-
National Aeronautics and
Space Administration

GRC-CONN-PLAN-0085 A
EFFECTIVE DATE: 05/17/2012

<u>Space Communications and Navigation</u> (SCaN) Testbed Project

National Aeronautics and Space Administration
John H. Glenn Research Center at Lewis Field, OH 44135

SCAN TESTBED PROJECT

SOFTWARE ASSURANCE PLAN

AUTHORIZED by CM when under FORMAL Configuration Control	
Date	**Signature**
5/22/12	*/s/ Robert E. Turk*

Distribution:

[ ] NASA (U.S. Gov. Only) [ ] Project Only [X] Government and Contractors

Availability:

[X] Public (No Restriction) [ ] Export Controlled [ ] Confidential/ Commercial [ ] Internal Use Only

CHECK THE MASTER LIST—VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE

PREFACE

National Aeronautics and Space Administration (NASA) is developing an on-orbit, adaptable, Software Defined Radio (SDR)/Space Telecommunications Radio System (STRS)-based testbed facility to conduct a suite of experiments to advance technologies, reduce risk, and enable future mission capabilities on the International Space Station (ISS). The Space Communications and Navigation (SCaN) Testbed Project will provide NASA, industry, other Government agencies, and academic partners the opportunity to develop and field communications, navigation, and networking technologies in the laboratory and space environment based on reconfigurable, software defined radio platforms and the STRS Architecture. The project was previously known as the Communications, Navigation, and Networking reConfigurable Testbed (CoNNeCT). Also included are the required support efforts for Mission Integration and Operations, consisting of a ground system and the Glenn Telescience Support Center (GRC TSC). This document has been prepared in accordance with NASA Glenn's Configuration Management Procedural Requirements GLPR 8040.1 and applies to the SCaN Testbed configuration management activities performed at NASA's Glenn Research Center (GRC). This document is consistent with the requirements of SSP 41170, Configuration Management Requirements, International Space Station, and GLPR 7120.5.30 Space Assurance Requirements (SAR).

This document establishes the process and responsibilities required to implement effective software quality assurance functions for the SCaN Testbed project at the Glenn Research Center (GRC).

DOCUMENT HISTORY LOG

Status (Preliminary/ Baseline/ Revision/ Canceled)	Document Revision	Effective Date	Description
Preliminary	Draft	03/20/2009	Initial Release
Preliminary	Draft 1		Post internal review
Preliminary	Draft 2	05/05/2009	Incorporate comments from review
Preliminary	Draft 3	05/19/2009	Add SBU, Fix page numbering
Preliminary	Draft 4	06/30/2009	Fixes per review comments
Preliminary	Draft 5	07/27/2009	Remove SBU Comments on CE and safety
Preliminary	Draft 6	08/07/2009	Double checked review comments and added missing statements
Preliminary	Draft 7	10/27/2009	More details in process audit planning
Preliminary	Draft 8	11/09/2009	Comments from reviewers
Preliminary	Draft 9	11/30/2009	Remove section references to SMDP and references to Ground and Payload Software Req document. It' just one document.
Preliminary	Draft 10	01/04/2010	Changes per SWCDR review RIDS Changes are highlighted, RIDS are in comment balloons.
Preliminary	Draft 11	02/02/2010	Further updates per RID comments
Preliminary	Draft 12	02/16/2010	Audit Schedule in Appendix E
Preliminary	Draft 13	02/18/2010	Update effort estimate to .85
Baseline	–	03/16/2010	Submit to CM; Changes from CDR eRoom Inspection
Revision	A	05/17/2012	Incorporated Change Request CONN-CR-0489

SIGNATURE PAGE

Prepared By:

/s/ Richard Plastow — *5/18/12*

Richard Plastow — Date
Software Assurance Engineer
Bastion Technologies

Concurred By:

/s/ Joshua E Freeh — *5/17/12*

Joshua Freeh — Date
SCaN Testbed Chief Engineer
NASA Glenn Research Center

Approved By:

/s/ Denise Varga — *5/19/12*

Denise Varga — Date
SCaN Testbed Software Engineering Lead
NASA Glenn Research Center

/s/ Diane Malarik — *5/17/12*

Diane Malarik — Date
SCaN Testbed Project Manager
NASA Glenn Research Center

TABLE OF CONTENTS

1.0 INTRODUCTION 1
1.1 Purpose 1
2.0 APPLICABLE DOCUMENTS 3
2.1 Applicable Documents 3
2.2 Controlling Documents 3
2.3 Impacted Documents 4
2.4 Order of Precedence for Documents 4
3.0 MANAGEMENT 5
3.1 Organization 5
3.1.1 Chief Safety and Mission Assurance (SMA) Officer (SMA Technical Authority) 6
3.1.2 SMA Lead 7
3.1.3 Software Assurance Engineer 7
3.1.4 Software Safety Engineer 8
3.2 Tasks 8
3.2.1 Software Safety Assurance 9
3.2.2 Evaluate Deviations and Waivers 9
3.2.3 Evaluate System Requirements Analysis Process 10
3.2.4 Evaluate System Design Process 11
3.2.5 Evaluate Software Design Process 12
3.2.6 Evaluate Coding and Unit Testing (Implementation) Process 13
3.2.7 Evaluate Unit Integration and Testing, CSCI Qualification Testing, and CSCI/HWCI Integration and Testing 14
3.2.8 Evaluate Software Verification and Validation Testing 15
3.2.9 Evaluate Flight Software Acceptance Testing 16
3.2.10 Evaluate Operation on Delivery to Launch Site 16
3.2.11 Evaluate Software Configuration Management (SCM) Process 17
3.2.12 Evaluate Operations 17
3.3 Roles and Responsibilities 18
3.3.1 Overview 18
3.3.2 SMA Lead 20
3.3.3 Software Assurance Engineer 20
3.3.4 Software Safety Engineer 20
3.4 Quality Assurance Resource Estimates 20
4.0 DOCUMENTATION 21
4.1 Purpose 21
4.2 Minimum Documentation Requirements 21
4.2.1 Software Requirements 21
4.2.2 Software Design 21
4.2.3 Verification and Validation 22
4.2.4 Verification and Validation Results 22
4.2.5 Software Acceptance 22
4.2.6 User Manuals 22
4.2.7 Software Configuration Management Plan 23
5.0 STANDARDS, PRACTICES, CONVENTIONS, AND METRICS 24
5.1 Purpose 24
5.2 Software Quality Program 24

5.2.1 Standard Metrics 24
6.0 SOFTWARE REVIEWS 25
6.1 Purpose 25
6.2 Minimum Requirements 25
6.2.1 Software Architecture Review SAR 25
6.2.2 Software Critical Design Review SWCDR 25
6.2.3 Functional Configuration Audit 25
6.2.4 Physical Configuration Audit 25
6.2.5 In Process Audits 26
6.2.6 Managerial Review 26
6.2.7 Software Configuration Management Plan Review 26
6.2.8 Post Implementation Review 26
7.0 TESTS 27
8.0 PROBLEM REPORTING AND CORRECTIVE ACTION 28
9.0 TOOLS, TECHNIQUE'S AND METHODOLOGIES 29
9.1 Software Classification 29
9.2 Software Quality Tools 29
10.0 MEDIA CONTROL 30
11.0 SUPPLIER CONTROL 31
12.0 RECORDS COLLECTION 32
12.1 Document Review Report 32
12.2 Audit/Assessment Results 32
12.3 Meetings 32
12.4 Test Verification Report 32
13.0 TRAINING 33
14.0 RISK MANAGEMENT 34
15.0 GLOSSARY 35
16.0 PLAN CHANGE PROCEDURE AND HISTORY 36
16.1 History 36
17.0 COMPLEX ELECTRONICS 37
17.1 Criticality Classification 37
17.2 Tasks 37
17.2.1 CE Safety Assurance 37
17.2.2 Evaluate System Requirements Analysis Process 37
17.2.3 Evaluate Design Phase 38
17.2.4 Evaluate Synthesis Phase 38
17.2.5 Evaluate Implementation Process 39
17.2.6 Evaluate Testing 39
18.0 SAFETY CRITICAL SOFTWARE TASKS 40
18.1 Determinating Criticality 40
18.2 Planning 40
18.2.1 Tools 40
18.2.2 Documentation 40
18.2.3 Resources 41
18.2.3.1 Training 41
18.3 Safety Related Concerns 41
18.4 Evaluate Software and CE Requirements 42
18.5 Evaluate Software Design 42

18.6 Evaluate Implementation 42
18.7 Evaluate Testing 43
18.8 Certification 43
18.9 Operations 44
18.10 Software Safety Plan 44
18.10.1 Requirements Implementation 44
18.10.2 Activities and Schedules 44
18.10.3 Organization 44
18.10.4 Project Schedule 45
18.10.5 Safety Documentation 45
18.10.6 Approval Process 45
APPENDIX A ACRONYMS AND ABBREVIATIONS 46
A.1 Scope 46
A.2 List of Acronyms and Abbreviations 46
APPENDIX B DEFINITIONS 48
B.1 Scope 48
B.2 List of Definitions 48
APPENDIX C SOFTWARE CLASSIFICATION REPORTS 51
APPENDIX D SAMPLE RECORDS 54
APPENDIX E AUDIT OVERVIEW AND SCHEDULE 57
APPENDIX F FCA/PCA PLAN 62
19.0 FCA/PCA PLAN 62
19.1 Scope 62
19.2 Functional Configuration Audit (FCA) 62
19.2.1 Objective 62
19.2.2 Entrance Criteria 62
19.2.3 Audit Participants 63
19.2.4 Schedule Dates 63
19.2.5 Opening Meeting 63
19.2.6 Audit Activities 63
19.2.6.1 Desk Audit 63
19.2.6.2 Interview 64
19.2.6.3 Reporting 64
19.2.7 Audit Follow Up 64
19.2.8 Closing Meeting 64
19.3 Physical Configuration Audit 65
19.3.1 Objective 65
19.3.2 Entrance Criteria 65
19.3.3 Schedule Dates 65
19.3.4 Opening Meeting 66
19.3.5 Audit Activities 66
19.3.5.1 Desk Audit 66
19.3.5.2 Interview 66
19.3.5.3 Reporting 66
19.3.6 Audit Follow Up 66
19.3.7 Closing Meeting 66

TABLE OF FIGURES

Figure 3-1—Functional Organization Chart 5

TABLE OF TABLES

Table 1-1—CoNNeCT CSCIs 2
Table 3-1—System Requirement Analysis 10
Table 3-2—System Design 11
Table 3-3—Software Design 12
Table 3-4—Coding and Unit Testing 13
Table 3-5—Integration Testing 14
Table 3-6—Verification and Validation Testing 15
Table 3-7—Acceptance Testing 16
Table 3-8—Deviation and Waiver Responsibility 18
Table 3-9—Creating SAP Responsibility 18
Table 3-10—Software Requirements Responsibility 18
Table 3-11—Software Design Responsibility 18
Table 3-12—Coding and Unit Test Responsibility 19
Table 3-13—Unit Integration and Testing Responsibility 19
Table 3-14—Software Acceptance Testing Responsibility 19
Table 3-15—Flight Software Acceptance Testing Responsibility 20
Table 18-1—Software Safety Planning 40
Table 18-2—Software Safety Testing 43
Table A-1—Acronyms 46
Table B-1—Definitions 48

1.0 INTRODUCTION

1.1 Purpose

The purpose of this Software Assurance Plan (SAP) is to establish the processes, and responsibilities required to implement effective quality assurance functions for the CoNNeCT project at the Glenn Research Center (GRC). CoNNeCT also includes software developed at other Centers or organizations for Software Defined Radios (SDR) not covered by this plan. Organizations outside of GRC are responsible for Software Assurance (SA) per contractual obligations. SA at GRC does not plan to review or monitor these activities. This is discussed in the CoNNeCT Software Management and Development Plan (SMDP), GRC-CONN-PLAN-0024.

When software is developed at other Centers or organizations the software assurance tasks and responsibilities will be determined, documented in that Center(s) Software Assurance Plan(s), and flowed down to the Center(s) Software Assurance personnel accordingly. That Center is responsible for its own Software Assurance activities and personnel consistent with its contract. Activities and issues can be discussed at a bi-weekly Safety and Mission Assurance telecom held between GRC and the other Centers.

