CPCCo
Central Plateau
Cleanup Company

One Focus · One Mission · One Hanford

Administrative Procedure, Level 1 - Company Wide

CPCC-PRO-EN-40357

Control System Software

Revision 1, Change 3

Published: 12/12/2024
Effective: 12/12/2024
Periodic Review Due Date:

Program: Engineering
Topic: Engineering Program

Technical Authority: Baker, Rachel K
Functional Manager: Kujath, Brett A

Use Type: Administrative

USQ Facility	USQ Review	Screener
Solid Waste Operations Complex	GCX-2 (Editorial Changes)	Carman, Hans
Canister Storage Building/Interim Storage Area	GCX-2 (Editorial Changes)	Garrett, Robert
Waste Encapsulation Storage Facility	GCX-2 (Editorial Changes)	Garrett, Robert
Transportation	**Exclusion Reason:** *N/A per Section 1.3*	
Capsule Storage Area	(Screening/Determination Performed (no issues)) *CSA-24-173*	Garrett, Robert
Below HazCat 3	GCX-2 (Editorial Changes)	Bullock, Susan
105 KW Facility	GCX-2 (Editorial Changes)	Meyer, Matthew
324 Building	GCX-2 (Editorial Changes)	Garrett, Robert
D4ES-Central Plateau	GCX-7 (Minor Change)	Griebel, Scott

JHA: Administrative
Periodic Review Due Date:01/30/2028
Rev. 1, Chg. 3

Change Summary

Description of Change

Fix typo in applicability section.

Control System Software

Published Date: 12/12/2024 **Effective Date: 12/12/2024**

TABLE OF CONTENTS

List of Appendixes

1.0 INTRODUCTION

1.1 Purpose

This procedure identifies the configuration management and software quality assurance (SQA) requirements applicable to control system software and support software by Central Plateau Cleanup Company (CPCCo).

This procedure implements the requirements of CPCC-RD-EN-1819, *Engineering Requirements*, and CPCC-MP-QA-599, *Quality Assurance Program,* with emphasis on the application to control system software.

1.2 Scope

This procedure covers the following activities:

Development, use, and management of control system software for configuration managed structures, systems, and components (CM SSC)

Development, use and management of support software that could affect the performance of control system software

This procedure does not cover the activities listed below. Management of the following software types is performed in accordance with CPCC-PRO-IRM-309, *Controlled Software Management*.

- Procurement, use, and management of Acquired (commercial-off-the-shelf [COTS]) Software used for engineering analysis and design
- Development, use, and management of Custom Developed Software used for engineering analysis and design
- Development, use, and management of Utility Calculation Software
- Procurement of services using Commercial Design and Analysis Software

1.3 Applicability

This procedure applies to the development, use and management of control system software and support software for physical plant systems.

1.4 Implementation

This procedure is effective upon publication.

2.0 RESPONSIBILITIES

2.1 Responsible Manager / Engineering Management

- Assigns technically competent Software Subject Matter Expert(s) (SME) for the organization, project, function, or facility, as applicable.
- Assigns technically competent Software Owner(s) (i.e., Design Authority/System Engineer) for the SSC utilizing control system software.

2.2 Design Authority/System Engineer

- Assigned as the Software Owner Manager for the applicable control system software and performs appropriate tasks for system software management.
- Provides input and approves requirements, acquisition, design, configuration management, testing, maintenance, and retirement work activities and documentation for control system software and support software as appropriate.

3.0 PROCESS

The following sections describe the software management requirements for control system software used by CPCCo.

3.1 Control System Software Management

Control system software is considered by engineering to be a component of the system it controls and is required to be managed such that the function, performance, and operation of the entire system is adequately maintained. As such, it is impractical to attempt to manage control system software as a separate entity from the rest of the system.

Due to the integrated relationship between software and the system it controls, the design, development, operation, and maintenance of control system software is performed as part of the overall system. Therefore, in addition to the unique requirements applicable to software, control system software is required to be designed and configuration controlled in the same manner as any other component of a CM SSC. For that reason, control system software design is performed in accordance with engineering design procedures, and operational configuration management is performed in accordance with engineering configuration management procedures.

