CONSTELLATION PROGRAM
EXTRAVEHICULAR ACTIVITY (EVA)
SYSTEMS PROJECT OFFICE (ESPO)
SOFTWARE ASSURANCE PLAN

The electronic version is the official approved document. Verify this is the correct version before use.
## REVISION AND HISTORY PAGE

<table>
<thead>
<tr>
<th>Status</th>
<th>Revision No.</th>
<th>Change No.</th>
<th>Description</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>ESPO 000066</td>
<td>Baseline (Reference CRD ESPO 000066)</td>
<td>12/01/09</td>
<td></td>
</tr>
</tbody>
</table>
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>SECTION</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. INTRODUCTION</td>
<td>5</td>
</tr>
<tr>
<td>1.1. Purpose</td>
<td>5</td>
</tr>
<tr>
<td>1.2. Scope</td>
<td>5</td>
</tr>
<tr>
<td>1.3. Document Organization</td>
<td>6</td>
</tr>
<tr>
<td>1.4. Change Authority/Responsibility</td>
<td>6</td>
</tr>
<tr>
<td>2. DOCUMENTS</td>
<td>7</td>
</tr>
<tr>
<td>2.1. Applicable Documents</td>
<td>7</td>
</tr>
<tr>
<td>2.2. Reference Documents</td>
<td>8</td>
</tr>
<tr>
<td>3. ORGANIZATION AND MANAGEMENT</td>
<td>8</td>
</tr>
<tr>
<td>4. SOFTWARE ASSURANCE PROGRAM</td>
<td>11</td>
</tr>
<tr>
<td>4.1. Life-cycle Activities</td>
<td>11</td>
</tr>
<tr>
<td>4.1.1. Initiation</td>
<td>11</td>
</tr>
<tr>
<td>4.1.2. Post RFP/MOU/MOA, Pre-Award</td>
<td>12</td>
</tr>
<tr>
<td>4.1.3. Post-Award, Pre-Implementation</td>
<td>13</td>
</tr>
<tr>
<td>4.1.4. Implementation and Development</td>
<td>14</td>
</tr>
<tr>
<td>4.1.5. Acceptance</td>
<td>14</td>
</tr>
<tr>
<td>4.1.6. Operation</td>
<td>15</td>
</tr>
<tr>
<td>4.1.7. Maintenance</td>
<td>16</td>
</tr>
<tr>
<td>4.1.8. Retirement</td>
<td>17</td>
</tr>
<tr>
<td>4.2. General Software Assurance Information</td>
<td>17</td>
</tr>
<tr>
<td>4.2.1. Software Quality</td>
<td>17</td>
</tr>
<tr>
<td>4.2.2. Problem Reporting Analysis and Corrective Action (PRACA)</td>
<td>19</td>
</tr>
<tr>
<td>4.2.3. Software Reliability</td>
<td>20</td>
</tr>
<tr>
<td>4.2.4. Software Verification and Validation (V&amp;V)</td>
<td>22</td>
</tr>
<tr>
<td>4.2.5. Software Independent Verification and Validation (IV&amp;V)</td>
<td>23</td>
</tr>
<tr>
<td>4.2.6. Software Safety</td>
<td>24</td>
</tr>
<tr>
<td>4.3. CSCI Software Classification</td>
<td>32</td>
</tr>
<tr>
<td>4.3.1. Caution, Warning, and Control CSCI</td>
<td>32</td>
</tr>
<tr>
<td>4.3.2. Communications and Navigation CSCI</td>
<td>32</td>
</tr>
<tr>
<td>4.3.3. Information Processing CSCI</td>
<td>33</td>
</tr>
<tr>
<td>4.3.4. Vehicle Interface CSCI</td>
<td>33</td>
</tr>
<tr>
<td>4.3.5. Tools and Equipment CSCI</td>
<td>33</td>
</tr>
<tr>
<td>4.3.6. Ground Software CSCI</td>
<td>33</td>
</tr>
<tr>
<td>4.3.7. Simulations</td>
<td>33</td>
</tr>
<tr>
<td>4.3.8. Data and Files</td>
<td>33</td>
</tr>
<tr>
<td>SECTION</td>
<td>PAGE</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>5. COMPLEX ELECTRONICS</td>
<td>33</td>
</tr>
<tr>
<td>5.1. Purpose</td>
<td>33</td>
</tr>
<tr>
<td>5.2. Scope</td>
<td>34</td>
</tr>
<tr>
<td>5.2.1. Roles and Responsibilities</td>
<td>34</td>
</tr>
<tr>
<td>5.2.2. Tasks</td>
<td>34</td>
</tr>
<tr>
<td>5.3. Documentation</td>
<td>39</td>
</tr>
<tr>
<td>5.4. Reviews</td>
<td>39</td>
</tr>
<tr>
<td>5.5. Audits</td>
<td>39</td>
</tr>
<tr>
<td>5.6. HDL Code Reviews</td>
<td>40</td>
</tr>
<tr>
<td>5.7. Test</td>
<td>41</td>
</tr>
<tr>
<td>5.8. Deliverables</td>
<td>41</td>
</tr>
<tr>
<td>6. RISK MANAGEMENT</td>
<td>41</td>
</tr>
<tr>
<td>7. SOFTWARE ASSURANCE PROGRAM METRICS</td>
<td>42</td>
</tr>
<tr>
<td>8. SOFTWARE ASSURANCE RECORDS</td>
<td>43</td>
</tr>
<tr>
<td>9. TRAINING</td>
<td>43</td>
</tr>
</tbody>
</table>

**APPENDIX**

| A | ACRONYMS AND ABBREVIATIONS AND GLOSSARY OF TERMS | 45 |
| B | OPEN WORK | 50 |
| C | PROVIDER DELIVERABLES | 52 |

**FIGURES**

| 1 | EVA SR&QA ORGANIZATION | 9 |
1. INTRODUCTION

1.1. Purpose

Software assurance is the planned set of activities to ensure conformance of software life-cycle products and processes to requirements, standards, and procedures. Software assurance includes the following disciplines: software safety, software reliability, software quality, software Verification and Validation (V&V), and Independent Verification and Validation (IV&V). Software Assurance personnel work closely with Software Engineering, who has the primary responsibility for building safety, reliability, and quality into the design and for verification activities.

The purpose of the Extravehicular Activity (EVA) Systems Project Software Assurance Plan is to:

a. establish the goals, responsibilities, activities, and necessary resources required to meet the software assurance requirements defined in CxP 70128, Constellation Program Software Assurance Plan

b. provide the framework necessary to ensure a consistent approach to software assurance across all software Computer Software Configuration Items (CSCIs), including the required interfaces and communication with the Program and other projects

c. ensure that safety, reliability, and quality is designed into EVA Software and that all Safety, Reliability, and Quality Assurance (SR&QA) requirements have been met

d. facilitate partnering with Software Engineering

e. facilitate the sharing of data with Systems Safety

f. apply software assurance expertise as specified by baselined, approved requirements

1.2. Scope

This document applies to the EVA Systems Project software and Complex Electronics Assurance (CEA) effort during all phases of the Project life cycle. Software includes firmware, data, complex electronics, Government Off-the-Shelf (GOTS) software, Modified Off-the-Shelf (MOTS) software, and Commercial Off-the-Shelf (COTS) software when included in an EVA System.

Henceforth, the EVA Systems Project Software Assurance Organization will be called the Acquirer Software Assurance Organization. The contractor Software Assurance Organization will be referred to as the Provider Software Assurance Organization and the Provider for the Contractor software. The contractor will act as the acquirer for any
lower software projects. The Provider can flow down these requirements to any contractor or subcontractor, who develops, tests, maintains, operates, or provides services for the software.

Contractors and other EVA Systems software providers will comply with this EVA Systems Project Software Assurance Plan. Contractors are directed by their Statement of Work (SOW) to develop a Software Assurance Plan using DRD CSSS-S-012 (RFP NNJ06161022R). Software providers internal to the National Aeronautics and Space Administration (NASA) may also be directed by their Internal Task Agreements (ITAs) to develop a Software Assurance Plan for each of their efforts. These Software Assurance Plans will describe how the software provider will manage software assurance in accordance with both its contract and NASA’s safety and assurance practices.

1.3. Document Organization

Section 2.0 of the plan contains the list of reference documents (information only) as well as applicable documents (directly required). Section 3.0 provides an overview of the organization and management of the EVA Software Assurance Organization. Section 4.0 contains the details of the Software Assurance Program by life cycle and general software assurance information. Section 5.0 contains the details for doing assurance on complex electronic devices by life cycle including general assurance information. Complex electronic devices include Field Programmable Gate Array (FPGA), Application-Specific Integrated Circuit (ASIC), System on Chip (SoC), Complex Programmable Logic Device (CPLD) and any variation of these devices. Section 6.0 through Section 8.0 addresses risk management, metrics, records, training, and change history. The appendices contain acronyms, abbreviations, and a glossary of terms; open work; provider deliverables; tailoring guidelines; and the Software Safety Litmus Test.

1.4. Change Authority/Responsibility

The Acquirer Software Assurance Manager is responsible for the maintenance of this Plan. This Plan and all its changes will be processed in accordance with CxP 72182, EVA Systems Project Configuration and Data Management Plan. It is expected that this Software Assurance Plan will be updated throughout the EVA Project to reflect any changes in software assurance activities. Proposed changes will be submitted to the Acquirer Software Assurance Manager for initial approval and then submitted by an EVA Systems Project Change Request (CR) to the EVA Systems Project Control Board (EVAPCB) for consideration and disposition. All CRs will include a complete description of the change and the rationale to justify its consideration.