This Software Assurance Plan provides the framework necessary to ensure a consistent approach to software quality assurance throughout the project life cycle. It defines the approach that will be used by the Software Quality (SQ) personnel to monitor and assess software development processes and products to provide objective insight into the maturity and quality of the software. The systematic monitoring of products, processes, and services will be evaluated to ensure they meet requirements and comply with National Aeronautics and Space Administration (NASA), Glenn Research Center , and project policies, standards, and procedures, as well as applicable Institute of Electrical and Electronic Engineers (IEEE) standards.

This plan covers the software listed below that is developed at Glenn Research Center for the CoNNeCT project from inception through shipment of the hardware. This applies to software, firmware, complex electronics, data, Government Off-the-Shelf (GOTS) software, Modified Off-the-Shelf (MOTS) software, and Commercial Off-the-Shelf (COTS).

Complex Electronics (CE) is used for developing at GRC the application specific part of an SDR called “waveform”. CE involves using a hardware description language to design and initially test a hardware device.

Waveform development at GRC involves programming of a Field Programmable Gate Array (FPGA) with this developed waveform.

Software Assurance highly recommends (not required) any code generated by an automated tool and directly used in software has assurance that the automated code generator produces correct code. This can be done by test, by documentation from the vendor, or analysis of other application use providing evidence of correctness.

The specific Computer Software Configuration Items (CSCI) includes Table 1-1.

Table 1-1—CoNNeCT CSCIs

CSCI	Software Type	Function
CoNNeCT Payload Avionics Software (PAS)	C++, C, COTS	Processes commands, data, and telemetry; commands of Software Defined Radios (SDR) s; monitors system health; controls heaters; and operates the antennae gimbal. This software provides other functions as listed in the CoNNeCT Software Management and Development Plan (SMDP), GRC-CONN-PLAN-0024.
CoNNeCT Ground Software (GSW)	C++, C, GOTS	Controls flight operations and conduct SDR experiments. See the CoNNeCT Software Management and Development Plan (SMDP), GRC-CONN-PLAN-0024 for further details.
CoNNeCT GRC GSFC TDRSS (GGT) Waveform.	C++,COTS, GOTS, Complex Electronics	Software and Complex Electronics that is jointly developed by GSFC and GRC and provides operational characteristics for the JPL SDR. This also provides other functions as listed in the CoNNeCT GGT Development Plan (SMDP), GRC-CONN-PLAN-0076.

2.0 APPLICABLE DOCUMENTS

This section lists the NASA/Government and non-NASA/Government specifications, standards, guidelines, handbooks, or other special publications applicable to the application of this document.

2.1 Applicable Documents

Applicable documents are those documents that form a part of this document. These documents carry the same weight as if they were stated within the body of this document.

Document Number	Applicable Document
AS9100B	Quality Management Systems - Aerospace Requirements
NPR 8715.3	NASA General Safety Program Requirements
SSP 50038B	Computer-Based Control System Safety Requirements

2.2 Controlling Documents

Document Number	Reference Document
GLM-QE-8700.2 Rev C2	Space Assurance Requirements and Guidelines
GLPR 7150.1	GRC Software Engineering Requirements
GLPR 8739.1	GRC Software Assurance
GRC-SW-7150.3	Software Project Planning
GRC-SW-7150.4	Software Project Monitoring and Control
GRC-SW-7150.5	Requirements Management
GRC-SW-7150.9	Software Configuration Management
IEEE 730-2002	Institute of Electrical and Electronics Engineers(IEEE) Standard for Software Quality Assurance Plans
NASA-GB-8719.13	NASA Software Safety Guidebook
NASA-GB-A201	NASA Software Quality Assurance Guidebook
NASA-GB-A302	NASA Software Formal Inspections Guidebook
NASA-STD-8719.13B	NASA Software Safety Standard
NPR 1441.1	NASA Records Retention Schedules
NPR 7120.5D	NASA Space Flight Program and Project Management Requirements
SMAP-GB-A301	NASA Software Quality Audits Guidebook

2.3 Impacted Documents

The following documents, of the latest revision issued, are used in the execution of this plan to the extent specified herein.

Document Number	Impacted Document
GRC-CONN-BCD-0014	CoNNeCT Baseline Concept Description
GRC-CONN-PLAN-0001	CoNNeCT Software Configuration Management Plan
GRC-CONN-PLAN-0006	CoNNeCT Product Assurance Plan
GRC-CONN-PLAN-0007	CoNNeCT Risk Management Plan
GRC-CONN-PLAN-0024	CoNNeCT Software Management and Development Plan (SMDP)
GRC-CONN-PLAN-0076	CoNNeCT GRC GSFC TDRSS (GGT) Waveform Development Plan
GRC-CONN-REQ-0077	CoNNeCT GRC GSFC TDRSS (GGT) Waveform Requirements Specification
GRC-CONN-SRD-0013	CoNNeCT System Requirements Document

2.4 Order of Precedence for Documents

In the event of a conflict between this document and other documents specified herein, the requirements of this document shall apply. In the event of a conflict between this document and higher level documents, the higher level documents shall take precedence over this document.

All documents used, applicable, control, or impacted, are to be the issues defined in the *CoNNeCT Project Plan* (GRC-CONN-PLAN-0004). Nothing in this document supersedes applicable laws and regulations unless a specific exemption has been obtained.

3.0 MANAGEMENT

3.1 Organization

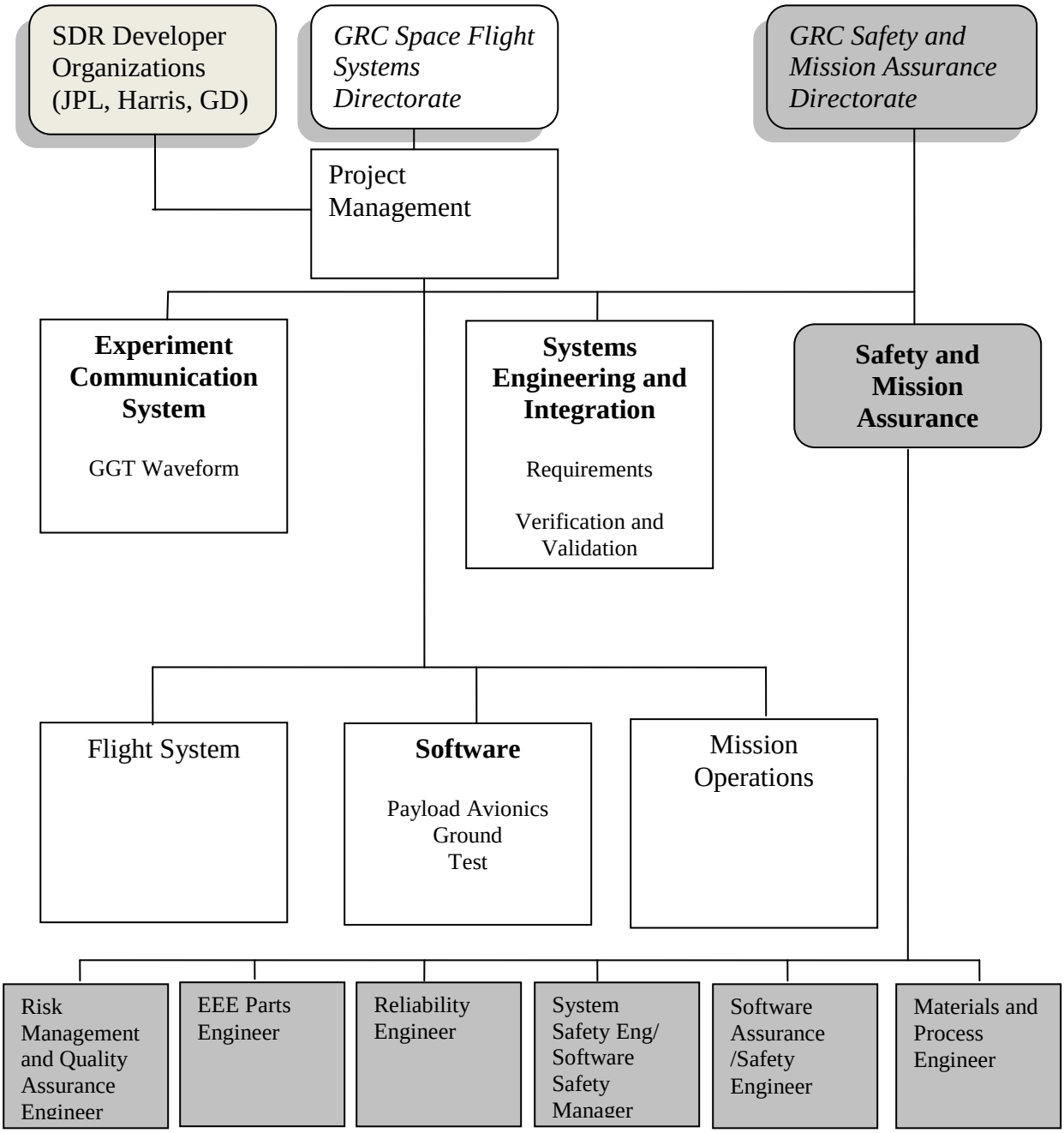

Figure 3-1—Functional Organization Chart

Figure 3-1 depicts a graphical representation of the organizations and disciplines which affect the quality of the software.

SDR Developer Organizations are responsible for the quality of software and complex electronics delivered per contract.

The **Software** discipline directly affects the quality by developing software for flight (Payload Avionics) and Ground.

The **Systems Engineering and Integration** has responsibility for requirements formation used for software development and verification and validation of the software.

The **Experiment Communications System** has responsibility for "waveform" development. The "waveform" can be considered the application executing on an SDR. The SDR functionality is achieved by the "waveform" it is executing.

Safety and Mission Assurance (SMA) has oversight responsibility for the products and processes used by the above groups. It has responsibility for the creation and maintenance of this plan.

Independence from the project is essential for objective reporting. SMA reports to a separate directorate from the project. Also, the Technical Authority (TA) process provides another means of independence separate from the project. The project's Chief SMA Officer (CSO) is the Software Assurance Technical Authority.

3.1.1 Chief Safety and Mission Assurance (SMA) Officer (SMA Technical Authority)

For the SMA branch the Chief SMA Officer (CSO) is on the primary technical authority path up through the GRC SMA Director to the GRC Director.

Independence is a key strength to SMA. SMA has the freedom, if the quality of the product is being jeopardized, to report this possibility directly above the level of the project by the CSO.

Independence of the TA is achieved because the CSO is not funded directly by the project and has a reporting path to the top of NASA, if necessary.

The CSO has directed the SMA Lead to act as his representative in daily activities. The CSO interacts directly with the project as needed.

- Duties include insight, oversight, identification, and development of compliance activities and delegation of responsibility for task execution.
- The CSO is the signature authority for plans for System Requirements Review, Preliminary Design Review, Critical Design Review, and Flight Readiness Review.
- Development of teams and tasks assignments to address SMA.
- Participates as a voting member of the project's Engineering Review Board (ERB) and Change Control Board (CCB).
- Escalate any non compliances, hazards, and risks to SMA management.

3.1.2 SMA Lead

The Safety and Mission Assurance (SMA) Lead is a representative of the CSO who covers daily project operations and activities. Important developments are reported as needed to the CSO.

Responsibilities include, but are not limited to:

- Provide general guidance and direction to the SA personnel responsible for conducting software quality activities.
- Assist SA personnel in the resolution of any non compliances, issues and/or risks identified as a result of software quality activities.
- Escalate any non compliances, hazards, and risks to project management and the project Chief SMA Officer (CSO), who holds the Software Assurance Technical Authority.
- Attends all formal milestone reviews and participates as needed.

3.1.3 Software Assurance Engineer

The Software Assurance Engineer is responsible for performing the tasks indicated within this document and communicating the status and results of such tasks to project management and the SMA Lead.

