project that is delivering and installing several unique capabilities, systems, and infrastructure. These capabilities, systems, and infrastructure will be permanently located at the SCV Cryogenic Loading Facility (CLF).

Figure 5. LO2 DTS Vehicle Simulator

5.2. Application Software Model: UPSS/Iron Rocket Simulator

This computer software configuration item (CSCI) simulates the UPSS and Iron Rocket systems for testing purposes. The simulator uses the FlowMaster COTS tool to model the UPSS and Iron Rocket systems (see Figure 6) and generate high-fidelity data that corresponds to various predefined nominal and off-nominal test scenarios. It then uses this data during testing to provide the appropriate telemetry data in response to AOS commands.

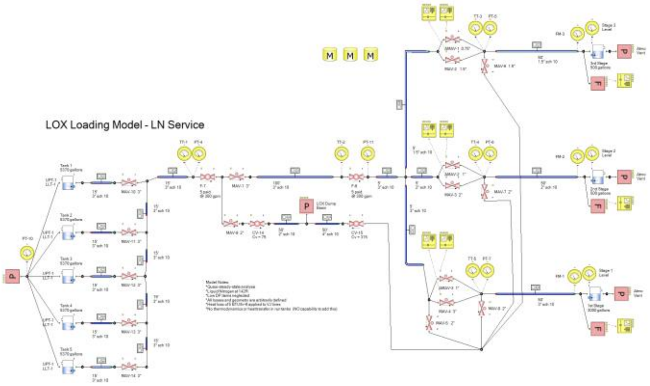


Figure 6. UPSS and Iron Rocket FlowMaster Model

6. TEST ARTICLE ARCHITECTURE

In order to successfully demonstrate the capabilities of Autonomous Operations System, several hardware and software components are used for testing different phases of the development. By means of testing the software in different phases, the AOS will accomplish a validation and verification process that is required to connect with other external systems.

6.1. AOS Application Development System

The AOS Application Development System is composed of a main computer for software development with four monitors for displaying data, visualization, domain maps and programmable code. In this computer system, the main application for controlling and monitoring the cryogenics propellant transfer for AOS is being developed. Within its local configuration, the knowledge of the system is being created by transferring mechanical, electrical and communication schematics into a domain map system. This domain map system receives data for the outside systems (PLC, UPSS/Iron Rocket Simulator, and Gateway) and feeds different subsystems (health management, automated sequencer control, etc.).

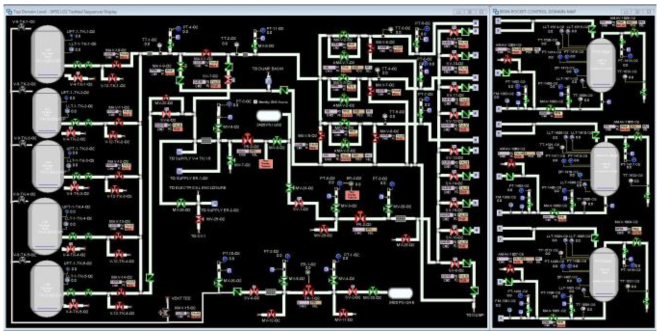


Figure 7. UPSS and Iron Rocket Control Map

The development of several subsystems within the AOS Application includes a visual representation of the domain map for commanding and control (see Figure **7**), an automatic sequencer controller (Figure 8), health management subsystems and plotting features.

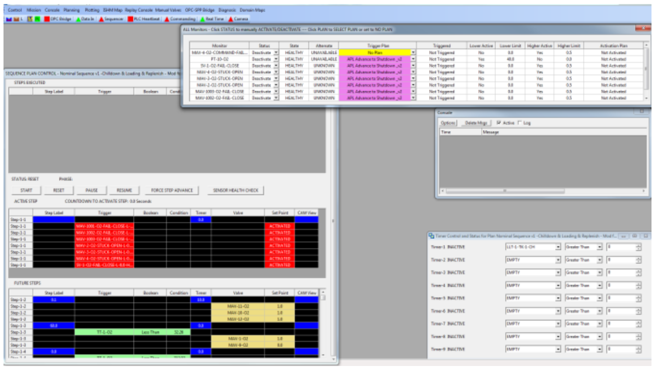


Figure 8. Automatic Sequencer Controller, Redline Monitoring, Timers, Console and Operations Display

