NOV 10 1994
Sta 11 43

ENGINEERING DATA TRANSMITTAL

Page 1 of 1

1. EDT 607105

2. To: (Receiving Organization)	3. From: (Originating Organization)	4. Related EDT No.:
Distribution	Equipment Development	NA
5. Proj./Prog./Dept./Div.:	6. Cog. Engr.:	7. Purchase Order No.:
RTG Transportation System 2C120	D. A. King	NA
8. Originator Remarks: This document is being transmitted for approval and release.		9. Equip./Component No.: System 140
		10. System/Bldg./Facility: NA
11. Receiver Remarks:		12. Major Assm. Dwg. No.: NA
		13. Permit/Permit Application No.: NA
		14. Required Response Date: NA

15. DATA TRANSMITTED

(A) Item No.	(B) Document/Drawing No.	(C) Sheet No.	(D) Rev. No.	(E) Title or Description of Data Transmitted	(F) Approval Designator	(G) Reason for Transmittal	(H) Originator Disposition	(I) Receiver Disposition
1	WHC-SD-RTG-SDP-001	All	0	Radioisotope Thermoelectric Generator Transportation System Subsystem 143 Software Development Plan	Q	1/2	1	

16. KEY

Approval Designator (F)	Reason for Transmittal (G)	Disposition (H) & (I)
E, S, Q, D or N/A (see WHC-CM-3-5, Sec.12.7)	1. Approval 4. Review 2. Release 5. Post-Review 3. Information 6. Dist. (Receipt Acknow. Required)	1. Approved 4. Reviewed no/comment 2. Approved w/comment 5. Reviewed w/comment 3. Disapproved w/comment 6. Receipt acknowledged

17. SIGNATURE/DISTRIBUTION (See Approval Designator for required signatures)

(G) Reason	(H) Disp.	(J) Name (K) Signature (L) Date (M) MSIN	(J) Name (K) Signature (L) Date (M) MSIN	(G) Reason	(H) Disp.
1/2	1	Cog.Eng. D. A. King DA 11-8-94 L6-38			
1/2	1	Cog. Mgr. F. W. Moore FWM 11/8/94 N1-25			
1/2	1	QA M. E. Riste MER 11/8/94 N1-25			
3	4	RTG Project File N1-25			
3	4	Central Files Orig. + 2 L8-04			

18.	19.	20.	21. DOE APPROVAL (if required) Ctrl. No.
D. A. King DA 11-8-94 Signature of EDT Originator — Date	F. W. Moore FWM 11/8/94 Authorized Representative for Receiving Organization — Date	F. W. Moore FWM 11/8/94 Cognizant Manager — Date	[] Approved [] Approved w/comments [] Disapproved w/comments

BD-7400-172-2 (04/94) GEF097

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

BD-7400-172-1 (07/91)

RELEASE AUTHORIZATION

Document Number:	WHC-SD-RTG-SDP-001, Revision 0
Document Title:	Radioisotope Thermoelectric Generator Transportation System Subsystem 143 Software Development Plan
Release Date:	November 9, 1994

This document was reviewed following the procedures described in WHC-CM-3-4 and is:

APPROVED FOR PUBLIC RELEASE

WHC Information Release Administration Specialist:

M. Boston — 11/9/94

M.N. Boston

SUPPORTING DOCUMENT

1. Total Pages 28

2. Title	3. Number	4. Rev No.
Radioisotope Thermoelectric Generator Transportation System Subsystem 143 Software Development Plan	**WHC-SD**-RTG-SDP-001	0

5. Key Words	6. Author
Radioisotope Thermoelectric Generator Transportation System	Name: D. A. King D A King Signature 11-10-94 D A K Organization/Charge Code 2C120/XJT~~43~~ EA

7. Abstract

This plan describes the activities to be performed and the controls to be applied to the process of specifying, developing, and qualifying the data acquisition software for the RTG Transportation System Subsystem 143 Instrument and Data Acquisition System.

8. RELEASE STAMP

OFFICIAL RELEASE BY WHC 43
DATE NOV 10 1994
Sta 11

RADIOISOTOPE THERMOELECTRIC GENERATOR TRANSPORTATION SYSTEM

SUBSYSTEM 143 SOFTWARE DEVELOPMENT PLAN

DISCLAIMER

CONTENTS

CONTENTS (continued)

LIST OF TABLES

This page intentionally left blank.

RADIOISOTOPE THERMOELECTRIC GENERATOR TRANSPORTATION SYSTEM SUBSYSTEM 143 SOFTWARE DEVELOPMENT PLAN

1.0 INTRODUCTION

1.1 PURPOSE

This plan describes the activities to be performed and the controls to be applied to the process of specifying, developing, and qualifying the data acquisition software for the Radioisotope Thermoelectric Generator (RTG) Transportation System Subsystem 143 Instrumentation and Data Acquisition System (IDAS). This plan will serve as a software quality assurance plan, a verification and validation (V&V) plan, and a configuration management plan.

1.2 SCOPE

This plan applies to all software that is an integral part of the RTG Transportation System IDAS. Specifically, the plan applies to software installed in the computers that are part of the RTG Transportation System IDAS. This plan applies to the entire development process, and includes the requirements, design, implementation, and operations and maintenance. This plan does not apply to any software that is not integral with the RTG Transportation System IDAS.