Responsibilities include, but are not limited to:

- Develop and maintain the project software assurance plan (SAP).
- Conduct process and product activities, as described within this plan, using objective criteria.
- Interface with Safety and Reliability personnel on software assurance activities.
- Identify and document non compliances, observations, and risks from all software assurance related activities to the SMA Lead.
- Attends SMA status meetings, as required.
- Communicate risks to risk management.
- Communicate results from assessments with relevant stakeholders.
- Ensure resolution of non compliances.
- Identify lessons learned that could improve processes for future products and support any Lessons Learned Workshops called for by the PM.
- Participates in the project’s ERB and CCB, when software issues are presented.
- Reviews informal unit testing activities.

- Attends all software related meeting, when possible.
- Attends all formal milestone reviews and participates as needed.
- Attend software risk management update sessions, when possible.
- Witnesses all formal verification and validation.
- Review all test plans and test procedure reports.

In addition, the SA Engineer is responsible for maintaining expertise in the latest methods and techniques in both Software Assurance and Software Development.

3.1.4 Software Safety Engineer

The Software Safety Engineer is responsible for performing the software safety assurance tasks indicated within this document and communicating the status and results of such tasks to project management and the SMA Lead.

The Software Assurance and Software Safety Engineer is the same person.

Responsibilities include, but are not limited to:

- Identify any safety critical commands or functions within the software.
- Ensures an audit of safety activities prior to Critical Design Review (CDR).
- Ensures the activities listed in Section 18 are carried out.

3.2 Tasks

This section summarizes the tasks (product and process assessments) to be performed during the development of the software. The GGT Waveform CSCI involves the use of Complex Electronics and additional tasks in Section 17.0 on Complex Electronics are to be performed.

SA shall perform the following tasks involving Document Reviews, Assessments, or Audits, Meeting attendance. The records of these tasks are described in Section 12 Records Collection.

3.2.1 Software Safety Assurance

In accordance with the Software Management & Development Plan, the software safety program shall ensure that:

- Safety-related deficiencies in specifications and design are identified and corrected.
- Software design incorporates positive measures to enhance the safety of the system.
- CSCI Design Documents will identify safety related commands and data via safety compliance data packages (which include Safety Analysis Reports and Safety Hazard Reports).

A Software Safety Litmus Test was done for each CSCI including CE using GLPR 8739.1 Appendix G and safety critical criteria was met for Payload Avionics Software. It has been determined that software controlling the inadvertent activation of RF energy (considered a Catastrophic Hazard) is safety critical. Software provides single fault tolerance for this function with two independent controls as part of an overall safety system being two (2) fault tolerant for Ka-Band RF energy per requirements of SSP 50038.

The NASA Software Safety Standard, NASA-STD-8719.13 shall be followed and the tasks in Section 18.0 on Safety Critical Software are to be performed.

3.2.2 Evaluate Deviations and Waivers

SA shall assist project management with requests for deviations and waivers, if required, and verify that the deviation or waiver request is processed in accordance with the Software Configuration Management Plan (SCMP) and approved by the appropriate approving authority.

3.2.3 Evaluate System Requirements Analysis Process

SA shall perform the tasks in Table 3-1. The artifacts produced are noted in the Method column and include Document Review Reports and Audit/Assessment Results. A more detailed schedule is shown in Appendix E.

Table 3-1—System Requirement Analysis

	Task	Method	Time
1	Ensure that all requirements are reviewed to determine if they are feasible to implement, clearly stated, consistent, and verifiable. SA is to be an active participant in these reviews.	Document Review of required documents Science, System Requirements down to Software Requirements.	At SRR Review
2	Ensure the necessary documentation is present leading up to the Software Requirements Review (SRR).	Document Review Science , System, down to Software Requirements.	At SRR Review
3	Confirm that a CM process is in place to control and manage the baseline requirements	Audit/Assessment of CM per Project CM Plan .	Before CDR
4	Confirm a CM process is in place for all CE artifact; Hardware Definition Language (HDL), Intellectual Property (IP), Synthesis Constraints, and Binary files, used to create hardware. This may be a drawing.	Audit/Assessment of SCM per project defined process or GRC-SW-7150.9 if none defined.	Before CDR
5	Confirm all software tools are Configuration Managed.	Audit/Assessment of SCM per project defined process or GRC-SW-7150.9 if none defined.	Before CDR
6	Confirm all CE tools are Configuration Managed.	Audit/Assessment of SCM per project defined process or GRC-SW-7150.9 if none defined.	Before CDR
7	CE Tool versions should remain the same after development starts.	Monitor CR Process.	
8	Ensure that changes to allocated requirements, work products, and activities are identified, reviewed, and tracked to closure. Completion signals the end of the Requirements phase, although additional requirements may still be defined and other requirements may be changed.	Monitor CR Process for Requirements changes.	Monthly

The results of these tasks shall be documented in the Software Assurance Folder in the CoNNeCT Project area on the eRoom server.

SA's recommendation for corrective action requires project management's disposition and will be processed in accordance with the project's requirements control process stated in the Software Management and Development Plan.

3.2.4 Evaluate System Design Process

A base lined set of Software Requirements is the criteria needed for the start of the Design Process. Base line is determined by project approval and document signature.

System-wide design decisions are decisions about the system's behavioral design and other decisions affecting the selection and design of system components. System architectural design is organizing a system into subsystems, organizing a subsystem into Hardware Configuration Items (HWCIs), Computer Software Configuration Items (CSCIs), and manual operations, or other variations (e.g., Computer Software Components CSCs), as appropriate.

SA shall perform the tasks in Table 3-2. The artifacts produced are Document Review Reports and Meeting Attendance Reports. A more detailed schedule is shown in Appendix E.

Table 3-2—System Design

	Task	Method	Time
1	Ensure that software design documents are prepared, reviewed, and consistent.	Document Review Software Design Document	At SW PDR Review
2	Verify that relevant design documents are updated and based on approved requirements.	Monitor CR Process for Design updates, Document Review Requirements to Design Traceability matrix Document.	After Software Architecture Baseline Before each milestone review
3	Ensure that design walkthroughs (peer reviews) evaluate compliance of the design to the requirements, identify defects in the design, and evaluate and report design alternatives.	Meeting Attendance of Design Walkthroughs and participation.	At project invitation
4	Verify resolution for identified defects, and ensure change control integrity.	Meeting Attendance Software Status Ask project for status of JIRA activity, Meeting Attendance Software Control Board (SCB). After release monitor CPAR resolution, review impact analysis reports and verify change implementation.	Monthly Attend MRB for software CPAR
5	Identify lack of compliance with standards and determine corrective actions.	Review NPR 7150.2 Class C Compliance Matrix	Once per month

The results of this task shall be documented using the CoNNeCT Software Assurance Folder in the CoNNeCT Project eRoom.

3.2.5 Evaluate Software Design Process

Preliminary design activity determines the overall structure of the software to be built.

A goal of detailed design is to define logically how the software will satisfy the allocated requirements.

For each CSCI, SA shall perform the tasks in Table 3-3. The artifacts produced are Document Review Reports and Meeting Attendance Reports. A more detailed schedule is shown in Appendix E.

Table 3-3—Software Design

	Task	Method	Time
1	Ensure that the software design process and associated design reviews are conducted in accordance with standards and procedures established by the project.	Meeting Attendance Design Peer Review	Throughout software design process
2	Ensure the necessary documentation and steps have been taken leading up to the Preliminary Design Review (PDR). The first portion of design ends with the resolution of actions from the PDR.	Assess Entrance Criteria for SW PDR Meeting Attendance Ask project for status of RID/RFA at software status meeting Examine list of PDR documentation	At SW PDR Monthly
3	Assure software requirements are traceable to the design.	Document Review Software Design and Requirements Traceability matrix	Prior to CDR
4	Ensure the necessary documentation and steps have been taken leading up to the Critical Design Review (CDR). The final portion of design ends with the resolution of actions from the CDR.	Assess entrance criteria for SW CDR Meeting Attendance Ask project for status of RID/RFA at software status meeting	At SW CDR Monthly
5	Ensure that action items resulting from reviews of the design are resolved in accordance with the applicable standards and procedures. Completion signals the end of design.	Meeting Attendance Software Status	Prior to each review

The results of this task shall be documented using the CoNNeCT Software Assurance Folder in the CoNNeCT Project eRoom.

3.2.6 Evaluate Coding and Unit Testing (Implementation) Process

Software implementation or coding is the point in the software development cycle at which the design is implemented. The process includes unit testing of the software code.

SA shall perform the tasks in Table 3-4. The artifacts produced are Audit Assessment Results and Meeting Attendance Reports. A more detailed schedule is shown in Appendix E.

Table 3-4—Coding and Unit Testing

	Task	Method	Time
1	Ensure that the coding process, associated code reviews, and software unit testing are conducted in conformance with the standards and procedures established by the project and as described in the Software Management and Data Plan.	Audit/Assessment of code Meeting Attendance Software Status Monitor Unit Testing activities at software status meetings Meeting Attendance Code Reviews	Anytime after coding has begun Monthly As called by project
2	Ensure the code implements key safety design features.	Audit/Assessment of code	When it's known that safety features have been coded.
4	Ensure that action Items resulting from reviews of the code are resolved in accordance with these standards and procedures.	Audit/Assessment of code	Anytime after coding has begun

The results of this task shall be documented using the CoNNeCT Software Assurance folder in the CoNNeCT Project area in eRoom.

SA's recommendation for corrective action requires project management's disposition and will be processed in accordance with the project's Change Request (CR) process.

3.2.7 Evaluate Unit Integration and Testing, CSCI Qualification Testing, and CSCI/HWCI Integration and Testing

Software integration and test activities combine individually developed components together in the developing environment to ensure that they work together to complete the software and system functionality. In the integration and test phase of the software development lifecycle, the testing focus will shift from individual component correctness to the proper operation of interfaces between components, the flow of information through the system, and the satisfaction of system requirements.

SA shall perform the tasks in Table 3-5. The artifacts produced are Document Review Reports, Test Verification Reports, and Meeting Attendance Reports. A more detailed schedule is shown in Appendix E.

Table 3-5—Integration Testing

	Task	Method	Time
1	Ensure that software test activities are identified, test environments have been defined, and guidelines for testing have been designed. SA will verify the software integration process; software integration testing activities are being performed in accordance with the SMDP, the software design, the plans for software testing, and established software standards and procedures.	Document Review of Test Plans	Prior to CDR
2	Review Software Test Plans to verify they describe a test activity that provides evidence that software requirements have been satisfied.	Document Review of Test Plans	Prior to CDR
3	Review Software Test Procedures for test environment, test data, acceptance criteria, and steps needed to complete the test.	Document Review of Test Procedures	As Available
4	Review Mission Simulation Test Plan(s) to verify it describes a test activity that provides evidence that software requirements have been satisfied.	Document Review of Test Plans	Prior to SAR
5	Review Mission Simulation Test Procedures for test environment, test data, acceptance criteria, and steps needed to complete the test.	Document Review of Test Procedures	Prior to SAR
6	Review End to End Test Plan to verify it describes a test activity that provides evidence that software requirements have been satisfied.	Document Review of Test Plans	Prior to SAR
7	Review End to End Test Procedures for test environment, test data, acceptance criteria, and steps needed to complete the test.	Document Review of Test Procedures	Prior to SAR
	Ensure documentation leading to Verification Readiness Review (VRR) is complete.	Assessment Entrance Criteria VRR	Prior to VRR
8	Ensure any transfer of control of code to personnel performing software integration testing or software performance testing is being accomplished in accordance with established software standards and procedures.	Witness CM Delivery of current code version (Modified Test Verification Report)	Before the start of final V&V testing
9	Verify that discrepancies discovered during software integration and performance tests are identified, analyzed, and corrected; software unit tests and software integration tests are executed as necessary to validate corrections made to the code; and the software unit's design, code, and test are updated based on the results of software integration testing, and corrective action process.	Meeting Attendance Software Status Ask project for status of JIRA activity,	Monthly
10	Randomly monitor test activities.		

The results of this task shall be documented using the CoNNeCT Software Assurance Folder in the CoNNeCT Project area of eRoom.

SA's recommendation for corrective action requires project management's disposition and will be processed in accordance with the project's Change Request (CR) process.

3.2.8 Evaluate Software Verification and Validation Testing

Software Verification Test(s) will be used to verify the system is ready for flight operations per SMDP. This is done using breadboard SDRs or Engineering Models, if possible.