6.2. AOS Bridge Development System

The AOS Bridge Development system is composed of an AOS bridge development main computer and a secondary computer used to run a basic User Datagram Protocol (UDP) server to test AOS bridge communications. In the main computer, the bridge code for the AOS Application is being developed. The development of the bridge code includes the capability of receiving telemetry and sending commands to a generic UDP server. The second computer running the generic UDP Server will provide a “test” network connectionless interface similar to the SPP to Common Industrial Protocol (CIP) Gateway code that the AOS Bridge will eventually connect to for PLC (Programmable Logic Controller) data. This generic UDP server will serve as an initial testing server to validate AOS communication code for a future integration with the SPP to CIP Gateway.

6.3. PLC Development System

The PLC Development System is composed of a set of six PLCs and a main computer for development. In this main computer, the code is being developed to send and receive data to the PLCs by means of Compact Unique Identifiers (CUIs). The software RSLogix 5000 is being used to program the PLC. In addition, Labview is being used as a secondary software application to develop a low fidelity simulator capable of supporting telemetry and commanding across the network. The low fidelity simulator allows modification to telemetry values of the different CUIs programmed in the PLC as well as displaying commands being received by the PLC across the network (see Figure 9).

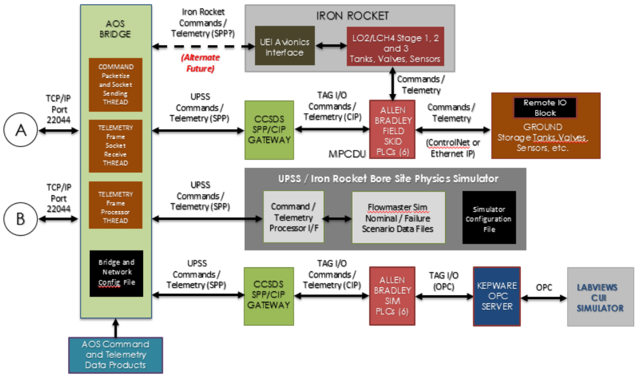


Figure 9. AOS Network Architecture with AOS Bridge connected to LabView Simulator and UPSS/Iron Rocket Simulator

7. TEST RESULTS

For testing the UPSS and Iron Rocket application developed using the Autonomous Operations System, the UPSS and Iron Rocket Simulator was used to provide a physics-based telemetry responses according to application commands. Several strategies for propellant loading transfer were explored to develop a nominal and off-nominal plan for cryogenic propellant transfer. For testing purposes, the physics-based model simulated liquid nitrogen (LN2) as the cryogenic commodity.

7.1. Nominal Operation Test Case

7.1.1. Chilldown

During the chilldown phase, liquid nitrogen is used to decrease the temperature of the system to a cryogenic liquid nitrogen temperature range (-321 °F). During this phase, liquid nitrogen is transferred from the three storage tanks to the vehicle interface valve. Boil-off gas generated during the cool down process is relieved through valves that are redirected to the exhaust line on the system. Once the main tank downstream temperature sensor (TT-1-O2 from Figure **7**) reaches cryogenic temperature, the main block valve (MAV-1-O2 from Figure **7**) is opened to allow cryogenic flow across the piping system from storage tanks up the vehicle interface (see Figure 10).

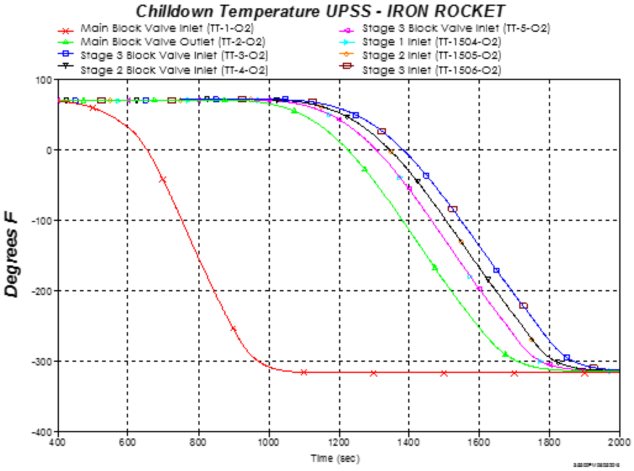


Figure 10. Chilldown Temperature: UPSS - Iron Rocket

7.1.2. Slow-Fast Fill

During this phase, the ullage pressure on the cryogenic storage tank is increased by means of a Pressure Building Unit (PBU) up to 50 psig to pressure-feed the system and increase the flow rate to the Stage 1 vehicle tank. The fill process for the vehicle tanks is a serial process. Once the Stage 1 is up to 100% full (see Figure 11), the other tanks follow the fill process (starting from Stage 2 followed by Stage 3) and Stage 1 enters into a replenish state.

