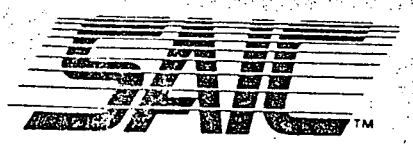
CAROLINA POWER AND LIGHT COMPANY
H. B. ROBINSON STEAM ELECTRIC PLANT UNIT 2
EMERGENCY RESPONSE FACILITY
INFORMATION SYSTEM
VERIFICATION AND VALIDATION PLAN

B. I. Cantor
N. C. Thomas

July 15, 1985

SAIC-85/1773&264D



Science Applications International Corporation
Post Office Box 4406, Lynchburg, Virginia 24502

TABLE OF CONTENTS

TABLE OF CONTENTS

(Continued)

TABLE OF CONTENTS

(Continued)

LIST OF APPENDIXES

PAGE COUNT SUMMARY

1. INTRODUCTION
CP&L EMERGENCY RESPONSE FACILITIES INFORMATION SYSTEM VERIFICATION AND VALIDATION PLAN

1.1 Objective

The objective of the Verification and Validation (V&V) program for the Carolina Power and Light Company (CP&L) H. B. Robinson Nuclear Power Plant Unit 2 Emergency Response Facility Information System (ERFIS) is to support CP&L in providing a quality system through independent technical review and evaluation.

The V&V effort described in this Plan supports the objective of providing documentation to support demonstration to the Nuclear Regulatory Commission (NRC) that an independent technical evaluation has been made on the functions provided by the ERFIS computer system with emphasis on the Safety Parameter Display System (SPDS).

The NRC requirements for computer system functions to support the control room (SPDS), TSC, and EOF operations are stated in NUREG-0737, Supplement 1. Additional NRC guidance information is found in NUREGs-0696, -0800, -0814, -0700, and in Regulatory Guides 1.97 and 1.23.

The ERFIS will be evaluated to determine that SPDS functions provide continuous and reliable display of SPDS plant parameters to control room operators. The SPDS function is required in order to keep the control room operator informed of the status of critical safety functions and alert to abnormal operating conditions.

Display of key plant parameters and archival/retrieval of this data are required to support the TSC and EOF functions. ERFIS provides these capabilities which will also be subject to V&V evaluation.

SPDS, TSC, and EOF computer functions have been incorporated with other plant computer functions such as the NSSS functions. These other plant computer functions provided by ERFIS will not be subject to V&V, but an evaluation of the noninterference of these functions with the SPDS functions will be included in the V&V evaluation.

1.2 Background

Due to the evolving nature of software quality as a technical discipline and because of the continuing concern with software quality, V&V has emerged as the systematic technical approach for evaluating the quality of software systems beyond traditional quality assurance and quality control programs. The V&V approach and level of effort described in this V&V Plan are oriented toward providing documentation for review by the NRC. The level of the V&V activity prescribed is a balance between standard industry procedures for nonsafety software and the industry approach utilized for safety system software.

To ensure that a separate technical evaluation of the system will be performed without programmatic bias, the V&V Team staff is independent of the Development Team and Quality Assurance program.

The V&V activities described in this plan will be performed by members of the SAIC Process Applications Division located in Lynchburg, Virginia. The ERFIS Development Team staff and Quality Assurance staff are members of the Energy and Software Sciences Division located in Huntsville, Alabama.

This V&V Plan serves to define the basic framework for V&V of the ERFIS and how it interacts with ERFIS development. All V&V activities will be performed according to the guidelines included in this Plan.

1.3 V&V Approach

The V&V program for the H. B. Robinson ERFIS is based on the V&V program for the Shearon Harris Nuclear Power Plant (SHNPP) ERFIS and will build on the results of the SHNPP program when appropriate. Since the two systems are intended to be essentially identical, tasks which were performed on the SHNPP V&V will not be repeated for Robinson. Rather, an evaluation of the Robinson documentation relative to that for Shearon Harris will be made and

differences (which are anticipated to be few in number and minor in nature) will be noted.

The steps being applied in the Verification and Validation of the ERFIS include:

- System Requirements Verification
- System Design Verification
- System Validation
- V&V Final Report

System Design Verification is included in the tasks to be performed, however a formal review of the design of the system is not planned since the design of the Robinson system is expected to be identical to the design of the Shearon Harris system. The activities to be performed during design verification are centered on the addition of design references to the Requirements Traceability Matrix. Figure 1-1* shows an overview of the V&V activities to be applied in evaluating the ERFIS, and Sections 2 through 5 describe each of these activities in more detail.

*Note: V&V Interactive Description (VVID) diagrams are used throughout this V&V Plan to depict the V&V activities and activity interactions. Appendix A describes the conventions used in these diagrams.