3.1.1 Support Software

Support software includes software tools and system software. System software is used to provide basic functionality and facilitate the operation and maintenance of the applicable control system software. Only software tools that may affect the performance of controls system software need to be placed under configuration control. Any changes to the software tool itself need to be evaluated for impacts to control system software. Both system software and support software need to be evaluated, reviewed, tested, and accepted for use. If accepted, the support software will be placed under configuration control.

3.1.2 Control System Software Design and Development

Control system software design and development is typically performed in conjunction with the design of the system. In some cases, such as retrofitting an existing system with a digital control system, the software design may be managed as a separate project. However, even in those cases, the control system software is still a component of the system and many of its attributes (e.g., requirements, design, testing, and operation) are dictated by the requirements of the parent system. Therefore, most, if not all, of the documentation required for the software will be the same documentation required for design of the overall system.

Control system software design follows the steps of the Engineering Design Process as described in CPCC-PRO-EN-40271, *Engineering Design Process*. This process closely parallels the software development process described in CPCC-PRO-IRM-309.

Actionee	*Step*	*Action*
Design Engineering Team	1.	PERFORM design analysis of functional requirements for the parent system including the following at a minimum: • The objective of the analysis • Design inputs and their sources • Results of literature searches or other applicable background data • Assumptions and indications of those assumptions that must be verified as the design proceeds • Identification of any computer calculation, including identification of the computer type, computer program name, and revision, inputs, outputs, evidence of or reference to computer program verification and the bases (or reference thereto) supporting application of the computer program to the specific physical problem
Design Engineering Team	2.	IDENTIFY AND DOCUMENT control system design requirements including the following, at a minimum: • Operating system • Functionality • Performance requirements • Installation considerations • Design inputs and their sources • Safety requirements • Interfaces • Design Constraints • Attributes • Security requirements
Control System Design Engineer	3.	ANALYZE software alternatives for the system and its control.

Actionee	Step	Action
Control System Design Engineer	4.	PREPARE control system software design documentation (i.e., Software Design Description or engineering equivalent) including the following, at a minimum: • A description of the major components of the software design as they relate to the system requirements • A technical description of the hardware and software components • A description of allowable or prescribed ranges for inputs and outputs • A list of integration points or interfaces • Hardware/software configuration • Numerical methods • Mathematical and/or physical models • Control flow • Control Logic • Data flow • Process flow • Data structures, process structures and the applicable relationships between data structures and process structures • Important steps in the design process and software engineering methods • Security features (e.g., vulnerability protection and cyber security) • Applicable reference drawings, specifications, codes, standards regulations, procedures, or instructions that establish software design requirement test, inspection, and acceptance criteria • Measures to mitigate potential problems and their consequences • Data model, associated drawings, diagrams, equipment lists, etc. • Identify programming standards and conventions used

Actionee	*Step*	*Action*
Design Verifier	5.	PERFORM design verification of the control system software design against the functional requirements and software specification in accordance with CPCC-PRO-EN-8336, *Design Verification*. This review shall: • Consider the requirements related to the activities of preparing the computer program for acceptance testing • Evaluate the technical adequacy of the design approach • Ensure internal completeness, consistency, clarity, and correctness of the software design • Verify the software design is traceable to the software design requirements
Control System Design Engineer	6.	CONSTRUCT the control system software; analyze, debug, and document as required.
	7.	IF the software (or some components of the software) will be Acquired COTS, THEN ENSURE software requirements are included in the control system procurement activities and documentation.
	8.	PREPARE user documentation, operating manuals/procedures, etc. for operation and control of the system.
	9.	SUPPORT installation of the control system hardware/software.

3.1.3 Control System and Support Software Acceptance Testing

Acceptance testing shall be performed prior to approval of the software for use. Configuration items shall be under configuration change control prior to starting acceptance testing. Acceptance testing shall be planned and performed for all software design requirements. Acceptance testing ranges from a single test of all software design requirements to a series of tests performed during software development. Performance of a series of tests provides assurance of correct translation between activities and proper function of individual modules. Testing shall include a comprehensive acceptance test performed in the operating environment prior to use.