7.1.3. Replenish

During this phase, a maximum tank fill level is achieved by the cryogenic commodity and a replenish algorithm is enabled (see Figure 12). This replenish algorithm monitors the Stage 1 tank level and commands a replenish valve (AMAV-3-O2 from Figure **7**). This replenish valve is controlled by a replenish algorithm that is executed by the Sequencer. This algorithm commands the replenish valve to open to 50% once the liquid level sensor (LLT-1604-O2) falls below 99.5%. This decrease in liquid level is due to boil-off of cryogenic commodity being excessed across the vent valve of the vehicle tank.

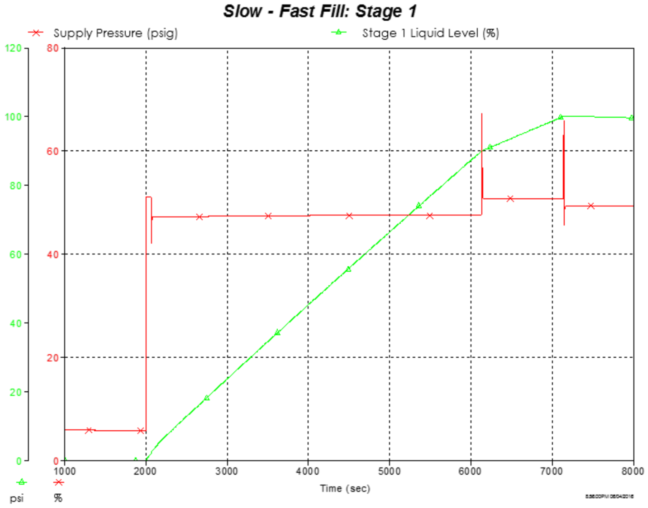


Figure 11. Slow-Fast Fill: Stage 1

Opening the replenish valve allows more cryogenic commodity into the vehicle tank. On the other side of the spectrum, if the liquid level surpasses beyond 100.5%, the replenish valve is commanded to close (0%). Over time, the loss in mass due to the venting of boil-off gases produces a decrease in liquid level of the vehicle tank and the replenish algorithm enters a new cycle. During nominal operations, the vehicle tank for Stage 1 undergoes for 1 cycle of the replenish state.

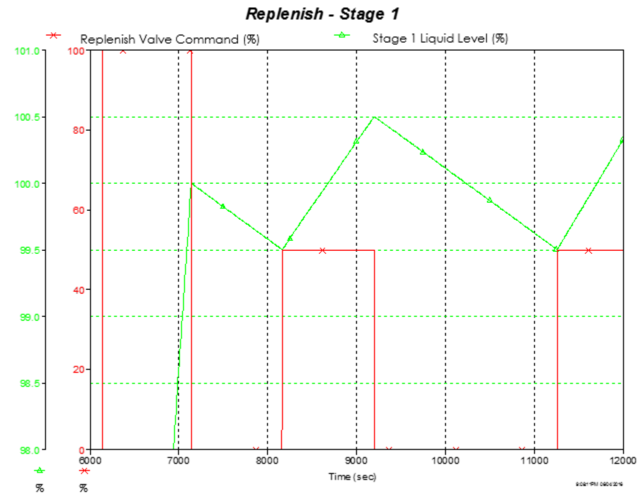


Figure 12. Replenish - Stage 1

This cyclic process is dependent on the conditions for the nominal operations. This process mimics a real launch operation where a real vehicle might stay in the launching platform for hours while maintaining liquid level conditions until vehicle launch. A typical launch vehicle undergoes several cycles to maintain required launch conditions while other parallel operations take place in preparation for launch.

