APPENDIX A

TECHNICAL PROCEDURE FOR THE PERFORMANCE OF THE ANALYSIS

eds nuclear

PROJECT INSTRUCTION

TITLE: Control Systems Power Supply and Sensor Malfunction Study

INSTRUCTION NUMBER: 0160-004-001

CLIENT: Pennsylvania Power and Light Company (PP&L)

PROJECT: Susquehanna Steam Electric Station (SSES)

JOB NUMBER(S): 0160-004-671

DIVISION(S) Systems Engineering

REV.	ISSUE DATE	PREPARED	APPROVED	CONCURRENCE
0	June 30, 1981	Alan Sawyer	W A Stevens	[illegible] Mabley
1	Aug. 14, 1981	Paul W. Lynches	W A Stevens	H. T. Rehm / J M Mabley
2	Dec. 17, 1981	Paul W. Lynches	W A Stevens	H. T. Rehm / J M Mabley

TABLE OF CONTENTS

TABLE OF CONTENTS (Cont.)

1.0 PURPOSE

The Susquehanna Steam Electric Station (SSES) Safety Evaluation Report (April, 1981) imposed additional requirements pertaining to Section 7.7 Control Systems Not Required for Safety. Specifically, the requirements include:

1. Identification of power sources or sensors that provide power or signals to two or more control systems

2. Analysis of the effects of the failure or malfunction of these common power supplies or sensors to determine if the resulting consequences are outside the boundary of Chapter 15 analysis or beyond the capabilities of operators or safety systems.

The Project Instructions contained herein define the methodology developed by EDS Nuclear to respond to these requirements. Project Instructions Change Notices will be issued in the event that the scope of work is modified or that new tasks are identified which fall outside the scope of existing tasks. The procedure for making changes to the Project Instructions is contained in Appendix E.

2.0 PROJECT INSTRUCTIONS

The specific Project Instructions are delineated herein by task number corresponding to the tasks identified in the scope of work sections of EDS proposal 16-11.

Task No. 1 Develop Administrative and Technical Procedures

Objective: To finalize the overall program scope and methodology.

1. Develop the Project Instructions, Interface Control Instructions and the Project Quality Assurance File.

   a. Project Instructions - The Project Instructions identify the design or analysis steps that are to be implemented by the project team in order to accomplish its defined tasks.

   b. Interface Control Instructions - The Interface Control Instructions (ICI) define the lines of communication between EDS, the client, and other support organizations. The ICI includes administrative procedures for maintaining written and verbal communications throughout all phases of the project.

   c. Quality Assurance File - The Quality Assurance File is the vehicle through which the EDS Quality Assurance Program is implemented at the project level.

   The development of the above documents will be accomplished in accordance with Rev. 15 of the EDS Quality Assurance Manual.

Task No. 2 Assemble Design Input Information

Objective: To assemble all pertinent information required to support the project.

1. Coordinate with PP&L to identify and collect the documentation required to support the project. Included in this documentation will be all items which will aid EDS in its efforts to identify common power supplies and sensors and to analyze the effects of their failure or malfunction upon the appropriate control systems.

2. In the process of identifying power supplies and sensors, it may be necessary to obtain amplifying information from either Bechtel or General Electric. EDS is authorized to coordinate directly with these organizations in order to expedite obtaining the required information. PP&L is to be informed of the need for this additional information.

3. The following information, as a minimum, will be transmitted to EDS:

   a. SSES Safety Evaluation Report - April, 1981
   b. SSES Final Safety Analysis Report
   c. System Descriptions (General Electric Specifications)
   d. Piping and Instrumentation Diagrams (P&ID)
   e. Electrical One Line Diagrams
   f. Electrical Elementary Diagrams
   g. Instrument Index
   h. Setpoint Index
   i. Functional Control Diagrams
   j. Loop Diagrams
   k. Plant Procedures - Operating/Abnormal/Emergency

4. All documents, drawings and other design inputs will be handled in accordance with Rev. 15 of the EDS Quality Assurance Control Manual. A memorandum will be submitted by the appropriate project personnel and approved by the Project Engineer indicating that verification has been conducted to ensure proper entry of all documentation into the QA File.

Task No. 3 Identification of Control Systems not required for safety.

Objective: To identify those Control Systems not required for safety whose failure or malfunction could impact on plant safety.

