b:\wp\ Effective date: 00/00/00 Print: 12/4/95	0AAA00-AA-0000	Rev. 0 General	Page 1 of 16

CONFIGURATION CONTROL OF THE PROBABILISTIC SAFETY ASSESSMENT

Quality	Safety-Related	Usage: **DRAFT**	Effective Date: 10/??/95

C. R. Grantom	(name)	(name)	Nuclear Fuel & Analysis
PREPARER	TECHNICAL	USER	COGNIZANT ORGANIZATION

Table of Contents Page

DRAFT

1.0 Purpose and Scope

1.1 To define, disposition, implement, and maintain the data inputs to the Probabilistic Safety Assessment (PSA) risk models.

1.2 This procedure is applicable to all components and human actions contained in the STP PSA risk models.

2.0 Definitions

2.1 Event Tree: graphical representations of succession of individual events which in combination identifies all possible sequences of events leading to a predefined failure event of interest (e.g., core damage).

2.2 Fault Tree: graphical representation of a failure event of interest or "top event" which illustrates the logical relationship all of the subevents contributing to that event.

2.3 PSA Inputs: The set of data and information required by the PSA to accurately reflect the design, procedural processes, and human interaction of the facility to be analyzed and to quantify the probability and uncertainty of selected events.

2.4 Basic Event: the lowest level of subevents that contribute to a fault tree top event.

2.5 Initiating Event: any event that can cause a plant trip or otherwise initiate a sequence of events with a significant probability of core damage

2.6 Recovery Factor: a numerical value used to determine the likelihood that human actions (i.e.,operator actions) successfully "recover" a component or function that has initially failed.

2.7 Success Criteria: the minimum level of system or equipment performance that must be achieved in order to satisfy a selected function of interest.

2.8 PSA Applications: analyses performed using the results of the PSA. These analyses are generally performed to support a specific activity (e.g., 50.59 review) or program (technical specification optimization/relaxation). A list of active applications is maintained by Risk and Reliability Analysis. Active applications support current STP operations.

3.0 References

3.1 STP Level 1 PSA with External Events (L1PSA), ST-HL-HL-???? dated ??????.

3.2 STP Level 2 PSA and Individual Plant Examination (L2PSA/IPE).

4.0 Responsibilities

4.1 Supervisor, Risk and Reliability Analysis ensures that requirements of this procedure are effectively implemented and identifies required PSA information contained in Addendum 1.

4.2 Station Management is responsible for providing the information described in Addendum 1 as identified by the Supervisor, Risk and Reliability Analysis.

5.0 Requirements

5.1 Appropriate Department Managers shall forward the identified information in Addendum 1 to the Supervisor, Risk and Reliability Analysis.

5.2 Risk & Reliability Analysis shall develop and maintain Event Tree and PSA System Notebooks containing the information in Addendum 2, as applicable.

5.3 The Event Tree/System Notebooks are approved by the Supervisor, Risk and Reliability Analysis.

5.4 On an 18 month cycle basis, the notebooks will be updated to reflect changes resulting from the data collected per Addendum 1 to this procedure, as applicable.

5.5 The changes are reviewed and incorporated into the PSA models as appropriate, as defined in Addendum 3 or other Desktop Instructions.

5.6 Once updated, the PSA is requantified, evaluated, and approved for use by the Risk & Reliability Analysis (RRA) group. Evaluation consists of reviewing the current results against the previous results and changes in input. PSA Risk Ranking (0PGP03-XX-0000) may be used to assist in the evaluation.

5.7 PSA applications will be updated and distributed to customer organizations.

6.0 Documentation

6.1 A PSA Update Report will be generated by RRA at least on an 18 month cycle basis describing changes and documenting the data the update was approved for use.