7.2. Serial Loading Vehicle Stage 1, 2, and 3

Similar to stage 1, the cryogenic propellant loading process for the stage 2 and stage 3 transitions to a replenish state once the liquid level for both tanks reaches 100%. In a serial manner, the stage 2 reaches 100% liquid level after the stage 1. Once on the replenish state, stage 2 executes 7 cycles during the nominal loading process. The difference in the amount of cycles is due to the volumetric capacity of the tanks: Stage 1, 2 and 3 have a capacity of 3000, 500 and 500 gallons respectively. The difference on specific heat for the 3 cryogenic tanks produces a difference in boil-off rate. For the smaller tanks (stage 2, 3), a higher boil-off rate is produced which generates a faster decrease in liquid level. The Sequencer commands the replenish valve for all the stages in a parallel execution algorithm which is constantly monitoring all the liquid level sensors (LLT-1604-O2, LLT-1609-O2, and LLT-1614-O2).

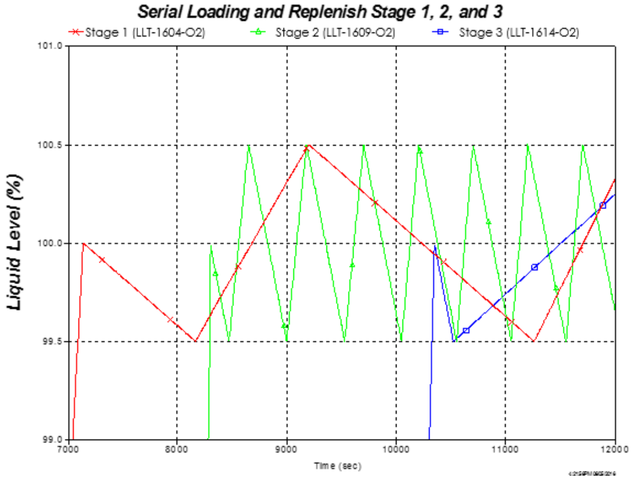


Figure 13. Serial Loading and Replenish for Stage 1, 2, and 3

7.3. Off-Nominal Operation Test Case

These tests will consist of a nominal loading operation followed by inserting preplanned anomalies into the simulation. Similar to previous off-nominal tests executed during the technology maturation of AOS in its first use on the Cryogenics Test Laboratory, common failure modes using a 3-stage loading sequence utilizing fully autonomous sequencing have been identified. As part of the off-nominal case scenarios for instrumentation-only failures, APL will identify the failure and allow the loading operation to continue; for failures requiring safing, APL will safe the system while identifying the fault condition to the operator. The simulator and system testing with UPSS/DTS will confirm these critical mitigation functions are working properly.

7.3.1. Non-safety Critical Failure: Instrumentation Failure

Non-safety critical failure can be categorized as hardware component failure that does not cause a catastrophic damage to the mechanical system or pose a risk to the mission. For instrumentation failure, the open indicator for the stage 1 inlet valve (MAV-1001-O2) is tested. This discrete open position indication is channelized with two different telemetry data objects. One signal provides a primary reading and another signal provides secondary (redundant) reading. The domain object elements have been modeled to correctly represent the physical behavior of a redundant signal system. In the real-hardware, the sensor is connected to two sets of PLCs. In this particular case, an instrumentation failure provides indication of a failure of one PLC. For this case, the primary reading was selected to fail by a signal loss action which produces a discrepancy in telemetry for the discrete position open indicator.