SA shall perform the tasks in Table 3-6. The artifacts produced are Test Verification Reports, Document Review Reports, Meeting Attendance Reports, and CPARs. A more detailed schedule is shown in Appendix E.

Table 3-6—Verification and Validation Testing

	Task	Method	Time
1	Ensure any transfer of control of code to personnel performing software integration testing or software performance testing is being accomplished in accordance with established software standards and procedures.	Witness CM Delivery of current code version (Modified Test Verification Report)	Before the start of final V&V testing
2	Verify that discrepancies discovered during performance tests are identified, analyzed, corrected, and verified through testing. If needed a new Test Procedure and or Test Report is created.	CPAR Entry (Test Verification Report) CPAR Tracking Meeting Attendance Participate in MRB for CPAR resolution	As required
3	Witness all software verification and validation tests and certify test results.	Test Verification Witness and signature test reports	As required
4	Review Test Reports.	Document Review Requirements Traceability matrix for completed test reports for each requirement	As available

3.2.9 Evaluate Flight Software Acceptance Testing

When all flight SDRs and all other flight components are available then final software testing is done on the flight system.

SA shall perform the tasks in Table 3-7. The artifacts produced are Test Verification Reports, Document Review Reports, Meeting Attendance Reports, and CPARs. A more detailed schedule is shown in Appendix E.

Table 3-7—Acceptance Testing

	Test	Method	Time
1	Ensure any transfer of control of code to personnel performing flight software testing is being accomplished in accordance with established software standards and procedures.	Witness CM delivery of current code version(Modified Test Verification Report)	Before use of code version for testing
2	Witness all tests, and certify test results.	Test Verification Witness and signature	As Required
3	Witness execution of Mission Simulation and End to End Test.	Test Verification Witness and signature	As Required
4	Review Test Reports.	Document Review test reports	Before SAR
5	Review Acceptance Data Package per Space Assurance and Guidelines (SARG).	Document Review ADP (software)	Before SAR
6	Verify that discrepancies discovered during test are identified, analyzed, corrected and verified through test.	CPAR Entry (Test Verification Report) CPAR Tracking Meeting Attendance Participate in ERB for CPAR resolution	As Required

3.2.10 Evaluate Operation on Delivery to Launch Site

There is no planned SA delivery activity.

3.2.11 Evaluate Software Configuration Management (SCM) Process

Software Configuration Management (SCM) is the discipline that applies technical and administrative direction and surveillance to (1) identify and document the functional and physical characteristics of Computer Software Configuration Items (CSCIs), (2) control the changes to CSCIs and their related documentation, (3) record and report information needed to manage CSCIs effectively, including the status of proposed changes and the implementation status of approved changes.

SA shall evaluate the following:

1. Ensure that configuration identification of documents, code, and computer data have established standards for titling, naming, and describing change status.

2. Ensure that baseline management of changes to the developmental baseline (including documents, code and computer data) are identified, reviewed, implemented, and incorporated in accordance with established procedures.

3. Ensure configuration control of changes to baseline documents and software are being managed in accordance with CM requirements as stated in the SCMP.

This shall be done through audit. Software documentation shall be audited following work instruction, Software Assurance Reviews and Audits: Configuration Management Review (GLWI-QE-8750.6) and a checklist based on CM Process Software Configuration Management (GRC-SW-7150.9). One audit will be held prior to CDR and one prior to SAR.

The results of this task shall be documented using the CoNNeCT Software Assurance Folder in the CoNNeCT Project area in eRoom.

3.2.12 Evaluate Operations

SA shall evaluate the following:

Approve any changes to on-orbit software and any data updates, as part of the SCB.

Ensure an impact analysis for any software changes that show the level of regression testing necessary and safety impacts is performed.

Witness the regression tests and certify test results.

3.3 Roles and Responsibilities

3.3.1 Overview

Table 3-8—Deviation and Waiver Responsibility

Deviation and Waivers	SA	SW Lead	Project Manager	Flight TA	CSO
Document Deviation		X			
Recommend Approval	X	X			
Approve			X [1]	X	X

[1] Does not include requirements of NPR 7150.2

Table 3-9—Creating SAP Responsibility

Create SAP	SA	SW	Project Manager
Develop	X		
Review	X	X	X
Approve	X		X

Table 3-10—Software Requirements Responsibility

Software Requirements Process	SA	SW	Project Manager
Develop software requirements and document		X	X
Review Documentation	X	X	X
Correct any defects found		X	
Approve		X	X

Table 3-11—Software Design Responsibility

Software Design Process	SA	SW	Project Manager
Develop SW Design and Document		X	
Review Design Documentation	X	X	X
Correct any defects found		X	
Approve		X	X

Table 3-12—Coding and Unit Test Responsibility

Coding and Unit Test	SA	SW	Project Manager
Develop Code		X	
Review Code	X	X	
Unit Test		X	
Correct any code defects		X	
Document Unit Test		X	
Review Documentation	X		

Table 3-13—Unit Integration and Testing Responsibility

Unit Integration and Testing	SA	SW	Project Manager
Integrate SW		X	
Document Test		X	
Review Test Document	X		X
Test Integrated SW		X	
Report Test Results		X	
Review Test Results	X		X
Report Problems	X	X	
Correct Problems		X	
Witness execution of test procedures for formal verification	X		

Table 3-14—Software Acceptance Testing Responsibility

Software Acceptance Testing	SA	SW	Project Manager
Execute Software Acceptance Test		X	
Witness Software Acceptance Test	X	X	
Document Test Results		X	
Report Problems	X	X	
Correct Problems		X	
Approve Software Acceptance Test	X		X

Table 3-15—Flight Software Acceptance Testing Responsibility

Flight Software Acceptance Testing	SA	SW	Project Manager	Flight SW TA
Execute Software Tests		X		
Document Test Results		X		
Review documentation	X			
Review Test Reports	X			
Execute Software Acceptance Test		X		
Witness Software Acceptance Test	X	X		
Report Problems		X		
Correct Problems		X		
Approve Corrected Problem		X	X	
Perform FCA	X			
Approve FCA		X	X	
Perform PCA	X			
Approve PCA		X	X	
Maintain Change Request Process	X			
Generate Acceptance Data Package (ADP)		X		
Approve ADP	X	X	X	X
Lessons Learned Report			X	
Support Delivery	X	X		

3.3.2 SMA Lead

See Section 3.1.2

3.3.3 Software Assurance Engineer

See Section 3.1.3

3.3.4 Software Safety Engineer

See Section 3.1.4

3.4 Quality Assurance Resource Estimates

Software assurance efforts were performed according to GLPR 8739.1. The Payload Avionics Software requires a Full/Medium SA effort. The Ground Software requires a Minimal effort. The GRC GFSC Waveform software requires a Medium effort.

These efforts correspond to a .75FTE.

The Software Safety effort is estimated to be Moderate based on available information. This should not require a significant amount of additional effort or approximately .10FTE

4.0 DOCUMENTATION

4.1 Purpose

This section identifies the minimum documentation governing the requirements, development, verification, and validation of software that falls within the scope of this software quality plan. Each document below shall be assessed (reviewed) by SA personnel.

4.2 Minimum Documentation Requirements

4.2.1 Software Requirements

The documents reviewed for software requirements include the following:

- Software Assurance Plan (GRC-CONN-PLAN-0085)
- Software Management and Development Plan (GRC-CONN-PLAN-0024)
- GGT Waveform Development Plan (GRC-CONN-0076)
- Software Configuration Management Plan (GRC-CONN-PLAN-0001)
- Software Requirements Specification (GRC-CONN-REQ-0084)
- GGT Waveform Requirements Specification (GRC-CONN-REQ-0077)
- Risk Management Plan (GRC-CONN-PLAN-0007)
- Space Assurance Requirements Guidelines (GLPR-7120.5.30)
- Software Requirements Traceability Matrix

4.2.2 Software Design

The documents reviewed for software design include the following:

- Payload Avionics Design Description
- Ground Software Design Description
- GGT Waveform Design Description
- Interface Control Document(s)

4.2.3 Verification and Validation

The documents reviewed for software verification and validation include the following:

- Test Plan(s)
- Test Procedure(s)
- Mission Simulation Test Procedure
- End to End Test Procedure
- Software Acceptance Test Plan

4.2.4 Verification and Validation Results

The documents reviewed for the results of software verification and validation include the following:

- Test Report(s)
- Software Acceptance Test Report
- Mission Simulation Test Report
- End to End Test Report
- FCA Report

4.2.5 Software Acceptance

- Acceptance Data Package
- Software Version Description Document
- PCA Report

4.2.6 User Manuals

The documents reviewed for operation include a user's manual for the Payload Avionics package and a user's manual for the GGT Waveform.

4.2.7 Software Configuration Management Plan

See CoNNeCT Software Configuration Management Plan, GRC-CONN-PLAN-0001.

Software Configuration Management (SCM) is the discipline that applies technical and administrative direction and surveillance to (1) identify and document the functional and physical characteristics of CSCIs, (2) control the changes to CSCIs and their related documentation, (3) record and report information needed to manage CSCIs effectively, including the status of proposed changes and the implementation status of approved changes.

SA shall evaluate the following:

- Assure that a SCM system is implemented and all code and computer data are baselined as soon as it is feasible prior to verification of software requirements.
- Assure that configuration identification of requirements, design, code, and computer data have established standards for titling, naming, and describing change status.
- Assure that baseline management of changes to the developmental baseline (including requirements, design, code, and computer data) are identified, reviewed, implemented, and incorporated in accordance with established procedures.
- Assure configuration control of changes to baseline software is being managed in accordance with CoNNeCT Software Configuration Management Plan, GRC-CONN-PLAN-0001.
- Assure all test plans and procedures are reviewed and configuration managed before testing.

This activity will be accomplished prior to CDR and produce Document Review Reports and Audit/Assessment Results

5.0 STANDARDS, PRACTICES, CONVENTIONS, AND METRICS

5.1 Purpose

This section highlights the standards, practices, quality requirements, and metrics to be applied to ensure a successful software quality program.

5.2 Software Quality Program

Software Assurance program for CoNNeCT at GRC is governed by GRC Software Procedural Requirement, GLPR-8739.1 which implement the agency Software Assurance Standard NASA-STD-8739.8, and the NASA-STD-8719.13B for safety critical software. Together these NASA documents establish a common framework for software assurance and safety processes and products throughout the life of the software. These practices and conventions are tools used to ensure a consistent and objective approach to software quality for all programs/projects.

5.2.1 Standard Metrics

The following standard metrics are the minimum planned metrics that will be collected, reported, and maintained in the area of software quality assurance:

- Number of SA activities (Planned vs. Actual)
- Number of non compliances (Open vs. Closed)

Additional Project metrics may also be collected, reported, and maintained, as required by the SMA Lead. Sample metrics include:

- Number of Peer Reviews attended (Planned vs. Actual)
- Number of Open vs. Closed Action Items from peer reviews
- Number of Open vs. Closed Software Problem Reports, with aging and trending over a specified time frame

6.0 SOFTWARE REVIEWS

6.1 Purpose

This section identifies the number and type of system/subsystem reviews and engineering peer reviews that will be supported by the SA Personnel. The Software Management and Development Plan (SMDP), the project milestone chart, and the SA personnel resource levels determine the reviews that are supported

6.2 Minimum Requirements

For each review listed below, SA will assess the review products to assure that review packages are being developed according to the specified criteria, the review content is complete, accurate, and of sufficient detail, and Requests for Action (RFA) are captured, reviewed, and tracked to closure. In addition, SA will assess the processes used to conduct the reviews to determine if appropriate personnel are in attendance, correct information is presented, entry and exit criteria are met, and appropriate documents are identified for update.

6.2.1 Software Architecture Review SAR

This review describes an overview of the software architecture and the major interfaces of the Payload Avionics. There may be a separate such review for the GGT Waveform and Ground software.

6.2.2 Software Critical Design Review SWCDR

This is a review of the detailed software design of the Payload Avionics, GGT Waveform, and Ground software.

6.2.3 Functional Configuration Audit

A Functional Configuration Audit (FCA) shall be performed by SA before Pre-Ship Review of the CSCIs Payload Avionics, to insure compliance to all software and International Space Station requirements. A FCA report will be generated and placed in Configuration Management. See Appendix F.

