This document was retrieved from the Boeing ISEARCH System.

Accession #: D196050340

Document #: SD-WM-CSCM-032

Title/Desc: SOFTWARE CONFIGURATION MGMT PLAN FOR SAMPLE TRUCKS NO 2 & 3 & 4 ALARM & CONTROL LOGIC
2. **To:** Characterization Plant Engineering
3. **From:** Characterization Equipment Engineering
5. **Proj./Prog./Dept./Div.:** Core Sampling / N4A23
6. **Ctg. Engr.:** T. D. Jarecki

8. **Originator Remarks:**
   Initial release of Computer Software Configuration Management Plan (CSCM) for the Programmable Logic Controller (PLC) in Rotary Mode Core Sample Trucks (RMCST) #2, 3 and 4.

11. **Receiver Remarks:**

<table>
<thead>
<tr>
<th>DATA TRANSMITTED</th>
<th>(F)</th>
<th>(G)</th>
<th>(H)</th>
<th>(I)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item No.</strong></td>
<td>(A)</td>
<td>(B)</td>
<td>(C)</td>
<td>(D)</td>
</tr>
<tr>
<td><strong>Document/Drawing No.</strong></td>
<td><strong>Sheet No.</strong></td>
<td><strong>Rev. No.</strong></td>
<td><strong>Title or Description of Data Transmitted</strong></td>
<td><strong>Approval Designator</strong></td>
</tr>
<tr>
<td>1</td>
<td>WHC-SD-WM-CSCM-032</td>
<td>0</td>
<td>COMPUTER SOFTWARE CONFIGURATION MANAGEMENT PLAN FOR CORE SAMPLE TRUCKS #2, 3, AND 4 PROGRAMMABLE LOGIC CONTROLLER</td>
<td>SQ</td>
</tr>
</tbody>
</table>

**Key**

- E, S, G, D or N/A
  - (see WHC-CM-5-5, Sec.12.7)
  - 1. Approval
  - 2. Release
  - 3. Information
  - 4. Review
  - 5. Post-Review
  - 6. Dist. (Receipt Acknow. Required)

**Reason for Transmittal**

- 1. Approved
- 2. Approved w/comment
- 3. Disapproved w/comment
- 4. Reviewed no/comment
- 5. Reviewed w/comment
- 6. Receipt acknowledged

**Signature/Distribution**

<table>
<thead>
<tr>
<th>Reason</th>
<th>Dis.</th>
<th>(J) Name</th>
<th>(K) Signature</th>
<th>(L) Date</th>
<th>(M) MSIN</th>
<th>(J) Name</th>
<th>(K) Signature</th>
<th>(L) Date</th>
<th>(M) MSIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>l</td>
<td>1</td>
<td>Cog. Engr. T. D. JARECKI</td>
<td></td>
<td>9/24/95</td>
<td></td>
<td>JD CRIDDLE</td>
<td></td>
<td>9/24/95</td>
<td>52-02</td>
</tr>
<tr>
<td>l</td>
<td>1</td>
<td>Cog. Mgr. JS SCHOFIELD</td>
<td></td>
<td>9/25/95</td>
<td></td>
<td>TR-FARIES</td>
<td></td>
<td>9/25/95</td>
<td>52-02</td>
</tr>
<tr>
<td>l</td>
<td>1</td>
<td>QA ML MCELROY</td>
<td></td>
<td>9/24/95</td>
<td></td>
<td>G. MCELROY</td>
<td></td>
<td>9/24/95</td>
<td>52-02</td>
</tr>
<tr>
<td>l</td>
<td>1</td>
<td>Safety JA HARVEY</td>
<td></td>
<td>9/24/95</td>
<td></td>
<td>A. HARVEY</td>
<td></td>
<td>9/24/95</td>
<td>52-02</td>
</tr>
<tr>
<td>l</td>
<td>1</td>
<td>Env.</td>
<td></td>
<td>9/24/95</td>
<td></td>
<td>A. HARVEY</td>
<td></td>
<td>9/24/95</td>
<td>52-02</td>
</tr>
</tbody>
</table>

**Approval Designator (F)**

- 1. Approval
- 2. Approved w/comment
- 3. Disapproved w/comment
- 4. Reviewed no/comment
- 5. Reviewed w/comment
- 6. Receipt acknowledged

**Disposition (H) & (I)**

- 1. Approved
- 2. Approved w/comment
- 3. Disapproved w/comment
- 4. Reviewed no/comment
- 5. Reviewed w/comment
- 6. Receipt acknowledged

