the Aerospace Medical Association; 8-12 Mayu 2011; Anchorage, AK; United States

Kanas, N., Saylor, S., Harris, M., Neylan, T., Boyd, J., Weiss, D., Baskin, P., Cook, C., Marmar, C. High vs. Low Crewmember Autonomy in Space Simulation Environments. Acta Astronautica, v. 67, no. 7-8, 2010 p. 731 - 738

Kanas, N., Harris, M., Neylan, T., Boyd, J., Weiss, D., Cook, C., Saylor, S. High vs. Low Crewmember Autonomy during a 105-day Mars Simulation Mission. Acta Astronautica, v. 69, no. 7-8, 2011 p. 240 – 244

Kennedy, Kriss J. NASA Habitat Demonstration Unit Project – Deep Space Habitat Overview. 41st International Conference on Environmental Systems (ICES), Portland, Oregon, USA, 17-21 July 2011.

Kortenkamp, D., Verma, V., Dalal, K.M., Bonasso, R.P., Schreckenghost, D., Wang, L., A Procedure Representation Language for Human Space Flight Operations. 9th International Symposium on Artificial Intelligence, Robotics, and Automation for Space, Los Angeles, CA, 2008.

A. Mathur, S. Deb, and K. Pattipati. Modeling and Real-Time Diagnostics in TEAMS-RT. Proc. American Control Conf., IEEE Press, 1998, pp. 1610–1614.

McCandless, J. W., McCann, R. S., Berumen, K. W., Gauvain, S. S., Palmer, V. J., Stahl, W. D., & Hamilton, A. S (2005). Evaluation of the Space Shuttle Cockpit Avionics Upgrade (CAU) Displays. In Proceedings of the 49th Annual Meeting of the Human Factors and Ergonomics Society.

McCann, R. S., Beutter, B. R., Matessa, M., McCandless, J. W., Spirkovska, L., Liston, D., Hayashi, M., Huember, V., Lachter, J., Ravinder, U., Elkins, S., Renema, F., Lawrence, R., & Hamilton, A. (2006). Evaluation of an Onboard Real-Time Fault Management Support System for Next-Generation Space Vehicles. Report to the Human Research Program

Tri, T., Kennedy, K., Toups, L., Gill, T., Howe, A. S. Planning and Logistics for the In-Field Demonstration of NASA's Habitat Demonstration Unit (HDU) Pressurized Excursion Module (PEM) at Desert Rats 2010. Proceedings of the International Conference on Environmental Systems, Portland OR. 2011.

Frank, J., Spirkovska, L., McCann, R., Pohlkamp, K., Wang, L., Morin, L. Autonomous Mission Operations. Proceedings of the IEEE Aerospace Conference. 2013.

Narasimhan, S., Gonzalez, R., Spirkovska, L., McCann, R., Frank, J., Lee, C. Advanced Caution & Warning System for Simulated Fluid Transfer Subsystem of a Deep Space Habitat. Proceedings of the 23d International Workshop on the Principles of Diagnosis. 2012.

Narasimhan S and Brownston L (2007), "*HyDE – A General Framework for Stochastic and Hybrid Model-based Diagnosis*", In 18th International Workshop on Principles of Diagnosis (DX 07). June, 2007, pp. 162-169.