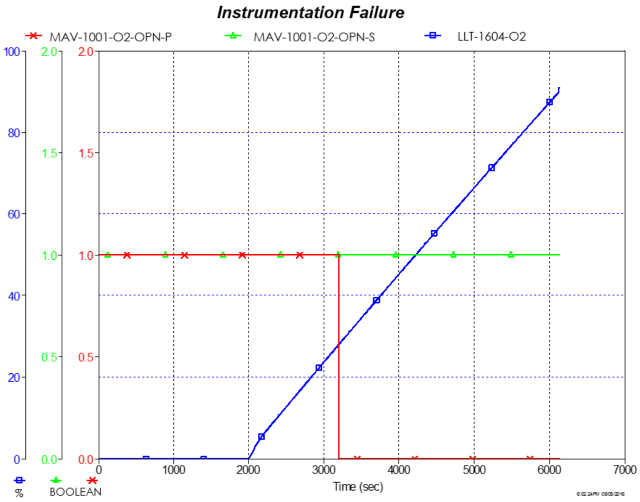
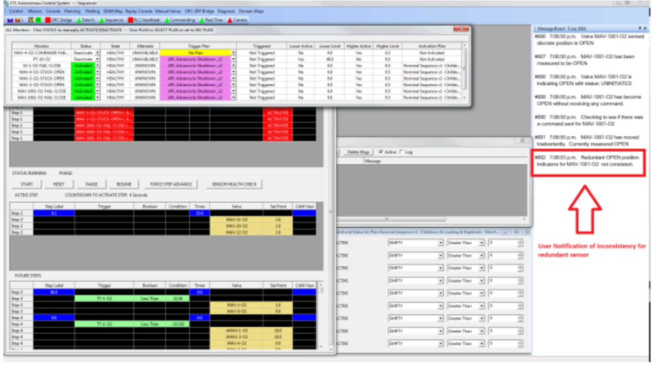


Figure 14. Instrumentation Failure. MAV-1001-O2-OPN-P: Primary Signal, MAV-1001-O2-OPN-S: Secondary Signal, LLT-1604-O2: Stage 1 Liquid Level Sensor

In Figure 14 the primary signal for the position indicator of MAV-1001-O2 shows an open state (Boolean Flag = 1.0). Similarly, the secondary signal for the position indicator initially shows an open state. During the loading of the stage 1 vehicle tank represented by LTT-1604-O2, the primary position indicator shows a close state (Boolean Flag = 0.0) while the secondary indicator shows an open state when the stage 1 tank is about 30% full.

The redundancy models, which are being executed on an asynchronous execution, are triggered once an event is detected. An evaluation of the telemetry produced several conclusions. First, the valve has moved inadvertently due to a change in the open indicator. Second, a redundant open position indicator for the valve in question is not consistent (see Figure 15). The mitigation procedure for this injected failure is to notify the operator of the instrumentation failure only and continue with nominal operations since instrumentation failure is being mitigated by a secondary sensor. The continuation of the nominal operations plan can be reflected on Figure 14 by observing that the stage 1 liquid level keeps increasing beyond 30% after the time segment (about 3200 seconds) that the open position telemetry inconsistency was found.


Message Board 5 Jun 2015

#886 7:06:50 p.m. Valve MAV-1001-O2 sensed discrete position is OPEN

#887 7:06:50 p.m. MAV-1001-O2 has been measured to be OPEN

#888 7:06:50 p.m. Valve MAV-1001-O2 is indicating OPEN with status: UNINITIATED

#889 7:06:50 p.m. MAV-1001-O2 has become OPEN without receiving any command.

#890 7:06:50 p.m. Checking to see if there was a command sent for MAV-1001-O2

#891 7:06:50 p.m. MAV-1001-O2 has moved inadvertently. Currently measured OPEN

#892 7:06:53 p.m. Redundant OPEN position indicators for MAV-1001-O2 not consistent.

User Notification of inconsistency for redundant sensor

Figure 15. AOS response to instrumentation failure during nominal operations.

7.3.2. Safety Critical Failure: Main valve mechanical failure

Safety critical failures can be categorized as hardware component failures that cause catastrophic damage to the mechanical system and poses a risk to the mission if being operated during a nominal operation. For this failure, the main fill valve for stage 1 tank (MAV-4-O2) has been selected. MAV-4-O2 has several telemetry components. A valve command signal which received the desired valve command and executes the command, a command response telemetry which acknowledges that the command signal is being received by the PLC, an open indicator, and a closed indicator.

During a Failure Mode Effect Analysis (FMEA), MAV-4-O2 was identified as a critical component during the cryogenic propellant transfer operations. Several failure modes have been identified associated with this valve. The selected failure mode present in this paper is a mode where the valve fails to respond to a given command, which can cause a catastrophic failure during cryogenic loading operation.

For the selected failure mode, the valve is commanded to a closed position after being open during a fast fill phase. Several responses are expected after a close command for this type of valve:

1. PLC acknowledges that the command closed has been received
2. Open indicator shows a 0.0 value in telemetry. This open indicator is a limit switch that turns on or off once the valve stem travels up or down,

respectively. Open indicator equals 1.0 when the valve is open and 0.0 when valve is closed.