This plan has been prepared in accordance with WHC-CM-6-1, *Standard Engineering Practices*; WHC-CM-3-10, *Software Practices*; and WHC-CM-4-2, QR 19.0, "Software Quality Assurance Requirements."

2.0 TERMINOLOGY

2.1 LIST OF TERMS

CSDD	Computer Software Design Description
CSRS	Computer Software Requirements Specification
DOE	U.S. Department of Energy
ECN	Engineering Change Notice
EDT	Engineering Data Transmittal
IDAS	Instrumentation and Data Acquisition System, Subsystem 143
PDR	Preliminary Design Review
ROC	Read Out Console for the RPSF Project
RPSF	Radioisotope Power System Facility Project
RTG	Radioisotope Thermoelectric Generator
SDP	Software Development Plan
V&V	Verification and Validation
WHC	Westinghouse Hanford Company

2.2 DEFINITIONS

Computer Software Media. This refers to the different kinds of tapes and discs used by the computer for storing and retrieving software (WHC-CM-6-1).

Computer Software. Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system. (IEEE 1987).

Configuration Management. The process of (1) identifying and defining the configuration items in a system; (2) controlling the release and change of these items throughout the system life cycle; (3) recording and reporting the status of configuration items and change requests; and (4) verifying the completeness and correctness of configuration items (IEEE 1987).

Software Life Cycle. The period of time that starts when a software product is conceived and ends when the product is no longer available for use (IEEE 1987).

Validation. The process of evaluating software at the end of the software development process to ensure compliance with software requirements (IEEE 1987).

Verification. The process of determining whether or not the products of a given phase of the software life cycle fulfill the requirements established during the previous phase. Verification includes reviewing, inspecting, testing, checking, auditing, or otherwise establishing and documenting whether or not items, processes, services, or documents conform to specified requirements (IEEE 1987).

3.0 OVERVIEW

3.1 DESCRIPTION OF RTG TRANSPORTATION SYSTEM AND ITS MISSION

The mission of the RTG Transportation System is to provide over-the-road transport of Radioisotope Thermoelectric Generators (RTGs) in the continental United States. The RTG Transportation System, designated as System 100, is comprised of four major systems. The four major systems are designated as the Packaging System (System 120), the Trailer System (System 140), the Operations and Ancillary Equipment System (System 160), and the Shipping and Receiving Facility Transport System (System 180).

System 120 is licensed (regulatory) hardware, which means that it is certified by the U.S. Department of Energy (DOE) to be in accordance with Title 10, *Code of Federal Regulations* (CFR), Part 71 (10 CFR 71). System 140, System 160, and System 180 are non-licensed (non-regulatory) hardware. This description lists the features associated with the Trailer System (System 140).

The Trailer System (System 140) consists of an exclusive use semitrailer and on-board support systems necessary to reliably and safely transport RTG Packages within the continental United States. The Trailer System (System 140) is segregated into five subsystems. These subsystems include the Semitrailer (Subsystem 141), Power Supply (Subsystem 142), Instrumentation and Data Acquisition (Subsystem 143), Package Temperature Control (Subsystem 144), and Package Mounting (Subsystem 145).

The Instrumentation and Data Acquisition System (IDAS) is required to display, monitor, and record critical System 120 and System 140 parameters. Critical parameters include temperature and flow data for the Package Temperature Control System (Subsystem 144), and diesel fuel levels for the Power Supply (Subsystem 142) fuel tanks. The IDAS is required to monitor these parameters and alarm any out-of-limits conditions. These parameters are also recorded electronically, along with Package shock and vibration data.

3.2 QUALITY GOALS

An important goal of the finished RTG Transportation System is to provide a safe and reliable shipping assembly for transporting RTGs. The IDAS must function reliably during over-the-road conditions and use redundancy wherever possible so that the failure of a single component does not jeopardize the mission.

The system must be capable of being operated, maintained, and serviced by the agency that will serve as the RTG Transportation System Custodian. Therefore, the system must be sufficiently designed and documented so that it can be provided as a turn-key system to the Custodian, which may be a DOE contractor other than Westinghouse Hanford Company (WHC). These goals have been used as the basis for choosing the quality assurance provisions of this plan.

4.0 DESCRIPTION OF THE DEVELOPMENT PROCESS

4.1 CONCEPT

The concept for the RTG Transportation System IDAS has evolved from the original RTG Transportation System specification document, WHC-S-4025 (Ferrell 1992). The system concept has been reviewed for suitability to the RTG Transportation System by evaluating the concept against this specification. More specific functional requirements for the RTG Transportation System IDAS have been defined in WHC-SD-RTG-FRD-001, *Functions and Requirements for the RTG Transportation System (System 100)* (Ard 1993). This functions and requirements document includes detailed requirements for the IDAS and has been used to develop the system concept.

The RTG Transportation System IDAS concept has been modeled after the Read-Out Console (ROC) data acquisition system that was designed and fabricated for the Radioisotope Power System Facility (RPSF) project at WHC. The ROC concept and

design was reviewed and approved by the RTG community before the RPSF program was terminated.

