

Title: Ares I-X Software Assurance Plan	Date: February 19, 2008	Page 1 of 12
Document No.: AI1-SYS-SAP	Revision: 1.00	



AI1-SYS-SAP

VERSION 1.00

National Aeronautics and
Space Administration

RELEASE DATE: FEBRUARY 19, 2008

ARES I-X

SOFTWARE ASSURANCE PLAN

Approved for Public Release; Distribution is Unlimited



Title: Ares I-X Software Assurance Plan	Date: February 19, 2008	Document Owner: Robert DeCoursey
Document No.: AI1-SYS-SAP	Version: Version 1.00	

REVISION HISTORY TABLE

	Date	Description
Version 0.1	January 2007	Draft Release for comments
Version 0.2	February 2007	Version .2
Version 0.3	April 2007	Version .3
Version 0.4	January 2008	Version .4 includes KSC and IV&V updates
Version 1.0	January 2008	Release version for XCB review
Version 1.1	February 2008	Edits following initial XCB brief-unofficial version
Baseline v 1.00	February 19, 2008	XCB approved document

Title: Ares I-X Software Assurance Plan	Date: February 19, 2008	Page 3 of 12
Document No.: AI1-SYS-SAP	Revision: 1.00	

Table of Contents

<u>Section</u>	<u>Page</u>
1. INTRODUCTION	4
1.1 Identification.....	4
1.2 Change Procedure.....	4
1.3 Purpose	4
1.4 Scope	5
1.5 Reference Documents	5
2. Roles and Responsibilities	6
2.1 Roles	7
2.2 Responsibilities	7
3. Verification & Validation	7
4. RETIREMENT.....	8
5. ACRONYMS	8
6. IX-SA CHECKLIST	9

Title: Ares I-X Software Assurance Plan	Date: February 19, 2008	Page 4 of 12
Document No.: AI1-SYS-SAP	Revision: 1.00	

1. INTRODUCTION

This Software Assurance Plan describes the organization and procedures to be used by National Aeronautics and Space Administration (NASA) to ensure that software mission assurance (SMA) is performed throughout the duration of the Ares I-X project and to provide confidence to management that approved processes are being followed, that high-quality products are being produced, and that the software activities comply with the application requirements and technical standards.

Software mission assurance is essential to improving the practice of software engineering and management and thus constitutes an integral part of the software engineering process.

The NASA Constellation Program (CxP) has identified the need to develop a flight test vehicle to gain technical insight and provide early risk reduction for design and development of the Crew Launch Vehicle (CLV) which includes the Crew Exploration Vehicle (CEV) and Launch Abort System (LAS).

1.1 Identification

This document is identified as the NASA LaRC Software Assurance Plan (SAP) for the Ares I-X project. This plan establishes the policies, standards, procedures, and practices for software assurance of all computer software for applications developed for the Ares I-X project. Moreover, this plan establishes a standards compliance perspective.

The Ares I-X project is organized by element including: Avionics, First Stage (FS), Upper Stage Simulator (USS), Crew Module/Launch Abort System (CM/LAS), Roll Control System (RoCS) and Kennedy Space Center (KSC) Ground Systems/Ground Operations (GS/GO). Software is organized as follows: ground, flight and test. KSC GS will be developing PLC's and other software needed to provide Ground Support Equipment (GSE) command and control and to maintain ground interface and range assets. The primary avionics and software provider is Lockheed Martin (LM)/ United Launch Alliance (ULA) in Denver Colorado; Honeywell in Tampa Florida is a sub-contractor and is developing the Ascent Thrust Vector Control (ATVC) unit.

1.2 Change Procedure

This plan is a living document and as a result additions, deletions, and modifications will occur as it is utilized. It will be updated as the work proceeds and the necessity arises. The baseline and Change Requests (CR) to this document are approved at the Ares I-X Control Board (XCB). Note that the Ares I-X Mission Manager can waive any request set forth in this plan provided this waiver is documented.

1.3 Purpose

The purpose of this Software Assurance Plan is to ensure the quality of newly developed and modified software by verifying that the requirements set out in AI1-SYS-SRQA are met.

Title: Ares I-X Software Assurance Plan	Date: February 19, 2008	Page 5 of 12
Document No.: AI1-SYS-SAP	Revision: 1.00	

1.4 Scope

The scope of this document includes the software assurance activities to be carried out by the software acquirer for the Ares I-X project. This document defines the actions that provide assurance that the software-related items delivered conform to their established and contracted technical requirements. Ares I-X project software assurance (IX-SA) will also ensure that standards, practices, procedures, and methods of the software development process are defined and applied.