The Cx ESPO (EVA Systems Project Office) is the appropriate NASA Office of Primary Responsibility (OPR) identified for this document.
2. DOCUMENTS

The list of applicable documents directly applies. The list of reference documents is for information only. In the event that the process approach documented in this Plan conflicts with any of the applicable documents, this Plan shall take precedent.

2.1. Applicable Documents

The following documents include specifications, models, standards, guidelines, handbooks, and other special publications. The documents listed in this paragraph are applicable to the extent specified herein.

CxP 70008 Revision A Constellation Program Master Integration and Verification Plan (MIVP)

CxP 70038 Constellation Program Hazard Analyses Methodology

CxP 70059 Baseline, Change 1 Constellation Program Integrated Safety, Reliability, and Quality Assurance (SR&QA) Requirements

CxP 70065 Baseline, Change 1 Constellation Program Computing Systems Requirements

CxP 70068-01 Baseline, Change 2 Constellation Program Problem Reporting, Analysis and Corrective Action (PRACA) Requirements, Volume 1: Problem Processing Requirements

CxP 70086 Baseline, Change 1 Constellation Program Software Verification and Validation Plan

CxP 70128 Revision A Constellation Program Software Assurance Plan

CxP 70146 Baseline, Change 1 Constellation Program Acceptance Data Package (ADP) Requirements

CxP 72182 Baseline March 15, 2007 EVA Systems Project Configuration and Data Management Plan

CxP 72183 Constellation Program Extravehicular Activity (EVA) Systems Project Office (ESPO) Risk Management Plan

CxP 72184 Revision C Constellation Program Extravehicular Activity (EVA) Systems Project Office (ESPO) Safety, Reliability, and Quality Assurance Plan

CxP 72268 EVA Software Development Plan

NPR 1441.1 NASA Records Retention Schedules
2.2. Reference Documents

The following documents contain supplemental information to guide the user in the application of this document.

CxP 70043  Constellation Program Hardware Failure Modes and Effects Analysis and Critical Items List (FMEA/CIL) Methodology

CxP 70055  Constellation Program Safety, Reliability, and Quality Assurance Plan

CxP 70056  Constellation Program Risk Management Plan

CxP 70071  Constellation Program Management Requirements

AS9100B  Quality Management Systems–Aerospace Requirements


NASA-GB-A301  NASA Software Quality Assurance Audits Guidebook


NASA-STD-8739.8  Software Assurance Standard

NPR 7150.2  NASA Software Engineering Requirements

NPR 8715.3  NASA General Safety Program Requirements

No Number  NASA Complex Electronics Handbook for Assurance Professionals

3. ORGANIZATION AND MANAGEMENT

The Johnson Space Center (JSC) SR&QA Directorate has overall responsibility for EVA System Project’s SR&QA. The JSC SR&QA Directorate is supported by Glenn Research Center (GRC) Program and Project Assurance Division (PPAD) performing software assurance, engineering, analysis, and integration activities for the EVA Systems Project. The GRC SR&QA Director will assign the responsibilities of EVA software assurance and EVA software safety. These responsibilities will be designated as EVA Software Assurance Manager and EVA Software Safety Manager to clarify roles and responsibilities. These roles and responsibilities can be delegated and/or
performed by one or multiple individuals. The GRC SR&QA Director is supported by an EVA Software Assurance Manager who has insight into each provider’s Software Assurance Program and across the EVA SR&QA disciplines (i.e., vertically and horizontally). The EVA Software Assurance Manager, supported by additional Software Assurance personnel at the Program level (e.g., Software Safety Engineers, Software Reliability Engineers, Software Quality Engineers, Software V&V Engineers), will work directly with the Provider Software Assurance Organizations in carrying out this plan. JSC SR&QA is the Acquirer Software Assurance Manager. GRC SR&QA is the Provider Software Assurance Manager to JSC and the Acquirer Software Assurance Manager to lower-level activities. Responsibilities of the Software Safety Manager are defined in Section 4.2.6 of this Plan.

FIGURE 1  EVA SR&QA ORGANIZATION
The Acquirer Software Assurance Manager will:

a. oversee the EVA Software Assurance Program, ensuring that all software assurance tasks complement and support the overall System Assurance Program to eliminate any duplication of effort

b. secure and monitor resources and staffing, including staff training

c. maintain a high-level schedule of EVA software assurance activities

d. report and escalate issues or noncompliance to the ESPO SR&QA Manager

e. establish consistent approaches to software assurance reporting, metrics, and records

f. address assurance issues and potential risks that may impact other provider projects

g. communicate status between organizational entities and provider projects

h. ensure that close communication and data sharing between Acquirer and Provider Software Assurance Organizations occur

i. ensure that IV&V’s managerial, technical and financial independence is preserved

j. keep the appropriate Safety and Mission Assurance Technical Authority (STA) apprised of issues and concerns and work with them to understand and resolve software related problems

k. ensure that all Provider software risks are identified, tracked, and closed in the EVA risk management database; this includes software safety and software reliability risks

l. compile all Provider software assurance status, summarize the maturity of the EVA Software Assurance Program, and provide a Program-level assurance report directly to the ESPO SR&QA Manager

m. participate in monthly CxP Software Assurance Working Group (SAWG) for reporting status to CxP Level II Software Assurance Team

The Provider Software Assurance Programs, at all levels, will implement the requirements of the EVA Systems Project.
4. SOFTWARE ASSURANCE PROGRAM

This section addresses the software assurance life-cycle activities and general software assurance information. References to the Acquirer and Provider Software Assurance Organizations and their expected activities are provided to establish the basis of assurance process and products.

4.1. Life-cycle Activities

For the remainder of this document, Software Assurance Managers are defined as either Acquirer or Provider. Life-cycle activities start at the development of the Request for Proposal (RFP), Memorandum of Understanding (MOU), Memorandum of Agreement (MOA) and/or NASA ITA and are completed with the software retirement.

4.1.1. Initiation

The Pre-Award Initiation tasks occur for the development of the RFP, MOU, MOA, and/or NASA ITA. These tasks belong to the Acquirer Software Assurance Manager and meet the requirements of Section 7.3.1 of CxP 70059, Constellation Program Integrated Safety, Reliability, and Quality Assurance (SR&QA) Requirements. The Acquirer Software Assurance Manager interfaces with the NASA Acquirer Project Manager.

The Acquirer Software Assurance Manager will:

a. Perform an initial Software Assurance Classification and Software Safety-Criticality Assessment per Appendix A of NASA-STD-8739.8, Software Assurance Standard. This Software Assurance Classification and Software Safety-Criticality Assessment is an independent assessment to be used as a baseline. If the software is determined to be safety critical, then Section 4.2.6 of this Plan is applicable.

b. Document any tailoring of software assurance activities and requirements (refer to CxP 70128, Appendix D for tailoring recommendations).

c. Obtain agreement on classification and safety-criticality evaluation with Provider EVA Software Assurance Manager. Disagreements will be elevated to the ESPO SR&QA Manager and GRC Software Engineering Technical Authority for final disposition.

d. Obtain agreement on software assurance tailoring with the ESPO SR&QA Manager, who has final disposition authority.

e. Participate in the process to identify, analyze, track, and control of risks.

f. Assess and verify that the RFP/MOU/MOA meets the implementation of this Plan.
The Acquirer Software Assurance Manager will verify that these items have been addressed within the RFP/MOU/MOA to improve software quality, cost estimation, risk management, and assure a comprehensive Software Assurance Program. The items include:

a. Software Classification Assessment and Software Safety-Criticality Evaluation

b. software assurance requirements (referenced above)

c. Capability Maturity Model Integration (CMMI) requirements for development and assurance; at minimum CMMI Level II for development and Product and Process Quality Assurance (PPQA)

d. required metrics as defined in Section 6.0 of this Plan

e. risk management requirements per CxP 70071, Constellation Program Management Requirements

f. deliverables (meeting the requirements of CxP 70059 and CxP 70065, Constellation Program Computing System Requirements)

g. contractual statements that include the appropriate oversight/insight requirements and associated deliverables to assure a comprehensive Software Assurance Program

4.1.2. Post RFP/MOU/MOA, Pre-Award

Tasks within this section define the software assurance activities once the RFP/MOU/MOA has been released but before a contract or NASA ITA has been awarded. These tasks meet the requirements for Section 7.3.2 of CxP 70059. The Acquirer Software Assurance Manager interfaces with the NASA Acquirer Project Manager.

The Acquirer Software Assurance Manager will:

a. Evaluate the proposal for compliance with the RFP/MOU/MOA.

b. Evaluate the proposal to verify that the provider’s organization meets the intent of CMMI Level II requirements. This can be done via an on-site assessment.

c. Participate in pre-award surveys and contract negotiations.

d. Coordinate with the NASA Acquirer Project Manager to update (if updates are necessary) the Software Assurance Classification and Software Safety-Criticality Assessment based on the accepted proposal information and/or development
approach; these assessments will be retained as quality records by the project and accessible by Software Assurance personnel.

4.1.3. **Post-Award, Pre-Implementation**

Post-award, pre-implementation tasks occur once the contract or NASA internal agreement has been awarded but development has not been initiated. These tasks meet the requirements of Section 7.3.3 of CxP 70059. During this time period, the Acquirer and the Provider Software Assurance Organizations are establishing working relationships with each other to assure open communication and status of assurance issues and/or risks.