6.2 PSA System Notebooks

6.3 PSA Event Tree Notebooks

6.4 PSA Plant Specific Data Analysis

7.0 Support Documents

7.1 Addendum 1 PSA Input Data

7.2 Addendum 2 PSA Notebook Contents

7.3 Addendum 3 Plant Change Screening & Flow Chart

7.4 Addendum 4 Notebook Update Methodology & Flow Chart

ADDENDUM 1 - PSA INPUT DATA

The data listed below is necessary only for systems and components within the scope of the PSA program or as defined in the PSA system and event tree notebooks.

Operations & Maintenance Data

- Failure/success data for PSA components (Plant Specific Data);
  - Equipment history
  - Number of equipment demands
  - Corrective Action program data
  - Control Room Logs
  - Operability Tracking
  - Condition Reports

- Actual planned and unplanned maintenance frequencies/durations for PSA components
  - Work Control information
  - Scheduling data and information
  - Equipment Clearance Order (ECO) data
  - Control Room Logs
  - Operability Tracking

- Actual testing frequencies/durations for PSA components
  - Scheduling data and information
  - Equipment Clearance Order (ECO) data
  - Control Room Logs

- Occurrences of initiating events
  - Condition Reports
  - SOERs

- Significant industry events
  - INPO Significant Operating Event Reports
  - NRC Information (e.g., Information Notices, Generic Letters)
  - Nuclear Network

- Technical Specifications

Engineering & Design Data

- Design Related Information
  - Updated Final Safety Analysis Report
  - Safety Evaluation Report
  - Design Basis Documents
  - Design drawings (P&IDs, Elementary Diagrams, Single Line Diagrams, Logic Drawings, etc.)
  - Design change information

- Thermohydraulic analyses and other selected Engineering Analyses;

Procedural Data

- Selected procedures and revision notification
  - Plant Surveillance Procedures (testing alignments)
  - Plant Maintenance Procedures (maintenance alignments)
  - Plant Engineering Procedures (maintenance alignments)
  - Plant Operating Procedures 02 Series (normal alignments)
  - Plant Operating Procedures 04 Series (abnormal alignments and conditions)
  - Plant Operating Procedures 05 Series (emergency operations)

- Other pertinent data (e.g., time supplemental purge valves are open, PORV block valves are closed)

ADDENDUM 2 - PSA NOTEBOOK CONTENTS

Event Tree Notebooks

- *Introduction* - describes event tree purpose and scope;
- *Assumptions/References* - lists assumptions and references from which they are derived;
- *Event Sequence Diagram* - (Front-line System Event Trees only) outlines equipment and operator actions required to mitigate/prevent a core damage event;
- *Event Sequence Block Descriptions* - (Front-line System Event Trees only) describes functional blocks contained in the event sequence diagrams;
- *Event Tree* - outlines succession of individual events which identify all possible sequences of events leading to a predefined failure event (e.g., core damage);
- *Fault Tree* - outlines top events which illustrate the logical relationship of the events leading to a particular event;
- *Macros* - defines split fraction logic rules used to link event trees;
- *Event Tree Top Event Descriptions* - defines systems, equipment, and operator actions included in the event tree structure;
- *Event Tree Binning Rules* - defines logic rules to group event tree sequences into common impacts for linking the next stage of event trees; and
- *Split Fraction Rules* - describes logic rules used to determine which split fractions should be assigned to a unique point in the event tree.

System Notebooks

- *Introduction* - describes fault tree purpose and scope;
- *System Function* - describes the process or purpose of the system;
- *Top Event Definitions* - defines the events for which system analysis provides quantification information;
- *System Success Criteria* - defines the minimum level of performance that will result in the system successfully performing its intended safety function as required by the event trees;
- *Support Systems* - defines systems and equipment which are required to successfully perform their function so that the analyzed system is capable of performing its intended safety function;
- *Systems Supported* - defines systems and equipment which depend on the analyzed system to perform its function so that they can perform their intended safety functions;
- *System Operations and Special Features* - defines pertinent information for normal operations and other characteristics which impact the analysis;
- *Potential for Initiating Event* - provides screening for the systems ability to cause an initiating event (e.g., reactor trip, turbine-generator trip);
- *Technical Specification Requirements* - provides information for success criteria and frequency of testing alignments;
- *Plant Procedures* - lists procedures used to define system alignments;
- *Assumptions* - lists items necessary to document areas not analyzed in part or in whole;

