START

0010052

SOFTWARE DEVELOPMENT and QUALITY ASSURANCE PLAN for the HANFORD WASTE VITRIFICATION PLANT

(SOW 3401.03)

INTRODUCTION

The Hanford Waste Vitrification Plant (HWVP) is a new facility which is to be built in the 200 Area of the DOE Hanford reservation. The purpose of the plant is to assist in the environmentally acceptable disposal of high level and transuranic waste by immobilizing it in borosilicate glass.

A number of computer systems are included as elements of an Integrated Management and Control System (IMACS) within HWVP. Two of these systems are distributed throughout the plant area. They are the Distributed control system (DCS) and the Health Protection Computer System (HPCS).

The roles of these two systems are similar in that they both collect data from field instruments, store it, display raw and processed data to operators and management using CRT displays and printed reports. This report reviews the role of each system, recommends a division of responsibilities, identifies the software needed and proposes a plan for effective development of any new software required.

Potential DCS and HPCS vendors will be limited to those who can demonstrate that they have a number of similar systems working in the field. Thus much of the software required will have been developed and tested before the HWVP application is addressed. Any software which needs to be developed specifically for HWVP will need to be designed to work with this existing software. Therefore, although the software development and quality assurance plans are expected to conform to published standards, exact details will depend on the the selected vendor and the design and methods used to develop his standard application software. As part of his proposal, each potential vendor will be required to describe his development and quality assurance plans and their conformance to acceptable standards described below.

RECEIVED JUL 1990 EDMC

DCS SYSTEMS ROLE

The Distributed Control System is the primary means of controlling the process operations and the source of data for process development studies and for the Waste Form Qualification procedure. The major on-line tasks are:-

Maintain communications with the Distributed Processing Units located around the plant

Continuously scan the process instruments and local control panels to record process performance and status data

Maintain control of process actuators

Perform periodic and on-demand calculations on the data

Report local and remote alarms and equipment status changes

Monitor system performance and provide bumpless failover for dual redundant items

Continuously refresh displays on operator terminals and consoles

Accept approved operator commands, data inputs and control parameters

Prepare periodic and on-request printed reports

Maintain an historical process data record

Maintain event and alarm logs

Maintain System Security

Maintain a log of the system, equipment and instrument status

Prepare periodic data reports for transmission to the MIS

HPCS SYSTEMS ROLE

The Health Protection Computer System is a part of the Health Protection System which monitors the environment within and around the plant. In addition, personnel exposure data is collected. The principal on-line tasks of the HPCS are:-

Maintain communication with multiplexers located around the plant

Continuously scan the Health Protection Instruments and record health protection data

Maintain local displays of environmental status

Perform periodic and on-demand calculations on the data

Report local and remote alarms and equipment status changes

Monitor system performance and provide bumpless failover for dual redundant equipment

Continuously refresh displays on operator terminals and consoles

Accept approved operator commands, data inputs and instrument setpoint parameters.

Prepare periodic and on-request printed reports

Maintain an historical data record

Maintain event and alarm logs

Maintain the Security of the System

Maintain a log of the system and instrument status

Prepare periodic reports for transmission to the MIS

From these task lists it can be seen that there is very little difference in the roles of the DCS and HPCS. The major differences are in the types of data, the locations at which

9011884124

control actions are processed and the volume of data being collected at the "host" computers over the Data Highways.

A "worst case" estimate of the communications load associated with data collection for the Waste Form Qualification Procedure requires a significant proportion of the Data Highway bandwidth offered by many DCS vendors. At this stage of the design it is not recommended that the DCS and HPCS roles are combined and performed on the same system. In fact in the rest of this report, they are assumed to be two independent systems although using a common source vendor and system design would obviously result in savings.

There are a small number of field instruments, mostly radiation monitors, which are of potential use to both the DCS and the HPCS. Such data could, for example, be collected by the HPCS and then transmitted over a communications line to the DCS. A second method is to permit both computer systems to read the same instrument directly.

Installing a dedicated communication link between the DCS and HPCS would involve costs for developing the associated custom software and provide another potential source for corrupting the data bases on the DCS and HPCS. Permitting both systems to interface with the same instrument involves some additional expense at the instrument and a duplication of the computer interface channels.

It is recommended that DCS and HPCS be designed to share common instruments rather than provide a communications channel between their respective "host" computers.