Software assurance activities for ground software developed by the Kennedy Space Center (KSC) in support of the Ares I-X test flight will be defined and documented in the Ares I-X KSC SR&QA plan.

Software assurance activities for flight and ground avionics software developed by Lockheed Martin (LM) and United Launch Alliance (ULA) in support of the Ares I-X test flight will be documented in the Ares I-X Avionics Software Assurance plan, DRD-4501QE-SAP.

Data generated via AI1-SYS-SRQA, KSC SRQA Plan and the LM/ULA Avionics Software Assurance plan, DRD-4501QE-SAP will be reviewed by the Project level SMA Lead (IX-SA) and presented at vehicle level reviews.

1.5 Reference Documents

The following list contains related documents which provide supporting information pertinent to the information in this Plan:

1. Ares I-X Flight Test Plan (FTP)
2. Avionics Requirements Documents (System and Software) (DRD 4501-SRS)
3. Avionics Mission Assurance Management Plan (DRD 4501-SAP)
4. Avionics Project Configuration Management Plan (DRD 4501-SDP)
5. Avionics Software Quality Assurance Plans (DRD 4501-SAP)
6. Avionics Software Metrics Report (DRD 4501-SMR)
7. Avionics Software Verification/Validation Plan (DRD 4501VR-VP)
8. Avionics Software Interface Design Description (DRD 4501-IDD)
9. Avionics Software Design Document (DRD 4501-SDD)
10. KSC NASA-STD-(I)-5005B, Standard for the Design and Fabrication of Ground Support Equipment
11. KSC SW-E-0002 Book 2, Space Shuttle Ground Support Equipment General Design Requirements – New GSE
12. KSC USA004615, Ground System Configuration Accounting
13. KSC USA004618, Integrated Process for Ground System Modification
14. KSC USA004621, Ground Systems Configuration Control Board Operations
15. KSC USA004642, Problem Reporting and Corrective Action System
16. KSC USA004655, System Assurance Analysis

Title: Ares I-X Software Assurance Plan	Date: February 19, 2008	Page 6 of 12
Document No.: AI1-SYS-SAP	Revision: 1.00	

17. KSC USA004773, Ground Operations Certification/Recertification Process and Documentation Requirements
18. KSC USA004778, Engineering Design Reviews
19. Ares I-X Safety, Reliability and Quality Assurance Requirements (AI1-SYS-SRQA)
20. Ares I-X Verification & Validation Plan, (AI1-SYS-VVP)

Plans related to the quality of Avionics software development include the Software Development Plan (DRD 4501SW-SDP) which describes the standards, schedule and procedures to be followed by the development team, the Software Configuration Management Plan (DRD 4501SW-SDP) which describes how products of this project shall be identified, baselined, and controlled, and the Software Test Plan (DRD 4501SW-STP) which describes how products of this project shall be tested.

Plans related to the quality of the Ground System implementation include USA PMP KSCGO-010-01 Ground Control System (GCS) Design, USA PMP KSCGO-010-02 GCS Implementation and GOP 500001 GCS Test Plan.

This plan has used the following technical standards as a guide:

- IEEE/EIA 12207.0 Standard for Information Technology – Software life cycle process
- IEEE/EIA 12207.1 Standard for Information Technology – Software life cycle process – Life cycle data
- IEEE Std 730-2002 IEEE Standard for Software Quality Assurance Plans
- ISO 9000-3:1991 Quality management and quality assurance standards – Part 3; Guidelines for the application of International Organization for Standardization (ISO) 9001 to the development, supply and maintenance of software
- SEI-TR-25 Key Practices of the Capability Maturity Model (CMM), Version 1.1, Carnegie Mellon University (CMU), Software Engineering Institute (SEI).
- NPD 2820.1 NASA Software Policies
- NASA-STD-8739.8 Software Assurance Standard
- NASA-STD-8719.13B Software Safety Standard
- NASA-GB-A201 Software Assurance Guidebook
- NASA-GB-001-96 Software Management Guidebook
- LMS-CP-5528 Software Planning, Development, Acquisition, Maintenance, and Operations
- LMS-CP-4754 Quality Assurance for Software Development and Acquisition

2. Roles and Responsibilities

Title: Ares I-X Software Assurance Plan	Date: February 19, 2008	Page 7 of 12
Document No.: AI1-SYS-SAP	Revision: 1.00	

2.1 Roles

For the purposes of this plan IX-SA will refer to the Ares I-X Project Software Assurance Manager based at LaRC and IPT-SA will refer to IPT Software Assurance Leads. The LaRC Mission Assurance Branch (MAB) organization is a separate organization (i.e., separate from the engineering organization) which reports directly to the Ares Mission Manager. The organization is obligated to fully advise the Ares I-X Mission Manager of the status of the software and the accompanying documentation.