6.2.4 Physical Configuration Audit

A Physical Configuration Audit (PCA) shall be performed by SA before deployment of the CoNNeCT to insure all loaded PAS software is the proper version and matches what is in Software Configuration. This includes vendor supplied software and waveforms. A PCA report will be generated and placed in Configuration Management. See Appendix F.

6.2.5 In Process Audits

SA shall perform a minimum of one additional audit of one of the processes named below.

- A schedule of audits is shown in Appendix E.
- Additional audits may be performed as needed.
- configuration management,
- requirements development,
- requirements management,
- project planning,
- project monitoring and control
- managing the measurement of software process and product

Unless defined in project documents the criteria used for these audits are defined in the GRC-SW-7150.X process where X is a specific number for the process. These processes can be found on the Software@Glenn website.

6.2.6 Managerial Review

This review is not planned.

Software Assurance shall participate in a monthly metrics review conducted by the SW Technical Authority

6.2.7 Software Configuration Management Plan Review

SA will review this plan and report any defects found.

6.2.8 Post Implementation Review

This section is not applicable to this plan.

7.0 TESTS

SA personnel will assure that the test management processes and products are being implemented per the Software Management and Development Plan and /or Test Plan(s). This includes all types of testing of software system components as described in the test plan, specifically during integration testing (verification) and acceptance testing (validation).

SA will assure that tests are conducted using approved test procedures and appropriate test tools, and that test anomalies are identified, documented, addressed, and tracked to closure. In addition, SA will assure that assumptions, constraints, and test results are accurately recorded to substantiate the requirements verification/validation status.

SA personnel will witness and certify formal verification and validation activities.

SA personnel will review post-test execution related artifacts including test reports, test results, problem reports, updated requirements verification matrices, etc.

8.0 PROBLEM REPORTING AND CORRECTIVE ACTION

Procedures for reporting, analyzing, prioritizing, and processing software changes are contained in CoNNeCT Software Configuration Management Plan (GRC-CONN-PLAN-0001).

Software changes can be the result of problems or defects found during test. These are tracked according to CoNNeCT Software Configuration Management Plan (GRC-CONN-PLAN-0001).

SA will:

- Attend CoNNeCT Software Control Board (SCB) meetings used to review and approve software changes.
- Review Change Requests (CR) used to create new software versions.
- Review any Software Impact Analysis done for completeness, correctness, and safety impact.

9.0 TOOLS, TECHNIQUE'S AND METHODOLOGIES

9.1 Software Classification

Software classification was performed in accordance to NPR 7150.2. Unofficial copies of the Software Classification Reports are in Appendix C. The official copies are on the CoNNeCT Software Assurance Folder in the CoNNeCT Project area in eRoom.

CoNNeCT Payload Avionics software was found to be class C. Class C was determined based on the characteristics of CoNNeCT as a test bed for SDR experiments used to collect science data and an examination of the definition of Class C software in NPR 7150.2. Class C is the classification for flight software and includes the return of science data.

The CoNNeCT Ground software was found to be class C. Because a portion of CoNNeCT Ground software is expected to command and control the in flight CoNNeCT software it is given the same classification as the flight software.

CoNNeCT GRC GFSC Waveform was found to be class C. The waveform is test software executing on a Software Defined Radio in flight and used to fulfill the return of science data.

Code generated by an auto code generator is treated as any other developed software. High level verification or simulation cannot be used as verification of correctness. This does not apply to Complex Electronics.

9.2 Software Quality Tools

Microsoft Office tools (i.e., Word, Excel, and PowerPoint) will be used for documentation of SA deliverables.

10.0 MEDIA CONTROL

Deliverables will be in soft copy, unless specified otherwise. See Section 12 for additional details on the collection and retention of key records.

11.0 SUPPLIER CONTROL

Supplier controls apply to the software provided by JPL for its SDR.

12.0 RECORDS COLLECTION

Software Assurance records include, but are not limited to, audit/assessment results, audit/assessment checklists, document review results, software assurance classification results, safety litmus test results, meeting attendance spreadsheet, test verification results, schedules, and as needed deliverables created throughout the life cycle.

After Software Acceptance the Software Assurance records will be placed under configuration management per the procedures defined in GRC-CONN-PLAN-0002, CoNNeCT Configuration Management Plan.

12.1 Document Review Report

Document Reviews require as input the document itself and any criteria defined in NPR 7150.2 for that document. A Document Review generates an output containing issues, questions, comments, and non compliances with established criteria. The output can be in the form of a spreadsheet as specified by the project or a report as shown in Appendix D. The output will be sent to the author and configuration management and stored in eRoom in the Software Assurance Folder.

12.2 Audit/Assessment Results

Assessments or Audits require as input a baselined document describing the process to be audited, any criteria defined in NPR 7150.2 for the process and any other applicable document specifying the process criteria. The output includes a checklist created specifically for the process which includes comments as to whether the checklist item was found or not and whether the evidence or lack of indicates a finding or to a lesser degree and observation. Checklists will be stored in eRoom. Appendix D shows a sample checklist. Findings are entered into an Audit Findings and Corrective Active Spreadsheet maintained in eRoom. An updated spreadsheet is sent to the specific person identified as responsible for the process (if any) the Project Manager and SMA Lead, Any specific items identified as “Findings” will be tracked and reported monthly to the SMA Lead until closure.

12.3 Meetings

Meetings attended are reported weekly and will be entered into a meeting spreadsheet maintained in the Software Assurance Folder in eRoom.

12.4 Test Verification Report

Test Verifications require as input a baseline test procedure. The output is a test verification report as described in GLWI-QE-8750.5 Software Assurance Reviews and Audits: Test Verification. Section 3 of the form will be used to capture information on anomalies before placing them in the CPAR system.

13.0 TRAINING

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

- Software Quality Assurance
- Software Quality Engineering
- Audits and Reviews
- Risk management
- Configuration Management
- Systems and Software Safety
- Software Reliability
- Verification and Validation

14.0 RISK MANAGEMENT

Risk management for CoNNeCT is defined in document GRC-CONN-PLAN-0007.

SA will attend software risk management update sessions, when possible.

The Software Lead shall notify the SMA Lead via email at least three (3) days prior to a risk management session unless this session is included as part of the monthly status.

15.0 GLOSSARY

See Appendix A

16.0 PLAN CHANGE PROCEDURE AND HISTORY

It is expected that this plan will be updated throughout the CoNNeCT Program to reflect any changes in software assurance activities. Proposed changes will be submitted to the SMA Lead for initial approval and then submitted by a CoNNeCT Change Request (CR) to the CoNNeCT Control Board for consideration and disposition. All CRs will include a complete description of the change and the rationale to justify its consideration.

16.1 History

See Document History Log at top of document.

17.0 COMPLEX ELECTRONICS

17.1 Criticality Classification

The Criticality Classification is considered "Moderate" based on the following from the Complex Electronics website (http://www.hq.nasa.gov/office/codeq/software/ComplexElectronics/l_planning2.htm).

The complex electronics executes mission-critical functions but there is redundancy in the system. Redundancy is based on a second S-band SDR and a kA band SDR.

The design is expected to be moderately complex.

The design is expected to have moderate risk due to one or more of these factors:

- Some requirements undefined or unstable.
- Aggressive schedule.

17.2 Tasks

In addition to the tasks listed in Section 3.2 for software the following is added for the GGT Waveform Development based on a Criticality Classification for Complex Electronics.

Tasks shall be completed either by Document Review or Audit/Assessment producing the reports identified in Section 12.

17.2.1 CE Safety Assurance

Complex Electronics is not safety-critical. See Section 3.2.1.

17.2.2 Evaluate System Requirements Analysis Process

SA shall perform the following tasks:

- Review of Fault Tree Analysis (FTA), if available, and Failure Modes and Effects Analysis for CE failures.
- Assure the CE technology used is identified at a high level.
- Ensure requirements evaluation including reviews.
- Assure an Interface Analysis focuses on key interfaces and timing.
- Assure the use of Decision Tables for the most important conditions.

17.2.3 Evaluate Design Phase

SA shall perform the following tasks in addition to those listed above:

- Assure traceability from complex electronics requirements to design blocks.
- If FTA exists assure failures to complex electronics are mapped to architecture blocks.
- If FMEA exists assure appropriate failures of complex electronics and how they impact the system.
- Assure analysis of all key interfaces and critical timing has been updated.
- Attend Design Reviews

Additional activities for someone with expertise in complex electronics include the following:

- Review the IP (Intellectual Properties) used in the design to ensure:
- The IP was properly integrated into the design.
- All unused functions are protected from accidental use.
- Proper clock values and timing were used for the IP.

17.2.4 Evaluate Synthesis Phase

SA shall perform the following tasks:

- Ensure the test bench is in CM upon completion.
- Assure complex electronics detailed design is under CM.
- Assure coding standards and best practices are used.

Additional activities for someone with expertise in complex electronics include the following:

- Review the constraints used as inputs to the synthesis process.
- Evaluate the simulations performed after design synthesis.
- Assure that timing simulations or static timing analysis was done.
- Verify simulations done included out of range inputs, inputs out of order.

The results of this task shall be documented using the CoNNeCT Software Assurance Folder in the CoNNeCT Project eRoom.

17.2.5 Evaluate Implementation Process

SA shall perform the following tasks:

- Verify tools specified in the GGT Waveform Development plan were the ones used.
- Verify that the device (FPGA) is programmed according to a defined process and correct file from CM.
- Verify that post-layout and post-programming verifications are performed.

17.2.6 Evaluate Testing

SA shall perform the following tasks:

- Review/approve test procedure(s).
- Ensure Quality Assurance witnesses the tests.
- Perform an FCA and PCA.
- Ensure all requirements and design trace to testing.

18.0 SAFETY CRITICAL SOFTWARE TASKS

18.1 Determinating Criticality

- Execute the Software Safety Litmus Test for each CSCI to determine if software is safety critical. A Software Safety Litmus Report will be stored in eRoom.

- Communicate this determination to the project system safety engineer (SSE) for inclusion in the system safety analyses.

18.2 Planning

The SAE shall perform the tasks in Table 18-1.

Table 18-1—Software Safety Planning

Task	Method	Time
Perform a risk assessment of the software per the NASA-GB-8719.13, Software Safety Guidebook and determine the software risk level.	Use procedure outlined in Guidebook NASA-GB-8719.13	See item below
Using the software risk level determine the software safety effort. Use NASA-GB-8719.13, Software Safety Guidebook to determine the activities based on the software safety effort.	Use procedure outlined in Guidebook NASA-GB-8719.13	Prior to CDR

The software safety effort is included in the Software Safety Litmus Test Report.

The following is based on an estimated “Moderate Effort” determination.

18.2.1 Tools

Assure the effects of COTS have been considered during the development. This includes but is not limited to the following:

- In the same manner that safety-critical software is tested for response to off-nominal or stress conditions, verify that the safety task still runs properly by ensuring safety testing includes testing the OS under stress conditions.

- This will be done by Document Review of test plans and test verification (witnessing execution of test procedures).

18.2.2 Documentation

1. Assure safety is addressed in the following documents; Software Requirements, Software Design, Software V & V Plans and Software Test Procedures.

2. Assure all changes to safety related sections in software documents are properly reviewed and approved and follow project change control procedures.

3. Assure safety related sections are included in the appropriate documents.

All items will be done by Document Review prior to start of V & V testing.

18.2.3 Resources

Resource estimates for software safety are described in Section 3.4 Quality Assurance Resource Estimates.

18.2.3.1 Training

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

- Software Quality Assurance
- Software Quality Engineering
- Audits and Reviews
- Risk Management
- Configuration Management
- Systems and Software Safety
- Software Reliability
- Verification and Validation
- General knowledge of CMMI and detailed knowledge of the Process and Product Quality Assurance (PPQA) process area

Training logs/records will be maintained by the Software Safety home organization and be made readily available for review (NASA-STD-8719.13B No 5.3.1).

18.3 Safety Related Concerns

Any software safety related concerns will be promptly brought to the attention of the System Safety Engineer and Software Lead. If the concern cannot be resolved the concern will be brought to the attention of the PM and SMA Lead for resolution (NASA-STD-8719.13B No 5.2.6.3).