The Acquirer Software Assurance Manager will:

a. assure that the Provider’s Software Assurance Plan is baselined, approved, and consistent with this Plan

b. verify the Provider’s organization meets the training requirements in Section 9.0 of this Plan

c. verify that the Provider's Software Assurance Plan, including configuration management, complies with CxP 70059 and CxP 70065, and meets contractual requirements

d. assure that each Provider's procedures for problem reporting, metrics, risk management, and software assurance reporting are in place and consistent with this Plan

The Provider Software Assurance Manager will:

a. perform a Software Assurance Classification per Appendix A of NASA-STD-8739.8 and obtain the Acquirer Software Assurance Manager’s approval to ensure agreement on the expected level of software assurance

b. provide evidence to the Acquirer Software Assurance Manager that the Provider's Software Assurance Organization is trained per Section 9.0 of this Plan

c. coordinate with the Acquirer Software Assurance Manager to approve and baseline the Provider's Software Assurance Plan

d. verify that the Provider's Software Assurance Plan, including configuration management, complies with CxP 70059 and meets contractual requirements

e. provide monthly status of assurance issues and risks to the Acquirer Software Assurance Manager
f. define procedures for problem reporting, metrics, risk management, and software assurance reporting (refer to Appendix C of this Plan for reporting details)

4.1.4. Implementation and Development

During implementation and development, the Acquirer Software Assurance Organization performs insight/oversight surveillance into the processes and products of the Provider. These tasks meet the requirements of Section 7.3.4 of CxP 70059.

The Acquirer Software Assurance Manager will:

a. Perform audits, reviews, analysis, and assessments to ensure the Provider’s software life-cycle processes and products are in adherence to contract requirements (this includes CxP 70065; CxP 70059; CxP 70086; Constellation Program Software Verification and Validation Plan; the Provider’s Software Assurance Plan; and configuration management processes). An assessment will be performed for each major milestone review.

b. Verify the Provider has developed and maintained a process to address software assurance on all types of software.

The Provider Software Assurance Manager will:

a. Provide insight that the Provider’s software life-cycle processes and products are in adherence to contract requirements. One way this can be done is by performing internal audits throughout the project lifecycle.

b. Provide access to data and status for the Acquirer Software Assurance Manager to perform surveillance.

c. Develop and maintain a process to address software assurance on all types of software applicable to the Provider. This includes flight and ground software, simulations, models and tools.

d. Provide software quality metrics to the Acquirer Software Assurance Manager.

4.1.5. Acceptance

During acceptance, the Acquirer Software Assurance Organization verifies that the software and the related products (e.g., requirements, design, code, documentation, and special instructions) meet all the requirements for certification/acceptance. These tasks meet the requirements of Section 7.3.5 of CxP 70059.
The Acquirer Software Assurance Manager will:

a. assess and concur certification/acceptance criteria and objective evidence prior to the Provider delivering the software for use by the EVA Systems Project.

b. assess any Acquirer facilities to verify readiness to install the software

c. assure that the Provider's risks and the results have been recorded in the EVA risk management database

d. assure that the lessons learned are recorded in the NASA lessons learned database

The Provider Software Assurance Manager will:

a. provide insight on the certification/acceptance criteria and objective evidence to verify accuracy and completeness prior to assessment/approval by the Acquirer Software Assurance Manager

b. assist, as required, in assessments of Acquirer facilities to verify readiness to install the software

c. enter the lessons learned from acquisition thru acceptance into the NASA lessons learned database

4.1.6. Operation

During the operation phase, the Acquirer Software Assurance Organization verifies that the Provider software assurance practices are maintained and utilized. These tasks meet the requirements of Section 7.3.6 of CxP 70059.

The Acquirer Software Assurance Manager will:

a. assess the Provider software assurance processes to ensure correct and expected operation of the software

b. perform periodic assessments to ensure the configuration management of the software and its related products is maintained

c. assess CRs, discrepancies, and software induced operational workarounds for safety impacts to the Provider and other projects

d. will approve software certification prior to use
The Provider Software Assurance Manager will:

a. Verify that the Provider software assurance processes are applied to ensure the correct operation of the software.

b. Assist, as requested, the Acquirer in performing periodic configuration management assessments.

c. Provide status on CRs, discrepancies and software induced operational workarounds that have safety impacts to the Acquirer Software Assurance Manager.

d. Provide certification evidence to acquirer Software Assurance Manager through the EVA Software and Avionics Control Panel (SACP) for approval prior to operational use. Certification evidence consists of the Acceptance Data Package (ADP) (CSSS-T-027).

4.1.7. Maintenance

During the maintenance phase, the Acquirer Software Assurance Organization verifies that the Provider software maintenance process meets the EVA requirements. These tasks meet the requirements of Section 7.3.7 of CxP 70059.

The Acquirer Software Assurance Manager will:

a. assess the Provider software maintenance processes for adherence to the Provider's development requirements, configuration management, and operations

b. assure that the Provider's licenses on tools, simulators, models, and test suites are transferred to and maintained by the maintenance organization

c. assure that the Provider's metrics are transferred to and maintained by the maintenance organization

The Provider Software Assurance Manager will:

a. assure that the Provider software maintenance processes are in adherence to the Provider's development requirements, configuration management, and operations

b. assure that the Provider's licenses on tools, models, and test suites are transferred to the maintenance organization

c. assure that the Provider's metrics are transferred to the maintenance organization
4.1.8. Retirement

At the end of the software life cycle, the Software Assurance Organization ensures that the proper retirement of the software is performed by the Provider Organization. These tasks meet the requirements of Section 7.3.8 of CxP 70059.

The Acquirer Software Assurance Manager will:

a. evaluate and approve the Provider's software retirement plan

b. verify that the software retirement plan includes the archival and disposal of software records; for safety-critical software, the plan will include safe termination of operation and retirement of safety-critical software with concurrence by the Acquirer Software Safety Manager

The Provider Software Assurance Manager will:

a. generate and obtain approval of the Provider's software retirement plan

b. ensure that archival and disposal of software records are in accordance to NPR 1441.1, NASA Records Retention Schedules

c. ensure that the safe termination of operation and use of safety-critical software is documented in the Provider's software retirement plan

4.2. General Software Assurance Information

The following sections provide a description of the EVA general software assurance activities including the software assurance disciplines (quality, reliability, V&V, IV&V, and safety), and problem reporting.

4.2.1. Software Quality

Software quality includes software quality assurance, quality control, and quality engineering. The Acquirer Software Assurance Manager, supported by Software Quality personnel, performs software quality on the Provider's processes and projects throughout the software life cycle.

The Acquirer Software Assurance Manager will:

a. assure that the implementation for the Providers' Software Quality Program complies with CxP 70059, Section 2.0 and Section 7.5.2

b. assure that the Provider's Software Assurance Plan documents the software quality activities to be performed for whole software life cycle and the records to be maintained per at least CMMI Level II PPQA requirements
c. assure that the Provider’s Software Assurance Plan conforms to the intent of IEEE 730-2002, IEEE Standard for Software Quality Assurance Plans, software quality plan

d. conduct quarterly audits of the Provider’s Software Assurance Organization to assure compliance with the Provider’s Software Assurance Plan and scheduled activities (audits will be performed per NASA-GB-A301, NASA Software Quality Assurance Audits Guidebook)

e. evaluate and approve the software portion of the Provider’s ADP per CxP 70146, Constellation Program Acceptance Data Package (ADP) Requirements

f. conduct in-depth assessments to identify and mitigate risks to the EVA system if issues are identified with the Provider’s processes, products, or their software assurance support

g. report software quality assurance/quality engineering activities and risks to ESPO SR&QA Manager and the CxP Level II Software Assurance Manager

The Provider Software Assurance Manager will:

a. Ensure the preparation, maintenance, and implementation of the Provider’s Software Quality Plan (this can be an independent plan or part of another plan such as the Provider’s Software Assurance Plan).

b. Perform periodic audits (both planned and unplanned) of the Provider’s processes to the Provider’s process requirements (e.g., configuration management, requirements management, project planning, project monitoring and control).

c. Provide evidence of completion of product and risks assessments for safety-critical software.

d. Approve formal test procedures to ensure compliance to the Provider's test plans; witness the qualification tests as specified in the Provider’s Software Quality Plan; witness acceptance tests. Government Mandatory Inspection Points (GMIPs) will be applied to tests involving safety critical software.

e. Ensure that test suites, simulators, models, and test data are ready for use, certified, and under configuration control.

f. Participate in peer reviews, inspections, and formal reviews (e.g., System Requirements Review [SRR], Preliminary Design Review [PDR], Critical Design Review [CDR], Test Readiness Review [TRR], and System Acceptance Review [SAR]) to insure that software products and processes meet standards and requirements.
g. Perform periodic audits of the Provider's products to the Provider's requirements (e.g., requirements traceability matrix, version description document).

h. Review and analyze Provider's metrics.

i. Review software nonconformances, issues, and risks.

j. Review any changes to the baselined, as built, or updates to operational software product prior to submission to the Acquirer.

k. Review the software verification plan to ensure quality processes are met.

l. Complete acceptance audits prior to every delivery of the ADPs per CxP 70146.

m. Review and approve all exceptions and deviations.

n. Provide objective evidence of the above activities in the monthly status report to the Acquirer Software Assurance Organization.

Evidence of audits, assessments, evaluations, and reviews will be made available to the Acquirer via Windchill and a dedicated directory for software records and artifacts.