1.4 References

The following documents were referenced in preparing this Plan:

1. Specification for Emergency Response Facilities Information System, CP&L Document L2-E-022, March 2, 1984.

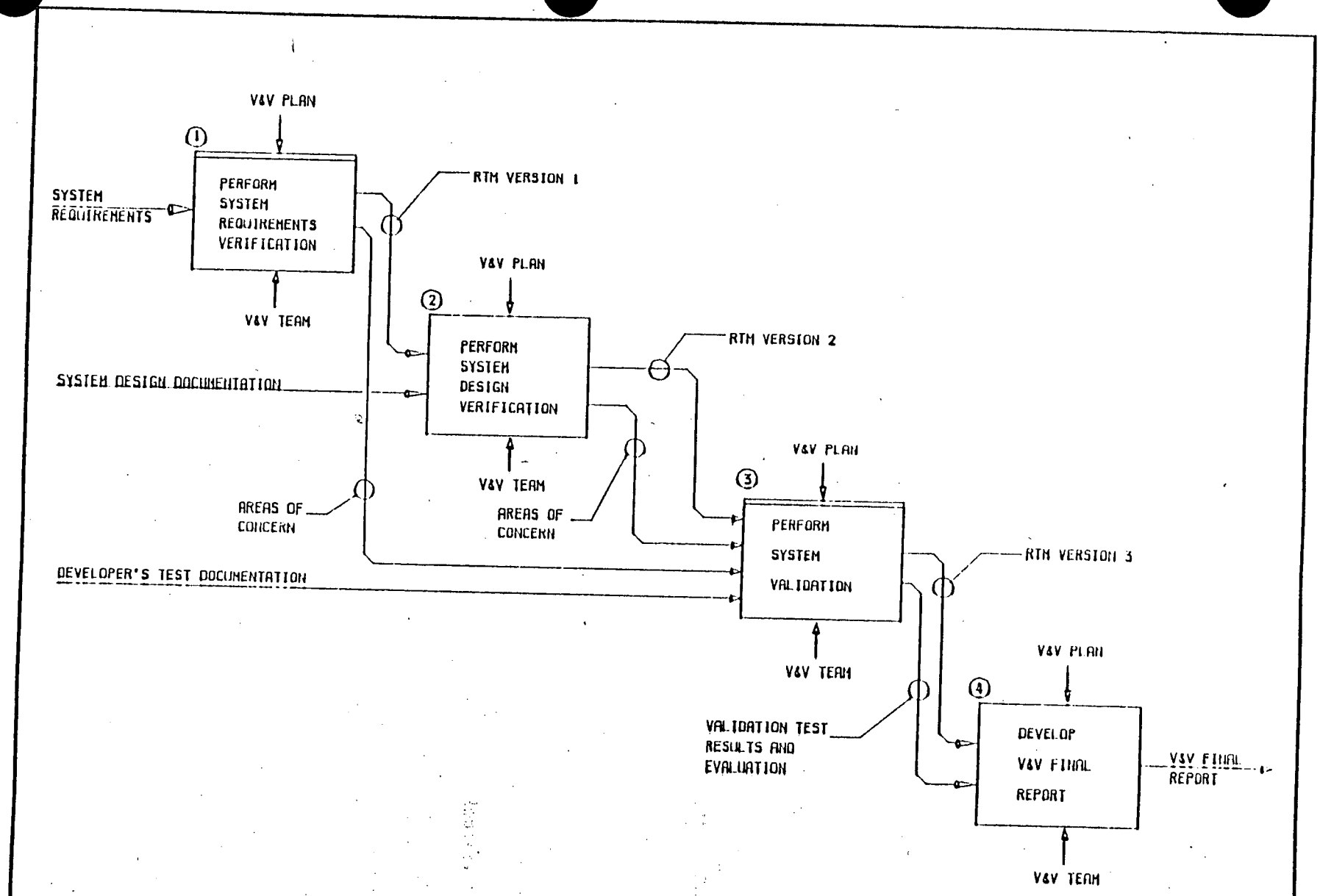
2. Verification and Validation for Safety Parameter Display Systems, NSAC-39, December, 1981.

The first document listed above contains the system requirements for the ERFIS.

Reference 2 provides guidelines for the level of effort appropriate for V&V of the ERFIS.

1.5 Organization and Content

Sections 2 through 5 of this plan provide definitions of each of the V&V activities, and a discussion of the specific areas covered in the final V&V report. Section 6 presents detailed discrepancy reporting and resolution procedures and Section 7 presents the format of the Requirements Traceability Matrix.



OVERVIEW OF V&V ACTIVITIES

FIGURE 1-1

2. SYSTEM REQUIREMENTS VERIFICATION

System Requirements Verification is a review of the system requirements documentation. The requirements will be identified and reviewed for correctness, completeness, consistency, feasibility, testability and traceability. Requirements verification will not include an evaluation of the SPDS design basis relative to applicable NRC requirements. Based on a preliminary review of the CP&L requirement specification (see Section 2.1.1) the matrix developed for Shearon Harris to link the system requirements to the NRC requirements (see CP&L SHNPP System Requirements Verification Report No. SAIC-84/1561&264, Appendix A) can be applied to the H. B. Robinson ERFIS as well.