1. In order to identify all Control Systems which impact on plant safety, it is first necessary to identify those plant safety functions that are required to be met during the modes of plant operation addressed in Chapter 15 of the SSES FSAR. The modes of plant operation are as follows:

   a. Reactor Shutdown/Head off
   b. Reactor Not Shutdown/Head off

c. Reactor Shutdown/Head on
d. Reactor Not Shutdown/Head on

Review Chapter 15 of the SSES FSAR and generate the list of the Safety Functions required by Chapter 15 to support those modes of plant operation. Document the Plant Operating Modes, Safety Functions, and FSAR References on Figure 1.

2. Transfer the plant modes of operation and associated supporting safety functions to the Control System Identification Diagram (CSID), as per Figure 2. These diagrams are designed to graphically present the following:

1. Plant Operating Modes
2. Plant Safety Functions
3. Control Systems
4. Power Supplies and Sensors (to be added during Task 4)

The detailed procedure for the preparation of the CSID's is contained in Appendix B. This procedure should be used for this task and all future tasks involving CSID input.

3. Once the key plant safety functions are identified, identify those control systems not required for safety and align them with their respective safety functions. Since these control systems taken individually are, by definition, not safety-related, it will be necessary to determine if and how each of these control systems affect each of the aforementioned safety functions. It is imperative that each of these control systems be carefully and completely analyzed, since it is quite possible that indirect effects on safety exist which may not have been previously addressed in the FSAR.

Transfer the control systems information to the CSIDs as per Figure 2. Annotate each control system on the CSID to show its relationship to <u>each</u> of its related safety functions, respectively.

In order to ensure that the control systems have been properly identified and matched with their respective safety function(s), the Project Engineer will conduct an independent check for each plant safety function.

Task No. 4 Identification of Power Supplies and Sensors

Objective: To identify all power supplies and sensors which provide power or signals to those control systems not required for safety.

1. For the purposes of this task and all future tasks, the following terms are defined:

   Control System Sensor - a device which responds to changes in a plant variable and converts the measured process variable into an electric or pneumatic signal.

   Control System Power Supply - the primary level electrical power source (i.e.; major instrumentation bus), AC or DC, to a component or sub-system of a control system.

   Cascading Power Supply Effect - the potential failure of higher level power supplies, up to and including the 120 VAC or 125 VDC bus, originating from the Control System Power Supply.

2. Analyze each control system identified in Task No. 3 to determine every power supply and sensor that provides power and signals, respectively, to that control system. This task will involve extensive use of P&ID's, Electrical One Line and Elementary Diagrams, Functional Control Diagrams, Instrument Index and Loop Diagrams. If the control system being analyzed is made up of sub-systems or components, it will be necessary to ascertain power supply and sensor information for each of these items.

3. Those cases which involve electro-mechanical sensors that are part of a control system will be handled by treating the mechanical and electrical sub-components separately. List the mechanical sub-components as a sensor for that control system. In addition, list the power supply for the electrical part of the component as one of power supplies to that control system.

4. In the identification of power supplies for each control system, it will be necessary to examine the cascading effect of higher level power supplies. Specifically, subsequent to identifying the primary level power supply, identify all successive higher level power supplies up to and including the 480V bus. The cascading effect is shown in Figure 3.

5. Each power supply and sensor identified in the task must be then added to CSID's. Note that for those control systems that contain sub-systems or components, the power supply and sensor information is added below each sub-system or component, respectively. Cascading power supplies will be handled as per Figure 2. Each of the higher level power supplies will include a letter in addition to the number (i.e.; "6a, 6b").

6. At this point, the CSID's will be complete. They now contain the following information:

    1. Plant Operating Modes
    2. Plant Safety Functions
    3. Control systems not required for safety
    4. Control systems - Sub-systems/Components (if applicable)
    5. Power supplies and sensors

    The Project Engineer will review all CSID's to ensure they are complete and properly formatted.

Task No. 5 Identify Power Supply and Sensor Commonality

Objective: To determine which power supplies and sensors provide power and signals to more than one control system.

1. Power supply and sensor commonality is to be determined through the examination of the CSID's. Commonality, for the purpose of this project, is defined as any power supply or sensor which provides power or signals to more than one control system for any safety function(s) in a particular plant operating mode.

2. Generate a Commonality Diagram (CD) for each common power supply and sensor determined through examination of the CSID's. See Appendix C for the detailed procedure for CD Preparation.