- *System Boundary* - defines the limit of the analysis relative to a physical of programmatic boundary;
- *Event Trees and Event Tree Split Fractions* - lists cross-references of the analyzed system to the associated event trees and split fractions;
- *Basic Event Cross Reference* - translates fault tree basic events to equipment descriptions and identification numbers;
- *Common Cause Modeling* - describes modeled common cause groups;
- *Maintenance Alignments* - describes the system configuration (including frequency and duration) when certain maintenance or testing activities are performed;
- *Recovery Factors Based on System Split Fractions* - lists operator actions necessary to restore the system or functions following failure of the analyzed system;
- *Modeling Notes* - provides other information relative to the system analysis;
- *Fault Tree* - outlines the graphical fault tree; and
- *References* - documents materials used in the system analysis.

INITIAL SCREENING CRITERIA

1. Is the change associated with a system modeled in the PSA?

   Yes____ No____

2. If yes, is it associated with a component modeled in the PSA?

   Yes____ No____

3. Could the change affect a system or event sequence modeled in the PSA?

   Yes____ No____

If any answer to the above questions is "Yes" then proceed to "PSA CHANGE EVALUATION"

If any answer was "No", then complete signature block and file in applicable System or Event Tree Notebook.

_____	_____	_____
Name (print)	Signature	Date

PSA CHANGE EVALUATION:

1. Does the change affect the items or attributes listed in Addendum 2? Yes____ No____

   1a) If "No," then document results.

   1b) If "Yes," then proceed to Question 2 below.

2. Does the change require a revision to the PSA Risk Model? Yes____ No____

   2a) If "No," then document results.

   2b) If "Yes," then proceed to Question 3 below.

3. Does the change require immediate update? Yes____ No____

   3a) If "No," then place change in "Pending PSA Changes" Notebook for next periodic PSA update.

   3b) If "Yes," then proceed to Question 4 below.

4. Does the change require requantification of the PSA model(s)? Yes____ No____

   4a) If "No," then place change in "Pending PSA Changes" Notebook for next periodic PSA update.

   4b) If "Yes," then update, requantify, and document PSA risk model change.

_____	_____	_____
Name (print)	Signature	Date

PLANT CHANGE SCREENING FLOW CHART

ADDENDUM 4
NOTEBOOK UPDATE METHODOLOGY & FLOW CHART

PSA NOTEBOOK UPDATE METHODOLOGY

Step 1 - Gather References
Review the reference list contained in the Event Tree or System Notebook from the most recent system package and gather the latest revision to the referenced documents. Some references may not be listed in the system package and must be located in the library. Based on the gathered references, update the system package reference list.

Step 2 - Highlight Drawings
[This step is only applicable to System Notebooks.] Using the Fault Tree(s), highlight the applicable drawings (i.e., P&IDs, Logic Diagrams, Elementaries, etc.) for the modeled components in order to verify system components with the PSA model.

Step 3 - Become Familiar with the System
For System Notebooks: Use the referenced drawings, procedures, and applicable UFSAR and DBD sections to verify the operation of the system and any special features related to the PSA model. Also, review the RISKMAN system notebook(s) for the system top event(s) to verify the PSA modeling of the system.
For Event Tree Notebooks: Verify that event tree top events are consistent with system level fault tree top events.

Step 4 - Update System Function Section
Review and, if required, update the System Function section by briefly describing the system and how the function(s) relate to the PSA.

Step 5 - Update System Operations and Special Features
Review, and if required, update the System Operations and Special Features section by describing the design basis of the system and defining any deviation from the design basis that was modeled in the PSA.

Step 6 - Identify System Boundary
Based on the design drawings and the system model, identify the analyzed boundary of the system. The analyzed boundary is defined as the system components analyzed in the PSA.