An overview of the System Requirements Verification activities is shown in Figure 2-1.

The System Requirements Verification activities and results are documented in the V&V Final Report.

2.1 Preparation for System Requirements Evaluation

2.1.1 Sources of System Requirements

The following document will be used as the source of H. B. Robinson ERFIS system requirements:

- Specification for Emergency Response Facilities Information System, CP&L Document L2-E-022, 2 March, 1984.

2.1.2 Identification of System Requirements

The system requirements list for the Shearon Harris Nuclear Power Plant will be used as the basis for the identification of system requirements for the H. B. Robinson ERFIS. Each requirement will be identified and assigned a unique identification number. Requirements will be numbered sequentially as they appear in the source document, so that the list (see 2.1.3) will reflect the organization of the document. For each requirement, an entry

will be made in the Requirements Traceability Matrix (RTM) to describe the requirement and its location in the document. The RTM entry categorizes each requirement and includes information on testable functions, support functions, etc. See Section 7 for a discussion of the Requirements Traceability Matrix.

2.1.3 Preparation of Requirements Traceability Matrix

The file of system requirements generated in 2.1.2 will be listed in a format showing item number, requirement description, and document reference. This listing will form version 1 of the Requirements Traceability Matrix (RTM). Section 7 describes the format of the RTM.

2.2 Evaluation of System Requirements

Formal evaluation of the System Requirements consists of the following activities: (1) evaluation of the System Requirements for their technical correctness and documentation completeness, (2) identification of areas of concern during validation testing, and (3) submitting Discrepancy Reports for any discrepancies found. These areas of effort do not necessarily indicate independent activities; they may be covered in parallel. Emphasis will be placed on those areas where deficiencies were identified in the Shearon Harris requirements verification and a determination will be made whether these deficiencies have been corrected for Robinson. Again, every effort will be made to build upon the evaluations performed for Shearon Harris to minimize unnecessary duplication of effort.

2.2.1 Evaluation of System Requirements for Technical Correctness and Documentation Completeness

A technical evaluation of the system functions is performed to determine the correctness, feasibility, and completeness of the system functions described in the CP&L requirements document. The system functions are assessed from a computer system perspective and a nuclear power plant perspective. System interfaces, functional performance, security provisions, and other operational characteristics of the system are evaluated. System processing requirements and calculations are reviewed to determine the system's ability to handle the plant input data and to provide the required system outputs.

The System Requirements documentation is reviewed for consistency, traceability, and understandability. Concerns regarding the adequacy of the System Requirements documentation are recorded throughout System Requirements Verification.

2.2.2 Identification of Validation Test Implications

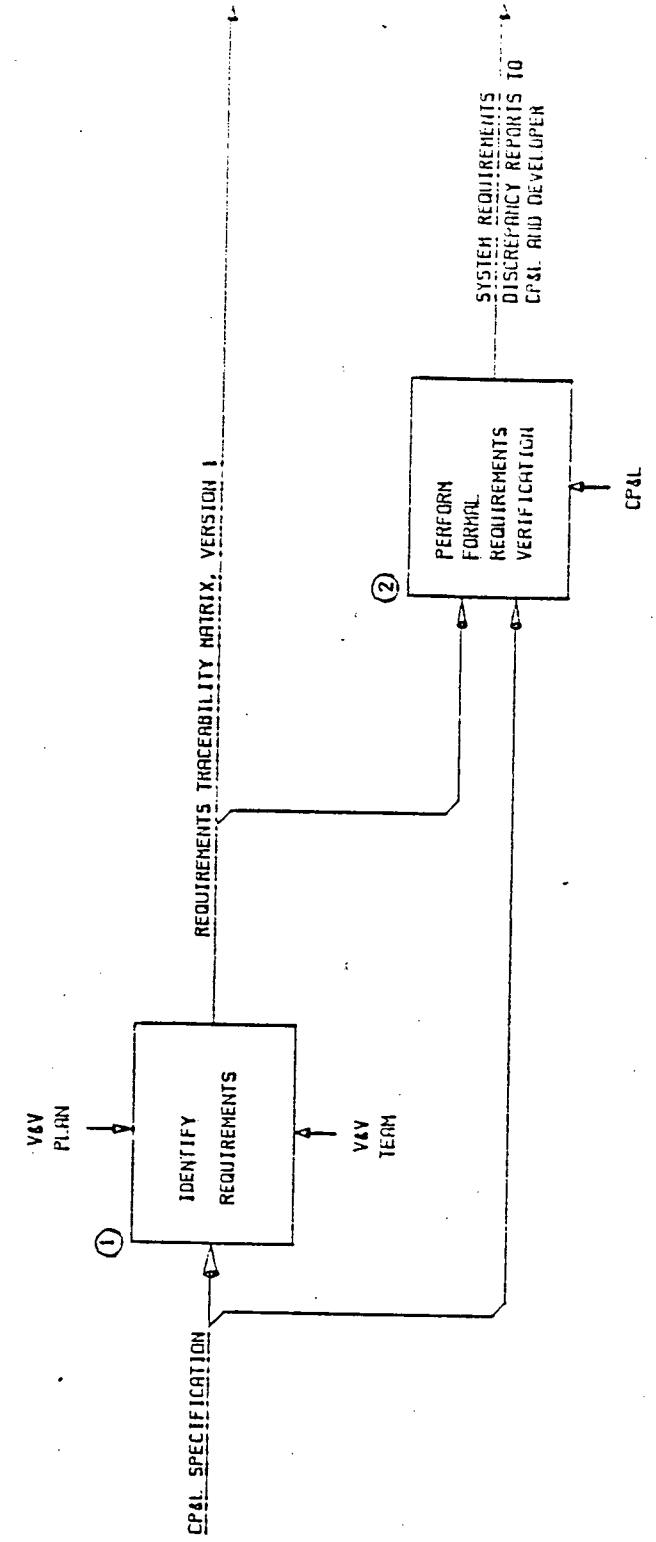
During System Requirements Verification activities, validation test implications are flagged and listed in the System Requirements Verification documentation. These include functions of major importance, functions which may be hard to test, functions which may significantly impact other important functions, and functions which have not been completely defined in the CP&L requirements documentation.