4.2.2. Problem Reporting Analysis and Corrective Action (PRACA)

Problem reporting and corrective action will be performed per CxP 70068-01, Constellation Program Problem Reporting, Analysis and Corrective Action (PRACA) Requirements, Volume 1: Problem Processing Requirements, and Section 7.5.3 of CxP 70059. Safety-critical problem reporting is addressed in the safety section of this Plan.

The Acquirer Software Assurance Manager will:

a. capture and report all nonconformances, defects, and corrective actions identified by the Acquirer

b. utilize the EVA Problem Reporting Analysis and Corrective Action (PRACA) system to track and trend data

c. manage and disposition actions, issues and nonconformances, to identify and analyze/recognize recurring or systemic issues that may warrant corrective and preventive action

The Provider Software Assurance Manager will implement a comparable reporting system at the project level.
4.2.3. Software Reliability

Software reliability is the likelihood that software will consistently perform its intended function under specified conditions. The emphasis for software reliability is a qualitative measure. Software assurance needs to assure that the software reliability process and methodology are implemented correctly and effectively to increase software and system reliability. This includes the following:

a. verifying that the Software Reliability Engineers have a viable plan and are following it
b. developing and delivering analyses results to the system reliability process
c. assuring that the results of the reliability analyses are fed back into software design in order to have, at a minimum, the appropriate level of fault tolerance and error handling

Software reliability includes the assurance of the reliability prediction and estimation program. Software metrics need to be collected and examined as the software development progresses throughout the life cycle. The metrics involve taking measures of the defects found to focus any needed improvements to either the software products or the software development process.

4.2.3.1. Software Reliability Activities

The Acquirer Software Assurance Manager, supported by Software Reliability Engineers, performs software reliability analysis on the Provider's processes and products with emphasis on failure mode identification and mitigation, error prevention, fault detection, isolation, recovery, and measurements to maximize reliability.

NOTE: Software reliability activities apply to Class A-C safety critical software only, as defined in CxP 70128.

The Acquirer Software Assurance Manager will:

a. assess and approve the Provider’s software reliability implementation as documented in the Provider’s Software Assurance Plan or an independent document (it will include techniques, methods, tools, metrics, analyses, and strategies)

b. assure the Provider’s software reliability requirements are compliant with CxP 70059, Section 7.5.4, and CxP 70065, Section 3.5, and included in the Provider’s software requirements specification; reliability requirements will address the following as applicable to the Provider:
1. Software Inhibits: Inhibits control must-not-work functions and cannot be removed by a software action; software inhibits provide a prerequisite condition to be checked prior to the execution of the hazardous command.

2. Redundancy: Software redundancy applies to must-work functions.

3. Fault tolerance: Includes intentional identification of failure modes and mitigation, and detailed assessment of expected performance; the Provider will use methodologies defined in CxP 70065, Appendix K.

c. assure that all Provider software reliability activities are performed and completed

d. participate in the Provider’s major life-cycle reviews

e. conduct independent assessments on Provider's Software Assurance Organization's software reliability analyses including quality metrics and trend evaluations (verify that the trend evaluations include lessons learned and root cause analysis)

f. conduct investigative tasks based on significant trends or issues, concerns, and risks identified throughout the Provider’s life cycle

g. summarize and elevate software reliability issues and findings to the ESPO SR&QA Manager and CxP Level II Software Assurance Manager

The Provider Software Assurance Manager will:

a. ensure the preparation, maintenance, and implementation of the Provider’s Software Reliability Plan (this can be an independent plan or part of the Provider’s Software Assurance Plan)

b. provide a monthly status report that summarizes software reliability activities (refer to Appendix C of this Plan for format information)

c. perform assurance on the reliability assessments (using the methods defined in Appendix K of CxP 70065) to identify, characterize, and analyze potential faults and failures in design and prioritize them, then identify methods to detect and prevent propagation of those faults and failures including the use of redundancy and software inhibits

d. document and obtain approval from the Acquirer Software Assurance Manager to use any software methodology not identified in CxP 70065, Appendix K

e. ensure that the Provider’s technical requirements and design will "build in" the required reliability into the system (e.g., failure mode identification and mitigation; fault tolerance; fault tolerance; fault detection, isolation, and recovery; error
handling; and redundancy) with the focus to identify and design out software failure modes

f. ensure availability of software reliability products to the Acquirer Software Assurance Organization through Windchill

g. ensure that reliability metrics will be available for lessons learned or root cause analyses

h. ensure that the Provider software reliability activities include (activities can be tailored with approval of the Acquirer Software Assurance Manager based on size, classification, and complexity):

1. Design and Operational Profile Development
2. Software Reliability Modeling
3. Reliability allocations
4. Reliability predictions
5. Reliability performance trending and evaluations
6. Reliability testing including development, qualification, and acceptance
7. PRACA data mining
8. Software product metrics

4.2.4. Software Verification and Validation (V&V)

The EVA Verification and Validation (V&V) Program, per CxP 70086, ensures that software being developed or maintained satisfies functional, performance, and other requirements at each stage of the development process and that each phase of the development process yields the right product.

The Acquirer Software Assurance Manager, supported by Software V&V personnel, will:

a. assure that the Provider’s Software V&V Plan complies with Section 7.5.5 of CxP 70059, and CxP 70086

b. assess and approve rationale for delivery with open nonconformances

c. participate in all project major milestone reviews, including, but not limited to, SRR, PDR, CDR, TRR, SAR, etc.

In support of the V&V Program, the Provider Software Assurance Manager will:
a. ensure the preparation, maintenance, and implementation of a Software V&V Plan

b. ensure test plans and reports are correct and complete (e.g., contain at a minimum, goals, scope, processes used, test facilities, resources, and regression testing)

c. verify that requirements are valid, unambiguous, correct, complete, consistent, operationally and technically feasible, and verifiable

d. ensure that formal and peer review action items and findings are completed and closed

e. verify that nonconformances or deficiencies occurring during testing are recorded

f. ensure that regression testing is conducted to address nonconformances or deficiencies have been corrected and that changes made to the software did not introduce new hazardous conditions

g. verify that the resolution of all nonconformances takes place prior to delivery (open nonconformances with rationale require approval from the Acquirer Software Assurance Manager)

h. ensure that the software meets all its requirements, including safety-critical requirements, and it behaves as expected when integrated with the system

i. verify that safety-critical software is traced back to the system-level hazards

j. obtain Acquirer Software Assurance Manager initial approval for all waivers and exceptions to any software requirements (this includes CxP requirements and Provider requirements; these waivers/exceptions have to be traced to the parent requirement and the impact analyzed and found acceptable)

For requirements that cannot be verified through testing, Acquirer (Level III requirements only) and Provider Software Assurance Managers will concur with both the Provider rationale (this will include any risk associated with the alternative method) for not performing a test and the alternative verification method (analysis, inspection, demonstration, and test) chosen to verify the requirement.

4.2.5. Software Independent Verification and Validation (IV&V)

EVA will utilize the NASA IV&V Facility to provide Software IV&V support. The NASA IV&V Facility determines the level of IV&V services to be provided based on a NASA Headquarters’ selection process with input from the results of the Software Assurance Classification Assessment, and a Safety Criticality assessment performed by the Center IV&V Liaison. When required, IV&V is performed by the NASA IV&V Facility with full technical, managerial, and financial independence from the EVA Systems Project Office. The NASA IV&V Facility will establish a formal agreement with the EVA
Systems Project Office. This agreement will define lines of communication; IV&V issue tracking, IV&V accessibility to project artifacts, and other logistics. After some initial analysis, the IV&V Facility develops an IV&V Project Execution Plan (IPEP) with a detailed schedule and work breakdown structure for performing the IV&V. The IPEP is an internal IV&V Facility document and is provided to the Project for information only.

To ensure the success of IV&V, the Provider will provide all information required for the IV&V effort to the NASA IV&V personnel. This includes, but is not limited to, access to all software reviews and reports, developer plans and procedures, software code, software documentation, and software problem reporting data. Wherever possible, the Provider will permit electronic access to the required information or furnish soft copies. IV&V Team will provide input/feedback as specified in the formal agreement. The IV&V results will be assessed by the Acquirer and Provider Software Assurance Managers.

For more details on the IV&V approach to software assurance reporting, records, and corrective action, see the EVA Systems Project Office formal agreements with the IV&V Facility <TBD 4-1>.

4.2.6. Software Safety

EVA relies on safety-critical systems in which software affects the control or containment of hazards. Software safety activities will focus efforts to eliminate or mitigate risks to a level acceptable to the Acquirer Software Safety Manager. These activities will include working with System Safety to analyze both the software and hardware contributions to a hazard and, from a systems perspective, design out hazards or reduce the severity and/or likelihood of occurrence of those hazards. Software safety is a joint effort between the Acquirer and the Provider. If the Acquirer Software Safety Manager determines the software to be safety-critical (Section 4.1.1 of this Plan), then the Provider must adhere to the requirements of Section 7.5.7 of CxP 70059, CxP 70065, and Section 4.2.6 of this Plan.