Acceptance testing shall demonstrate, as appropriate, that the software:

a) Properly handles abnormal conditions and events, as well as credible failures.

b) Does not perform adverse unintended functions.

c) Does not degrade the system either by itself or in combination with other functions or configuration items.

While the steps below are written as 3 discrete steps: plan the test, perform the test, and document the results. In practice, these may be performed in an iterative fashion with multiple phases of testing as appropriate.

Control system software testing is documented via test documentation as described in CPCC-PRO-EN-286, *Testing of Equipment and Systems*. However, there are specific items that must be included in the test documentation. These items are detailed in the steps below.

Actionee	*Step*	*Action*
Design Authority	1.	ENSURE test plan documentation includes the following as applicable: • Required Tests and test sequence • Required ranges of input parameters • Identification of the stages at which testing is required • Criteria for establishing test cases • Requirements for testing logic branches • Requirements for hardware integration • Anticipated output values • Acceptance criteria • Reports, records, standard formatting, and conventions
Testing Personnel	2.	PERFORM acceptance testing of the control system and the overall system. Testing shall provide traceability of test results to specified functional requirement for the software and system as described in CPCC-PRO-EN-286.
Design Authority	3.	ENSURE the test report contains the following information: • Computer program tested, including system software used • Computer hardware used • test equipment and calibrations, where applicable • date of test • tester or data recorder • simulation models used, where applicable • test problems • results and applicability • action taken in connection with any deviations noted • person evaluating test results • acceptability
Design Verifier	4.	PERFORM OR UPDATE design verification of the control system software design against the functional requirements and software specification in accordance with CPCC-PRO-EN-8336. This review shall provide assurance of satisfactory completion of the software development cycle including acceptance testing.

3.1.4 Control System and Support Software Registration and Documentation

Actionee	*Step*	*Action*
Design Authority	1.	IDENTIFY the safety classification of the control system software in accordance with CPCC-PRO-EN-20050, *Engineering Configuration Management.*
		a. IF the software is Safety Class or Safety Significant, THEN ENSURE it is added to the safety equipment list (SEL) of the parent system.
	2.	REGISTER the software in the Hanford Information Systems Inventory (HISI).
	3.	ENSURE the following HISI items are completed in accordance with CPCC-PRO-IRM-309 for the software: • The Software Grading Checklist is completed and approved by the Software SME • The system Design Authority is identified as the Software Owner • Management roles and responsibilities have been established and training has been completed by software team members • Software has been identified, registered, and the grade level determined

NOTE: *If complexity of Control System software warrants, a Control System Software Management Plan may be prepared, outside of control system documentation.*

4. PREPARE Software Management Plan or equivalent, as appropriate, to include the following, at a minimum:
   - Description of the control system function and configuration
   - HISI ID, HISI Acronym, and grade level of the software
   - Reference to design basis, testing, and supporting documentation (Identification of equivalent engineering documentation used to fulfill SQA requirements are listed in Appendix A)
   - Description of hardware and software components of the control system, including unique identification and version of components as required
   - Method for performing configuration management, change control, status accounting, installation, backup, and archiving of control system software

Actionee	Step	Action
Design Authority	5.	ENSURE the following references are made: • The System ID for the parent CM SSC is identified in the HISI • The HISI ID number for the control system software is identified in the System Information contained within the Document Management & Control System (DMCS)
	6.	ENSURE the following are performed: • Required software documentation is prepared and released for the appropriate grade and type of the control system software, in accordance with CPCC-PRO-IRM-309. Refer to Appendix A for engineering documentation equivalencies for SQA documentation • Software related documentation required to be configuration managed is identified with the configuration baseline documentation of the parent system as identified in DMCS • The training and qualification requirements for the system operators is identified
	7.	SUBMIT the control system software approval for use in HISI, in accordance with CPCC-PRO-IRM-309, sections 3.5, “Approval for Use,” and 3.6, “Software Installation and Checkout,” as applicable.
Facility Operations	8.	ACCEPT the control system for beneficial use (Approve for Use).

3.1.5 Control System and Support Software Operation and Maintenance

Once the system and its control system software has been accepted for beneficial use by Operations, the software is managed as a component of a CM SSC and placed under configuration management as described in CPCC-PRO-EN-20050.