18.4 Evaluate Software and CE Requirements

- Review the software requirements of each CSCI against the system requirements, software standards, generic software safety requirements, hazard reports, and safety analyses and assure any missing software safety requirements are added.

- Assure software safety requirements are clearly identified.

- Assure software safety requirements have bi-directional traceability through all development activities.

- Assure a software requirements traceability matrix (spreadsheet) for all software safety requirements is created by software engineering and includes traceability of each safety requirement to design and implementation and test **.**

These activities shall be done prior to CDR by Document Review of requirements documents, design documents, V&V documents and requirements traceability matrix (NASA-STD-8719.13B No 5.2.5).

18.5 Evaluate Software Design

- Assure that all software safety requirements are incorporated in the design.

- Assure a review the failure modes of the operating system and other tasks. (While failure of other tasks has a slight possibility of affecting the safety task, the risk is very slight.)

- Assure the effects of interrupts, timing, event sequences, hardware failures, communication problems, etc. are considered on the safety-critical task.

These activities shall be done by audit of the design and subsequent report prior to the start of V & V testing (NASA-STD-8719.13B No 5.2.5).

18.6 Evaluate Implementation

- Assure that all safety-critical software requirements and design elements are incorporated in the code.

- Verify all source code files that implement safety-critical requirements/design have a comment block at the top that indicates these files are safety-critical.

- Review the coding standard against the appropriate language checklist in NASA-GB-8719.13. Provide any elements of the checklist not in the coding standard to the developers for inclusion in the coding standard.

- Assure that the coding standard is used by software developers.

The above activities shall be done by audit of safety critical code and subsequent report prior to the start of V & V testing.

18.7 Evaluate Testing

Table 18-2—Software Safety Testing

	Task	Method	Time
1	Utilize testing to verify safety-critical software operates correctly in a variety of conditions, including load, stress, and sensor failures, while the system is performing multiple tasks.	This is done by Document Review of V & V Test Planning documents including off-normal test planning prior to V & V testing.	Prior to start of V&V testing
2	Use the traceability matrix to verify all software safety requirements, design elements, and code components are tested.	This is done by Document Review of the Requirements traceability matrix post V & V testing	Post V & V Testing
3	Sign off on software safety verifications after reviewing the test plan/procedure, witnessing the test, and reviewing the test report and data.	Test Verification and Signature on test report	
4	Verify test reports are prepared for module and task testing of safety-critical source code, and that these reports are put into the CM system.	Audit/Assessment of CM test documents	Prior to SAR
5	Verify software safety requirements are included in the system tests and that the acceptance test includes verification of the safety system. (System tests include simulated hardware failures and operator errors.).	Document Review system test plans and procedures	prior to CDR.
6	Witness system testing of software safety requirements. Verify that the software and test plans/procedures were generated from CM controlled documents prior to the start of test.	Test Verification and Signature of test report	During testing
7	Review system documentation and assure that the system test procedures incorporate testing of all identified failures. (While it is not practical to test for all possible failures, system documentation can provide potential failures that the software must handle correctly and safety.	Document review Test Procedures	Prior to system verification testing

18.8 Certification

A certification process consists of a review of safety critical test reports and a subsequent report signed by the Software Lead.

18.9 Operations

The project SAE (or another person who can fulfill the functions) will:

- Approve any changes to on-orbit software and any data updates, as part of the SCB.
- Assure an impact analysis for any software changes is done and shows the level of regression testing necessary and safety impacts.
- Witness the regression tests.
- Review the user manuals and operational procedures and assure that safety features (e.g., error message lists), or actions that can impact the safety features, are clearly identified.
- Bullet item 4 is done by Document Review. Bullet item 3 is done by Test Verification. Bullet items 1 and 2 are done by monitoring CR process for software.

18.10 Software Safety Plan

The activities in this section are intended to satisfy the requirements of a Software Safety Plan. A separate plan will not be done. To aid in tracking compliance several paragraph will end with a number such as (No 5.2). This number indicates the section in NASA-STD-8719.13B that the paragraph is addressing.

18.10.1 Requirements Implementation

The requirements of NASA STD 8719.13B will be implemented by the software design, coding, software and system verification and software assurance members of the project. Software Safety activities shall be included as part of software development and not a separate activity (No 5.2.4).

Program safety requirements are generated by software analysis of hazard reports in the Flight Safety Data Package (FSDP). This results in system safety requirements which flow down to software safety requirements. The requirements are implemented in the software design of the PAS, tracked by a requirements traceability matrix and verified by demonstration testing (NASA-STD-8719.13B No 5.2.6.2).

18.10.2 Activities and Schedules

The activities and estimated times noted in Section 18.1 through Section 18.9 shall be done (NASA-STD-8719.13B No 5.2.5).

18.10.3 Organization

The organizational relationships between software, software safety and software assurance are shown in Section 3.1 (NASA-STD-8719.13B No 5.2.6). The Software Assurance Engineer acts as the Software Safety Engineer.

IV & V is not used for testing (NASA-STD-8719.13B No 5.2.6.1).

18.10.4 Project Schedule

Since software safety is included as a part of software development separate scheduling is not required (NASA-STD-8719.13B No 5.2.6.4).

The number of audits and schedule can be derived from Section 18.1 through Section 18.9. A table is also shown in Appendix E.

18.10.5 Safety Documentation

Safety documentation includes Audit and Assessment Reports, Document Review Reports, safety related sections of Software Test Plans and Procedures, traceability matrices including requirements and safety and the flight safety data package. (No 5.6.1)

18.10.6 Approval Process

The project's change and approval process for documents applies to safety related sections of such documentation. For further details see GRC-CONN-PLAN-002 Configuration Management. (NASA-STD-8719.13B No 5.6.2)

APPENDIX A ACRONYMS AND ABBREVIATIONS

A.1 Scope

This appendix lists the acronyms and abbreviations used in this document.

A.2 List of Acronyms and Abbreviations

Table A-1—Acronyms

ADP	Acceptance Data Package
ASIC	Application Specific Integrated Circuit
CCB	CoNNeCT Control Board
CDR	Critical Design Review
CE	Complex Electronics
CM	Configuration Management
CoNNeCT	Communications, Navigation & Networking re-Configurable Test-bed
COTS	Commercial Off-the-Shelf
CR	Change Request
CSC	Computer Software Component
CSCI	Computer Software Configuration Item
FCA	Functional Configuration Audit
FPGA	Field Programmable Gate Array
GD	General Dynamics
GGT	GRC GSFC TDRSS Waveform
GOTS	Government Off-the-Shelf
GRC	Glenn Research Center
GSFC	Goddard Space Flight Center
GSW	Ground Software
HDL	Hardware Definition Language
HWCI	Hardware Configuration Item
IEEE	Institute of Electrical and Electronics Engineers
IP	Intellectual Property
ISS	International Space Station
JPL	Jet Propulsion Laboratory
LLIS	Lessons Learned Information System
MOTS	Modified Off-the-Shelf
NPD	NASA Policy Directive
PAP	Product Assurance Plan
PCA	Physical Configuration Audit
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
PPAD	Program and Product Assurance Division
PRACA	Problem Reporting, Analysis and Corrective Action
QA	Quality Assurance
RFA	Request for Action
SA	Software Assurance
SAP	Software Assurance Plan
SARG	Standard Assurance Requirements and Guidelines

SCB	Software Control Board
SCMP	Software Configuration Management Plan
SDR	Software Defined Radio
SMA	Safety and Mission Assurance (Directorate)
SMDP	Software Management and Development Plan
SQ	Software Quality
SQA	Software Quality Assurance
SRR	Software Requirements Review
SW	Software
TDRSS	Tracking and Data Relay Satellite System
TSC	Telescience Support Center
V&V	Verification and Validation
VDS	Verification Data Sheet
VRR	Verification Readiness Review

APPENDIX B DEFINITIONS

B.1 Scope

This appendix lists the definitions used in this document.

B.2 List of Definitions

Table B-1—Definitions

Activity: (1) Any of the project components or research functions that are executed to deliver a product or service or provide support or insight to mature technologies. (2) A set of tasks that describe the technical effort to accomplish a process and help generate expected outcomes.

Advanced Technology Development: ATD is one of four interrelated NASA product lines. ATD programs and projects are investments that produce entirely new capabilities or that help overcome technical limitations of existing systems. ATD is seen as a bridge between BAR and actual application in NASA, such as FS&GS projects or elsewhere. ATD projects typically fall within a Technology Readiness Level (TRL) range of 4 to 6.

Architecture and Design: A description of the mission elements, their interfaces, their logical and physical layout, and the analysis of the design to determine expected performance and margins. Includes System Design Synthesis, System Design Analysis, and System Design Validation products.

Baseline: An agreed-to set of requirements, designs, or documents that will have changes controlled through a formal approval and monitoring process.

Configuration Management: A systematic process for establishing and maintaining control and evaluation of all changes to baseline documentation, products (Configuration Items), and subsequent changes to that documentation which defines the original scope of effort. The systematic control, identification, status accounting, and verification of all Configuration Items throughout their life cycle.

Contractor: Per NPR 7123.1, a “contractor” is an individual, partnership, company, corporation, association, or other service having a contract with the Agency for the design, development, manufacture, maintenance, modification, operation, or supply of items or services under the terms of a contract to a program or project within the scope of this NPR. Research grantees, research contractors, and research subcontractors are excluded from this definition.

Customer: The organization or individual that has requested a product and will receive the product to be delivered. The customer may be an end user of the product, the acquiring agent for the end user, or the requestor of the work products from a technical effort. Each product within the system hierarchy has a customer. A subset of “stakeholders.” (Refer to Stakeholder.)

Decision Authority: The Agency’s responsible individual who authorizes the transition at a KDP to the next life-cycle phase for a program/project.

Designated Governing Authority: The management entity above the program, project, or activity level with technical oversight responsibility.

Entry Criteria: Minimum accomplishments each project needs to fulfill to enter into the next life-cycle phase or level of technical maturity.

Exit Criteria: Specific accomplishments that should be satisfactorily demonstrated before a project can progress to the next product-line life-cycle phase.

Expectation: Statements of needs, desires, capabilities, and wants that are not expressed as a requirement (not expressed as a “shall” statement) is to be referred to as an “expectation.” Once the set of expectations from applicable stakeholders is collected, analyzed, and converted into a “shall” statement, the “expectation” becomes a “requirement.” Expectations can be stated in either qualitative (nonmeasurable) or quantitative (measurable) terms. Requirements are always stated in quantitative terms. Expectations can be stated in terms of functions, behaviors, or constraints with respect to the product being engineered or the process used to engineer the product.

Flight Systems and Ground Support: FS&GS is one of four interrelated NASA product lines. FS&GS projects result in the most complex and visible of NASA investments. To manage these systems, the Formulation and Implementation phases for FS&GS projects follow the NASA project life-cycle model consisting of phases A (Concept Development) through F (Closeout). Primary drivers for FS&GS projects are safety and mission success.

Formulation Phase: The first part of the NASA management life cycle defined in NPR 7120.5 where system requirements are baselined, feasible concepts are determined, a system definition is baselined for the selected concept(s), and preparation is made for progressing to the Implementation phase.

I**mplementation Phase**: The part of the NASA management life cycle defined in NPR 7120.5 where the detailed design of system products is completed and the products to be deployed are fabricated, assembled, integrated, and tested; and the products are deployed to their customers or users for their assigned use or mission.

Interface Control Document (ICD): A specification of the mechanical, thermal, electrical, power, command, data, and other interfaces that system elements must meet.

Key Decision Point: The event at which the Decision Authority determines the readiness of a program/project to progress to the next phase of the life cycle (or to the next KDP).

Level 1 Requirement: A Project's fundamental and basic set of requirements levied by the Program or Headquarters on the project.

Logical Decomposition: The decomposition of the defined technical requirements by functions, time, and behaviors to determine the appropriate set of logical models and related derived technical requirements. Models may include functional flow block diagrams, timelines, data control flow, states and modes, behavior diagrams, operator tasks, and functional failure modes.