4.2.6.1. General Software Safety Activities

The Acquirer Software Safety Manager will:

a. evaluate and concur with the Provider’s software safety-criticality evaluation (the assessment will be performed per CxP 70128, Appendix E; the assessment will be evaluated at each major milestone addressing any changes to the system or software design as the project progresses through the life cycle)

b. perform periodic assessments to assure that the Provider’s software safety processes and procedures are approved and implemented to meet EVA software safety requirements
c. evaluate and concur with the Provider’s Software Safety Plan (this can be an independent plan or part of the Provider’s Software Assurance Plan, reference the Provider’s section for contents)

d. assure that software safety processes, products, and artifacts are under configuration control throughout the software life cycle

e. evaluate and concur with changes to baselined safety-critical software (this is done through participation in control boards; this includes all changes, modifications, and patches that effect safety critical requirements, design, code, data, systems, equipment, test plans, procedures, simulators, models, test suites, or criteria will be evaluated to determine the effect of the proposed change on the system safety)

f. communicate software safety activities and issues to ESPO SR&QA Manager and CxP Level II Software Assurance Manager

The Provider Software Safety Manager will:

a. Perform software safety-criticality assessment, as part of the system criticality assessment, per CxP 70128, Appendix E at initiation and at each major milestone (the assessment will determine the applicability of software safety requirements; the Provider Software Safety Manager will gain concurrence from the Acquirer Software Safety Manager).

b. Communicate software safety issues, concerns and status to the Acquirer Software Assurance Manager (provide monthly status reports to the Acquirer Software Assurance Manager per Appendix C of this Plan; this includes risks and safety concerns).

c. Present software safety analysis results and artifacts at the Provider’s major milestone reviews.

d. Assure the Provider’s software safety processes and procedures are concurred to by the Acquirer and are implemented throughout the Provider’s life cycle to meet EVA software safety requirements.

e. Generate the Provider’s Software Safety Plan. The Acquirer Software Safety Manager will concur with the plan. The plan will contain, at minimum, the following:

1. List of all software safety-related documentation, deliverables, staffing, and resources.

2. The process for escalating software safety issues within the Provider’s team and the decision-making process for addressing software safety issues.

3. Required training for software safety practitioners.
4. Software design, coding, and safety standards.

5. The relationship among system safety, software assurance, SR&QA, and software development efforts.

6. If the plan is documented in several documents, cross references will be provided to the software safety activities.

f. Assure that the Provider’s software safety processes, products, and artifacts are under configuration control throughout the software life cycle.

g. Evaluate and concur with the changes made during the development and prior to base-lining the safety-critical software (the Acquirer Software Safety Manager will approve the changes once the software has been delivered).

4.2.6.2. Software Safety Analysis

Software safety analysis includes an analysis of the system hazards to determine the involvement of software to those system hazards (referred here as a Software Hazard Analysis) and a detailed software analysis of the faults and failure modes.

The Acquirer Software Safety Manager will:

a. evaluate and concur with the Provider’s Software Hazard Analysis; ensure it has been integrated into the Provider’s system hazard analysis; ensure that any accepted risks do not affect other Providers (see details below for required items to be included)

b. identify and elevate to the ESPO SR&QA Manager the levels of acceptable risk exposure and describe how each integrated hazard has been eliminated, mitigated, controlled, or accepted

c. concur with the Provider’s software methodology for performing the analysis that identifies the software faults and failure modes; the preferred EVA software methodology is Fault Tree Analysis (FTA) or Failure Modes and Effects Analysis (FMEA); details can be found in Appendix K of CxP 70065 and CxP 70043, Constellation Program Hardware Failure Modes and Effects Analysis and Critical Items List (FMEA/CIL) Methodology

d. evaluate and concur with the results of the Provider’s analysis of the software faults and failures

The Provider Software Safety Manager will:

a. Assure that the software hazard analysis is conducted per CxP 70038, Constellation Program Hazard Analyses Methodology, for each major milestone as
part of the system hazard analysis; Appendix A.5 of CxP 70038 has details specific to software hazard analysis. The analysis will include the following:

1. identification of acceptable risk exposure
2. description of how each identified hazard has been eliminated, mitigated, controlled, or accepted
3. determination if the software is a contributing factor (cause, control, mitigation)
4. a trace of the system hazards to the software hazards to the requirements and design options to the specific CSCI and code
5. identification of the software error or computing system failure that can result in a hazard, loss of a hazard control, or loss of safety-critical functions
6. identification of hazardous commands that create an unsafe condition or reduce the control of a hazard
7. verification that the “must work” and “must not work” functions are identified and controlled
8. verification methods
9. definition of the boundaries of the computer-based control system (this only applies to Providers using computer-based controls for hazards)
10. verification that the software hazard analysis is integrated into the system hazard analysis

b. Perform a software analysis of the faults and failure modes on the Provider’s safety critical software for each major milestone review to incorporate changes as the project design matures; FMEA and FTA are the preferred EVA assessment methods; the Provider can use an assessment methodology not defined in CxP 70065, Appendix K. The analysis will include the following:

1. identification of failure modes, local and system effects, software faults which can contribute to a hazard, and necessary safety features
2. identification of the most important CSCIs to perform a software FMEA (the software FMEA should generate a software critical items list)
3. identification of assumption and ground rules to be used in the analysis
4. analysis worksheets for each identified failure mode (this needs to include corrective actions and design improvements; see CxP 70043 for details on completing the worksheets)

5. integration of the software analysis worksheets into the system report

The Acquirer Software Safety Manager will concur with the analysis methodology and analysis results for both the hazards and FMEAs. This approval will be accomplished through the EVA SR&QA Board.

4.2.6.3. Software Safety Requirements

The Acquirer Software Safety Manager will:

a. assure that the Provider’s system-level hazards trace to their software safety requirements and are maintained throughout the project life cycle

b. evaluate and approve all Provider’s waivers and exceptions to software safety requirements (this includes CxP requirements and Provider requirements; these waivers/exceptions have to be traced to the applicable system hazard and the risks qualified)

The Provider Software Safety Manager will:

a. ensure that the Provider’s software requirements specification clearly identifies the software safety requirements

b. ensure that Providers using computer-based controls for hazards meet the control system safety requirements within Section 3.5 of CxP 70065

c. ensure that the Provider develops and maintains a bidirectional mapping between Class A and Class B (per NPR 7150.2, NASA Software Engineering Requirements) software safety requirements and system hazards which traces down to software design, implementation (i.e., code), and verification

d. obtain Acquirer Software Safety Manager initial approval for all waivers and exceptions to any software requirements (this includes CxP requirements and Provider requirements; these waivers/exceptions have to be traced to the system hazard and the risk qualified)
4.2.6.4. Software Safety Design/Implementation

The Acquirer Software Safety Manager will:

a. perform periodic assessments of the Provider’s Software Assurance Organization to verify compliance to the Provider’s software safety plan and Section 4.2.6 of this Plan

b. participate in the Provider’s milestone reviews (this includes evaluation of the safety data package, software hazard analysis, faults and failure modes analysis, criticality assessment and incorporation of software safety requirements into the Provider’s design)

c. provide oversight of the Provider’s conformance to design documentation and implementation of software safety requirements through code analysis

The Provider Software Safety Manager will:

a. Assure that the Provider’s software design meets the software safety requirements (evaluation of the Provider’s software design will be performed for each major milestone).

b. Assure that the Provider’s software design analysis includes:

1. verification that all software safety requirements are included in the detailed design and that no untraceable functions (functions without requirements) have been added

2. implementation of the software safety requirements to prevent, control, or mitigate the identified hazards

3. assessment for the introduction of new hazards due to design choices

4. assessment of the possible compromise of existing hazard controls due to design choices

5. effects of COTS/legacy/reused software and tools in the development/verification of safety-critical software

6. identification of all relevant hazardous commands; this includes internal and external automated commands, and user commands

c. Evaluate and concur with the Provider’s approach to software safety aspect of the design as documented in the Provider’s Software Design Document.
d. Verify the Provider’s conformance to design documentation and implementation of software safety requirements through code analysis (this involves tracing the requirements to the design and to the code; this can be performed as a manual code review or with code analysis tools; it verifies conformance to coding standards and software safety design features).

4.2.6.5. Software Safety Testing

The Acquirer Software Safety Manager will:

a. approve, as required, alternate verification methods through approval of a waiver(s) (testing is the preferred verification method)

b. monitor the V&V test efforts for software safety requirements and assure that all the requirements have been evaluated and that any system hazards related to software have been eliminated or controlled

c. evaluate and concur with the Provider’s software safety test results

The Provider Software Safety Manager will:

a. map each software safety requirement to one or more verification methods with testing as the preferred method (if testing is not feasible, prior approval of the verification method by the Acquirer Software Safety Manager is required; prior approval includes specifying the alternate method in the verification requirement)

b. witness/monitor formal software safety tests; this activity includes:

1. verification that analysis results confirm compliance with safety requirements and safe operation of the system

2. verification that the test plans, procedures, and results are documented

3. verification that testing addresses the software failure modes that were identified in safety analyses

4. verification that test results include safety concerns and discrepancies

5. verification that appropriate testing is conducted for each new system configuration

6. verification that the appropriate level of regression testing takes place

7. verification that testing includes both nominal and off-nominal inputs and conditions
8. verification that V&V testing is performed only using certified models, simulators, and tools

c. obtain concurrence of the Acquirer Software Safety Manager on the software safety test results (these results will become part of the Provider’s system safety data package)

4.2.6.6. Software Safety Certification

The Acquirer Software Safety Manager will:

Review and provide final approval of the certification for operational use of all safety critical software systems (the certification process will be done in accordance with the processes defined in CxP 70008, Constellation Program Master Integration and Verification Plan (MIVP), as well as require reviews with the Provider’s Software Safety organization and Software Assurance personnel; the process includes the verification that all software safety requirements have been met).