Operation and Maintenance of control system software includes the following activities:

- Management of the software as a configured item in accordance with CPCC-PRO-EN-20050 and the Software Management Plan or equivalent and configuration control of the software, associated hardware, and configuration documentation.
- Problem identification and disposition.
- Change control for control system software and hardware changes.
- Identification and performance of operational testing as required.
- Retirement of the software when the parent system in inactivated or decommissioned.

Actionee	Step	Action
Design Authority	1.	MAINTAIN operation, technical aspects, and configuration control of the control system software, hardware, and configuration documentation. a. MAINTAIN version control of the control system components (hardware and software) to identify the current configuration. b. MANAGE the software in accordance with the Software Management Plan or equivalent and archive older versions of the software.
System Operator	2.	OPERATE the system in accordance with operating procedures or manuals.
	3.	NOTIFY the Design Authority of problems, issues, or requested changes.
Design Authority	4.	ADDRESS identified problems, issues, or requested changes.
	5.	PERFORM changes, when needed, using one of the following methods: • For software only changes that does not affect the functional requirements of the parent system, the change may be performed with a Problem Report/Change Request (PR/CR) form or Engineering Package (EP) as described in CPCC-PRO-EN-20050. • For software changes that affects the functional requirements of the system or requires control system hardware changes, modify the system using an EP or Facility Modification Package (FMP) as described in CPCC-PRO-EN-20050 and CPCC-PRO-EN-2001, *Facility Modification Package Process*.
	6.	IDENTIFY testing requirements for changes in the PR/CR, EP, FMP, or test procedure, or Work Package.
	7.	PERFORM testing in accordance with test documentation AND DOCUMENT in a Work Package, test procedure, or PR/CR.
	8.	Upon inactivation or decommissioning of the parent system, RETIRE the controls system software in accordance with the Software Management Plan, or equivalent.

4.0 FORMS

None

5.0 RECORD IDENTIFICATION

None

6.0 SOURCES

6.1 Requirements

CPCC-MP-QA-599, *Quality Assurance Program*
CPCC-PRO-IRM-309, *Controlled Software Management*
CPCC-RD-EN-1819, *Engineering Requirements*

6.2 References

CPCC-PRO-EN-2001, *Facility Modification Package Process*
CPCC-PRO-EN-20050, *Engineering Configuration Management*
CPCC-PRO-EN-286, *Testing of Equipment and Systems*
CPCC-PRO-EN-40271, *Engineering Design Process*
CPCC-PRO-EN-54907, *Software Commercial Grade Dedication*
CPCC-PRO-EN-8336, *Design Verification*

Appendix A - Equivalent Engineering Documentation for Software Quality Assurance

The following table provides a crosswalk between the software quality assurance documentation required by CPCC-PRO-IRM-309, *Controlled Software Management* and the equivalent types of engineering documentation. This matrix applies to control system software used to control CM SSCs.

Appendix A - Equivalent Engineering Documentation for Software Quality Assurance			
CPCC-PRO-IRM-309 SQA Document	**Equivalent Engineering Document**	**Reference**	**Work Activity[1]**
Functional Requirements Document	Design Requirements Document	CPCC-STD-EN-40255	SPM
	Process & Instrumentation Diagram (P&ID)	CPCC-STD-EN-40279	
Software Management Plan / Software Configuration Mgmt Plan	Software Management Plan	CPCC-PRO-IRM-309	SPM, SRM, SCM
	System Design Description (SDD)	DOE-STD-3024	
	Control System Description (CSD)	---	
Acquisition Documents (i.e. SOW)	Statement of Work (SOW)	CPCC-PRO-AC-40468	PSM
Software Requirements Spec.	Control Philosophy Document	---	SRM, SRIM, VV
	Control System Description (CSD)	---	
	Equipment Specification	CPCC-STD-EN-40280	
	System Design Description (SDD)	DOE-STD-3024	
Software Design Description	Control Philosophy Document	---	SRM, SDI, SS
	Control System Description (CSD)	---	
	Process & Instrumentation Diagram (P&ID)	CPCC-STD-EN-40279	
	Ladder Logic Diagrams	CPCC-STD-EN-40279	
	System Design Description (SDD)	DOE-STD-3024	
Requirements Traceability Matrix	Design Verification Matrix	CPCC-PRO-EN-8336	SRIM, VV
	Design Review (30%/60%/90%)	CPCC-PRO-EN-40271 CPCC-PRO-EN-8336	
Code Walkthrough	Report, Verification Checklist, etc.	---	SDI, VV
User Documents	Standard Operating Procedure	CPCC-PRO-MS-589	TSS