**Signature of EDT**

- Signature: [Signature]
- Date: 9/24/95

**Authorized Representative**

- Name: [Name]
- Date: 9/25/95

**Significant Manager**

- Name: [Name]
- Date: 9/25/95
## RELEASE AUTHORIZATION

<table>
<thead>
<tr>
<th>Document Number:</th>
<th>WHC-SD-WM-CSCM-032, REV 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Title:</td>
<td>Software Configuration Management Plan for Sample Trucks #2, 3, and 4 Alarm &amp; Control Logic</td>
</tr>
<tr>
<td>Release Date:</td>
<td>9/26/95</td>
</tr>
</tbody>
</table>

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

**APPROVED FOR PUBLIC RELEASE**

**WHC Information Release Administration Specialist:**

Kara Broz  
9/26/95

**TRADEMARK DISCLAIMER.** Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors.

This report has been reproduced from the best available copy. Available in paper copy. Printed in the United States of America. To obtain copies of this report, contact:

Westinghouse Hanford Company - Document Control Services  
P.O. Box 1970, Mailstop H6-08, Richland, WA 99352  
Telephone: (509) 372-2420; Fax: (509) 376-4989
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Configuration Management Plan for Sample Trucks #2, 3, and 4 Alarm &amp; Control Logic</td>
<td>WHC-SD-WM-CSCM-032</td>
<td>0</td>
</tr>
</tbody>
</table>

5. Key Words
Software, Configuration, Sample Truck, Alarms, Control Logic, PLC, RMCST

6. Author
Name: J. C. Akers
Signature: [Signature]
Organization/Charge Code: 57C00 / N4A23

7. Abstract
This document establishes the methods for configuration control of the Sample Truck Alarm and Control logic. Responsibility for documentation change control and custody are described.
COMPUTER SOFTWARE CONFIGURATION

MANAGEMENT PLAN

FOR SAMPLE TRUCKS #2, 3, AND 4

PROGRAMMABLE LOGIC CONTROLLER

August, 1995

J. L. Dowell & J. C. Akers

Prepared for:
Westinghouse Hanford Company
P.O. Box 1970
Richland, Washington 99352
CONTENTS

1.0 INTRODUCTION .................................................. 1
  1.1 Purpose ...................................................... 1
  1.2 Scope ........................................................ 1
  1.3 Overview .................................................... 1
  1.4 Definitions & Acronyms ..................................... 1

2.0 MANAGEMENT ..................................................... 2
  2.1 Organization ................................................ 2
  2.2 Responsibilities ........................................... 2
  2.3 Interface Control .......................................... 2
  2.4 Implementation ............................................ 2
  2.5 Policies and Procedures .................................. 2

3.0 SOFTWARE CONFIGURATION MANAGEMENT ACTIVITIES ....... 2
  3.1 Configuration Identification ............................. 3
  3.2 Configuration Control .................................... 4
  3.3 Configuration Status Accounting ......................... 4
  3.4 Audits and Reviews ....................................... 4
  3.5 Access Control ............................................. 4
  3.6 Backup and Recovery ...................................... 5

4.0 TOOLS, TECHNIQUES, AND METHODOLOGIES ................. 5

5.0 SUPPLIER CONTROL ............................................ 5

6.0 RECORDS COLLECTION AND RETENTION ....................... 6
1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to establish methods and guidelines for configuration control of the RMCST Alarm & Control logic; it does not authorize work to be performed. In addition, the responsibility for custody and maintenance of this control logic is delineated. It is intended this document meet the requirements of WHC-CM-4-2 Quality Assurance Manual and WHC-CM-3-10 Software Practices Manual.

1.2 Scope

This document is limited to the alarm and control logic as documented in drawings H-2-89459, ALARM & CONTROL LOGIC DIAGRAM (TRUCK #2) and [for Trucks 3 and 4] H-2-690069, ALARM & CONTROL LOGIC DIAGRAM (RMCST).

The Alarm & Control system has been designed to perform the initial alarm (sound the horn and turn on the strobe), alarm acknowledged and alarm reset indications via the alarm lights. Control of four (4) purge gas SOVs, the Hoist motor and brake are also part of the system. It can also shut off the drill rig engine (by removing power from the fuel pump and ignition system) under certain conditions. The PLC is a completely self-contained component of the RMCST system.

1.3 Overview

The Alarm & Control system is part of a mobile system, the Rotary Mode Core Sample Truck (RMCST). The RMCST is designed to take a vertical sample out of the waste tanks. The Alarm & Control system monitors several alarm points, actuates the horn and strobe as part of the alarm sequence and also provides limited control functions. It can also shut off the drill rig engine under certain conditions.