3. Closed indicator shows a 1.0 values in telemetry. This closed indicator is a limit switch that turns on or off once the valve stem travels down or up, respectively. Closed indicator equals 1.0 when the valve is closed and 0.0 when valve is open.

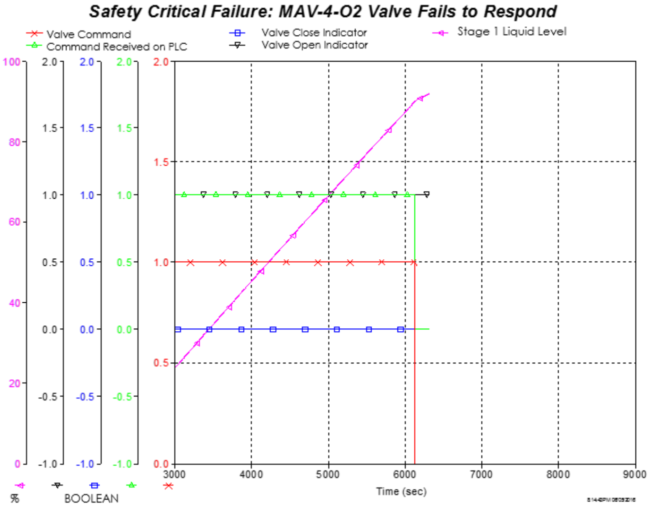


Figure 16. Safety critical failure for main fill stage 1 valve

In Figure 16 the valve in question is commanded closed at the end of the stage 1 fill phase. In nominal operations, after stage 1 reaches 100% on the liquid level sensor the main fill valves closes and the nominal plan transitions to a replenish state. In this particular scenario, the following telemetry is received after the main fill valve is commanded closed and a nominal valve travel time have elapsed:

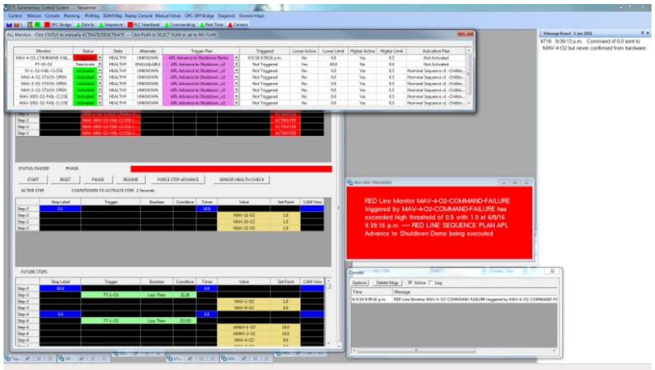
1. PLC acknowledges that the command 'CLOSE' has been received

2. Open indicator shows a 1.0 value in telemetry. This indicates the valve is open.

3. Close indicator shows a 0.0 values in telemetry. This indicates the valve is open.

Based on the failure analysis, the valve has failed to close and all telemetry indicates that even if the command was received by the PLC, the valve remains in its original position. In this case, if valve does not close, there exists a potential to overfill the stage and send liquid into the vent line which may result in a catastrophic failure.

This failure scenario has been modeled in AOS and a response to protect the system has been programed. Figure 17 shows the system response of AOS to the described failure. Once the failure is detected, the model triggers a flag which is being monitored by Redline Monitoring. The redline monitoring evaluates the received flag with the established threshold and triggers the redline. The redline violation generates an automated response to stop any current plan execution and proceeds to execute any mitigation plan associated with the redline monitor. For this particular case, the mitigation plan represents a series of commands to be executed with the purpose of shutting down the nominal operation and protecting the system from any catastrophic failure. In addition, the operator receives a notification that shows a brief description of the event, time of trigger and automated mitigation plan to be executed.



RED Line Monitor MAV-4-O2-COMMAND-FAILURE triggered by MAV-4-O2-COMMAND-FAILURE has exceeded high threshold of 0.5 with 1.0 at 6/8/16 9:39:16 p.m. — RED LINE SEQUENCE PLAN APL Advance to Shutdown Demo being executed

Figure 17. AOS response to safety critical failure of main stage 1 fill valve not responding to commands.