Appendix A - Equivalent Engineering Documentation for Software Quality Assurance			
CPCC-PRO-IRM-309 SQA Document	**Equivalent Engineering Document**	**Reference**	**Work Activity[1]**
	Control System Description (CSD)	---	
Unit Testing	Engineering Package (EP)	CPCC-PRO-EN-2001	SDI, VV
	Problem Report/Change Request Form (PR/CR)	CPCC-PRO-IRM-309	
	Test Specification/Procedure	CPCC-PRO-EN-286	
Test Plan & Cases	Problem Report/Change Request Form (PR/CR)	CPCC-PRO-IRM-309	VV
	Acceptance Test Plan/ Specification/Procedure	CPCC-PRO-EN-286	
	Engineering Package (EP)	CPCC-PRO-EN-2001	
	Work Package (WP)	CPCC-PRO-WKM-12115	
Acceptance Test Report	Problem Report/Change Request Form (PR/CR)	CPCC-PRO-IRM-309	VV
	Acceptance Test Report	CPCC-PRO-EN-286	
	Engineering Package (EP)	CPCC-PRO-EN-2001	
	Work Package (WP)	CPCC-PRO-WKM-12115	
Contingency Plan	Software Management Plan	CPCC-PRO-IRM-309	SPM, SRM
	Standard Operating Procedures (SOP)	CPCC-PRO-MS-589	
Software Installation Plan	Software Management Plan	CPCC-PRO-IRM-309	SPM, SDI
	Work Package (WP)	CPCC-PRO-WKM-12115	
	Vendor Information (VI)	CPCC-PRO-EN-440	
User Qualification	Operator Qualification	---	TSS
User Training	Operator Training	---	TSS
Operational/Periodic Testing	Surveillance	---	VV, CPCC
	Preventative Maintenance Work Package	CPCC-PRO-WKM-12115	
Change Request/Problem Report	Problem Report/Change Request Form (PR/CR)	CPCC-PRO-IRM-309	CPCC, SCM
	Engineering Package (EP)	CPCC-PRO-EN-2001	
Retirement Plan/Checklist	D&D Document	--	SPM, SCM
	Software Management Plan	CPCC-PRO-IRM-309	
	System Design Description (SDD)	DOE-STD-3024	
Data Security Plan (OUO)	Data Security Plan	CPCC-PRO-IRM-309	SRM, SRIM, VV, SS

Appendix A - Equivalent Engineering Documentation for Software Quality Assurance			
CPCC-PRO-IRM-309 SQA Document	**Equivalent Engineering Document**	**Reference**	**Work Activity[1]**
Disaster Recovery Plan	Emergency Procedures (system alarms, emergency plans)	CPCC-PRO-MS-589	SPM, SRM
	Software Management Plan	CPCC-PRO-IRM-309	
	System Design Description (SDD)	DOE-STD-3024	
Justification for Continued Use	Justification for Continued Use	CPCC-PRO-IRM-309	SCM, SRM, SDI, SS
Authorized Users List	Qualified Operators Statement/List	---	TSS, VV
Usage Log	Not Applicable to Control Software	NA	SCM, VV, SS
Commercial Grade Dedication	Commercial Grade Dedication	CPCC-PRO-EN-54907	PSM

[1] Work Activity Key

SPM	Software Project Management & Quality Planning	VV	Verification and Validation
SCM	Software Configuration Management	SDI	Software Design & Implementation
SRM	Software Risk Management	SS	Software Safety
PSM	Procurement and Supplier Management	TSS	Training of Personnel in the Design, Development, Use, and Evaluation of Safety Software
SRIM	Software Requirements Identification and Management	CPCC	Problem Reporting and Corrective Action