Each diagram will start with the common power supply or sensor then branch off to the affected control systems. Each control system shown on the Commonality Diagram must be annotated to show which safety function(s) it supports. Figure 4 is an example of a Commonality Diagram.

3. An independent check will be conducted on each plant operating mode in order to ensure that all common power supplies and sensors have been determined.

Task No. 6 Perform Failure Modes and Effects Analysis

Objective: To analyze the effects of power supply and sensor failures or malfunctions on control systems and plant performance.

1. In order to completely analyze the effects of the failure or malfunction of those common power supplies and sensors, a Failure Modes and Effects Analysis (FMEA) will be conducted on each common power supply and sensor determined in Task No. 5. The following information, germane to the effect of the failure or malfunction on the control system and plant performance, must be included:

   a. Name of power supply or sensor being analyzed
   b. Failure mode(s)
   c. Symptoms and local effects
   d. Inherent Compensating Provisions
   e. Effect(s) upon control systems/plant performance

   The detailed procedure to be used in FMEA preparation is contained in Appendix D.

2. The information required to generate the FMEA shall be obtained by conducting a detailed systems analysis on each control system and its constituent parts.

3. The Failure Modes and Effects Analysis will be presented in tabular form as per Figure 5.

Task No. 7 Determination of the Impact of Malfunctions on Plant Safety.

Objective: To determine the impact on plant safety of the simultaneous malfunction of control systems resulting from common power supply or sensor failure or malfunction.

1. The effects on plant performance and control system operation as determined through the Failure Modes and Effects Analysis is to be utilized in the determination of the impact on plant safety resulting from common power supply and sensor failure or malfunction. The impact of each failure on plant safety will be determined as follows:

   a. Conduct a functional safety analysis on each of the failure effects noted in the FMEA. The result of this analysis will be a list of plant safety-related conditions associated with each multiple control system failure.

   b. Compare the resulting plant safety-related conditions with those safety responses previously documented in Chapter 15 of the SSES FSAR. A determination must be made to ensure that these parameters are bounded by the analyses in the Chapter 15.

   c. In addition, analyze each plant safety-related condition to verify that in addition to being bounded by Chapter 15 analyses, the conditions would not require action or response beyond the capabilities of operators or safety systems.

      1. To accomplish the operator portion of this task, conduct a comparison between the operator action required to mitigate the resulting abnormal conditions and the operator actions delineated in the SSES FSAR Chapter 15.

      2. To accomplish the safety system portion of this task, utilize the safety analysis described in Chapter 15 and the information from the safety system detailed descriptions to verify that the resulting conditions are adequately covered by the safety system capabilities.

2. Documentation of the analyses performed in Item 1 should be accomplished as follows:

   a. Chapter 15 comparitive analyses - document in tabular form as shown on Figure 6. Items to be included are:

      1. Plant condition(s) resulting from common power supply or sensor failure.

2. Corresponding Chapter 15 responses.

b. Operator or Safety System capabilities - document in tabular form as shown in Figure 7. Items to be identified are:

1. Plant condition(s) resulting from common power supply or sensor failure.

2. Corresponding operator responses as per the appropriate procedure.
3. Corresponding Safety System responses as per the specific section of the FSAR.

c. For Final Report purposes, present the analyses shown on Figures 6 and 7 in paragraph form in the main body of the report.

Task No. 8 Recommendation for Modification or Reanalysis

Objective: To identify those control systems failures not bounded by Chapter 15 analysis and to recommend further action.

1. In the event that, in the performance of Task No. 7, it is determined, through analysis, that the resulting plant safety-related conditions are not bounded by Chapter 15 analyses, recommendations are to be made as delineated below:

a. Plant Modifications - Conduct analysis of plant conditions resulting from the control system failures and provide recommendations for plant modifications to resolve this problem. Possible modifications that are to be provided in this task include:

1. Modify or provide separate power supply
2. Modify or add another sensor
3. Add channel separation
4. Add or delete a component
5. Provide for automatic bus transfer

b. Chapter 15 Recommendations for Reanalysis - Conduct a review of plant conditions resulting from the control system failures and provide recommendations for reanalysis of Chapter 15 to properly bound those plant conditions.

2. Document the results of Task No. 8 as follows:

   a. Document the plant safety-related condition and its corresponding recommendation for plant modification or Chapter 15 reanalysis in tabular form as per Figure 8.

   b. For Final Report purposes, present the analyses shown on Figure 8 in paragraph form in the main body of the report.