2.2.3 Discrepancy Reporting

Problems and variances found as a result of the System Requirements evaluation will be reported as formal discrepancies. Discrepancies will be documented and submitted for resolution as they are found. Refer to Section 6 for further details on discrepancy reporting and resolution procedures.

2.3 Documentation of System Requirements Verification Activities

The System Requirements Verification activities are summarized and evaluation results are documented in the Final Verification and Validation Report.



PERFORM SYSTEM REQUIREMENTS VERIFICATION

FIGURE 2-1

3. SYSTEM DESIGN VERIFICATION

The key objective of the Design Verification activity is to determine that the design is consistent with the System Requirements. A correlation should be made between the System Requirements and the system capabilities described in the design documentation. This correlation will be used to complete the link between the Validation Tests and the System Requirements in the Requirements Traceability Matrix. The scope of the Verification and Validation for the Robinson ERFIS was never intended to include a formal design verification activity due to the anticipated similarities between the Robinson and Shearon Harris designs. If CP&L desires, however, the scope can be expanded to include a detailed design evaluation based on the differences between the two systems and the hopefully more mature state of the system design documentation for the Robinson system. Due to the schedule constraints, any expanded design verification activities will need to be performed after validation on the as-built system.

3.1 Addition of Design References to the Requirements Traceability Matrix

The main activity to be performed during the system design verification will be the addition of design references to the Requirements Traceability Matrix (RTM). During the course of this work the design documentation will be scrutinized and any inconsistencies with requirements, and later with test references, will be noted and reported as discrepancies.

3.2 Discrepancy Reporting

The discrepancy reporting procedures described in Section 6 will be followed during System Design Verification. Discrepancies and problems will be reported as they are found during the System Design Verification activity.

3.3 Documentation of System Design Verification Activities

The System Design Verification activities are summarized and evaluation results are documented in the Final Verification and Validation Report.

4. SYSTEM VALIDATION

System Validation is an "end-to-end" evaluation of the system functions to demonstrate that the system meets the System Requirements. Demonstration of acceptable operation of implemented functions is accomplished through a planned testing and evaluation process. Validation testing will be accomplished by using the SAIC, Huntsville factory acceptance tests as the validation tests, and evaluating the results of these tests against the system requirements.

Figure 4-1 illustrates the System Validation activities. The steps of System Validation are (1) review of Validation Test Procedures, (2) addition of Validation Test Procedures references to the Requirements Traceability Matrix, (3) performance of Validation Testing, (4) evaluation of Validation Test Results, and (5) the writing and resolution of System Validation discrepancy reports.

The System Validation activities and results will be documented in the Final V&V Report.

Procedures for the performance of these System Validation steps are included in the sections below.

4.1 Preparation of Validation Test Procedures

The Factory Acceptance Test Procedures will be written by SAIC, Huntsville and will be approved by CP&L prior to running the tests.

The Factory Acceptance Test Procedures should include for each test the specific input, the capability or function being tested, and the expected output. The Test Procedures should also describe the test set-up and initialization, test case execution sequence, data recording procedures, actions that must be performed by the operator, and methods of test case termination. The methods to be used for immediate data reduction, interpretation, and evaluation should also be described for each test case. Acceptance criteria must be established to support evaluation of the test results. Actions required of or available to the test operator in the event of operation error or execution problems should also be described. Test environment must be specified for each test.