The role of the DCS is then to collect the data associated with process operations and control. The HPCS duties are to monitor the internal and external environments of the plant and to ensure the safety of plant personnel. No communications channel is required to pass data between the two systems.

SOFTWARE REQUIRED

In this section the types of software needed for the DCS and HPCS are discussed. To some extent the discussion must be general in nature since the exact definition of the software (and the names used) will vary from vendor to vendor and the specific approach

adopted. Because of the similarity of the DCS and HPCS systems, the same type of software is required for both.

Most data acquisition systems are designed to be useful in more than one application. To achieve this the software code is usually designed to be configured by the data or "table driven." That is the code doesn't use embedded values, rather they are entered as part of the application data. In the same way the sequence of algorithms used for each control loop is entered as application data.

Thus any application is made up of two parts, the standard software which is designed and coded by programmers working for the systems vendor. This software is normally available and used directly in compiled machine code form. The second part is the data tables, specific to the application and must originate with the users, Fluor Daniel (FD) and Westinghouse Corp. (WHC).

9011138412243

Systems Software

Some software supplied with computer systems is fundamental to their operation. This software is not specific to HWVP, or even data acquistion and process control, it is supplied as completely standard software. Included are operating systems, software debuggers and run time analyzers.

Standard Application Software

Much of the application software which perform data acquisition and control will be vendor standard applications packages. They include field instrument scanning, process and sequential control, data bases, spreadsheets, system health checks, operator display builders, report generators, communications between the DPUs or multiplexers and the "host" computers.

Support Software

The support software is generally run in an interactive or batch mode either when the system is not functioning or on redundant equipment which is in the standby mode. This software which supports the real time standard applications is normally included with the standard package offered by the vendors. They include

detailed hardware diagnostics, software languages and compilers, data base generators, spreadsheet, data base query and statistical application building and test software, communications packet builders, display and report generators.

HWVP Specific Application Software

A second class of application software is very specific to the requirements of HWVP. Examples are HP records management, Radiation/Special work permits, Engineering Records, advanced control algorithms,special control sequences and operator prompt routines. Some of these applications such as the special control sequences and advanced algorithms may require custom programming of real time application modules. However, many can be implemented using standard software such as spreadsheets, databases and statistical packages.

POTENTIAL NEW SOFTWARE

The applications which are expected to require custom programming are listed in Table B1 for the DCS and Table C1 for the HPCS. In addition, Tables B2 and C2 identify the data bases and tables and application data which need to be loaded into each system to configure them to the HWVP needs.

DEVELOPMENT of SOFTWARE

Past experience in many industries, including that developing software systems, shows that the development of a new product is more likely to be successful if the development process follows a standardized procedure with formal reporting points and documentation.

Generally, development of the HWVP design is subject to the provisions of ANSI/ASME NQA-1 : "Quality Assurance Program Requirements for Nuclear Facilities." In practice this requires that software for HWVP is designed, coded, documented and tested following various standards promulgated by the IEEE. In addition, some of the software involved with collecting data on product quality is subject to the provisions of NUREG 0856 "Final Technical Position on Documentation of Computer Codes for High-Level Waste Management."

9011130412444

These various standards are listed in TABLE A attached. Precise identification of the standards to be applied to each piece of software will be one of the tasks to be completed in detailed design. Applicability of the standards to the various classes of software are discussed below.

Much of the software and documentation to be used on the DCS and HPCS has been developed and tested over a number of years. Even if possible, it would be prohibitively expensive to request a demonstration of compliance with all of these standards. Such software must be judged on reputation and past performance with the documentation accepted on an "as-is" basis. This class of software is expected to include the Systems Software, the Standard Application Software and the Support Software.

In order to minimize the risk associated with development of the IMACS, it is intended that the hardware and software will be proven "standard off the shelf software." Despite this aim, there is a requirement to develop some HWVP specific software. All such software will be developed in accordance with the standards listed in Table A.

ELEMENTS of the SOFTWARE DEVELOPMENT and QUALITY ASSURANCE PLANS

The development of software should follow a logical and planned chain of events designed to minimize the total effort needed to implement the desired system. For the most part, the IEEE specifications require that a formal plan for each of the steps is approved before the work is started and that each step is documented as it is completed. To assure the quality of the software product, the documentation must, at a minimum, consist of a requirements specification, a test and verification plan and the certified test results. These documents must be maintained for all steps of the development process from a top management overview down to the individual details. Based on this "top down" approach a typical chain of events to for managing software development is outlined below.