4.2 REQUIREMENTS

From the RTG Transportation System functions and requirements document (Ard 1993), a Computer Software Requirements Specification (CSRS) document shall be produced by WHC. The CSRS is a detailed specification for the RTG Transportation System IDAS software. There shall be a single CSRS for the RTG Transportation System IDAS and it shall apply to the integrated system, but it shall be organized by software subsystems. It shall be verified by a review that coincides with the RTG Transportation System, System 140 Preliminary Design Review. The RTG Transportation System IDAS software shall be validated against the CSRS by means of formal validation testing at the end of the development process.

4.3 DESIGN

Next, the design process shall break the RTG Transportation System IDAS software into its software components. The functional specification and interfaces for these components shall be defined, and the method of implementation shall be selected. The responsibility for producing each of the software components shall rest with the WHC lead software engineer (see Section 8.0).

A Computer Software Design Description (CSDD) shall be prepared by WHC. The CSDD shall describe the integrated RTG Transportation System IDAS software in terms of its breakdown into the software components and their interfaces. It shall be verified at a preliminary stage of completion by an informal review, and verified at completion by a review that is related to the RTG Transportation System final design review. User documents shall be also be reviewed during the design phase in draft form.

4.4 IMPLEMENTATION

After the design is approved, each software component shall be implemented by the WHC lead software engineer. Prototype development will be performed during the entire software implementation phase. In this process, software subroutines and algorithms are created, tested, and debugged. After the software changes have been rigorously exercised, the code is saved as a unique prototype revision (see Section 9.2.4). Then additional changes are made, tested, and saved. This process repeats itself many times as the software evolves into the finished product. At each step, all aspects of the program are tested to verify that new code does not adversely affect established code. In the final stages of prototype development, test loads are connected to the data acquisition system to simulate actual operating conditions.

WHC shall produce an overall software operation manual that applies to the Subsystem 143 IDAS. This manual shall be integrated into an Operating and Maintenance Manual for the RTG Transportation System 140 Trailer System.

An implementation review shall be conducted to verify that the integrated data acquisition system software meets its design requirements, and that the required documentation is acceptable.

WHC shall produce the testing documents, which shall be used for V&V testing of the finished RTG Transportation System IDAS software.

4.5 TESTING

After implementation is complete, the software components shall be tested prior to installing Subsystem 143 in the Custom Semitrailer Assembly. A design verification test shall be performed as described in WHC-SD-RTG-TP-010, *Test Plan/Procedure for Design Verification and Acceptance of the Instrumentation and DAS Subsystem 143*. The test plan will be designed to thoroughly test the computer program and integrated system. It shall verify that the design requirements are met and the software is ready for final acceptance testing.

The final system acceptance test, described in WHC-SD-RTG-TP-011, *Final Acceptance Test Plan for the RTG Transportation System, System 100*, will be performed after Subsystem 143 is installed in the Custom Semitrailer Assembly. At that time, the final testing will validate the integrated System 140 subsystems.

When testing is complete, all of the verification records (results of various reviews, evaluations, and component tests) and the validation records (results of the validation testing) shall be collected and issued by WHC, and a V&V report shall be prepared by WHC. A review shall be held to evaluate the records and the report.

The software components shall be placed under WHC configuration management prior to integrating Subsystem 143 into System 140. Change control shall be under the authority of the RTG Transportation System Subsystem 143 cognizant engineer and cognizant manager, and WHC shall be responsible for performing any modifications to the code. Change control shall conform to WHC standard engineering practices when validation testing begins.

The CSRS, CSDD, testing documents, software operation manual, and V&V report shall be the responsibility of WHC and shall be released and controlled according to WHC standard engineering practices for supporting documents. Technical reference manuals shall be the responsibility of the software vendor and shall be maintained in the RTG Transportation System Subsystem 143 project file. All other documentation shall be entered into the RTG Transportation System project file.

5.0 RTG TRANSPORTATION SYSTEM SUBSYSTEM 143 SOFTWARE LIFE CYCLE

5.1 DESCRIPTION OF LIFE CYCLE

The development process described in Section 4.0 is based on a standard software life cycle model. As suggested in Section 4.0, the RTG Transportation System IDAS life cycle model consists of the following five phases:

- Requirements phase
- Design phase
- Implementation phase
- Testing phase
- Operation and maintenance phase.

This software life cycle is based on WHC-CM-3-10, *Software Practices* 1.1 and IEEE Software Engineering Standard 1012-1986, "IEEE Standard for Software Verification and Validation Plans," (IEEE 1987).

5.2 LIFE CYCLE ACTIVITIES

Table 1. Life Cycle Activities.