Task No. 9 Report Submittal

Objective: To document all methods, assumptions, findings, conclusions and recommendations.

1. Prepare a preliminary report of the results of this study for submittal to PP&L as per the NRC requirements levied in the April, 1981 Safety Evaluation Report. This report will include all pertinent information and data and will document all methods, assumptions, analyses, results, conclusions and recommendations. PP&L will be requested to review this preliminary report and to comment on its content.

2. Subsequent to PP&L's review of the preliminary report, incorporate all comments agreed upon by PP&L and EDS in a Final Report.

3.0 QUALITY ASSURANCE

1. Engineering work associated with each of the tasks in Section 2.0 will be performed in accordance with Revision 15 of the EDS Quality Assurance Manual.

2. The checking criteria to be used for this work is itemized below. This criteria is in addition to those items set forth in Attachment A of EDS QAP 3.6 of Rev. 15 to the QA Manual.

   a. Control System Identification Diagrams

      1. Does each CSID contain only one Plant Operating Mode and is it clearly identified?
      2. Are the safety functions properly identified under the Plant Operating Mode?
      3. Are the control systems required for each safety function properly identified?
      4. Does each control system have the appropriate annotation linking it to its respective safety function?
      5. Are components and sub-systems properly indicated below each control system (where applicable)?
      6. Are power supplies and sensors clearly identified for each control system?
      7. Has the diagram revision information been properly entered?

   b. Commonality Diagrams

      1. Does the Commonality Diagram reflect only one power supply or sensor? Is it properly identified?
      2. Are the control systems common to that power supply or sensor properly identified and annotated to show plant mode and safety function affected by this commonality?
      3. Are components and sub-systems related to the control system properly identified?
      4. Has the diagram revision information been properly identified?