The IX-SA is responsible for the fulfillment of, and for ensuring compliance with, the software quality assurance activities defined in this document. The IX-SA has clearly defined authority and responsibility. The IX-SA is responsible for ensuring that processes are applied as intended and that products are of high quality. The IX-SA provides senior management with an independent evaluation of the effort, and it provides a direct reporting line to the senior management of the Ares I-X project to resolve problems.

2.2 Responsibilities

The IX-SA has the responsibility for assuring that all software development phases of the software life cycle are conducted in accordance with requirements and standards. The Mission Assurance Manager (MAB) at LaRC shall select an IX-SA representative experienced with the activities of the software life cycle processes and that has background in software engineering principles with experience in developing software.

The IX-SA representative will exercise oversight of all SMA planning and activity in concert with the partners' IPT-SA. Each software development team shall have an IPT-SA. The IPT-SA should notify the IX-SA representative of upcoming significant meetings/teleconferences, audits, evaluations, reviews, surveys, newly released documents and revisions, testing, acceptance, and delivery.

3. Verification & Validation

NASA IV&V facility will conduct an Independent Assessment (IA), this IA shall employ tasks from the Independent Verification and Validation (IV&V) Work Breakdown Structure (WBS), but is not required to be done in-phase with the Ares I-X Project. This effort shall focus on:

- Assessing the appropriateness of the reuse of the Atlas V avionics package in the Ares I-X FTV, this will be accomplished by creating a System Reference Model (SRM) and correlating this SRM with Atlas V avionics design.

An independent V&V contractor shall be selected and will focus on:

- Implementation of the NASA GNC algorithm
- New avionics software subsystems including ATVC, RoCS and Sequencing

Title: Ares I-X Software Assurance Plan	Date: February 19, 2008	Page 8 of 12
Document No.: AI1-SYS-SAP	Revision: 1.00	

- Analysis of test data
- Avionics Software that affects safety

The avionics IPT along with the IX-SA will manage the Ares I-X V&V efforts. The independent V&V contractor has not been tasked to review any ground software developed by KSC.

4. RETIREMENT

The IX-SA will verify the transfer and maintenance of any licenses, simulators, models, and test suites from the provider/developer to NASA. The current list of items to be controlled includes:

- GC3 hardware located in the Mobil Launch Platform (MLP)
- Ascent Thrust Vector Control model in the SIL, this includes both hardware VME chassis and analog board as well as the software simulation.
- Final GN&C algorithm, design, parameters and test report data
- Final Sequencing algorithm, design, parameters and test report data
- DFI and OFI dataset from flight
- Miscellaneous avionics boxes from both the SIL as well as the vehicle following recovery

5. ACRONYMS

This section contains an alphabetical list and definitions of all acronyms and abbreviations used in the document and any word used in a non-standard way.

AVIO	Ares I-X Vehicle Integration Office
CDR	Critical Design Review
CMM	Capability Maturity Model
CMU	Carnegie Mellon University
CP	Center Procedure
DET	Development, Engineering & Test
EEE	Electrical, Electronic and Electromechanical
FS	First Stage
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
ISO	International Standards Organization
IPT-SA	Ares I-X Integrated Product Team Software Assurance Lead
IX-SA	Ares I-X Software Assurance (Project Level) Mgr.
KSC	Kennedy Space Center
LaRC	Langley Research Center
LM	Lockheed Martin
LMS	Langley Management System
MAB	Mission Assurance Branch

Title: Ares I-X Software Assurance Plan	Date: February 19, 2008	Page 9 of 12
Document No.: AI1-SYS-SAP	Revision: 1.00	

NASA	National Aeronautics and Space Administration
OMA	Office of Mission Assurance
PDR	Preliminary Design Review
PLC	Programmable Logic Controller
RoCS	Roll Control System
SA	Software Assurance
SAE	Software Assurance Engineer
SCMP	Software Configuration Management Plan
SEI	Software Engineering Institute
SE&I	Ares I-X Systems Engineering and Integration
SDP	Software Development Plan
SMA	Software Mission Assurance
SMA-MP	Software Mission Assurance Management Plan
SMAE	Software Mission Assurance Engineer
SRR	Software Requirements Review
STD	Standard
SVVP	Software Verification and Validation Plan
USS	Upper Stage Simulator