Phase	Activities
Requirements	Establishes detailed requirements for the integrated software from the RTG Transportation System Functions and Requirements document. An outline test plan may be produced at the same time as the CSRS to help assess the testability of the CSRS.
Design	Translates the detailed requirements into a computer software design description, which is a description the integrated software that shows its breakdown into software components and describes their function and interfaces.
Implementation	Produces working software components from the design description. The method of implementation is determined by the lead software engineer.
Testing	Verifies software design prior to integration of Subsystem 143 into the Custom Semitrailer Assembly. A design verification test shall be performed to verify that all design requirements are met and the software is ready for final acceptance testing.
	Integrates Subsystem 143 into the RTG Transportation System Custom Semitrailer Assembly. Software is placed under WHC configuration management at beginning of System 140 testing phase. During the integration period, change control is under control of RTG Transportation System Subsystem 143 cognizant engineer.
	Validates the software by formal testing of the complete system according to validation testing procedures. Currently, change control is under WHC Document Control procedures.
Operations and maintenance	Uses software for its intended purpose. Residual errors are removed and enhancements may be added during the useful life of the software. Ownership of the RTG Transportation System IDAS is transferred from WHC engineering to the DOE specified RTG Transportation System Custodian.

5.3 LIFE CYCLE DELIVERABLES

Table 2. Life Cycle Deliverables.

Phase	Deliverables	Responsible	Section
Requirements	Computer software requirements specifications	WHC	6.1
	Software development plan	WHC	(all)
Design	Computer software design description	WHC	6.2
	User Documents (draft) - Software operation manual - Technical reference documents	WHC	6.3
	Software testing documents: - Software test plan (draft) - Software test procedures (outline) - Software test specifications (draft)	WHC	6.4
Implementation	User documents - Software operation manual - Technical reference documents	WHC	6.3
	Computer software	WHC	6.6
	Software testing documents: - Software test plan - Software test procedures - Software test specifications	WHC	6.4
	User training	Custodian	6.5
Testing	Verification and validation report	WHC	6.7
	Verification and validation records	WHC	6.8
Operations and Maintenance	(Modifications repeat the same process as above and will generate the same deliverables, as appropriate)		x

5.4 VERIFICATION AND VALIDATION

Table 3. Verification and Validation Data.

Phase	Verification and validation activity	Resp	Section
Requirements	Software requirements review	WHC	7.1.1
Design	Software design review	WHC	7.1.2
	Prototype software (optional)	WHC	7.1.3
Implementation	Preparation of test cases	WHC	7.2.2
	Software implementation review	WHC	7.1.1
	Software component testing	WHC	7.1.4
	Code evaluation (optional)	WHC	7.1.2
Testing	Validation testing	WHC	7.2.1
	Verification and validation review	WHC	7.1.1
Operations and maintenance	(Any of the above, as appropriate)		

NOTE: Each of these activities shall be documented. The accumulated set of these documents plus the V&V report shall constitute the V&V records (see Section 6.8)

5.5 SCHEDULING THE RTG TRANSPORTATION SYSTEM SUBSYSTEM 143 LIFE CYCLE

A project schedule has been established for the RTG Transportation System as defined in the RTG Transportation System Program Management Plan, WHC-SD-RTG-PMP-001 (Jordal 1994). The software activities and deliverables specified in this software development plan shall be synchronized to the key milestones in that schedule according to the guidelines given in Table 4.

Table 4. RTG Transportation System Milestones.	
Phase	Related RTG Transportation System Milestone
Requirements	The requirements review shall coincide with the RTG Transportation System 140 Preliminary Design Review (PDR). This will end the requirements phase.
Design	A preliminary level of the CSDD shall be reviewed by an informal peer review.
	The design review of the finished CSDD shall coincide with the RTG Transportation System 100 Final Design Review (FDR). Design reviews of individual software components may occur prior to the FDR.
Implementation	The implementation phase will end when the software is ready for verification testing prior to integration into the Custom Semitrailer Assembly.
Testing	The testing phase will coincide with the RTG Transportation System Subsystem 143 verification testing and System 100 final acceptance testing.
Operations and maintenance	The operations and maintenance phase will begin when RTG Transportation System 100 final acceptance testing is finished and the RTG Transportation System has been accepted by the RTG Transportation System Custodian.

6.0 DELIVERABLES

6.1 COMPUTER SOFTWARE REQUIREMENTS SPECIFICATION

The CSRS is a complete and exact description of the functions that the software is expected to perform. The CSRS shall be the basis of both design and validation testing and it shall derive from the RTG Transportation System functions and requirements document, WHC-SD-RTG-FRD-001 (Ard 1993).

There shall be one CSRS for the RTG Transportation System IDAS software which shall apply to the integrated system. It shall be structured so that each subsystem is sufficiently independent to facilitate selective design, implementation, and testing.

6.2 COMPUTER SOFTWARE DESIGN DESCRIPTION

The CSDD shall describe the design of the RTG Transportation System IDAS software in terms of its decomposition into software components. In addition, the CSDD shall describe the functions of individual software components and the interfaces between them. A single CSDD shall address the IDAS software as an integrated system. Its primary purpose shall be to ensure that each software component is well enough defined so that it can be implemented with high confidence of success, it will integrate into the finished system, and the resulting integrated system will meet the functional requirements.

A typical decomposition is hierarchical and begins at the top level by showing the execution units (processes, tasks, programs) and their intercommunication. The subsequent levels of decomposition break each process into modules (sub-programs, functions, objects). Structure charts (IEEE 1987) are one appropriate decomposition format for traditional procedural languages such as C. Alternate or additional decomposition strategies (such as object class hierarchies) can be used where they are more appropriate. The RTG Transportation System Subsystem 143 cognizant engineer shall approve the methods used (see Section 8.0).