4.2 Review of Validation Test Procedures

The V&V Team will review the Factory Acceptance Test Procedures for completeness, correctness, understandability, and feasibility. The reviewed Factory Acceptance Test Procedures plus the V&V Team comments and discrepancies will then become the Validation Test Procedures.

4.3 Addition of Validation Test Procedures References to the Requirements Traceability Matrix

As part of the preparation of the Requirements Traceability Matrix, test case references from the Validation Test Procedures are added to the Matrix for all capabilities or functions being tested. Section 7 describes the format of the Requirements Traceability Matrix.

4.4 Performance of Validation Testing

SAIC, Huntsville will furnish test data. SAIC, Huntsville will perform and document all tests, and SAIC, Lynchburg will witness the testing activity. Appendix B presents guidelines for the monitoring of the validation testing. (Note that since the validation tests are also the factory acceptance tests, CP&L will also be monitoring the tests, but this is not part of the V&V effort.) The V&V Team may request retesting or modification of the tests to meet the V&V objectives. Problems encountered or deviations from the Validation Test Procedures will be noted by the V&V Team and may be reported as discrepancies.

4.5 Documentation of Validation Test Evaluation

SAIC, Lynchburg will perform evaluation of test results furnished by SAIC, Huntsville, and will document the results of this evaluation in the Final V&V Report.