1.4 Definitions & Acronyms

ADP - Automated Data Processing (Equipment)
CEE - Characterization Equipment Engineering
CPE - Characterization Plant Engineering
CPU - Central Processing Unit
ECN - Engineering Change Notice
EPROM - Erasable Programmable Read Only Memory
FIRMWARE - Software stored in PROM or EPROM
I/O - Input/Output (to the PLC)
PLC - Programmable Logic Controller
PLC Logic - Software resident in the PLC memory that, by monitoring various inputs, actuates the outputs to implement the operational sequence.
QA - Quality Assurance
RAM - Random Access Memory
RMCST - Rotary Mode Core Sample Truck
SOV - Solenoid Operated Valve
2.0 MANAGEMENT

2.1 Organization

Two organizations, Characterization Equipment Engineering (CEE) and Characterization Plant Engineering (CPE), share the responsibility of maintaining the software present in the PLC.

2.2 Responsibilities

Both CEE and CPE are responsible for identifying the needed modifications, implementing changes, and requesting changes to the control logic in order to support tank farm operational needs. CPE has Cognizant authority over the RMCST equipment and is responsible for the operation of the equipment. CEE has Design authority over the RMCST equipment and is the custodian of the control logic software. Both organizations must approve any changes to the PLC software.

2.3 Interface Control

CEE shall be the primary interface point for all items regarding the design of RMCST control logic. All change/modification requests shall be submitted to CEE and CPE for approval and implementation.

2.4 Implementation

This plan will be fully implemented as soon as it's released and will apply to RMCST #2, 3 and 4. There is no PLC system on truck #1.

2.5 Policies and Procedures

The following policies and procedures are used to implement this plan.

- WHC-CM-3-10 Software Practices
- WHC-CM-4-2 Quality Assurance Manual
- WHC-CM-6-1 Standard Engineering Practices

3.0 SOFTWARE CONFIGURATION MANAGEMENT ACTIVITIES

Two groups are responsible for the software configuration. These groups are listed in section 2.0 and below along with their respective responsibilities.

- Characterization Plant Equipment (CPE) Cognizant Engineer Authority
- Characterization Equipment Engineering (CEE) Design Engineer Authority
Both groups must authorize any changes to the PLC software and associated hardware. The changes will be documented using the Engineering Change Notice (ECN) procedure(s) listed in WHC-CM-6-1 Standard Engineering Practices. Both groups are responsible for reviewing the related documentation for the changes. Typically, any changes to the PLC software will be documented on an ECN. Any other documentation associated with an ECN (ie, USQ) will be reviewed as well.

The design specification is documented in WHC-SD-WM-SDS-005, System Design Specification for Rotary Mode Core Sample Trucks 2, 3, and 4 Programmable Logic Controller.

3.1 Configuration Identification

The PLC software and hardware is documented on the drawings listed below. The PLC software is documented on the ALARM AND CONTROL DIAGRAMS and the hardware is documented on the INSTRUMENT ENCLOSURE ASSEMBLY drawing(s). The electrical connections are documented on the ELEMENTARY and ELECTRICAL CONNECTION DIAGRAMS.

Truck # 2 Drawings (partial list)
- H-2-83111, ELEMENTARY DIAGRAM TRUCK #2
- H-2-83112, INSTRUMENT ENCLOSURE ASSEMBLY TRUCK #2
- H-2-81785, ELECTRICAL CONNECTION DIAGRAM TRUCK #2
- H-2-81840, CONTROL CONSOLE ASSEMBLY (TRUCK #2)
- H-2-140300, CORE SAMPLER TRUCK #2 ASSEMBLY
- H-2-89459, ALARM AND CONTROL DIAGRAMS (TRUCK #2)

Truck # 3 and 4 Drawings (partial list)
- H-2-690000, CORE SAMPLER TRUCK ASSEMBLY RMCST
- H-2-690068, INSTRUMENT ENCLOSURE ASSEMBLY
- H-2-690069, ALARM AND CONTROL DIAGRAMS
- H-2-690070, ELEMENTARY DIAGRAM RMCST
- H-2-690071, ELECTRICAL CONNECTION DIAGRAM RMCST
- H-2-690090, CONTROL CONSOLE ASSEMBLY

The latest approved revision number to the control logic is maintained on sheet 1 of the archival/documentation copy of the control logic. The EPROM shall have an adhesive label applied over the erasing window with the revision number on it. The revision number on the EPROM shall match the latest revision number shown on sheet 1 of the ALARM AND CONTROL DIAGRAM drawing. The only ADP hardware is the PLC and is identified on the INSTRUMENT ENCLOSURE ASSEMBLY drawing(s).

The PLC system does not generate any type of hard copy reports during operation. Also, the system doesn't have any removable media other than the EPROM (firmware) listed previously.
3.2 Configuration Control

The configuration control process for the PLC software is governed by the following manuals/procedures.