6. IX-SA CHECKLIST

MANAGEMENT:

1. Is the IX-SA performed by an individual who is organizationally independent of the software project and has the skills, responsibility, authority, and organizational freedom to permit objective software product and process evaluations?
2. Is the IX-SA performing the following tasks?
 - Ensures that each activity identified in the software plan is performed in accordance with the plan
 - Ensures that each software product identified in the software plan or project plan is prepared and undergoes software product IV&V and corrective action as defined in the plan
 - Prep Ares I-X records of software quality assurance activities and maintains those records for the life of the project
 - Provides recommendations for process and product improvement to the software manager and software team

DOCUMENTATION:

3. Is the IX-SA ensuring that the implementation of the software satisfies requirements, the documentation listed below is suggested:
 - Software Requirements Specification
 - Software Design Description

Title: Ares I-X Software Assurance Plan	Date: February 19, 2008	Page 10 of 12
Document No.: AI1-SYS-SAP	Revision: 1.00	

- Software Verification and Validation Plan
- Software Verification and Validation Report
- Software Configuration Management Plan
- Software Development Plan
- Standards and Procedures Manual
- Software Project Management Plan

STANDARDS, PRACTICES, CONVENTIONS, AND METRICS:

4. Are the standards, practices, conventions and metrics to be applied identified and is it stated how compliance with these items is to be monitored and assured? The subjects covered include the basic technical, design, and programming activities involved, such as documentation, variable and module naming, programming, inspection, and testing. The following information is suggested:

- Documentation standards
- Logic structure standards
- Coding standards
- Commentary standards
- Testing standards and practices
- Selected SMA product and process metrics such as branch metric, decision point metric, domain metric, error message metric, and requirements demonstration metric.

REVIEWS AND AUDITS:

5. Are the technical and managerial reviews and audits to be conducted defined?
6. Is it stated how the reviews and audits are to be accomplished?
7. Is it stated what further actions are required and how they are to be implemented and verified?
8. Suggested Reviews:
 - Software Requirements Review
 - Preliminary Design Review
 - Critical Design Review
 - Software Verification and Validation Plan (SVVP) Review
 - Functional Audit
 - Physical Audit
 - In-process audits
 - Managerial reviews
 - Software Configuration Management Plan Review
 - Post-mortem Review
 - User Documentation Review

TEST:

9. Are all the tests not included in the SVVP for the software identified by the software plan and are the methods to be used stated?

Title: Ares I-X Software Assurance Plan	Date: February 19, 2008	Page 11 of 12
Document No.: AI1-SYS-SAP	Revision: 1.00	

PROBLEM REPORTING AND CORRECTIVE ACTION:

10. Are the practices and procedures to be followed for reporting, tracking and resolving problems identified in the software development and maintenance process?
11. Are the specific organizational responsibilities concerned with their implementation stated?

TOOLS, TECHNIQUES, AND METHODOLOGIES:

12. Are the special software tools, techniques, and methodologies that support SMA identified, their purposes stated, and their use described.

CODE CONTROL:

13. Are the methods and facilities used to maintain, store, secure, and document controlled versions of the identified software during all phases of the software life cycle defined? This may be implemented in conjunction with a computer program library.

MEDIA CONTROL:

14. Are the methods and facilities to be used to identify the media for each computer product and the documentation required to store the media stated, including the copy and restore process; and protect computer program physical media from unauthorized access or inadvertent damage or degradation during all phases of the software life cycle?

SUPPLIER CONTROL:

15. Are the provisions stated for assuring that software provided by suppliers meets the established requirements?

RECORDS COLLECTION, MAINTENANCE, AND RETENTION:

16. Has the SMA documentation to be retained been identified?
17. Are the methods and facilities to be used to assemble, safeguard, and maintain this documentation stated?
18. Has the retention period been designated?

TRAINING:

19. Are the training activities necessary to meet the needs identified?

RISK MANAGEMENT:

20. Are there methods and procedures specified and employed to identify, assess, monitor, and control areas of risk arising during the software life cycle?

NASA LESSONS LEARNED:

21. Has the NASA lessons learned database been updated as necessary?

Title: Ares I-X Software Assurance Plan	Date: February 19, 2008	Page 12 of 12
Document No.: AI1-SYS-SAP	Revision: 1.00	

SOFTWARE CERTIFICATION PRIOR TO FLIGHT

22. The IX-SA will comment on and give recommendation concerning the certificate of qualification prior to flight.