> The Software Development Plan is the top level view of the computer role which identifies the various tasks, the interfaces between them and whether they are to be performed using standard software or specially designed custom software. Usually, this plan is written from the users point of view and is the formal request document for the custom software.

The Software Requirements Specification is prepared by a systems analyst as a formal reply to the work request. It is a detailed document which identifies the work to be performed, the check points and test points used to measure progress and validity.

In the Software Design phase, the Software Requirements are broken down into individual modules each of which performs a single separate activity. The description of these modules includes: the interfaces to other modules, the design of associated data structures and the test methods and parameters for the module. In this phase, there will be a number of review meetings to determine the functionality and consistency of the design and conformance to the Software Requirements specification.

Once the software design is complete, individual modules can be coded and tested almost immediately. Initial testing is performed on a module stand alone basis using dummy interfaces to the other modules. Once module testing is complete, the modules can be progressively linked together and tested until the complete application is checked out. This testing will be accomplished in accordance with a previously agreed verification and validation plan.

As each part of the project design becomes firmed up, the data, design and code must be placed under configuration control.

An integral part of any software development is complete documentation of the code and associated user manuals both of which should be subject to end user and independent peer reviews. In addition, the project documentation should include the development and design plans, the verification and validations plans and the results of design reviews, verification and validation checks and the results of all quality audits conducted during the course of project execution.

It is anticipated that most of the custom software will be developed by third parties; either the DCS and HPCS vendors or specialists such as the Pacific Northwest Laboratories of Battelle Institute (PNL). For the most part such vendors will

9011880245

already have planning and quality assurance procedures in place as part of their normal operations. To utilise as much of this expertise at as minimum cost as possible each vendor will be asked to include, as part of his proposal, a plan for meeting andd conforming with all of the requirements of the standards listed in Table A.

APPLICATION DATA

Wherever possible, the design of the software will be table driven or rely on algorithm selection data to configure the software specifically to the requirements of HWVP. For the most part, this data is to be prepared by F-D and as the system is installed by the operating engineers. Methods for documenting the application data for both standard applications and custom software for the DCS is under development by F-D. This effort will be completed early in detailed design and will be extended to the HPCS system at that time. This documentation will be subject to a review by WHC at which time they will be formally introduced as the method for documenting the software applications during detailed design.

It is anticipated that the documentation will consist of logic and sequential control diagrams, proforma CRT displays, proforma reports, data bases of the I/O, operator assignments, display groupings, alarm hierarchies and security levels. It is expected that the development of the application data and diagrams will be subject to a formal development procedure similar to that described for custom software described above. The exact procedure to be adopted will be developed early in detail design as the nature of the data becomes more apparent.

In common with all the engineering of HWVP, these items will be developed by F-D and then subject to review by WHC. When the review process has been successfully concluded, the data will then become subject to configuration control.

MANPOWER REQUIREMENTS

The manpower needed to implement the custom software, application data and software configuration data are estimated in Tables B, C and D attached. These estimates are for the custom software and data bases to be generated prior to delivery, for systems

9011884124 7

installation and checkout and for minor modifications which become apparent during systems commissioning. No estimate has been made at this time for the development and implementation of the advanced control schemes envisaged which WHC staff propose to install on site.

It is recommended that most of the custom software be developed by the systems vendors since they will have experienced staff who know all of the nuances of integrating the new software with their standard application packages. In addition, it is probable that the vendor staff will have already developed a similar application which can be modified for use by HWVP.

At the moment, it is not anticipated that the DCS will be used for the Waste Form Qualification Process other than as a supplier of data. If the DCS is to be more involved in the WFQ process then the code is developed by PNL and installed after the DCS is delivered to HWVP.

The preparation of the configuration and application data should be prepared by FD and handed over to the systems vendors for loading and use in the systems acceptance tests.

INSTALLATION, CHECKOUT and MODIFICATION

Table D lists the manpower requirements for systems installation and checkout. These estimates are made on the assumption that the vendors will perform rigorous Factory Acceptance Tests and that one of the Vendors will be responsible for implementing the DCS and HPCS communications to the MIS computer which will in turn be the subject of a thorough Factory Acceptance Test.