6.3 USER DOCUMENTS

The *Software Operation Manual* describes how to use the integrated RTG Transportation System IDAS software for its intended purpose, and how to recover from operational errors. There shall be a single such manual for the RTG Transportation System IDAS. It shall be prepared in draft form during the design phase and shall be completed during the Implementation Phase to a degree that facilitates integration and validation testing of the software. It is expected that some revision may take place during the testing phase.

This document shall have a section organized according to the normal tasks a user would perform with the system, a section organized as a reference for menus and displays, and a section organized as a tutorial for inexperienced users. During the design phase, the reference section would be the most complete, and the other sections would be less developed. Because the system will be based on a graphic user interface (GUI) with pull-down or pop-up menus and dialogue boxes, the reference section may contain hard copies of display windows (screen dumps) with accompanying descriptions.

The suppliers of software products shall be responsible for providing one or more technical reference documents for each software product. These documents will vary according to the type of software product and nature of its use. All technical reference documents to be supplied must be available during the implementation phase.

An operating manual shall be supplied with the software product if it has an interface with an operator.

6.4 SOFTWARE TESTING DOCUMENTS

The complete set of software testing documents consists of a test plan, test procedures, and test specifications, as defined by *Standard Engineering Practices* 4.2 (WHC-CM-6-1). For the design phase, the full set of software testing documents is produced in a preliminary and incomplete form that supports only the software implementation effort: software test plan (draft); software test procedures (outline); software test specifications (draft). For the testing phase, the full set of software testing documents shall be completed.

6.5 USER TRAINING

During and after final acceptance testing, WHC shall provide operational training to the organization designated as the RTG Transportation System Custodian. At that time, training will be provided to operate the Subsystem 143 IDAS.

6.6 COMPUTER SOFTWARE

Computer software includes computer codes, command files, configuration description files, and data directly related to the operation of computer systems. It includes source, object, and executable formats, and data in its multiple forms such as binary and text files, and database tables. Software shall conform to RTG Transportation System Subsystem 143 software coding standards (to be established by the RTG Transportation System Subsystem 143 cognizant engineer). The software shall be placed under configuration management as described in Section 9.0.

6.7 VERIFICATION AND VALIDATION REPORT

The V&V report summarizes all the V&V activities that have been performed upon all the software components during the life cycle and explains how the results of these activities prove the acceptability of the RTG Transportation System Subsystem 143 integrated software.

6.8 VERIFICATION AND VALIDATION RECORDS

V&V records are the collected, documented results of all the V&V activities which have been performed on all the software components. This includes the following.

- Independent review reports
- Design review completion reports

- Test results and test reports
- V&V report.

7.0 VERIFICATION AND VALIDATION

The V&V provisions of this plan identify and describe those software development activities (summarized in Section 5.5) whose primary purpose is to establish confidence and to provide objective evidence that the software adequately and correctly performs all its required functions. Verification refers to the process of evaluating the products of a single phase of the life cycle against the inputs to that phase. Validation refers to objectively testing the finished software product against the CSRS. The V&V activities are integrated into the software development process during all phases of the life cycle.

7.1 VERIFICATION METHODS

Verification activities shall consist of independent reviews, formal design reviews, code evaluations, and software component testing. Prototype software may be used optionally as an adjunct to these activities at the discretion of the lead software engineer (see Section 8.0). Section 5.5 establishes the minimum verification activities required, and suggests additional activities which may be performed for individual software components at the discretion of the RTG Transportation System Subsystem 143 cognizant engineer.

7.1.1 Independent Reviews

Independent reviews shall be conducted by reviewers independent of those responsible for the design being reviewed. The primary materials reviewed shall be one or more of the deliverables for the life cycle phase in which the review is performed. The function of the review shall be to establish that the reviewed materials adequately satisfy the requirements of the baseline documents that were input to the life cycle phase. A written report of the review will be prepared and comments and action items from the review will be entered into and tracked by the RTG Transportation System project comment database.

Independent reviews shall be conducted according to *Engineering Practice*, Section 4.1 (WHC-CM-6-1). All reviews shall be documented as part of the V&V records. The specific reviews required are as follows.

Software Requirements Review. The software requirements review is conducted at the end of the requirements phase to ensure that the requirements stated in the CSRS are adequate, technically feasible, and complete, and that they

accurately conform to the functions and requirements for the associated RTG Transportation System. The software requirements review is part of the preliminary design review for the RTG Transportation System, System 140.

Software Design Review. The software design review evaluates the technical adequacy, completeness, and correctness of the detailed design before the start of actual coding. The software design review (1) evaluates the acceptability of the detailed design depicted in the computer software design description; (2) establishes that the detailed design satisfies the requirements of the CSRS; and (3) reviews compatibility with other software and hardware with which the software component is required to interact. Reviews shall be coordinated with the RTG Transportation System project schedule as noted in Section 5.5.