The Provider Software Safety Manager will:

a. Assure that all safety-critical software has been certified prior to release for operational use (this includes tools, COTS, legacy, and reuse software).

b. Evaluate and approve that all software safety activities have been completed prior to acceptance/certification by the Acquirer Software Safety Manager (present the certification products to the Acquirer Software Safety Manager. The items required to be included in the certification data package are:

1. identification of all software related hazards

2. identification of all hazard controls that are implemented with software

3. identification and bidirectional tracking of all software safety requirements to implementation

4. verification results and approved waiver/exceptions for all software safety requirements

5. verification that all safety discrepancy dispositions and operational workarounds have the approval of the Acquirer Software Safety Manager
4.2.6.7. **Operational Use of Safety-Critical Software**

The Acquirer and Provider Software Safety Managers will:

a. evaluate software safety CRs; this includes assessment of regression testing, and verification of the new requirements for impacts to the existing safety critical software

b. assure the operational documentation includes all safety-related commands, data, input/output sequences, expected user responses, corrective actions, and a description of the error messages

The Acquirer Software Safety Manager will evaluate and approve updates to the user’s guide for safety impacts.

4.3. **CSCI Software Classification**

Each EVA System software CSCI will be evaluated in accordance to NPR 7150.2 Appendix B. A software safety litmus test shall be performed using NASA-STD-8739.8 Appendix A.1 to determine if the software is safety-critical. If the software is found to be safety-critical, Section 4.2.6 shall be followed. Software assurance will use NASA-STD-8739.8, Appendix A.2, to determine the Software Class. NASA-STD-8739.8, Appendix A.4, will be used to determine the minimum set of quality assurance activities that need to be done. Software assurance, GRC Code QE, will keep a copy of each evaluation available for inspection.

4.3.1. **Caution, Warning, and Control CSCI**

The Caution, Warning, and Control CSCI is classified as Class A requiring full/high assurance coverage. The safety litmus test determined the CSCI to be safety critical. This makes Section 4.2.6 applicable.

4.3.2. **Communications and Navigation CSCI**

The Communications and Navigation CSCI is classified as Class A requiring full/medium assurance coverage. The safety litmus test determined the CSCI to not be safety critical.

It was assumed that basic navigational functionality to return from a 10 km walk-back scenario will be hardware-based (no software, no firmware/complex electronics). This is possible if a Radio Direction Finder and simple directional tone or needle is used. This is an assumption that will be revisited once the operational scenarios, requirements, and architecture firm up and FMEA/hazard analyses are done. If software/firmware or complex electronics are to be used, this CSCI will be reclassified as safety critical.
4.3.3. Information Processing CSCI

The Communications and Navigation CSCI is classified as class C requiring medium assurance coverage. The safety litmus test determined the CSCI to not be safety critical.

4.3.4. Vehicle Interface CSCI

The Vehicle Interface CSCI is classified as class A requiring full/high assurance coverage. The safety litmus test determined the CSCI to be safety critical. This makes Section 4.2.6 applicable.

4.3.5. Tools and Equipment CSCI

The Tools and Equipment CSCI is classified as class TBD 4-2. The safety litmus test determined the CSCI to TBD 4-3.

4.3.6. Ground Software CSCI

The Ground Software CSCI is classified as class TBD 4-4. The safety litmus test determined the CSCI to TBD 4-5.

4.3.7. Simulations

No independent simulations are planned at this time. Any simulations done by the previously assessed CSCIs will be classified the same as the CSCI using the simulation.

4.3.8. Data and Files

No independent data or files are planned at this time. Any data/file developed for previously assessed CSCIs will be classified the same as the CSCI.

5. COMPLEX ELECTRONICS

5.1. Purpose

The purpose of this section is to document the CEA tasks and resources required to support the EVA Systems Project. This Complex Electronics Assurance Plan (CEAP) will be used to assure that the complex electronics being developed for the EVA Systems Project meets the technical requirements of the project, operates safely, and is developed according to sound development processes throughout its lifecycle. Software assurance efforts for complex electronics will be directed at the individual complex electronics component level before system integration.
The responsibility for assuring that Complex Electronics Development (CED) activities are conducted in accordance with requirements and standards is shared between the Acquirer and the Provider.

### 5.2. Scope

The assignment of CEA tasks is derived from the Classification Assessment performed per CxP 70059, and the following considerations:

a. The complex electronics executes safety-critical functions.

b. The complex electronics executes mission-critical functions and is a single point of failure.

c. The design is expected to be highly complex.

EVA is classified as government furnished equipment for the CxP. As such, the assurance guidelines and requirements are derived from CxP 70059 and CxP 70065.

#### 5.2.1. Roles and Responsibilities

Software assurance will be the primary assurance organization during the software programming and verification up to burning the complex electronics.

Hardware assurance will be the primary assurance organization once the complex electronics becomes hardware.

Changes or modifications to the complex electronics will be assessed by hardware and software assurance.

#### 5.2.2. Tasks

The goal of CEA is to assure the safety, reliability, and quality of the device by:

a. verifying that the documented development processes and controls used by the project are adhered to and effective

b. evaluating the development products (i.e., complex electronics design and documentation, for completeness and correctness)

CEA functions as part of the development team, not as an external entity with only limited interaction with the project. In order to function effectively and meet its goals, CEA:

a. attends project meetings
b. is an integral part of the complex electronics document review process

c. performs on scheduled audits of the various development activities

d. reports results of activities

5.2.2.1. Complex Electronics Development (CED) Phases

Complex electronics follow a combination of the software and hardware development phases. Up until the point where the CED design is actually transformed into hardware, the development follows a basic software development lifecycle process. It is important to note that the software design will be slightly modified during the burning and pre-burning processes due to optimization and other factors. Deliverables for milestone reviews are defined per Appendix C.

Due to the nature of the CED process, it is not possible to verify all requirements prior to the implementation of the design. As such, the Software Assurance personnel are required to maintain involvement during the hardware testing of complex electronic devices. To ensure that all requirements are adequately tested, software assurance will participate in the review and traceability of requirements to test plans, test cases, and task performance sheets at the complex electronic component level.

5.2.2.2. Complex Electronics Requirements Phase

The complex electronics requirements phase (a component phase) begins at the PDR and is completed before the system CDR.

a. Requirements for the subsystem(s) that the complex electronics resides in should be complete and baselined. As with the system requirements, the level of fidelity must be sufficient to allow derivation of the complex electronics requirements to commence.

b. The proposed complex electronics technology set (e.g., FPGA, ASIC, SoC, chip family) is identified at a high level.

CEA shall review the System Requirements Document, the Complex Electronics Requirements Document, project safety data package, and other sources of complex electronics requirements.

a. Requirements evaluation, complete assessment against all criteria.

b. Detailed analysis of throughput, bandwidth, and timing.

c. Traceability analysis, tracing from higher-level requirements to complex electronics requirements and the reverse.
d. Review of fault trees and FMEAs for
   
   1. complex electronics failures and

   2. affects of other failures on the complex electronics.

CEA shall participate in all project requirements reviews for complex electronics. This includes both informal and formal reviews.

5.2.2.3. Complex Electronics Preliminary Design Phase

CEA shall review the selected tools for applicability to the design process and evaluation of known tool defects or operational workarounds. CEA shall verify, through Hardware Design Language (HDL) code review or audit, that a design/coding standard has been defined and is being used by the developer.

a. Update detailed analysis of all interfaces and timing.

b. Trace from complex electronics requirements to design blocks and the reverse. Verify all functionality in the design is covered by requirements.

c. If FTA exists, map appropriate failures to complex electronics architectural blocks.

d. If FMEA exists, add appropriate failures of complex electronics architectural blocks and trace to system impacts.

e. Planned measures, tools, methods, and procedures have been applied.

f. Electrical, Electronic, and Electromechanical (EEE) parts approval of chip selection.

5.2.2.4. Complex Electronics Detailed Design Phase

The complex electronics detailed design phase (component phase) begins at the system CDR and is complete before the system TRR.

CEA shall perform the tasks and analyses as defined below:

a. Evaluate the detailed design as part of the System CDR.

b. Review and assign GMIPs to ensure Quality Assurance will witness the developer's simulations and tests.

c. Ensure that the complex electronics detailed design is under configuration control. At the end of the phase, ensure that the detailed design is approved and baselined.
Additional assurance activities require someone with expertise in complex electronics.

a. Review the constraints specified by the design engineer as input into the synthesis process for reasonableness.

b. Assess the simulations that were performed after design synthesis is completed. Did the addition of timing information affect the outcomes of the simulations? Did the simulations look at worst-case timing, including incoming signals?

c. Ensure that timing simulations or static timing analyses were performed.

d. Verify that the simulations performed included out-of-range inputs, inputs that arrived in an incorrect order, and other “real world” problems that can be anticipated.

5.2.2.5. Implementation Phase

The complex electronics implementation phase (component phase) begins after the system TRR and is complete by the SAR.

a. review problem reports for anomalies and problems that could be caused by complex electronics or that can adversely impact the complex electronics

b. perform Functional and Physical Configuration Audits

c. perform a formal audit of the CED process

d. verify that the tools specified in the project plans were the ones used. Note any discrepancies and the rationale for using a different tool

e. audit the configuration management process to ensure the HDL code and toolset used are CM controlled

f. verify that the device is programmed according to a defined process and that it is witnessed by Quality Assurance personnel

g. verify that post-layout and post-programming verifications are performed/record any anomalies or problems using the appropriate problem reporting process

h. assess problem reports relating to complex electronics for adequate root cause identification and appropriate corrections

5.2.2.6. Complex Electronics Testing Phase

The complex electronics testing phase (component phase) begins after the complex electronics implementation phase (component phase) and is complete by the SAR.
Testing will trace to each individual complex electronics before integration into the EVA system.