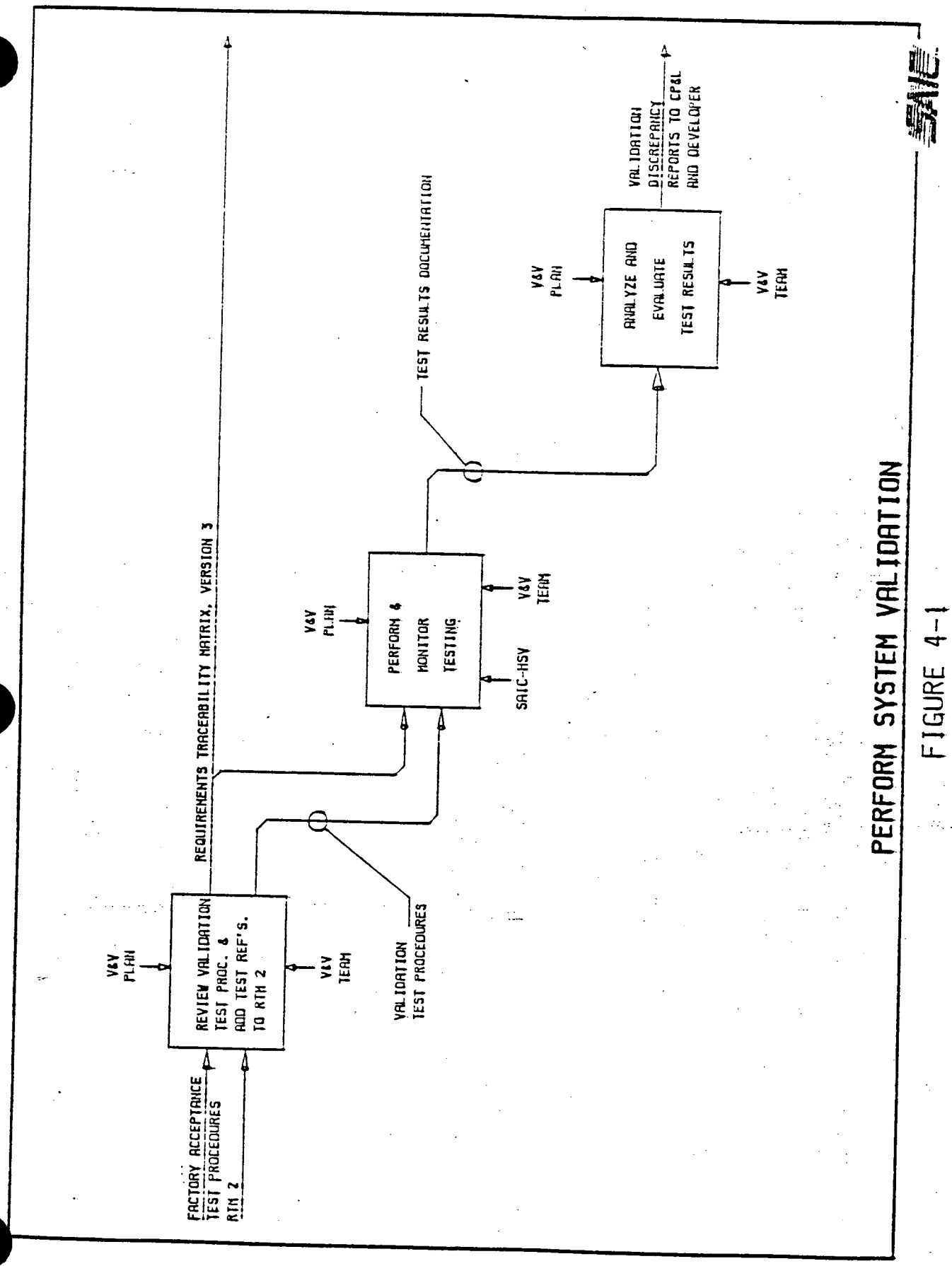

PERFORM SYSTEM VALIDATION
FACTORY ACCEPTANCE TEST PROCEDURES
RTM 2
REVIEW VALIDATION TEST PROC. & ADD TEST REF'S. TO RTM 2
V&V PLAN
V&V TEAM
REQUIREMENTS TRACEABILITY MATRIX, VERSION 3
VALIDATION TEST PROCEDURES
PERFORM & MONITOR TESTING
V&V PLAN
V&V TEAM
SAIC-HSV
TEST RESULTS DOCUMENTATION
ANALYZE AND EVALUATE TEST RESULTS
V&V PLAN
V&V TEAM
VALIDATION DISCREPANCY REPORTS TO CP&L AND DEVELOPER

FIGURE 4-1

5. V&V FINAL REPORT

5.1 Objective

The purpose of this activity is to document the V&V activities performed throughout the project.

The intent of this document is to provide an overview of the V&V activities performed, summarize the results of each activity and provide an overall assessment of the system's quality based on the V&V evaluation results.

5.2 Organization and Content

The V&V Final Report provides traceability of the Verification and Validation activities throughout the project. Each activity is described and includes reference to the system development documentation evaluated, and the V&V documentation generated as a result of the activity. Discrepancy and discrepancy resolution results generated throughout V&V will be referenced. A summary of the discrepancies reported and resolved will be provided and any discrepancies left unresolved will be identified.

This document will be organized to facilitate evaluation of the ERFIS system by CP&L and the NRC.

A preliminary outline of the V&V Final Report contents is shown in Figure 5-1.

Figure 5-1

V&V FINAL REPORT OUTLINE

1. Overview
   - Summary of V&V Plan
   - Identification of V&V Documentation
   - Other Project References
   - Overview of V&V Activities

2. System Requirements Review
   - Objectives
   - Summary of Activities
   - Summary of Results
   - Deficiencies Identified/Resolved
   - References

3. Design Review
   - Objectives
   - Summary of Activities
   - Summary of Results
   - Deficiencies Identified/Resolved
   - References

4. Validation Test
   - Summary of Test Procedures
   - Summary of Test Execution
   - Summary of Test Results
   - Deficiencies Identified/Resolved
   - References

5. Summary and Conclusions
   - Development of Traceable/Auditable Quality Product

Appendix A - Requirements Traceability Matrix

Appendix B - Discrepancy Reports

6. DETAILED DISCREPANCY REPORTING AND RESOLUTION PROCEDURES

Problems and inconsistencies found during formal Verification and Validation activities will be reported by the V&V Team as discrepancies. Resolutions to the discrepancies reported will be prepared by either CP&L or by SAIC - Huntsville.

Some of the typical problems that may be identified and reported as discrepancies are:

- deviations from CP&L functional requirements
- deviations from documentation requirements
- documentation inconsistencies
- incorrect design logic or implementation
- incorrect results (from system testing).

Standard Discrepancy Report forms will be available for reporting discrepancies throughout V&V. A sample Discrepancy Report form is shown in Figure 6-1. Figure 6-2 shows a continuation page if needed for the Discrepancy Report.

The Discrepancy Report form contains three parts. The first part will describe the discrepancy, the second part will describe the resolution, and the third part will describe the discrepancy report status.

6.1 Report Discrepancy

The V&V Team will complete PART 1 of the form which describes the discrepancy. The following information will be supplied (the numbers below correspond to the numbered items in Figure 6-1 PART 1):

(1) Discrepancy Report Serial Number (unique identifier)
(2) Date on which discrepancy was found
(3) Project identification
(4) V&V Team member preparing the report
(5) Date of preparer's signature
(6) V&V task underway when the discrepancy was found
(7) V&V Team member reviewing the report

(8) Date of reviewer's signature
(9) Identification of development document(s) where problem was found
(10) Description of the problem or variance
(11) Estimate of impact on system

Discrepancies and problems found during V&V evaluation and testing are reported to CP&L and SAIC - Huntsville for consideration. The Discrepancy Report will be resolved based on actions or justification by either CP&L or SAIC - Huntsville, as appropriate. All Discrepancy Reports should be included in the project files, even those requiring no action. If CP&L determines that no action is required, this must be stated along with the justification in the resolution report.

6.2 Resolve Discrepancy

Discrepancy Reports should be entered into SAIC - Huntsville's Configuration Management system. Discrepancy resolutions involving system changes will be provided by the appropriate Development Team members designated by SAIC - Huntsville. The Development Team members responsible for implementing the change will complete PART 2 of the Discrepancy Report (refer to Figure 6-1). The following information will be supplied by the Development Team:

(12) Description of resolution and action taken
(13) Developer responsible for the problem resolution
(14) Date of developer's signature

The Discrepancy Report will be returned to the V&V Team when the problem has been resolved and tested and the necessary approvals by Project Management have been obtained.