APPENDIX A

FIGURES

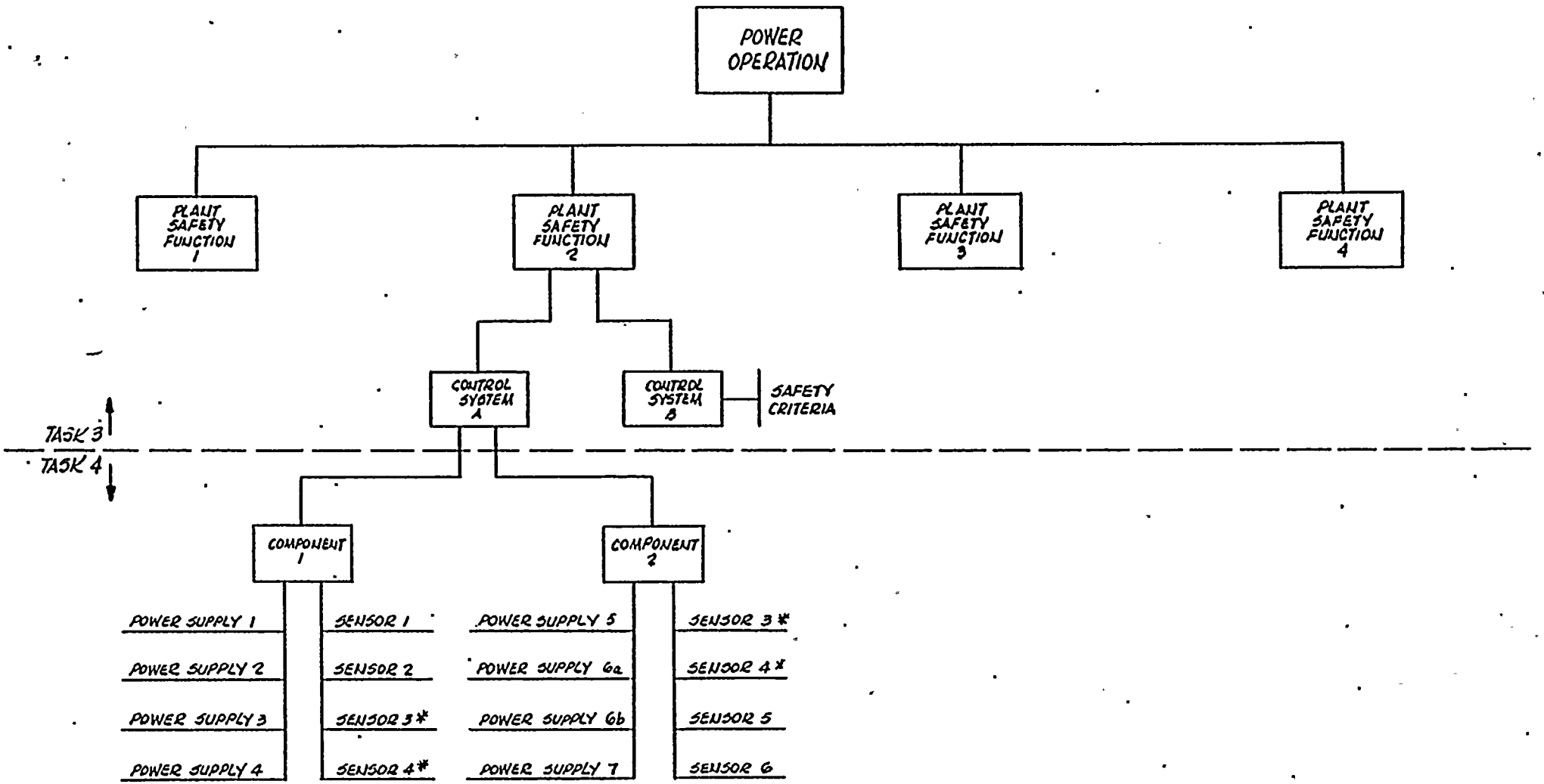
FIGURE 1

PLANT OPERATING MODE

SAFETY FUNCTIONS

Title	Description	References

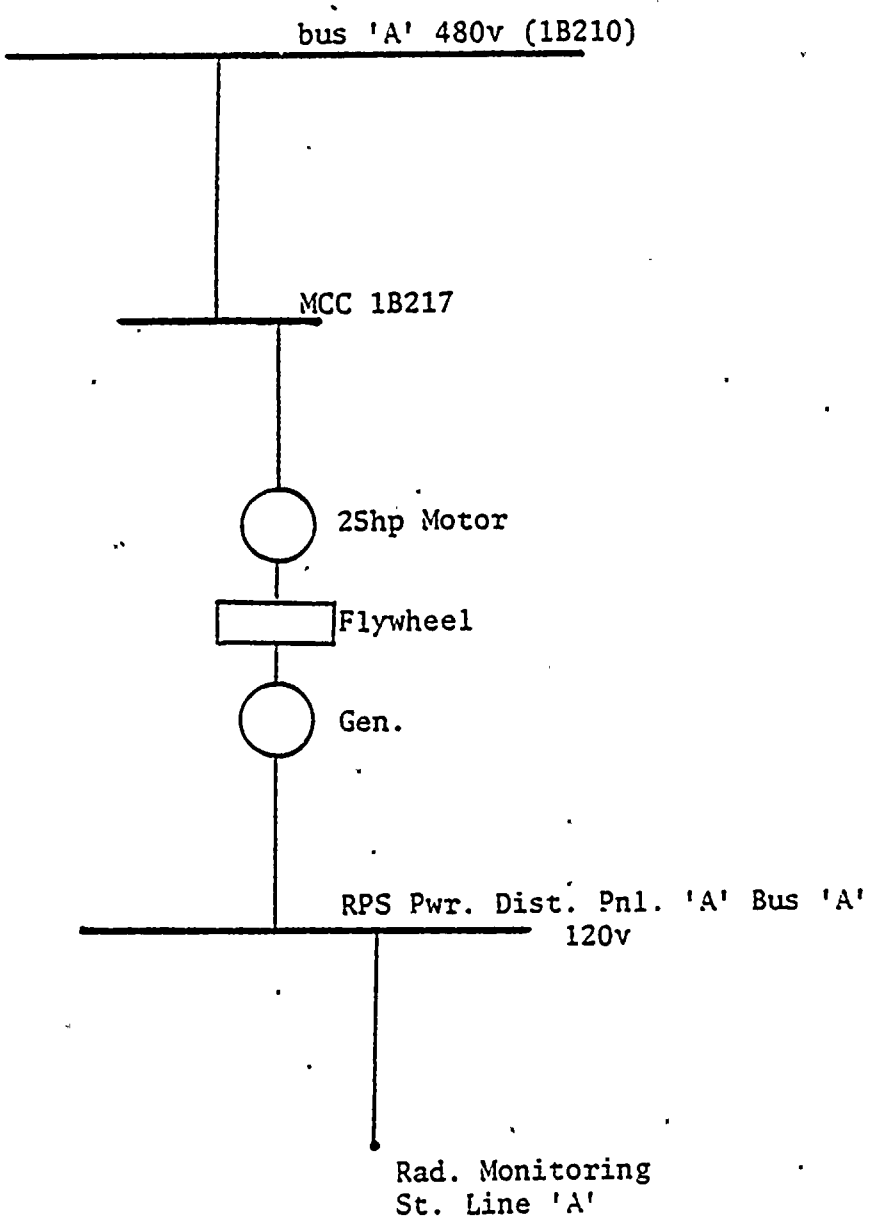
CONTROL SYSTEM IDENTIFICATION DIAGRAM (CSID)