Software Implementation Review. The software implementation review is an evaluation of the completed software, user documents, and test documents to determine that (1) the software is complete, satisfies computer software design description, and is ready to begin integration for validation testing; (2) user documents are complete and correct enough to use in testing; and (3) testing documents are complete and adequate for the testing phase to begin. The results of any software component testing shall also be reviewed (see Section 7.1.4).

V&V Review. The software V&V review evaluates the adequacy of the completed software V&V activities and the V&V report. The V&V review is performed at the end of the testing phase.

7.1.2 Code Evaluation

Code evaluation is a set of procedures and error-detection techniques for reading of code by a group of people. Two types of code evaluation that may be used for the RTG Transportation System IDAS software are code inspections or code walkthroughs. These techniques, which are described in Chapter 3 of Myers (1979), may be performed on selected modules at the discretion of the RTG Transportation System Subsystem 143 cognizant engineer.

7.1.3 Prototype Software

Prototypes will be used extensively throughout the development process (see Section 4.4). The purpose of prototypes is to provide users and other parties affected by the software a chance to acquire some hands-on experience with the proposed software to make informed comments and ensure that the requirements and design for the proposed software accurately address the needs of the application. Prototype software is also useful for assessing the human factors provisions of the data acquisition system.

7.1.4 Software Component Testing

Software component testing occurs at the end of implementation phase to show that a software component meets its design requirements and is ready to be integrated for final acceptance testing. Component testing is accomplished by performing the Subsystem 143 design verification test plan. This test is not the same as the validation testing described in Section 7.2; the test is only concerned with the software components, whereas validation testing is concerned with the integrated RTG Transportation System IDAS installed in the Custom Semitrailer Assembly.

7.2 VALIDATION TESTING

7.2.1 Software Validation Testing

Software validation testing is the process of testing the software to prove that it meets original specifications as defined in the CSRS. Validation testing shall occur during the testing phase of the software life cycle and shall be the key vehicle for bringing the software into commission for operations. The software will be installed into RTG Transportation System Subsystem 143 and the complete system will then be tested as part of System 140.

Validation testing shall be planned and conducted in accordance with the provisions of the RTG Transportation System final acceptance test plan and *Standard Engineering Practices*, 4.2 (WHC-CM-6-1).

Validation testing consists of subjecting the integrated RTG Transportation System IDAS software to all its test cases (see Section 7.2.2). The inputs defined by each test case shall be applied and the responses of the software under test shall be captured and evaluated against the expected results also defined in each test case.

7.2.2 Test Case Preparation

As described in Section 7.2.1, validation testing is defined by a set of test cases; each test case contains (1) a set of inputs to be applied to the software; (2) a set of expected results; and (3) a description of the environment in which the test case is to be applied. Test cases for software components shall be developed at the same time that it is being designed and coded, and the preparation is considered part of the verification process. Test cases shall be part of the software testing documents (see Section 6.4).

Test cases shall be based upon the CSRS. A minimum set of test cases would exercise all the primary functions of the software as defined strictly by its externally specified behavior ("black box" testing). Where the source code to a software component is available, additional test cases can be created based on the knowledge of the internal structure and details of the code ("white box" testing).

8.0 RESPONSIBILITIES

RTG Transportation System Subsystem 143 Cognizant Engineer. The RTG Transportation System Subsystem 143 cognizant engineer shall interpret how this software development plan is applied to the integrated system and to each software component and shall coordinate and approve work of software components. He or she shall also determine whether a piece of software is integral to the RTG Transportation System Subsystem 143 and therefore covered by this plan.

Lead Software Engineer. The lead software engineer shall have responsibility for producing one or more software components. The lead software engineer shall ensure that the software components are properly acquired and controlled according to this software development plan and guidelines established by the RTG Transportation System Subsystem 143 cognizant engineer. Specific responsibilities include (1) helping establish the functional requirements for software; (2) making decisions on design issues; (3) complying with requirements of this software development plan; (4) preparing documents; (5) allocating and scheduling resources; and (6) ensuring that configuration management requirements are followed.

RTG Transportation System Lead. The RTG Transportation System lead is responsible for overall direction and coordination of the RTG Transportation System project, and shall be responsible for ensuring that the software deliverables and schedule are acceptable with respect to the schedule and technical requirements of the RTG Transportation System.

Cognizant Manager. The cognizant manager shall be responsible for ensuring that reviews and approvals appropriate to the approval designators are obtained for software and other configuration items. The WHC technical manager who is assigned responsibility for the RTG Transportation System shall be considered the cognizant manager.

Software Custodians. Software custodians shall be responsible for the physical custody of the software assigned to them. This shall involve control of access to the software, distribution to users, control of media, and physical protection, and other duties defined in Section 9.0 of this plan. The software custodian shall also be the single point of contact for problem reporting.

Quality Assurance. WHC Quality Assurance is responsible for reviewing and approving software deliverables as noted in Section 10.0 of this plan.

9.0 CONFIGURATION MANAGEMENT

This section identifies the items that are part of the software configuration and describes the process for controlling release and change of these configuration items. Configuration items defined by this plan are the life cycle deliverables described in Section 5.4.