6.3 Evaluate Discrepancy Resolution

The V&V Team may review the discrepancy resolution and system change documentation as appropriate to determine the potential impact of the resolution on the system. The V&V Team will have access to change and error reports and approval forms. This information should provide proper tracking of the implemented change to the system documentation and should reference the methods used to test the change (if required).

The V&V Team will ensure that all applicable documentation changes have been made and system retest methods (if required) have been employed. The impact that the changes may have on other parts of the system is checked.

Due to the similarity between the Shearon Harris and Robinson systems it was anticipated that a small number of discrepancies (less than ten) would result from the Robinson ERFIS review. If this is not the case, then the V&V scope can be increased if desired by CP&L to allow the V&V team to resolve these additional discrepancies. Resolution of some of these discrepancies may involve the repetition of previous V&V tasks and this activity is not included in the current V&V scope.

PART 3 of the Discrepancy Report is signed-off by the V&V Team when the discrepancy report has been closed. If the resolution action is not satisfactory, then the Discrepancy Report will be left open and returned to CP&L for appropriate action.

The following information will be supplied on PART 3 of the Discrepancy Report (the numbers below correspond to numbered items in Figure 6-1 PART 3):

15) V&V Team member's initials (if the report is considered closed)
16) V&V Team member's position
17) Date Discrepancy Report was closed.
18) V&V Team comments.

DISCREPANCY REPORT SERIAL NO.: 0 (1) DATE: / / (2)

PROJECT: (3)

PREPARED BY: DATE: / /
SIGNATURE: (4) (5)

V&V TASK: (6)

REVIEWED BY: DATE: / /
SIGNATURE: (7) (8)

PART 1

DOCUMENT(S) WHERE DISCREPANCY EXISTS:
(9)

DESCRIPTION OF DISCREPANCY: PAGE 0 OF 0
(10)

ESTIMATE OF IMPACT:
(11)

PART 2

RESOLUTION ACTION:
(12)

ISSUED BY: (13) DATE: (14)

PART 3

DISCREPANCY RESOLVED					
	INITIAL (15)				
	POSITION (16)				
	DATE (17)				

COMMENTS:
(18)

Figure 6-1
Discrepancy Report Form

DISCREPANCY REPORT	SERIAL NO.:	PAGE 2 OF 2	DATE: 04/17/85
PROJECT:		V&V TASK:	

DESCRIPTION OF DISCREPANCY:

Figure 6-2
Discrepancy Report Continuation Form

7. REQUIREMENTS TRACEABILITY MATRIX

The Requirements Traceability Matrix (RTM) consists of nine columns, illustrated in Figure 7-1.

7.1 RTM Version 1

The first column contains sequential item numbers for requirements. Requirements are identified and numbered in the order in which they appear in the documents. Thus, the RTM reflects the organization of the requirements documents. Columns 2, 3, and 4 contain a reference to the document where each requirement appears. Column 5 contains a text description of each requirement. Column 6 contains an item titled "CLASS", which will be filled in with a code to indicate the following:

T - indicates a testable function

C - indicates a testing consideration

B - indicates a design basis requirement

S - indicates a support function

When identification of requirements is complete and the first six columns are filled in, RTM Version 1 is completed.

7.2 RTM Version 2

During Design Verification, design references obtained from the SAIC Functional Specification corresponding to requirements are entered in Column 7 to form RTM Version 2.

7.3 RTM Version 3

RTM Version 3 is the completed Requirements Traceability Matrix, with Validation Test Procedures references and results entered in Columns 8 and 9. The completed Requirements Traceability Matrix will be included in the Final V&V Report.