CEA shall perform the following tasks in conjunction with hardware quality engineering as appropriate:

a. review and approve test plans and procedures/witness testing and review test results.

b. ensure all requirements and design elements trace to test, analysis, or inspection/perform backward trace.

c. perform a formal audit of the complex electronics testing process

d. audit the configuration management process

e. verify that problems and anomalies are being recorded in the project problem reporting/corrective action system, and that the problem resolutions are correct, approved, and properly implemented

f. ensure that all safety verifications are performed

5.2.2.7. Acceptance and Release

Software assurance is complete once the individual complex electronics have completed testing. Hardware assurance will perform integration testing.

CEA shall perform the following process tasks:

a. review and approve test plans and procedures

b. witness testing and review test results

c. audit the problem reporting/resolution process

d. perform an analysis for any changes to the design, considering the testing that has occurred before and the possibility of affecting other parts of the system

5.2.2.8. Operations and Maintenance

Significant changes to complex electronics shall go through the requirements-design-implement-test life cycle in some form. The assurance activities required by those life-cycle phases shall be applied in an appropriate manner, tailored to the original criticality classification of the device and the complexity and amount of change in the design.
5.2.2.9. Complex Electronics Supporting Processes

5.2.2.9.1. Safety

If the complex electronics is safety-related, the CEA shall:

a. review the outputs of the system safety process, such as the Preliminary Hazard Analysis and subsequent analyses

b. feed back to the system safety engineer information on design changes within the complex electronics, or that affect the complex electronics

c. provide the system safety engineer with the results of evaluations and analyses

d. include evaluations of the safety-related design aspects in design evaluations and reviews

e. ensure that test procedures provide sufficient verification of the safety features in both nominal and fault/failure (off-nominal) scenarios

5.2.2.9.2. Problem Reporting and Resolution

CEA shall input observed complex electronics anomalies and problems into the project’s problem reporting/resolution system. CEA shall review the root cause evaluation process for any problem determined to be caused by the complex electronics. CEA shall concur with the resolution to any problem which is caused by, or that can affect, complex electronics. CEA shall periodically review the problem reporting/resolution system to identify complex electronics related problems that may have been misidentified.

5.3. Documentation

CEA shall review the documents specified in C2.0, Provider Deliverables, for completeness, accuracy, and compliance to CxP 70086 and CxP 70065. Documents will be approved, if applicable, prior to their formal submittal to configuration control.

5.4. Reviews

Peer reviews, inspections, and formal reviews (e.g., SRR, PDR, CDR, TRR, and SAR) will be held to insure the HDL and complex electronic device meets standards and requirements. CEA will have the ability to attend these reviews as deemed prudent.

5.5. Audits

CEA shall audit the CED and related processes for the EVA Systems Project according to the procedures identified in this section. CEA shall plan and maintain audit
schedules based on life-cycle phases, the complex electronics products of each phase and past audit results. Prior to the start of each audit, CEA shall:

a. review the standards, practices, requirements, and procedures of the area being audited

b. prepare or modify as needed the audit checklists

CEA audits shall cover the following areas:

a. Requirements management
b. Risk management
c. Planning
d. Configuration management and change control
e. PRACA System
f. Testing
g. Complex Electronics Development (CED) folders
h. Safety Plan

Audits may include more than one area when possible.

CEA may request support from the engineering organization responsible for the area being audited. This support may be in the form of personnel, records, files, and procedures. Examinations during an audit may include both processes and products. The results of the audits shall be documented.

5.6. HDL Code Reviews

CEA shall perform HDL code reviews separately or as part of the peer review process to verify compliance to the design and coding standards and to verify traceability to the requirements. The complex electronics design and “coding” may be conducted by developing a model and subsequently auto-generating the HDL code from the model. Less emphasis would be placed on the code review if the model is correct and the auto coder is certified to accurately translate the model into code, rendering the code review less useful.

If so, assurance should include the following:

a. independent design review of the model
b. certification of the auto-coder (certify that the auto-coder accurately translates the model into code)

5.7. Test

All EVA complex electronics tests are identified in the Verification and Validation Plan.

5.8. Deliverables

The provider Software Assurance Manager shall provide at a minimum the following items:

a. an engineering drawing of the as-delivered complex electronics device, which includes:
   1. toolset used including version information
   2. optimization information
b. the HDL code, source code, or Unified Modeling Language (UML) model
c. test Bench and timing models used
d. binary file used to create the delivered complex electronics device
e. requirements verification matrix which traces back to all parent requirements and shows self-imposed requirements

Complex electronics that are determined to be safety critical require the following additional deliverables:

a. Complex Electronics Verification and Validation Plan
b. Complex Electronics Safety-Criticality Assessment and Assurance Classification
c. Complex Electronics Assurance Plan (CEAP)
d. Complex Electronics Inputs into the Safety Data Package

6. RISK MANAGEMENT

Risks will be routinely addressed by the Acquirer Software Assurance Manager and formally documented by the Provider Software Assurance Manager. The Acquirer Software Assurance Manager will document risks concerning multiple Providers or posing potential impact to the EVA system. All risks will be reported to the EVA Project Manager on a monthly basis for integration into the EVA risk management database.

7. SOFTWARE ASSURANCE PROGRAM METRICS

The Software Assurance Measurement Program will meet the following high-level goals:

a. Improve future planning and cost estimation

b. Provide realistic data for progress tracking

c. Provide indicators of software quality

d. Provide baseline information for future process improvement activities

The Acquirer Software Assurance Manager will monitor, analyze, and control software assurance support based on metrics gathered from the Program and the Providers. Potential process improvement or corrective action may be applied in areas such as resources, planned process and product assessments, and training for Software Assurance personnel.

The Acquirer Software Assurance Manager will prepare the EVA metrics from the following metrics provided by the Provider Software Assurance Manager:

a. EVA software assurance effort and funds expended (planned versus actual)

b. number of completed software assurance tasks or deliverables (planned versus actual)

c. summary of EVA corrective actions against software assurance activities (open versus closed)

d. number and risk level of risks identified by EVA Software Assurance personnel, trends from Provider measures (e.g., defect classifications, rework)

e. summary of quality, reliability, safety, and V&V status (planned and completed activities)

The Provider Software Assurance Manager will define a set of Software Assurance metrics in the Provider’s Software Assurance Plan. At a minimum, the metrics would include the following:

a. Test maturity (e.g., number of test cases applied)

b. Quality measures (e.g., defect density)
c. Extent and cost of rework (e.g., amount that needs rework)

d. Development characteristics (e.g., software size, amount of reuse, etc.)

Required Software development metrics can be found in CxP 72268, EVA Software Development Plan.

8. SOFTWARE ASSURANCE RECORDS

Software assurance records include, but are not limited to, assessment results, software assurance classification results, reliability analyses, hazard analyses, assurance plans, schedules, metrics, risks, status, and deliverables created throughout the life cycle. Software assurance records include all records and deliverables from the disciplines of software quality, software safety, software reliability, and V&V.

The Acquirer and Provider Software Assurance Managers will:

a. assure that the EVA Systems Project software assurance records are maintained on Windchill (this facilitates information availability and data sharing across EVA and the Providers)

b. initiate communication with the IV&V Facility to acquire and maintain the applicable monthly IV&V reports

c. ensure that the archival and disposal of software assurance records and documents will be documented in the Provider’s retirement plan

9. TRAINING

Acquirer and Provider Software Assurance personnel will have fundamental knowledge in the following areas/disciplines through prior experience, training, or certification in methodologies, processes, and standards:

a. Software Quality Assurance

b. Software Quality Engineering

c. Audits and reviews

d. Risk management

e. Configuration management

f. Systems and Software Safety

g. Software reliability
h. Contracts/Contractor Surveillance

i. Verification and Validation (V&V)

j. International Organization for Standardization (ISO) AS9100B, Quality Management Systems–Aerospace Requirements

k. General knowledge of CMMI and detailed knowledge of the PPQA process area

Training logs/records will be maintained by the assurance practitioner’s home organization and be made readily available for review.
APPENDIX A
ACRONYMS AND ABBREVIATIONS
AND GLOSSARY OF TERMS

A1.0 ACRONYMS AND ABBREVIATIONS

ADP  Acceptance Data Package
ASIC  Application-Specific Integrated Circuit
BIT   Built-In Test
BITE  Built-In Test Equipment
CEA   Complex Electronics Assurance
CEAP  Complex Electronics Assurance Plan
CED   Complex Electronics Development
CDR   Critical Design Review
CIL   Critical Items List
CMMI  Capability Maturity Model Integration
COTS  Commercial Off-the-Shelf
CPLD  Complex Programmable Logic Device
CR    Change Request
CSCI  Computer Software Configuration Item
CxP   Constellation Program
DRD   Data Requirements Document
EEE   Electrical, Electronic, and Electromechanical
EEPROM Electrically Erasable Programmable Read-Only Memory
ESPO  EVA Systems Project Office
EVA   Extravehicular Activity
EVAPCB EVA Systems Project Control Board
FCA/PCA Functional Configuration Audit/Physical Configuration Audit
FMEA  Failure Modes and Effects Analysis
FPGA  Field Programmable Gate Array
FTA   Fault Tree Analysis
GMIP  Government Mandatory Inspection Point
GOTS  Government Off-the-Shelf
GRC Glenn Research Center