Step 7 - Review the Basic Event Cross-Reference List
Compare the Basic Event Cross-Reference List to the Fault Tree(s) to ensure that the correct components and failure modes are listed. Modify the Basic Event Cross-Reference if necessary.

ADDENDUM 4
NOTEBOOK UPDATE METHODOLOGY & FLOW CHART

Step 8 - Identify Support and Supported Systems
Identify support and supported systems, as applicable, and define the analyzed boundary conditions. Support systems are those systems upon which the subject system relies upon for effective operation. Supported systems are those systems that rely on operation of the subject system for effective operation. The analyzed boundary conditions are the states of the support systems for which the subject system is analyzed.

Step 9 - Review Modeling Assumptions
Review, and if required, update PSA modeling assumptions.

Step 10 - Identify Any Potential Initiating Events
Identify the potential for any initiating events (e.g., LOCA, Transients, etc.) based on the system configuration.

Step 11 - Update Top Event Definitions
Based on the PSA model and the system description, review the top event definitions and update, if necessary.

Step 12 - Verify System Success Criteria
Verify the system success criteria based on the UFSAR, Technical Specifications, DBDs, or procedures. The system success criteria are the minimum system operating requirements to satisfy the top event.

Step 13 - Update the System Technical Specification Requirements
Update the system Technical Specifications requirements by obtaining a copy of the current applicable Technical Specifications section(s).

Step 14 - Document Plant Procedures Related to Systen.
For Operations, Maintenance and Engineering procedures, document those procedures Related to the System, noting any special alignments and/or testing configurations required by the procedure. This section should include any additional testing and test frequencies specified by the Technical Specifications. Document specific procedural steps that provide key modeling assumptions, operational features, system alignments or component actuations.

ADDENDUM 4
NOTEBOOK UPDATE METHODOLOGY & FLOW CHART

Step 15 - Document System Maintenance Alignments
Based on station procedures and the RISKMAN system report, document the system maintenance alignments, providing specific documentation as to the composition of each alignment and the procedure steps where the alignments were identified. For example, does an alignment include a human error term for failure to return to normal alignment or is it simply comprised of unavailability due to maintenance?

Step 16 - Identify Event Trees and Split Fractions
Identify the event trees in which the System Level Fault Tree top events are questioned and document descriptions of the event tree split fractions based on the RISKMAN system notebook.

Step 17 - Document Common Cause Modeling Methodology
Document the System Common Cause modeling scope as appropriate. Define common cause groups and provide information relative to why certain components are not included in Common Cause models.

Step 18 - Identify System Recovery Split Fractions
Identify and describe any system split fractions used in the operator recovery analyses.

Step 19 - Update the Modeling Notes
Review and, if required, update the Modeling Notes section by providing a brief overview of the model.

Step 20 - Update the Fault Tree Description(s)
Briefly describe the fault tree(s) included in the system package.

Step 21 - Any Potential Modeling Changes?
Determine if any of the above changes will potentially affect the system model.

Step 21a - Document Potential Modeling Changes
Document any potential changes to the model arising as the result of the system package update.

Step 22 - Any Open Items?
Determine if the system package contains any outstanding issues which cannot be resolved without further guidance.

ADDENDUM 4
NOTEBOOK UPDATE METHODOLOGY & FLOW CHART

Step 22a - Document Open Items
Document and provide status for the open items.

Step 23 - Submit the Package for Review
Submit the system package for review to the PSA project team.

Step 24 - Resolve Comments
Resolve any resulting comments on the package.

Step 25 - Any Changes to the Model?
Identify if any of the potential PSA changes will, in fact, change the model.