8. CONCLUSIONS

The AOS has proven to be a fully autonomous control software capable of integrating automated control with ISHM to command and control cryogenic propellant loading operations under a safe environment. The APL has given AOS the incentive to evolve from its previous version meant for laboratory only operations and expand its capabilities to encompass the necessary components and features needed to command and control ground support equipment (GSE) that is currently undergoing Class B Safety Critical certification for future application on flight hardware.

The complexity of GSE capable of supporting flight hardware increases the need to improve robustness on a command and control system. In addition, it motivates the development of a real-time response system capable of ensuring safe operations even on the unforeseen circumstances where a critical failure may occur.

AOS has made possible an increase in the NASA Technology Readiness Level (TRL) from validation in laboratory environment (Level 4) to validation in relevant environments (Level 5). Current efforts are aimed to increase the TRL to produce a product relevant to ground or space environment (Level 6) and generalize the capabilities to be applicable to a wide variety of industrial systems. In addition, modifications and redesign of AOS are aimed to grant a software safety critical Class B classification under a new software called Autonomous Operations Mission Development Suite (AO MDS).

ACKNOWLEDGMENTS

The authors of this paper will like to thank Mark Turowski and Justin Junell for providing a UPSS and Iron Rocket model and communications simulator used to validate operations performed with AOS. Recognition is due to all the people who worked in development and validation of the technology reported in this paper: John (Jay) Gurecki, Justin Youney, Johanna Johnson, Caylyne Shelton, Scott Ditto, David Moyer, Fernando Figueroa, and Robert Johnson.

Support for this work was provided by NASA Advanced Exploration Systems under the leadership of Jason Crusan and Richard McGuinnis.

NOMENCLATURE

ACS	Automated Control Sequencer
AOS	Autonomous Operations System
AO MDS	Autonomous Operations Mission Development Suite
APL	Autonomous Propellant Loading
CIP	Common Industrial Protocol
CLF	Cryogenic Loading Facility
COTS	Commercial-Off-The-Shelf
CSCI	Computer Software Configuration Item
CTL	Cryogenics Test Laboratory
CUI	Compact Unique Identifier
DAQ	Data Acquisition
DTS	Development Test Site
FMEA	Failure Mode Effect Analysis
GHe	Gaseous Helium
GN2	Gaseous Nitrogen
GSE	Ground Support Equipment
GSI	G2 Gateway Standard Interface
GUIs	Graphical User Interfaces
IDE	Integrated Development Environment
ISHM	Integrated System Health Management
KB	Knowledge Base
LCH4	Liquid Methane
LN2	Liquid Nitrogen
LO2	Liquid Oxygen
MPCDU	Mobile Power and Communication Distribution Unit
PHM	Prognostics and Health Monitoring
PLC	Programmable Logic Controller
SCV	Small Class Vehicle
SPP	Space Packet Protocol
SSME	Space Shuttle Main Engine
TCP/IP	Transmission Control Protocol/Internet Protocol
TRL	NASA Technology Readiness Level
UDP	User Datagram Protocol
UPSS	Universal Propellant Servicing System

REFERENCES

Davidson M., Stephens J., (2004) *Advanced Health Management System for the Space Shuttle Main Engine*. 40th AIAA/ASME/SAE/ASEE Join Propulsion Conference and Exhibit 11-14 July 2004, Fort Lauderdale, Florida.

Walker M., (2010). *Next generation prognostics and health management for unmanned aircraft*. IEEE Aerospace Conference, 6-13 March 2010 Big Sky, Montana.

Figueroa F., Melcher K. (2001). *Integrated Systems Health Management for Intelligent Systems*. Infotech@Aerospace 2011, 29-31 March 2011, St. Louis Missouri.

Antsaklis P. J., Passino K. M., Wang S. J., (1991). *An Introduction to Autonomous Control Systems*. IEEE control systems 11(4)

Rafeed Leon H. M., Shoeb A., Rahman S., Ahmed M. U., Islam S., (2016). *Design and economic feasibility analysis of autonomous hybrid energy system for rural Bangladesh*. 2016 4th International Conference on the Development in the Renewable Energy Technology (ICDRET) 7-9 Jan. 2016, Dhaka

Venkatesh, M., Kapadia R., Walker M., Wilkins K., (2013). Integrated Systems Health Mangement (ISHM) Toolkit. NASA Tech Briefs, January 2013; 23.