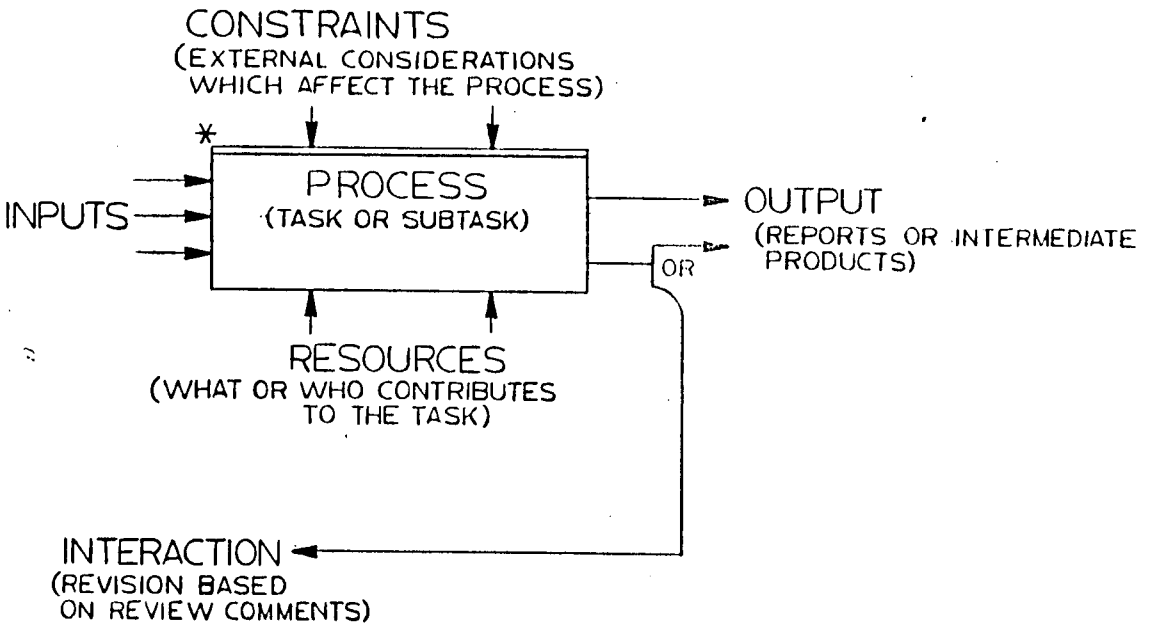
REQUIREMENTS TRACEABILITY MATRIX - CP&L ROBINSON

ER NUM	DOCUMENT	SECTION	PAGE	REQUIREMENT DESCRIPTION	CLASS	DESIGN REFERENCE	TEST PROCEDURE	TEST RESULT

Figure 7-1
Requirements Traceability Matrix

APPENDIX A

* NOTE: STRIPE AT THE TOP OF ACTIVITY BOX INDICATES THAT THERE IS A DRAWING WHICH SHOWS FURTHER DETAIL OF THE ACTIVITY



CONVENTIONS USED IN V&V INTERACTIVE DESCRIPTION DIAGRAMS

Figure A-1

Appendix B - Test Monitoring

This appendix describes the role of the V&V Team during testing. Note that for the H. B. Robinson ERFIS, system validation testing will be combined with the factory acceptance tests. The following guidelines should be used by the V&V Team during testing:

1. The V&V Team should be allowed to witness any portion of the testing, however, V&V Team presence is not required to conduct a test.

2. The V&V Team should have access to a copy of all test results and revisions to the controlled test procedure document.

3. The V&V Team should be provided with a copy of the Test Procedures for all tests to be run on a given day.

4. The V&V Team should maintain a Validation Test Log. The log will be maintained in a log book which will become part of the official V&V documentation. During the performance of the testing it may be expedient to keep notes on the Test Procedures themselves, as there may not be time to keep up with the log book. However, the log book should be updated periodically when there is a break in the testing. The marked Test Procedures will also become a part of the V&V documentation. The log should contain reference to any reviewer comments or discrepancy reports issued during testing. If desired, the developers and QA may obtain a copy of the Validation Test Log. The log should describe the testing and any supporting information or observations of the V&V Team.

5. The V&V Team should meet with the developer's QA Representative on a regular basis to insure that QA's documentation of the test results contains sufficient information to support the validation effort. The meetings with the QA Representative should occur at least every other day and preferably every day during the course of the testing.

6. The testing should be monitored to ensure that the procedures are followed and that system performance is acceptable. If possible, before or during system testing the capability matrix should be checked off and filled in to indicate a system function has been tested. Beyond this, the V&V Team should monitor for the use of good test practices. The following list is a checklist of items to be considered. A "no" to any of these questions should be recorded in the Validation Test Log. If a serious problem is uncovered, a discrepancy report form (PART 1) should be issued. Other, less serious problems or questionable areas should be reported via the reviewer comment form. (Refer to Page B-4 for Reviewer Comment form and to Pages 6-4 and 6-5 for the Discrepancy Report form.):

- Is the test objective and scope of the test clear to the test engineer and those involved in judging system acceptability?
- Can tests be run according to the procedure?
- Does the system response meet or exceed the acceptance criteria?
- Is the test result being properly documented?
- Is there subjective judgment involved in deciding whether the acceptance criteria are met?
- Are the test personnel following their own QA and configuration management procedures?
- Is the system (hardware/software) and test system (hardware/software) under administrative and document control to ensure procedures are being followed?
- Is the system response repeatable?
- Are there any spurious, unexplained responses?

- Are there any system responses that are obvious problems, for cases not strictly covered by procedure?
- Is the test equipment properly calibrated?
- Are test procedure changes handled in an acceptable, controlled fashion?
- When tests fail, is proper consideration given to retest?

REVIEWER'S COMMENT	SERIAL NO.:
PROJECT:	DATE:
V&V TASK: VALIDATION TESTING	ISSUED BY:

DOCUMENT(S) UNDER REVIEW:

QUESTION OR ANOMALY:

COMMENTS:

Figure B-1
Reviewer Comment Form