* COMMON SENSORS

FIGURE 2

FIGURE 3 - Cascading Power Supply



SIMPLIFIED COMMONALITY DIAGRAM

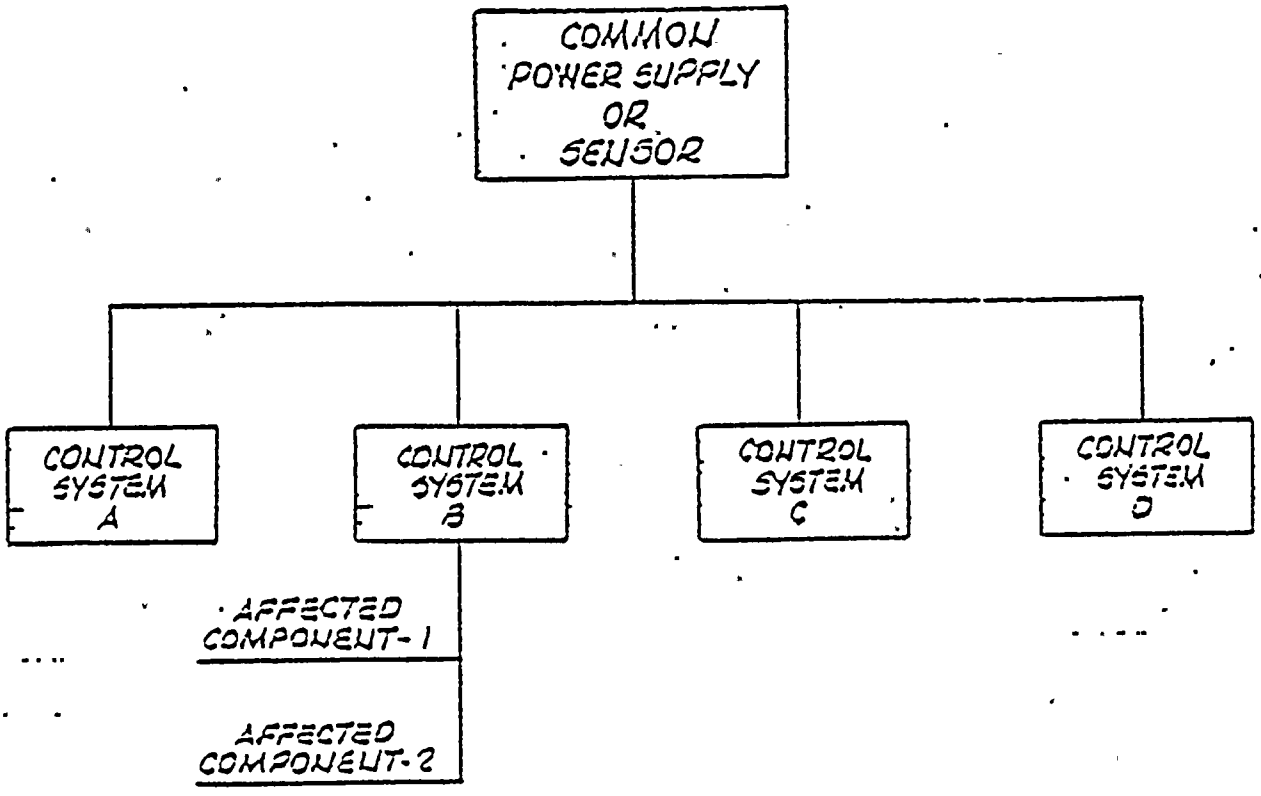


FIGURE 4

FIGURE 5

Facility:
Docket:

FAILURE MODES AND EFFECTS ANALYSIS

Sheet _____ of _____

Common Power Supply or Sensor: _____ CSID: _____

Control System Affected: _____ CD: _____

Job No. _____
Prepared by: _____
Date: _____ Rev. _____
Checked by: _____ Date: _____
Approved by: _____ Date: _____

Component Name and Number	Failure Mode	Symptoms and Local Effects Including Dependent Failures	System Inherent Compensating Provision	Summary: Effect Upon Control System	Summary: Effect Upon Plant Performance

FIGUR

Plant Conditions - Power Supply or Sensor Failure/Malfunction	Plant Response - Chapter 15 Analysis

FIGURE 7

Plant Conditions - Power Supply or Sensor Failure/Malfunction	Operator Response	Safety System Response Per FSAR

FIGURE

Plant Conditions Not Covered by Chapter 15 Analysis	Recommendation

FIGURE 9

PROJECT INSTRUCTIONS CHANGE NOTICE LOG

PROJECT:

CLIENT: PROJECT INSTRUCTION NO.:

JOB NO.: REVISION NO.:

PICN #	DATE	SUBJECT AND/OR DESCRIPTION	STATUS

FIGURE 10

eds nuclear

FILE: _____

COPY:

PROJECT INSTRUCTION CHANGE NOTICE

PICN No. _____

PROJECT:

CLIENT: PROJECT INSTRUCTION NO.:

JOB NO.: REVISION NO.:

Prepared By: _____ Date _____

Approved By: _____ Date _____

Concurrence By: _____ Date _____

APPENDIX B

CSID PREPARATION

Using the format shown in Figure 2, complete the CSID as follows:

1. Enter the plant operating mode. For the purposes of this project, there are four modes that will be analyzed. A CSID will be prepared for each mode.

2. Enter the plant safety functions required to support each plant operating mode.

3. Enter the control systems required to support each of the respective safety functions. Note that a control system may appear more than once on each CSID depending upon the number of safety functions it supports.

   a, Annotation of control system relationship to each safety function should be located adjacent to the control system box.

4. Enter the power supplies and/or sensors associated with each control system as shown in Figure 2.

   a. If components or sub-systems for each control system are required, enter them in separate boxes below the control system box. Then add the power supply and sensor information below the component or sub-system.

5. Any revision to the diagram should be noted on the diagram itself. Revisions should be handled in accordance with EDS QAP 3.2.

APPENDIX C

COMMONALITY DIAGRAM PREPARATION

Using the format shown in Figure 4, complete the Commonality Diagram as follows:

1. Enter the common power supply or sensor.

2. Enter the control systems supported by that common power supply or sensor.

   a. Annotate the control system entry to indicate which plant mode and safety function(s) are related to that control system.
   b. Enter control system components and/or sub-components below each control system entry where applicable.

3. Any revision to the diagram should be noted on the diagram itself. Revisions should be handled in accordance with EDS QAP 3.2.

APPENDIX D

FMEA PREPARATION

Using the format shown in Figure 5, complete the FMEA as follows:

1. Enter the title block information as per Figure 5. For system, enter control systems affected; for sub-system, enter the sub-system if applicable; for equipment, enter the power supply or sensor being analyzed.

2. Enter the title of the failed component or subsystem "Name" column.

3. Enter the type of failure in the "Failure Mode" column.

4. Enter the symptoms associated with the failure as it relates to the control systems affected in the "Symptoms and Local Effects" column.

5. Briefly describe the plant response that would compensate for this failure. Enter this in the "Inherent Compensating Provisions" column.

6. In the "Effect" columns describe in detail the effects upon the control systems and plant performance.

APPENDIX E

CHANGES TO THE PROJECT INSTRUCTIONS

Change to the Project Instructions are to be handled as follows:

1. Changes to the Project Instructions must be properly controlled. Minor changes shall be controlled by the Project Instruction Change Notice Log (Figure 9) and the Project Instruction Change Notice (PICN) (Figure 10). Major changes shall be controlled through revisions. Each new revision shall incorporate the PICN's issued since the last revision. Both PICN's and revisions to Project Instructions must be prepared, approved and concurred with the level of personnel commensurate with those that originally signed the Project Instructions.

2. The PICN Log in the Project QA File (with the Project Instructions) shall be the master copy and kept current by the Project Engineer. PICN's shall be distributed to all personnel that receive copies of the Project Instructions.