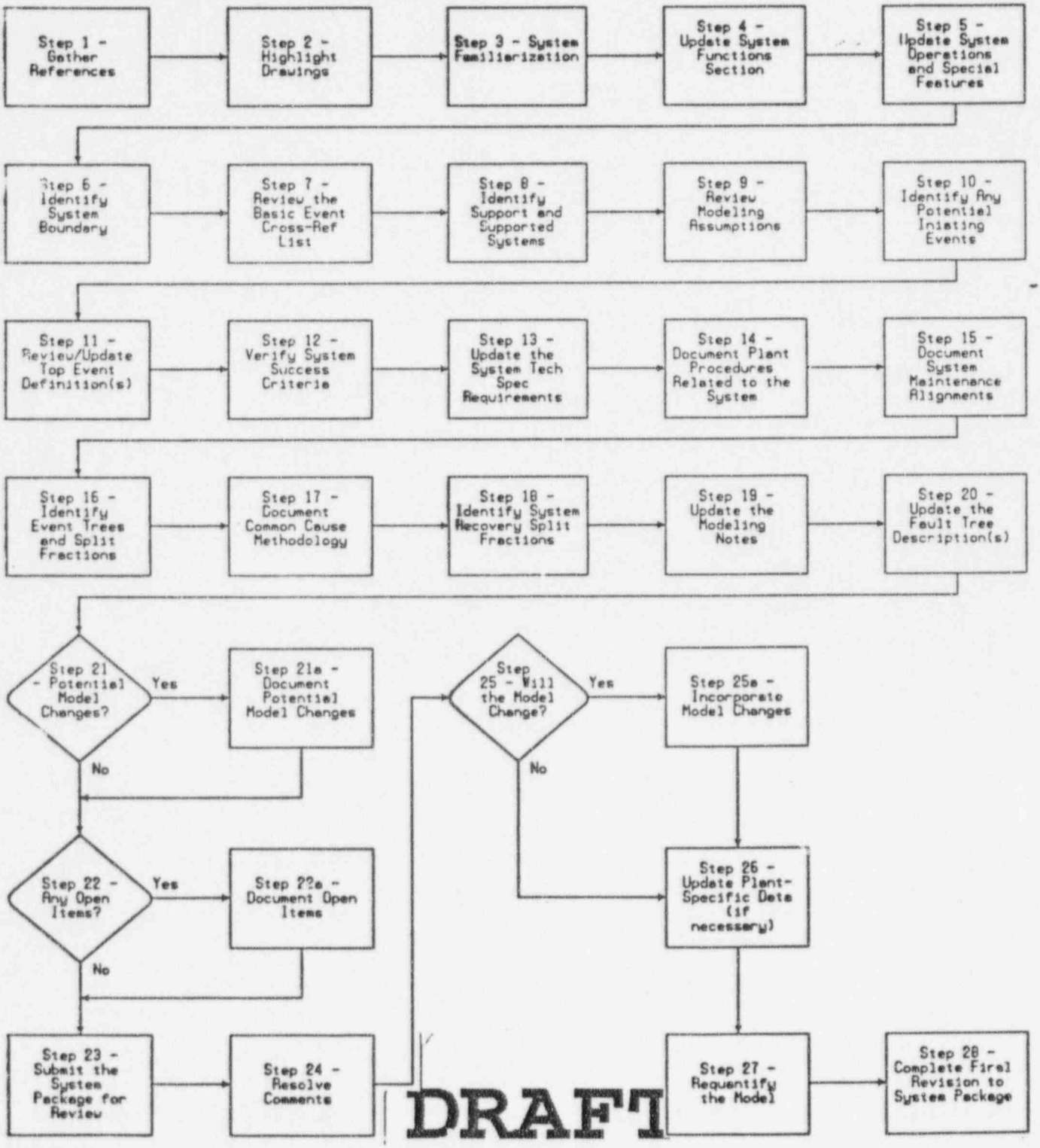
Step 25a - Incorporate Model Changes
Incorporate any final model changes, including fault tree changes, rule modifications, maintenance alignment revisions, etc.

Step 25b - Requantify the Model
Requantify the model for the incorporated model changes.

Step 26 - Complete the Final Revision
Complete the final revision to the package based on the changes to the model and/or resolution of comments.