Measure of Effectiveness: A measure by which a stakeholder's expectations will be judged in assessing satisfaction with products or systems produced and delivered in accordance with the associated technical effort. The MOE is deemed to be critical to not only the acceptability of the product by the stakeholder but also critical to operational/mission usage. An MOE is typically qualitative in nature or not able to be used directly as a "design-to" requirement.

Measure of Performance: A quantitative measure that, when met by the design solution, will help ensure that an MOE for a product or system will be satisfied. These MOPs are given special attention during design to ensure that the MOEs to which they are associated are met. There are generally two or more measures of performance for each MOE.

Other Interested Parties: A subset of "stakeholders," other interested parties are groups or individuals that are not customers of a planned technical effort but may be affected by the resulting product, the manner in which the product is realized or used, or have a responsibility for providing life-cycle support services. A subset of "stakeholders." (Refer to Stakeholder.)

Operations Concept: A concept that defines how the mission will be verified, launched, commissioned, operated, and disposed of. Defines how the design is used to meet the requirements.

Peer Review: Independent evaluation by internal or external subject matter experts who do not have a vested interest in the work product under review. Peer reviews can be planned focused reviews, conducted on selected work products by the producer's peers to identify defects and issues prior to that work product moving into a milestone review or approval cycle.

Product: A part of a system consisting of end products that perform operational functions and enabling products that perform life-cycle services related to the end product or a result of the technical efforts in the form of a work product (e.g., plan, baseline, or test result).

Product-Based WBS Model: Refer to WBS model.

Product Realization: The act of making, buying, or reusing a product, or the assembly and integration of lower level realized products into a new product, as well as the verification and validation that the product satisfies its appropriate set of requirements and the transition of the product to its customer.

Program: A strategic investment by a mission directorate (or mission support office) that has defined goals, objectives, architecture, funding level, and a management structure that supports one or more projects.

Project: (1) A specific investment having defined goals, objectives, requirements, life-cycle cost, a beginning, and an end. A project yields new or revised products or services that directly address NASA's strategic needs. They may be performed wholly in-house; by Government, industry, academia partnerships; or through contracts with private industry. (2) A unit of work performed in programs, projects, and activities.

Realized Product: The desired output from the application of the four Product Realization Processes. The form of this product is dependent on the phase of the product-line life cycle and the phase exit criteria.

Relevant Stakeholder: Refer to Stakeholder.

Requirement: The agreed upon need, desire, want, capability, capacity, or demand for personnel, equipment, facilities, or other resources or services by specified quantities for specific periods of time or at a specified time expressed as a "shall" statement. Acceptable form for a requirement statement is individually clear, correct, feasible to obtain, unambiguous in meaning, and can be validated at the level of the system structure at which stated.

Risk: The combination of the probability that a program or project will experience an undesired event (some examples include a cost overrun, schedule slippage, safety mishap, health problem, malicious activities, environmental impact, failure to achieve a needed scientific or technological breakthrough or mission success criteria) and the consequences, impact, or severity of the undesired event, were it to occur. Both the probability and consequences may have associated uncertainties. (Reference 7120.5.)

Software: As defined in NPD 2820.1, NASA Software Policy.

Specification: A document that prescribes, in a complete, precise, verifiable manner, the requirements, design, behavior, or characteristics of a system or system component.

Stakeholder: A group or individual who is affected by or is in some way accountable for the outcome of an undertaking. The term "relevant stakeholder" is a subset of the term "stakeholder" and describes people or roles that are designated in a plan for stakeholder involvement. Since "stakeholder" may describe a very large number of people, a lot of time and effort would be consumed by attempting to deal with all of them. For this reason, "relevant stakeholder" is used in most practice statements to describe the people identified to contribute to a specific task. There are two main classes of stakeholders. Refer to "customers" and "other interested parties."

Success Criteria: Specific accomplishments that must be satisfactorily demonstrated to meet the objectives of a technical review so that a technical effort can progress further in the life cycle. Success criteria are documented in the corresponding technical review plan.

System: (a) The combination of elements that function together to produce the capability to meet a need. The elements include all hardware, software, equipment, facilities, personnel, processes, and procedures needed for this purpose. (Refer to NPR 7120.5.) (b) The end product (which performs operational functions) and enabling products (which provide life-cycle support services to the operational end products) that make up a system. (Refer to WBS definition.)

Systems Approach: The application of a systematic, disciplined engineering approach that is quantifiable, recursive, iterative, and repeatable for the development, operation, and maintenance of systems integrated into a whole throughout the life cycle of a project or program.

Systems Engineering Life-Cycle: Concept Studies (Phase A), Preliminary Analysis and Definition (Phase B), Design (Phase C), Development (Phase D), Mission Operations (Phase E) and Disposal (Phase F) are the systems engineering life-cycle phases. Development includes Acquisition, Fabrication, and Integration; Verification and Preparation for Deployment; and Deployment and Operations Verification.

Systems Engineering Management Plan (SEMP): The SEMP identifies the roles and responsibility interfaces of the technical effort and how those interfaces will be managed. The SEMP is the vehicle that documents and communicates the technical approach, including the application of the common technical processes; resources to be used; and key technical tasks, activities, and events along with their metrics and success criteria.

System Safety Engineering: The application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

System Structure: A system structure is made up of a layered structure of product-based WBS models. (Refer to WBS definition.)

Technical Performance Measures: The set of critical or key performance parameters that are monitored by comparing the current actual achievement of the parameters with that anticipated at the current time and on future dates. Used to confirm progress and identify deficiencies that might jeopardize meeting a system requirement. Assessed parameter values that fall outside an expected range around the anticipated values indicate a need for evaluation and corrective action. Technical performance measures are typically selected from the defined set of Measures of Performance (MOPs).

Technology Readiness Level: Provides a scale against which to measure the maturity of a technology. TRLs range from 1, Basic Technology Research, to 9, Systems Test, Launch, and Operations. Typically, a TRL of 6 (i.e., technology demonstrated in a relevant environment) is required for a technology to be integrated into an SE process.

Technical Risk: Risk associated with the achievement of a technical goal, criterion, or objective. It applies to undesired consequences related to technical performance, human safety, mission assets, or environment.

Validation (of a product): Proof that the product accomplishes the intended purpose. Validation may be determined by a combination of test, analysis, and demonstration.

Validated Requirements: A set of requirements that are well-formed (clear and un-ambiguous), complete (agrees with customer and stakeholder needs and expectations), consistent (conflict free), and individually verifiable and traceable to a higher-level requirement or goal.

Verification (of a product): Proof of compliance with specifications. Verification may be determined by test, analysis, demonstration, and inspection.

Waiver: A documented agreement intentionally releasing a program or project from meeting a requirement. (Some Centers use deviations prior to Implementation and waivers during Implementation).

WBS Model: Model that describes a system that consists of end products and their subsystems (perform the operational functions of the system), the supporting or enabling products (for development; fabrication, assembly, integration, and test; operations; sustainment; and end-of-life product disposal or recycling), and any other work products (plans, baselines) required for the development of the system.

APPENDIX C SOFTWARE CLASSIFICATION REPORTS

Software Assurance Classification Report

1. Project Name Connect Payload Manager on ISS	2. Date 7/06/09
3. Project Manager Ann Over	
4. Software Assurance Manager Mark Luboski	

Software Assurance Classification Criteria

5a. Software Safety Litmus Test	Yes	No
Is the Software Safety-Critical?	☒	☐
Is Human Life a Risk Factor?	☒	☐
5b. Determination for Class E, F, G, or H Software	Yes	No
If F or G, is SA being performed?	☐	☐
OSMA Involvement?	☐	☐
5c. Software Classification Score	Score: 22000	

5d. Software Class	A	B	C	D	E	F	G	H
	☐	☐	☒	☐	☐	☐	☐	☐

5e. Software Assurance Effort/Priority	Full/ High	Full/ Medium -High	Medium / Medium	Minimal/ Low	None
	☒	☐	☐	☐	☐

6. Comments
Software Class is based on Appendix B of NASA NPR-7150.2. Class C Mission Support Software (Flight).

Software Assurance Effort is based on Table A-3 in NASA-STD-8739.8.
Class C software is normally Medium/Medium.
However, the “Safety Criticality requires Full

7. Date 12/04/09	Signature of Software Assurance Manager Mark Luboski
8. Date	Signature of Project Manager

Software Assurance Classification Report

1. Project Name Connect Ground Support	2. Date 11/21/08
3. Project Manager Ann Over	
4. Software Assurance Manager Richard Plastow	

Software Assurance Classification Criteria

5a. Software Safety Litmus Test	Yes	No
Is the Software Safety-Critical?	☐	☒
Is Human Life a Risk Factor?	☐	☒
5b. Determination for Class E, F, G, or H Software	Yes	No
If F or G, is SA being performed?	☐	☒
OSMA Involvement?	☐	☒
5c. Software Classification Score	Score: 1060	

5d. Software Class	A	B	C	D	E	F	G	H
	☐	☐	☒	☐	☐	☐	☐	☐

5e. Software Assurance Effort/Priority	Full/ High	Full/ Medium -High	Medium / Medium	Minimal/ Low	None
	☐	☐	☐	☒	☐

6. Comments
Ground software controls a Class C set of orbiting software.

7. Date 11/21/08	Signature of Software Assurance Manager Richard A. Plastow /s/
8. Date	Signature of Project Manager

Software Assurance Classification Report

1. Project Name GRC GFSC Waveform	2. Date 05/05/09
3. Project Manager Ann Over	
4. Software Assurance Manager Mark Luboski	

Software Assurance Classification Criteria

5a. Software Safety Litmus Test	Yes	No
Is the Software Safety-Critical?	☐	☒
Is Human Life a Risk Factor?	☐	☒
5b. Determination for Class E, F, G, or H Software	Yes	No
If F or G, is SA being performed?	☐	☐
OSMA Involvement?	☐	☐
5c. Software Classification Score	Score: 22000	

5d. Software Class	A	B	C	D	E	F	G	H
	☐	☐	☒	☐	☐	☐	☐	☐

5e. Software Assurance Effort/Priority	Full/ High	Full/ Medium -High	Medium / Medium	Minimal/ Low	None
	☐	☐	☒	☐	☐

6. Comments
The waveform directly controls the in-flight radio.
Software Assurance Effort is based on Table A-3 in NASA-STD-8739.8.

7. Date 05/05/09	Signature of Software Assurance Manager Mark Luboski
8. Date	Signature of Project Manager

APPENDIX D SAMPLE RECORDS

GRC Software Assurance Record
Document Review
Section 1

Document Title:	**Number**	**Date/Ver**	**Project**
Configuration Management Plan			

Reviewer/Phone	**Originator/Phone**	**Date Reviewed**	**Date Closed**

Section 2

Ref #	**Sec.**	**Pg #**	**Para**	**Major, Minor, Comment**		**Closed**
1						
2						
3						
4						

Section 3

Ref #	**Result**	**Date**
1		
2		
3		
4		

Sample Checklist

Project:
Process: Configuration Management
Related Document:

		Y, N NA	F, O	Comment
	Section 3.5 Document Initiation and Acceptance Process			
1	Show how the CoNNeCT eRoom folders have been divided into sections for review, baseline, non-baseline, and information documents.			
2	Are there baseline reports?			
3	Provide an example of reviewer comments described in step 6.			
	Section 4.0 Configuration Identification			
4	Are numbering assignments for documents published in the CoNNeCT eRoom (bullet 4)?			
	Section 4.3 Document Identification and Numbering Scheme			
5	Show how the GRC Bloodhound Configuration Management System also tracks document numbers.			
6	Pick a document number and show it is tracked in both systems?			
7	Is there a master listing of recognized document types maintained by CM and a copy in the project eRoom.			
	Section 4.3.1 Document Signature Requirements			
8	Check released documents for proper signatures (6). author, applicable lead engineer, System Engineering Representative, SMA Representative, Project Manager Configuration Management.			
	Section 4.4 Drawing Numbering Scheme			
9	Examine a released drawing; Does its number follow the scheme?			