Existing software development plans do not anticipate a requirement for a large software development effort on site prior to start up. Unless these plans are changed during the course of detailed design, staging the systems in a transitory location at Hanford prior to final installation is not recommended.

9011080412480

TABLE A

REFERENCES

ANSI/ASME NQA-1 : "Quality Assurance Program Requirements for Nuclear Facilities"

NUREG 0856 "Final Technical Position on Documentation of Computer Codes for High-Level Waste Management"

ANSI/IEEE 730 - 1984 : "Standard for Software Quality Assurance Plans"

ANSI/IEEE 828 - 1983 : Standard for Software Configuration Management Plans"

ANSI/IEEE 983 - 1986 : "Guide for Software Quality Assurance Planning"

ANSI/IEEE 1012 - 1986 : "Standard for Software Verification and Validation Plans"

ANSI/ANS 10.4 - 1987 : "American National Standard Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry"

TABLE B1

DCS CUSTOM SOFTWARE

These estimates are the time required (in man-months) to design, code, test and document the custom software. The software listed below will, for the most part, be table driven and comprise two modules. The first is the on-line module which will perform the task in real time. The second module is run off-line and is used by an engineer in interactive mode to prepare the driving tables for the on-line modules.

Inplementation of Complex Controls (YICs) 40 @ 4 man weeks	40 man months
Implementation of Operator Interactive Displays, Interlocks and Sequences 3 @ 12 man weeks	9 man months
Special algorithms for Advanced Control Functions 10 @ 8 man weeks	20 man months
Communication between DCS and PLC/PC based Local Panels. 6 @ 6 man weeks	9 man months
Communication between the DCS and the MIS	3 man months
Modify Alarm Servicing for Hierarchical Processing	3 man months
TOTAL	84 months

9011884125O

TABLE B2

DCS APPLICATION SOFTWARE CONFIGURATION

These estimates are the man months required to load the application data from databases, drawings and diagrams prepared by F-D and to check and test it.

Load from data base files and check the application data bases including: I/O, calculated variables, alarms, historical and Grouped displays 10000 @ 10 man mins.	10 man months
Load from diagrams and check Analog loop algorithms, discrete interlocks and permissive logic 2000 @ 1 man hour	12 man months
Load from diagrams and check Complex logic logic and operator interactive sequences 600 @ 1 man day	30 man months
Load from diagrams and narratives operator DCS interactive sequences 100 @ 1 man week	25 man months
Prepare graphic displays and Reports 150 @ 1 man day	8 man months
Design and Configure Training Software	3 man months
APPLICATIONS TOTAL	88 man months

9011841251

TABLE C1

HPCS CUSTOM SOFTWARE

These estimates are the time required (in man-months) to design, code, test and document the custom software.

Configure and test Data Bases/Spreadsheets.	6 man months
Configuration and on-line implementation of Statistical Analysis	3 man months
Communication between the HPCS and the MIS	3 man months
TOTAL	12 months

TABLE C2

HPCS APPLICATION SOFTWARE CONFIGURATION

These estimates are the man months required to load the application data, check it and test from databases, drawings and diagrams prepared by F-D.

Load from data base files and check the application data bases including: I/O, alarms, spreadsheets and calculated data. 5000 points @ 10 man mins.	5 man months
Load local alarm displays 100 @ 1 man hour	1 man month
Prepare graphic displays 50 @ 2 man days	5 man months
Prepare Standard reports 25 @ 1 man day	1 man month
Design and configure Training Software	3 man months
APPLICATIONS TOTAL	15 man months

9011884253

TABLE D

INSTALLATION, CHECKOUT and MODIFICATION

These estimates are the man months required to check out the systems after installation, to modify the systems to meet the plant as-built and changes in control philosophy and to change the initially installed control loops as indicated during the systems commissioning phase.

	DCS	HPCS
Prepare Site Test Plans	3 man months	3 man months
Check DPU/Multiplexer/Field Addresses	6 man months	3 man months
Check and Tune Communication Legs	6 man months	2 man months
Check Communications Software	2 man months	1 man month
Modify Applications Data Base	6 man months	6 man months
Modify Graphics/Reports	6 man months	6 man months
Modify Communications	2 man months	2 man months
Update System Documentation	9 man months	6 man months
Reconfigure Control Loops	9 man months	-
INSTALLATION TOTALS	49 man months	29 man months