- WHC-CM-3-10 Software Practices
- WHC-CM-4-2 Quality Assurance Manual
- WHC-CM-6-1 Standard Engineering Practices

Any changes to the PLC software will be documented by an ECN to one of the ALARM AND CONTROL drawings. This process will be performed per WHC-CM-6-1 Standard Engineering Practices. The archival/documentation copy of the control logic for Truck #2 is maintained on drawing H-2-89459, ALARM & CONTROL LOGIC DIAGRAM (TRUCK #2). The archival/documentation copy of the control logic for Trucks #3 & 4 is maintained on drawing H-2-690069, ALARM & CONTROL LOGIC DIAGRAM (RMCST). When a change is done to the software the revision level, as shown on the applicable drawing, is incremented by one. Because the H-2 drawings are the archival copy of the control logic the user is not required to maintain backup EPROM copies.

After an ECN to the ALARM AND CONTROL drawing is approved and released the specified changes can be performed. This involves entering the necessary software changes to the control logic into a PLC system. Typically, the new version of the software is entered on a spare PLC system like the one in the RMCST. The new version of software is then "burned" into a blank EPROM and a label is put on the EPROM with the RMCST number, date and revision level. The new firmware (software & EPROM) is then installed into the truck's PLC CPU module.

The ADP hardware is controlled per WHC-CM-6-1 Standard Engineering Practices. Any changes to the hardware are done per these procedures.

The authority for changes to this system is shared by CPE and CEE. Any changes to this system must be approved by both organizations.

3.3 Configuration Status Accounting

The status and configuration of the system is accounted for through the existing ECN/drawing system per WHC-CM-6-1 Standard Engineering Practices.

3.4 Audits and Reviews

All changes to this system are reviewed by CPE (Cognizant Engineering Authority), CEE (Design Engineering Authority), QA and Safety.

3.5 Access Control

While this PLC does not have security features in the conventional sense (i.e., passwords) casual unauthorized changes to the control logic in the EPROM are deterred as outlined in the following two scenarios:
1. Changing the existing EPROM in the field. First another EPROM must be programmed elsewhere before it could be changed in the field. Changing the EPROM requires at least two vendor specific peripherals: the EPROM programmer and the hand-held programmer (with special keypad and interface), plus another blank EPROM or an EPROM eraser, an external 5 volt dc power supply and another CPU base (to use its RAM prior to loading it into the EPROM).

2. Remove the EPROM and install the RAM into the field CPU; then the RAM can be changed in the field using the (vendor specific) hand-held programmer. Then a vendor specific peripheral (the hand-held programmer) must be used to change the RAM. However this is not a quick matter: first the right type of RAM must be acquired, then experience has shown to manually load all the logic into the RAM requires a minimum of 2 hours by an experienced user. If the RAM were to be changed en masse by downloading an EPROM, that effort would require all the equipment in scenario 1 (above); then the EPROM programmer would need to be in the field with the PLC.

Note: RAM currently is not, and probably never will be used in the PLC on the RMCST.

3.6 Backup and Recovery

The RMCST alarm & control logic is maintained in the PLC EPROM memory (firmware) and does not need or use battery backup. In the event that the control logic in the EPROM is corrupted, the user/custodian can reprogram another EPROM (based on H-2-89459 or H-2-690069), using the EPROM Writer Unit.

4.0 TOOLS, TECHNIQUES, AND METHODOLOGIES

Any control logic development may be performed on the RMCST (if not needed for field work) or a mockup. The mockup can be a spare PLC system configured to simulate the RMCST. A mockup will need, at a minimum, the following equipment:

- PLC Chassis with power supply
- PLC CPU Module
- Hand-Held Programmer
- EPROM Writer Unit
- Blank EPROM (D27C256)

There are at least two manufacturers of this equipment that meet the same form fit and function. The part numbers for this equipment is listed on the ALARM AND CONTROL drawings, Note 6. See section 3.2 Configuration Control for more detail on the EPROM programming procedure.

5.0 SUPPLIER CONTROL

Upgrades from the PLC vendor, although not anticipated, will be controlled via the procurement process and procurement specification.
Note: Field use of equivalent modules (see sheet 1 of the archival(documentation copy of the control logic drawing) for maintenance and replacement shall not require verification and validation testing. There are several vendors who make compatible controllers and I/O modules; among them GE/Fanuc, TI/Seimens and PLC Direct.

6.0 RECORDS COLLECTION AND RETENTION

Since this is a control system and doesn't generate any data no record collection/retention procedure or system is needed. Any changes to the system will be documented with the existing ECN/drawing system.