ADDENDUM 4
NOTEBOOK UPDATE METHODOLOGY & FLOW CHART

NOTEBOOK UPDATE FLOW CHART



DRAFT

h:\wp\ Effective Date: 00/00/00 Print: December 4, 1995	0AAA00-AA-0000	Rev. 0 General	Page 1 of 6

PROBABILISTIC SAFETY ASSESSMENT RISK RANKING

Quality	Safety-Related	Usage: **DRAFT**	Effective Date: 10/??/95

C. R. Grantom	(name)	(name)	Nuclear Fuel & Analysis
PREPARER	TECHNICAL	USER	COGNIZANT ORGANIZATION

Table of Contents Page

1.0 Purpose and Scope

Describe the methods and criteria used to rank the risk significance of systems, components, and operator actions within the scope of the PSA. This procedure is applicable to those items contained in the STP risk models.

2.0 Definitions

2.1 Risk Ranking: the process by which systems, structures, and components within the scope of the PSA analysis are grouped based on their risk significance.

2.2 Importance Measures: standard calculations which quantify the significance of systems, structures, and components within the scope of the PSA analyses.

2.3 Fussell-Vesely: an importance measure which is defined as the ratio of the difference of the core damage frequency (or other figure of merit) with the component failed from the core damage frequency with the component successful over the average core damage frequency.

2.4 Risk Achievement Worth: an importance measure which is defined as the ratio of the core damage frequency (or other figure of merit) given the component is failed to the average core damage frequency.

2.5 Common Cause: a portion of the system analysis that evaluates components to determine their vulnerability to multiple component failures due to a common, shared event and not a dependent event.

2.6 Risk Reduction Worth: an importance measure which is defined as the ratio of the core damage frequency (or other figure of merit) given the component is successful to the average core damage frequency.

3.0 References

3.1 South Texas Project Level 1 Probabilistic Safety Analysis

3.2 South Texas Project Level 2 Probabilistic Safety Analysis and Individual Plant Examination

3.3 EPRI PSA Applications Guide, TR-105396, August 1995

4.0 Responsibilities

4.1 Supervisor, Risk and Reliability Analysis ensures that the requirements of this procedure are effectively implemented.

4.2 Expert Panel is responsible for approving the risk ranking criteria.

5.0 Requirements

5.1 PSA inputs shall be defined and incorporated in the PSA Configuration Control Procedure (0aaann-aa-0000).

5.2 The PSA risk models shall be quantified and sensitivity studies performed as described in Addendum 1.

5.3 The quantification results shall be compiled to reflect key importance measures associated with, at a minimum, core damage frequency and large early release frequency.

5.4 The contribution of the systems, equipment, operator actions, and initiating events shall be listed in order of their importance measures.

5.5 Thresholds defining high, medium, and low risk significance for average core damage frequency and average large early release frequency shall be developed.

5.6 Technical bases for establishing the threshold values shall be documented.

5.7 On a periodic basis, as established in "Configuration Control of the PSA" (0aaa00-aa0000), the risk ranking of components shall be be generated, reviewed, approved, and submitted to the Expert Panel/Expert Panel Working Groups.

6.0 Documentation

6.1 A risk ranking report will be periodically issued concurrent with plant specific updates.

7.0 Support Documents

Addendum 1 Risk Ranking Process
Addendum 2 Risk Significance Thresholds

ADDENDUM 1

RISK RANKING PROCESS

RISK RANKING CRITERIA

Risk Ranking Tasks:

Quantify all risk models based on the average figures of merit (i.e., core damage frequency, large early release). Perform top event importance, split fraction importance, and basic event importance quantifications with all standard importance measures.
Purpose: Average quantification establishes level for overall risk ranking and level of plant performance.

Quantify all risk models based on the removal of all maintenance unavailability contributions. Perform top event importance, split fraction importance, and basic event importance quantifications with all standard importance measures.
Purpose: Quantifies optimum level of defense-in-depth.

Quantify all risk models based on the removal of all operator recovery actions. Perform top event importance, split fraction importance, and basic event importance quantifications with all standard importance measures.
Purpose: Provides risk ranking with primary emphasis on equipment availability and reliability.