		Y, N NA	F, O	Comment
10	Does it have the required signatures?			
	Section 4.5.2Deliverable Document Review Process			
11	Show how is status accounting provided in the VSS library?			
	Section 4.6 Document Tracking			
12	Show a status accounting matrix document on all deliverable documents received from the contractors.			
13	Show an example of a weekly and monthly deliverable status report.			
	4.7.3.1 Export Control			
14	Who is the Center Export Representative (CER) for the project?			
15	Where in the review process does the Center Export Representative (CER) review documents for proper Export Control.			
	Section 4.9 Monthly Deliverable Status Reports			
16	Did the CDM provide a copy of the tracking matrix to the project Manager this month? This matrix shows all DRD deliverables, date due to the government, and status of delivery.			
	Section 7.1 Change Initiation			
17	Show a CR form from eRoom folder CM FORMS?			

APPENDIX E AUDIT OVERVIEW AND SCHEDULE

Process Audit Schedule

Payload Avionics and Ground			
Process	**Planned Audit Time**	**SAP Section**	**CSCI**
Project Planning	March 2010	6.2.5	Payload Avionics Software (PAS) PAS, Ground
Measurement and Analysis	April 2010	6.2.5	PAS, Ground
Configuration Management	April 2010	3.2.3 Table 3.1 items 3,5,	PAS, Ground
Design Audit (Safety)	April 2010	18.5	PAS
Code Audit (Safety)	May 2010	3.2.6 Table 3.4 items 1,2,3,4; 18.6	PAS
Project Monitoring and Control	June 2010	6.2.5	PAS, Ground
Requirements Management	July 2010	6.2.5	PAS, Ground
Process Product Quality Assurance (if required)	Aug. 2010	6.2.5	
Supplier Agreement Management	Sept. 2010	6.2.5	
Configuration Management (Safety)	Nov 2010	18.7 Table 18.2 Item 4	PAS
FCA	Dec 2012	6.2.3	PAS
PCA	Dec 2012	6.2.4	PAS

GRC CFSC TDRSS Waveform			
Process	**Planned Audit Time**	**SAP Section**	**CSCI**
Project Planning	April 2010	6.2.5	GGT
Configuration Management	May 2010	3.2.3 Table 3.1 items 4,6; 17.2.4 bullet 2	GGT Waveform (Complex Electronics)
Complex Electronics	June 2010	17.2.2, 17.2.3, 17.2.4 17.2.5 17.2.6	GGT
Measurement and Analysis	July 2010	6.2.5	GGT
Requirements Management	August 2010	6.2.5	GGT
Configuration Management	Sept 2010	3.2.3 Table 3.1 Item 7	GGT
Project Monitoring and Control	Oct 2010	6.2.5	GGT
FCA	Dec 2010	17.2.6	GGT
PCA	Dec 2010	17.2.6	GGT

A checklist similar to that shown in Appendix D will be created (if none available) based on the process defined by the project and used as a audit guide.

The checklist will be filled in and an Audit Report (sample shown below) will be created and sent by email to the person(s) audited, the Program Manager, and SMA Lead. The checklist and report will be combined into one document and stored ineRoom. Any Findings will be recordfed in a spreadsheet for tracking corrective actions.

Product Audit Schedule

Document	Estimated Review Time	SAP Section
Software Requirements Specification (GRC-CONN-REQ-0084)	Feb 2010	3.2.3 Item 1,2 18.2.2 all bullets 18.4 all bullets
GRC GSFC TDRSS Waveform Requirements	March 2010	3.2.3 Item 1,2
Ground Software Requirements	Feb 2010	
Software Design (PAS)	Feb 2010	3.2.4Table 3.2I tem 1,
Ground Software Design Description	Feb 2010	3.2.4 Table 3.2 Item 1
GGT Waveform Design Description	March 2010	Table 3.2 Item 1 17.2.3 Bullet 1
Software Test Plans (PAS) and Ground)	March 2010	3.2.7 Table 3.5 Item 1,2,4,6 18.2.1, 18.2.2 18.7 Table 18.2 Item 1
Software Test Procedures (PAS and Ground)	March 2010 April 2010	3.2.7Table 3.5 Item 3,5,7 18.2.1, 18.2.2 18.7 Table 18.2 Items 5,7
Software Test Reports (PAS and Ground)	July 2010	3.2.8Table 3.6 Item 4 3.2.9 Table 3.7 Item 4
Acceptance Data Package	Feb. 2011	3.2.9 Table 3.7 Item 5
Software Requirements Traceability Matrix	March 2010	18.7 Table 18.2 Item 2
User Manual	March 2011	18.9 Bullet 4
Operations Procedures	March 2011	18.9 Bullet 4

Sample Audit Report

CoNNeCT Software Process Audit Report
Date of Audit:
Auditor:
Processes Audited:
Persons Audited:
Observations:
Findings:
Corrective Action Required :
Comments:

CoNNeCT Audit Findings and Corrective Actions

CoNNeCT Audit Findings and Corrective Actions

Report Date: **<Date>**

Total Findings Open **0**

Total Findings Closed **0**

Rec #	Audit Date	Process or Product Audit	Finding Description	Corrective Action (CA) Description	Assignee	Planned CA Due Date	Re-Assess-ment Date	Date Closed	Status

APPENDIX F FCA/PCA PLAN

19.0 FCA/PCA PLAN

19.1 Scope

This plan applies to the software developed for the Avionics system of the SCAN test bed. This software is known as Payload Avionics Software (PAS). Items used to define, develop, verify and control this software are within the scope of theses audits. This includes documentation such as requirements, verification reports, test reports, inspection reports, problem reports and waivers/deviations. The systems that are used for both configuration management and problem tracking and control are included.

19.2 Functional Configuration Audit (FCA)

The FCA is an audit conducted to verify that:

- The development of a configuration item has been completed satisfactorily.
- The item has achieved the performance and functional characteristics specified in the functional or allocated configuration identification.
- Operational and support documents are complete and satisfactory.

FCA is essentially a review of the configuration item's test/analysis data, including software unit test results, to validate the intended function or performance stated in its specification is met.

19.2.1 Objective

This audit is held to verify that the PAS actual performance complies with its Functional Specifications or Software Requirements and Interface Requirements specifications. This is done to comply with section 5.5.1.1 of the NASA Software Assurance Standard 8739.8.

19.2.2 Entrance Criteria

The following information shall be made available to the FCA team prior to the start of the FCA. A detailed list of specific document items and their revision levels in the CM system must be provided.

1. Designation of CSCI Version(s)
2. Software Requirements Specifications.
3. Any document referenced in a requirement that adds or refines the definition of the requirement,
4. Software Test Reports and/or "As Run" procedures
5. Software Inspection Reports,
6. Software Requirements Traceability Matrix,
7. A list of all Payload Avionics Commands tested
8. A list of all telemetry items tested.
9. Any software waiver and deviation either approved or in process,
10. A list of requirements that are intended to be verified at a later date.

19.2.3 Audit Participants

During the audit the Audit Lead and Software Lead are the points of contact.

The FCA team will audit the provided documents during the audit. Interviews of Software Team member are not required but the software lead should be available if questions arise that hold up the FCA.

19.2.4 Schedule Dates

Monday Jan 16	Tuesday Jan 17	Wednesday Jan 18	Thursday Jan 19	Friday Jan 20
	Opening Meeting	Entrance Criteria made available FCA In Progress	FCA In Progress	FCA In Progress
Monday Jan 23	Tuesday Jan 24	Wednesday Jan 25	Thursday Jan 26	Friday
FCA In Progress	FCA In Progress Interview Software	Closing Meeting	Presentation to Management	

19.2.5 Opening Meeting

The opening meeting will review audit objective, scope, timetable, and any question concerning the audit. If desired it can be a simple email announcing the start of the audit and soliciting any questions. The exact method will be determined by mutual agreement between the Audit Lead and Software Lead.

19.2.6 Audit Activities

19.2.6.1 Desk Audit

Using the information provided, the audit team will review the Software Requirements Specifications. Each requirement will be confirmed in the provided Software Requirements Traceability Matrix. The matrix is expected to provide the verification method and artifacts (e.g. test procedure and test reports) that show completion of verification, for each requirement.

The test report document will be used to examine the test. The test is reviewed and determined whether the requirement is tested and also the completeness or effectiveness of the test. The requirement can be assessed as either Fully verified, Partially verified, or Not Verified. A Fully Verified requirement means the “as written” requirement and test match and the test effectively verifies all aspects of the requirement. A Partially Verified requirement means either the "as written” requirement and test do not completely match

or the test verifies some but not all aspects of the requirement. A requirement is Not Verified if it is not found in either the matrix or Test Report or the test is not found to be effective.

Partially verified or Not verified requirements are considered findings.

Each requirement will be entered into a report with its assessment.

19.2.6.2 Interview

After all requirements are assessed an interview with the Software Lead and or designated representatives will be held to review any findings and provide an opportunity to provide clarification and any other supporting documentation before its entered into the preliminary finding report. The interview will also consist of a review of selected problems that have been closed. The Software Lead will be asked to show how selected problems were addressed.

19.2.6.3 Reporting

At the end of each day the Audit Lead will issue a simple summary report of the day's activities including any "potential" findings. Within 10 days of the closing meeting the final finding report will be placed in CM for review and signature.

19.2.7 Audit Follow Up

No follow up is planned before shipment.

19.2.8 Closing Meeting

The closing meeting will include the formal presentation of the results Exit Criteria

The following must be answered in the affirmative to signal a successful exit from the FCA

- Were all FCA Entry criteria found to be acceptable?
- Were all FCA discrepancies recorded and addressed during the Closing meeting?
- Has a FCA Report been completed and is ready for CM?

19.3 Physical Configuration Audit

19.3.1 Objective

A PCA is an audit conducted to verify that each configuration item, as built, conforms to the technical documentation that defines it. A PCA verifies that:

- All items identified as being part of the configuration are present in the product baseline
- No items that are not part of the CM controlled baseline product are present in the configuration
- The correct version and revision of each part are included in the product baseline
- They correspond to information contained in the baseline's configuration status report

A PCA is performed to provide an independent evaluation that the coded software has been described adequately in the documentation that and that the software and its documentation have been captured in the configuration management database and are ready for delivery.

19.3.2 Entrance Criteria

The following information shall be available for the PCA team prior to the start of the PCA. A detailed list of specific document items in the CM system or a CD containing this information shall be provided.

1. Designation of CSCI release
2. Software Version Description Document
3. CM Released CD with current release of software
4. List of all files on current Flight Avionics file system, "as built" with file byte sizes,
5. List of all run time files (log files) expected to be found on the Flight Avionics files system

19.3.3 Schedule Dates

Monday Jan 16	Tuesday Jan 17	Wednesday Jan 18	Thursday Jan 19	Friday Jan 20
			Opening Meeting Entrance Criteria made available	PCA In Progress
Monday Jan 23	Tuesday Jan 24	Wednesday Jan 25	Thursday	Friday
PCA In Progress		Closing Meeting		

19.3.4 Opening Meeting

This will follow the guidelines of the FCA opening meeting.

19.3.5 Audit Activities

19.3.5.1 Desk Audit

The audit team will review the "as built" list of files on the Flight system and compare them to the CM Released file system and the Software Version Description Document. The byte size of the "as built" list of files must match that of the files on the CM Released CD and Software Version Description Document. Any file that does not match is a finding.

Any file described as part of the PAS in the Version Description Document and not found in the "as built" list of files is a finding.

Any file found on the "as built" list but not found in the CM Released CD or Software Version Description Document becomes a "potential" finding.

19.3.5.2 Interview

After the review an interview with the Software Lead will be held to discuss any "potential" findings and provide an opportunity to provide clarification or any other supporting document before a "potential" finding becomes finding.

19.3.5.3 Reporting

Reporting will be the same as described in the FCA.

19.3.6 Audit Follow Up

Any file found on the "as built" list of files that is not listed in the SVD or CM or on the list of expected files needs to be addressed either by removal or a report indicating why the file should remain on the system. Within 10 days of the closing meeting an updated "as built" list of files or a preliminary report of files found but not to be removed should be available from the Software Lead.

19.3.7 Closing Meeting

The closing meeting will include the formal presentation of the results Exit Criteria

The following must be answered in the affirmative to signal a successful exit from the PCA

- Were all PCA Entry criteria found to be acceptable?
- Were all PCA discrepancies recorded and addressed during the Closing meeting?
- Has a PCA Report been completed and is ready for CM?