9.1 CONFIGURATION CONTROL OF DOCUMENTS

Documents that are defined in Section 5.4 as the responsibility of WHC shall be controlled as supporting documents. Vendor documentation shall be the responsibility of the supplier of the software product, and two copies shall be furnished to WHC; one copy shall be maintained in the RTG Transportation System Subsystem 143 project file, the other copy shall be available for field reference.

Supporting documents shall be issued a supporting document number according to *Standard Engineering Practices* 1.1 (WHC-CM-6-1). They shall be released via an Engineering Data Transmittal (EDT) form according to *Standard Engineering Practices*, 1.6 (WHC-CM-6-1). Changes to released supporting documents shall be controlled via an Engineering Change Notice (ECN) according to *Standard Engineering Practices*, Section 2.2 (WHC-CM-6-1).

Supporting documents shall be released during the software life cycle phase in which they are created, unless they are noted as being in draft or outline form in Section 5.4. Supporting documents may be presented in an unreleased form at the review and then released following incorporation of comments from that review. Prior to release, the documents shall be controlled by the RTG Transportation System Subsystem 143 cognizant engineer.

9.2 CONFIGURATION CONTROL OF SOFTWARE

9.2.1 Identification of Software

The RTG Transportation System IDAS software shall be issued a supporting document number according to *Standard Engineering Practices* 1.1 (WHC-CM-6-1). A computer software description (*Standard Engineering Practices* 2.1, Section 5.3.2, WHC-CM-6-1) bearing this number shall be prepared and maintained as the actual entity of release and change control. This document shall list the identification and revision levels of all the software components which comprise the integrated software; the document numbers and revision levels of related supporting documents; the name of the software custodian (see Section 9.2.3) and identification of the software repositories (see Section 9.2.2) which physically contain the software components; and a listing of identification and revision levels of all the modules that make up each software component.

Software components shall be controlled as computer files. These files may contain various kinds of data or program modules. Appropriate identifiers shall be assigned by the lead software engineer to files, modules, and any separately identifiable parts of modules. All files, modules, and procedures shall carry their identifier so that it displays on listings and outputs, wherever this is practicable. The lead software engineer shall maintain and control assignments of specific identifiers to software components.

The identifier for software components shall be further applied such that it is readily apparent in an appropriate format on the RTG Transportation System Subsystem 143 computer systems on which it resides. For example, software file names, as they appear in the computer system file directories, should reflect the file identifier.

9.2.2 Physical Control of Software

Computer software shall be physically controlled from a software repository. Software repositories shall be implemented on the standard file system for the computers which are used by the RTG Transportation System IDAS. A directory structure shall be established for each repository that contains the files that make up a configuration of the software component. This directory structure shall be hierarchical and shall resolve to a single root directory for all the directories that contain the files for a single revision of the software component. Each revision of the software component shall be a complete stand-alone copy (as opposed to only the changes from an earlier revision). Archiving utilities can be used to contain revisions of the software so long as it is possible to reconstruct a verbatim copy from the archive, including the directory structure.

Access control to the repository shall be provided by the security feature of the computer system on which it is implemented. The software custodian for the repository shall ensure that these security features are properly applied. Only one individual at a time shall be authorized to make modifications to a software component.

The software repository shall contain the master copy of a software component, and all application copies shall be made from the master copy. Backups of the contents of the software repository shall be made to ensure protection from loss or damage. At least two separate backup copies of the repository shall be maintained at all times, and shall be kept in physically separated locations to prevent a single facility accident from destroying both copies.

Standard commercial software packages are received on the manufacturer's standard distribution media (mag tape, floppy disk), and are installed from that media onto the target computer. The distribution media shall be retained and controlled by the software custodian (see Section 9.2.3) and shall serve the purpose of a software repository. Backup copies and copies for installation shall be controlled by the license agreement with the manufacturer and by WHC practices for use of commercial software.

Introduction of new software components or new versions of existing software component into the software repository is controlled. Refer to Section 9.2.4 for an explanation of these controls.

9.2.3 Software Custodian

The software custodian is the designated person who maintains control of and access to computer software and its media. The software custodian is responsible for the software repository and controls all access to it, all distributions of software from it, and all backups of it.

9.2.4 Release And Change Control of Software

The RTG Transportation System IDAS software shall be released via an EDT form according to *Standard Engineering Practices* 1.6 (WHC-CM-6-1). Changes to released software shall be controlled via an ECN according to *Standard Engineering Practices* 2.2 (WHC-CM-6-1). The EDT and any ECNs shall be applied to the computer software description (see Section 9.2.1). The lead software engineer shall deliver a copy of the approved EDT or ECN to the software custodian with media copies of the software itself. The software custodian shall then add the software from the media copy to the repository and log the change.

Prior to release, changes to the software shall be controlled by the RTG Transportation System Subsystem 143 cognizant engineer or by the lead software engineer (see Section 8.0). Thus, the software repository shall be established by the lead software engineer when the first software components appear. Additions or changes to unreleased software within the repository shall be the responsibility of the RTG Transportation System Subsystem 143 cognizant engineer or lead software engineer during the time it is being created and debugged. No audit trail of changes to software items in the repository is required prior to initial release of the software.