Quantify all risk models based on the removal of all common cause contributions. Perform top event importance, split fraction importance, and basic event importance quantifications with all standard importance measures.
Purpose: Provides focus of risk ranking based equipment combinations outside the scope of common cause failures.

Quantify selected risk models and vary failure rates of common equipment categorized as low risk. Selection should based on active components that appear in a majority of system level analyses such as relays, check valves, motor operated valves, etc.
Purpose: To determine if non-linear impacts to key figures of merit can occur.

Compare the risk rankings from the above quantifications and note variance in importance measures for like and similar components.

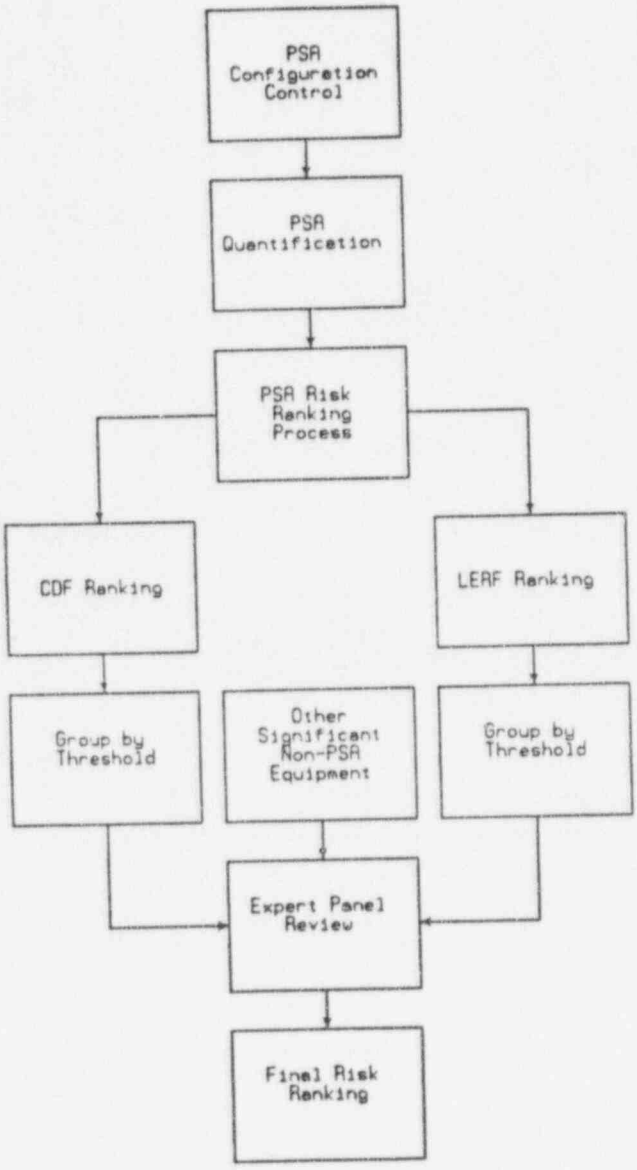
Identify boundaries between levels of importance (See Addendum 2 for the technical basis for risk significance thresholds).

Classify equipment based on the above results and document for Expert Panel.