HDL Hardware Design Language

IEEE Institute of Electrical and Electronics Engineers

IPEP IV&V Project Execution Plan

ISO International Organization for Standardization

ITA Internal Task Agreement

IV&V Independent Verification and Validation

JSC Johnson Space Center

MIVP Master Integration and Verification Plan

MOA Memorandum of Agreement

MOTS Modified Off-the-Shelf

MOU Memorandum of Understanding

NASA National Aeronautics and Space Administration

NPR NASA Procedural Requirement

OPR Office of Primary Responsibility

PDR Preliminary Design Review

PPAD Project Assurance Division

PPQA Process and Product Quality Assurance

PRACA Problem Reporting Analysis and Corrective Action

RFP Request for Proposal

S&MA Safety and Mission Assurance

SACP Software and Avionics Control Panel

SAR System Acceptance Review

SAWG Software Assurance Working Group

SoC System on Chip

SOW Statement of Work

SRR System Requirements Review

SR&QA Safety, Reliability and Quality Assurance

STA Safety and Mission Assurance Technical Authority

SW Software
### A2.0 GLOSSARY OF TERMS

This section contains glossary terms that are important to this plan.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquirer</td>
<td>The entity or individual who specifies the requirements and accepts the resulting software products. The acquirer is usually NASA or an organization within the Agency but can also refer to the Prime contractor.</td>
</tr>
<tr>
<td>Anomaly</td>
<td>An unexpected event such as hardware or software malfunction, departures from established procedures or performance, process escapes, quality escapes and suspected problems, or a deviation of system, subsystem, and/or hardware or software performance outside certified or approved design/performance specification limits.</td>
</tr>
<tr>
<td>Complex Electronics</td>
<td>Programmable devices that can be used to implement specific hardware circuits. Some examples are FPGA, SoC, ASIC, and CPLD.</td>
</tr>
<tr>
<td>Design-ware</td>
<td>Hardware Design Language (HDL) code that will be used to create a binary file that defines the logic design to create in the hardware. Some examples of HDL are Verilog, Very High-level Design Language (VHDL), or even C. The HDL code itself is never put on the hardware device.</td>
</tr>
<tr>
<td>Executable code</td>
<td>Binary object file, compiled from assembly language or a high-level language such as C++ or Java, for a processor to execute.</td>
</tr>
<tr>
<td>Firmware</td>
<td>Executable code, source code, files, and data stored on a read-only device (e.g., Electrically Erasable Programmable Read-Only Memory [EEPROM], executable code stored on complex electronics).</td>
</tr>
<tr>
<td>Insight</td>
<td>Surveillance mode requiring the monitoring of acquirer identified metrics and contracted milestones. Insight is a continuum that can range from low intensity like reviewing quarterly reports to high intensity such as performing audits and reviews.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Noncompliance</td>
<td>Failure to comply with a requirement, procedure, standard, or specification.</td>
</tr>
<tr>
<td>Oversight (Surveillance)</td>
<td>Surveillance mode that is in line with the provider’s processes. The acquirer retains and exercises the right to concur or nonconcur with the provider’s decisions. Nonconcurrency must be resolved before the provider can proceed. Oversight is a continuum that can range from low intensity, such as acquirer concurrence in reviews, to high intensity oversight, in which the customer has day-to-day involvement in the provider’s decision-making process (e.g., software inspections).</td>
</tr>
<tr>
<td>Provider</td>
<td>The entities or individuals that design, develop, implement, test, and maintain the software products. A provider may be a contractor, a university, a separate organization within NASA or within the same organization as the acquirer.</td>
</tr>
<tr>
<td>Software</td>
<td>Executable code, source code, files, and data stored on a Read-Write device (e.g., hard drives, flash, RAM). This includes all software, firmware, data, computer programs for complex electronics, Government Off-the-Shelf (GOTS) software, Modified Off-the-Shelf (MOTS) software, and Commercial Off-the-Shelf (COTS) software when included in a NASA system.</td>
</tr>
<tr>
<td>Software Assurance</td>
<td>The planned and systematic set of activities that ensure that software life-cycle processes and products conform to requirements, standards, and procedures. [IEEE 610.12-1990] For NASA, this includes the disciplines of Software Quality, Software Safety, Software Reliability, Software Verification and Validation (V&amp;V), and Independent Verification and Validation (IV&amp;V).</td>
</tr>
</tbody>
</table>
| Software Error           | a. Mistake in engineering, requirement specification, or design.  
b. Mistake in design, implementation or operation that could cause a failure.                                                                 |
<p>| Software Failure         | The inability of a system or component to perform its required functions within specified performance requirements. (IEEE Standard 610.12-1990)                                                                 |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Fault</td>
<td>Any change in state of an item that is considered to be anomalous and may warrant some type of corrective action. Examples of faults include device errors reported by Built-In Test (BIT)/Built-In Test Equipment (BITE); out-of-limits conditions on sensor values; loss of communication with devices; loss of power to a device; communication error on bus transaction; software exceptions (e.g., divide by zero, file not found); rejected commands; measured performance values outside of commanded or expected values; an incorrect step, process, or data definition in a computer program; etc. Faults are preliminary indications that a failure may have occurred.</td>
</tr>
<tr>
<td>Software Hazard</td>
<td>A hazard caused by incorrect software control of hazardous hardware. The software might be functioning correctly (according to its requirements) or in a failure mode.</td>
</tr>
</tbody>
</table>
APPENDIX B

OPEN WORK

B1.0 TO BE DETERMINED

The table below lists the specific To Be Determined (TBD) items in the document that are not yet known. The TBD is inserted as a placeholder wherever the required data is needed and is formatted in bold type within brackets. The TBD item is numbered based on the section where the first occurrence of the item is located as the first digit and a consecutive number as the second digit (i.e., <TBD 4-1> is the first undetermined item assigned in Section 4.0 of the document). As each TBD is solved, the updated text is inserted in each place that the TBD appears in the document and the item is removed from this table. As new TBD items are assigned, they will be added to this list in accordance with the above-described numbering scheme. Original TBDs will not be renumbered.

TABLE B1-1 TO BE DETERMINED ITEMS

<table>
<thead>
<tr>
<th>TBD</th>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-1</td>
<td>4.2.5</td>
<td>A documented agreement between ESPO and NASA IV&amp;V does not exist yet.</td>
</tr>
<tr>
<td>4-2</td>
<td>4.3.5</td>
<td>The software components that will be in the Tools and Equipment CSCI have not been determined yet, so a classification cannot be done.</td>
</tr>
<tr>
<td>4-3</td>
<td>4.3.5</td>
<td>The software components that will be in the Tools and Equipment CSCI have not been determined yet, so a safety critical determination cannot be made.</td>
</tr>
<tr>
<td>4-4</td>
<td>4.3.6</td>
<td>The software components that will be in the Ground Software CSCI have not been determined yet, so a classification cannot be done.</td>
</tr>
<tr>
<td>4-5</td>
<td>4.3.6</td>
<td>The software components that will be in the Ground Software CSCI have not been determined yet, so a safety critical determination cannot be made.</td>
</tr>
</tbody>
</table>
B2.0 TO BE RESOLVED

The table below lists the specific To Be Resolved (TBR) issues in the document that are not yet known. The TBR is inserted as a placeholder wherever the required data is needed and is formatted in bold type within brackets. The TBR issue is numbered based on the section where the first occurrence of the issue is located as the first digit and a consecutive number as the second digit (i.e., <TBR 4-1> is the first unresolved issue assigned in Section 4.0 of the document). As each TBR is resolved, the updated text is inserted in each place that the TBR appears in the document and the issue is removed from this table. As new TBR issues are assigned, they will be added to this list in accordance with the above-described numbering scheme. Original TBRs will not be renumbered.

**TABLE B2-1 TO BE RESOLVED ISSUES**

<table>
<thead>
<tr>
<th>TBD</th>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX C
PROVIDER DELIVERABLES

C1.0 SOFTWARE ASSURANCE REPORTING

Each Provider Software Assurance Manager will report quarterly to the Acquirer Software Assurance Manager. Quarterly reporting will be electronically submitted and will cover the software disciplines of quality, reliability, V&V, and safety. The format for each discipline will include:

a. planned versus actual activities
b. significant accomplishments/issues (see the respective sections for detailed Provider information)
c. summary of corrective and preventive actions
d. status of deliverables
e. software assurance risks in the EVA risk management database
f. audit reports including inspection records, review records, and Functional Configuration Audit/Physical Configuration Audit (FCA/PCA) reports
g. quality costs and schedules
h. metrics (Section 6.0 of this Plan)

C2.0 PROVIDER DELIVERABLES

This identifies the set of artifacts and deliverables to be developed by the Provider in compliance with CxP 70065. This list is provided as the minimum set of documentation listed in Section 4.0 of this Plan.

a. Software Assurance Classification and Software Safety-Criticality Assessment
b. Software Assurance Plan (DRD CSSS-S-012)
c. Software Development Plan (DRD CSSS-T-036)
d. Software Safety Plan (See Section 4.2.6.1) (DRD CSSS-S-012)
e. Software inputs into the Safety Data Package (See Section 4.2.6.2)
f. Software Requirements Specification (DRD CSSS-T-042)
g. Configuration Management Plan (DRD CSSS-M-004)
h. Risk Management Plan (DRD CSSS-M-006)

i. Software Verification and Validation Plan (See master Verification Plan)

j. Program Review Packages (Acceptance/Certification Data Packages)

k. Software Design Documentation (DRD CSSS-T-043)

l. Coding standards (See Software Development Plan)

m. Software Version Description Document (DRD CSSS-T-052)

n. Software User Guides (DRD CSSS-T-051)

o. Software Maintenance Plan (DRD CSSS-T-050)

p. Project software