Versions of software shall carry lettered revision numbers prior to release and numbered revision numbers after release. The revision numbers shall be displayed on each configuration item in the same place and with the same prominence as the item's identification. Prototype and feature test software (see Section 7.1.3) shall not be released, but shall be controlled as pre-release software as noted above.

9.2.5 Problem Reporting And Corrective Action

9.2.5.1 Testing Phase Problems. During the testing phase of the software life cycle (and after initial release of the software), problem reporting and corrective action shall be implemented by the testing procedures and tracked by the test log for the RTG Transportation System.

9.2.5.2 Operations Phase Problems. During the operations and maintenance phase of the software life cycle, problems, errors, or difficulties with the

software, or requests for changes shall be reported on a Software Change Request and Problem Report (SCR/PR), which shall be similar in format to the example in *Software Practices* 6.3 (WHC-CM-3-10).

- Each SCR/PR shall be numbered. A log shall be maintained to track each SCR/PR.
- SCR/PRs shall be delivered to the software custodian who shall enter them into the SCR/PR log and forward them to RTG Transportation System Subsystem 143 cognizant engineer.
- The RTG Transportation System Subsystem 143 cognizant engineer shall assess the problem or change request and assign it to individuals with appropriate qualifications.
- A determination shall be made as to whether a problem requires corrective action, whether corrective action requires changes to the baseline configuration, and how extensive the modification will be. If modifications are extensive, changes to baseline documents such as computer software requirements specifications or computer software design descriptions may be required, and a "mini-life cycle" may be used with appropriate V&V.
- If no corrective action is needed, the SCR/PR may be closed out at that point.
- If modification is required, resources are assigned, authority to modify the affected software components is granted by the RTG Transportation System cognizant engineer to a designated software engineer, and working copies of software to be modified are distributed from the software repository. This effort may involve coordinating work among local and offsite organizations. For problems involving standard commercial software, the commercial supplier may offer a new revision of the software, or may only provide suggested work-arounds. For problems involving WHC developed software, any changes may require review and approval by the RTG Transportation System cognizant manager.
- When modifications to software components are complete and verified, an ECN is approved and issued for the new versions of the software and any affected documents (a single ECN can cover many SCR/PRs). The new version of the software is delivered to the software custodian who introduces it into the software repository, and the RTG Transportation System Subsystem 143 is re-certified by validation testing. The SCR/PR is closed out at this point.

9.2.6 Physical Media Control

Computer software media (also simply referred to as media) is the different kinds of tapes and discs used by the computer for storing and retrieving software in electronic form (as opposed to printed on paper).

Physical media control ensures that the stored data or software comes from a known and approved source, is traceable to its source, is physically retrievable, and cannot be lost or compromised by day-to-day operations or catastrophic events. The provisions of physical media control are as follows.

- A log shall be kept by the software custodian of when software is copied onto physical media from the software repository (backup copies are not included). Each copy shall have a serial number.
- Media shall carry a label containing:
  - Software component identifier
  - Serial number (from the log) and date of copy
  - Responsible individual/organization
  - Initials of software custodian

9.2.7 Configuration Status Accounting And Reporting

A database shall be established for tracking existence and status of all configuration items. The RTG Transportation System Subsystem 143 cognizant engineer shall be responsible for establishing and maintaining this database.

10.0 APPROVAL DESIGNATOR LEVELS

The approval designator level and approval signature requirements for each deliverable are defined as designator "Q." The approval designator of all RTG Transportation System Subsystem 143 software and documentation has been determined according to WHC-CM-3-5, Section 12.7 (WHC-CM-3-5).

11.0 REFERENCES

Ard, K. E., 1993, *Functions and Requirements for the RTG Transportation System (System 100)*, WHC-SD-RTG-FRD-001, Westinghouse Hanford Company, Richland, Washington.

Ferrell, P. C., 1992, *Specification for RTG Transportation System*, WHC-S-4025, Westinghouse Hanford Company, Richland, Washington.

Myers, G. J., 1979, *The Art of Software Testing*, John Wiley and Sons, New York, New York.

IEEE, 1987, *Software Engineering Standards*, Institute of Electrical and Electronics Engineers, New York, New York.

Jordal, R. R., 1994, *RTG Transportation System Program Management Plan*, WHC-SD-RTG-PMP-001, Westinghouse Hanford Company, Richland, Washington.

Page-Jones, M., 1980, *The Practical Guide to Structured Systems Design*, Yourdon Press, New York, New York.

WHC-CM-3-5, *Document Control and Records Management*, Westinghouse Hanford Company, Richland, Washington.

WHC-CM-3-10, *Software Practices*, Westinghouse Hanford Company, Richland, Washington.

WHC-CM-4-2, *Quality Assurance Manual*, QR 19.0, "Software Quality Assurance Requirements," Westinghouse Hanford Company, Richland, Washington.

WHC-CM-6-1, *Standard Engineering Practices*, Westinghouse Hanford Company, Richland, Washington. Referenced sections are as follows:

- 1.1 Engineering Document Identification
- 1.2 Preparation of Engineering Specifications
- 1.6 Engineering Data Transmittal (EDT)
- 1.7 Engineering Document Approval and Release Requirements
- 2.2 Engineering Document Change Control
- 4.1 Design Verification Requirements
- 4.2 Testing Practices