ADDENDUM 1

RISK RANKING PROCESS

RISK RANKING FLOW CHART



ADDENDUM 1

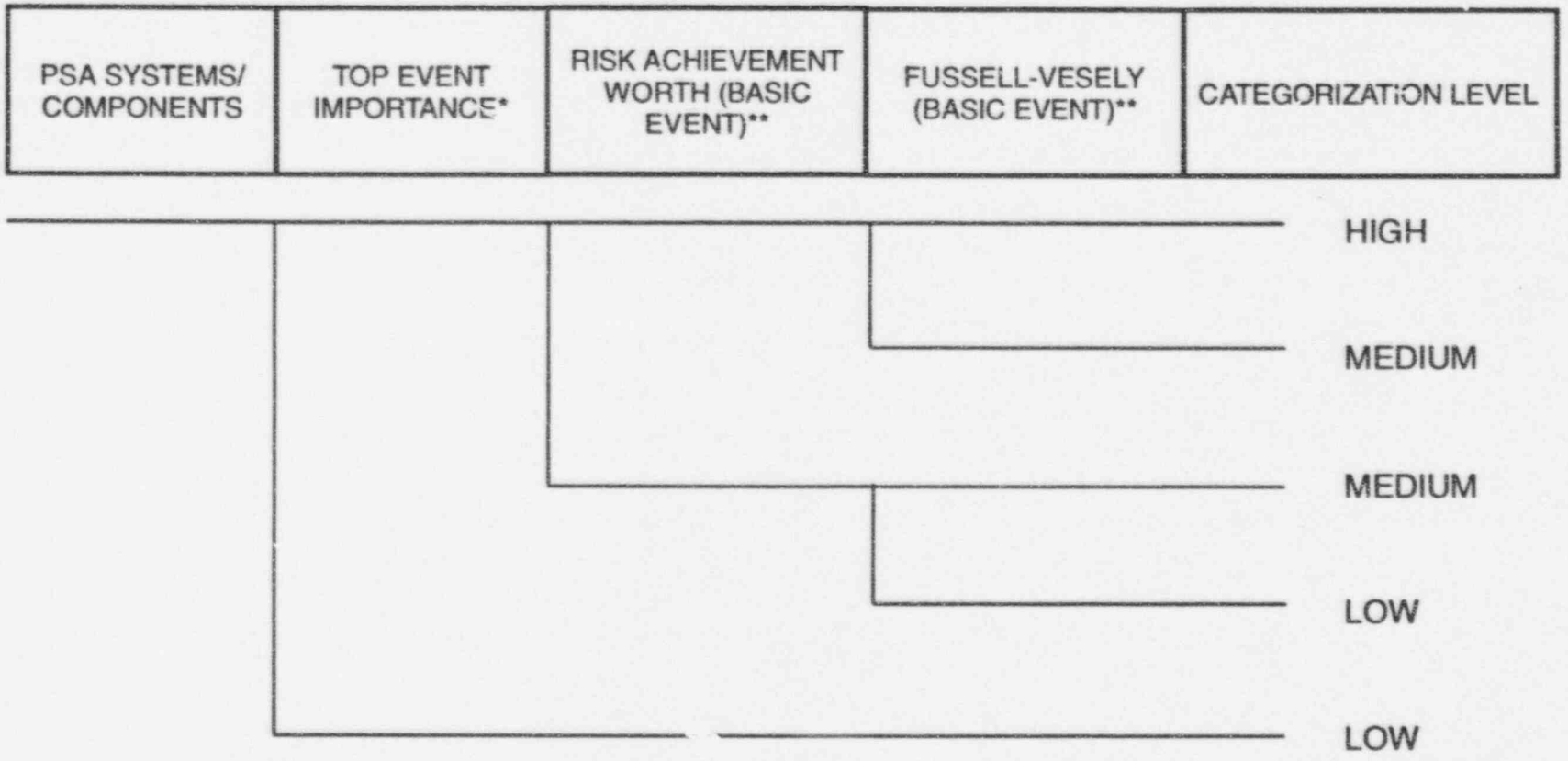
RISK RANKING PROCESS

The basis for the risk significance thresholds is as follows:

- For the low category, top event importance is used as a first filter to segregrate systems and components whose cumulative contributions are less than a prescribed value. The prescribed threshold values are obtained from Figures 4-1 and 4-2 of Reference 3.3 which is based on the current values of core damage frequency (CDF) and large, early release frequency (LERF).

- By using top event importance the combined effects of components which comprise the scope of the top event are quantified. If the top event importance is less than the specified threshold by Reference 3.3, then a high degree of confidence is obtained to conclude that none of the components within the scope of the top event have any risk significance.

RISK SIGNIFICANCE DECISION TREE



* - From PSA Applications Guide, Figure 4-1.

** - From PSA Applications Guide, Figure 4-2.