

h:\wp\h Effective date: 00/00/00 Print: 12/4/95	0PGP02-ZA-XXXX	Rev. 0 General	Page 1 of 12
PROBABILISTIC SAFETY ASSESSMENT PROGRAM			
Quality	Safety-Related	Usage: DRAFT	Effective Date: 1/02/96

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

<u>Table of Contents</u>	<u>Page</u>
1.0 Purpose and Scope	2
2.0 Definitions	2
2.1 Configuration Control	2
2.2 Software Control	2
2.3 Application Control	2
3.0 References	2
4.0 Responsibilities	3
5.0 Requirements	3
5.1 Configuration Control of the PSA	3
5.1.1 Scope of Analyses	3
5.1.2 Risk Models and Documentation	3
5.1.2 Data Analysis - Scope and Overview	6
5.1.3 PSA Methodology	7
5.1.4 PSA Assumptions	7
5.2 PSA Software Control	7
5.2.1 Scope and Overview	7
5.2.2 Software Configuration Control	8
5.2.3 Software Development and Enhancement	8
5.3 PSA Application Control	8
6.0 Documentation	8
6.1 Selected Stand-Alone Reports	8
6.2 Periodic Reports	8

DRAFT

	0aaann-aa-0000	Rev. 0	Page 2 of 12
PROBABILISTIC SAFETY ASSESSMENT PROGRAM			

1.0 Purpose and Scope

To define the structure, functions, controls, and applications of the South Texas Project (STP) Probabilistic Safety Assessment (PSA) program. This procedure is applicable to structures, systems, components, and human actions within the scope of the PSA for all plant operating modes and configurations are applicable to this procedure. The PSA program includes the STP Level 1 PSA (Reference 1), the Level 2 PSA/IPE (Reference 2), updates to these models, and analyses performed using these models.

The control elements associated with the STP PSA program are:

- Configuration Control;
- Software Control; and
- Application Control.

These elements provide the necessary controls to establish risk-based analyses performed at STP and to ensure that they contain appropriate technical bases and are documented with respect to plant design, procedural processes, and plant performance. The relationship between these control elements is show in Figure 1.

2.0 Definitions

- 2.1 Configuration Control - activities necessary to identify, evaluate, and disposition changes or revisions to items containing PSA inputs.
- 2.2 Software Control - activities related to maintaining computer software configuration control.
- 2.3 Application Control - activities related to updating or revising risk-based evaluations or other risk-based deliverables within the scope of PSA models, as appropriate.

3.0 References

- 3.1 Level 1 PSA
- 3.2 Level 2 PSA/IPE
- 3.3 Fire PSA Update
- 3.4 Risk-Based Evaluation of Technical Specifications
- 3.5 PLG's Appendix B Software QA Program
- 3.6 ORAM Model Documentation.
- 3.7 STP Probabilistic Shutdown Safety Assessment

DRAFT

	0aaann-aa-0000	Rev. 0	Page 3 of 12
PROBABILISTIC SAFETY ASSESSMENT PROGRAM			

4.0 Responsibilities

Supervisor, Risk & Reliability Analysis assures that the requirements of this procedure are satisfied.

5.0 Requirements

5.1 Configuration Control of the PSA

5.1.1 Scope of Analyses

PSA configuration control is comprised of the following areas:

- Risk Models and Documentation;
- Data Analysis;
- Methodology; and
- Assumptions

The STP PSA Program provides plant specific risk analyses of the STP units. Date and time stamps are used to establish the ~~status~~ of plant design and processes at the time of any analysis applicable to the PSA Program. The date and time stamps provide traceability of the results of a PSA analysis to the plant configuration at the time the analysis was performed.

5.1.2 Risk Models and Documentation

Risk model documentation includes identification of references and other materials used to establish and model the response of the plant to various initiating events, operator actions, and recovery actions. Key components of risk model documentation include:

- Plant Models;
- System Models;
- Spatial Interactions Analysis; and
- System Success Criteria.

5.1.2.1 Plant Models

At the plant level, event trees are used to model the response of the plant to an initiating event (e.g., plant trip). Event trees include important

DRAFT

	0aaann-aa-0000	Rev. 0	Page 4 of 12
PROBABILISTIC SAFETY ASSESSMENT PROGRAM			

systems and operator actions necessary to prevent core damage. Quantification of event trees provides the likelihood of core damage given an initiating event. The STP PSA event trees and their relationships are shown in Figure 2. Event tree notebooks are maintained, and generally contain the following information:

- *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.

5.1.2.2 System Models

On a system level, analyses are used to quantify the availability/reliability of plant equipment important to safety. Top events are defined for each system or function in terms of that system's success criteria. Fault trees are used to develop cutsets which lead to failure of a top event. The generated cutsets are modified to account for common cause failures, test and maintenance alignments, and unique boundary conditions.

System notebooks are developed to document the system models and their associated fault trees. Systems with components modeled in the

DRAFT

	0aaann-aa-0000	Rev. 0	Page 5 of 12
PROBABILISTIC SAFETY ASSESSMENT PROGRAM			

PSA are shown in Figure 3 along with their respective system notebooks. The system notebooks generally contain the following information:

- *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 or 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;

DRAFT

	0aaaann-aa-0000	Rev. 0	Page 6 of 12
PROBABILISTIC SAFETY ASSESSMENT PROGRAM			

- *Fault Tree* - outlines the graphical fault tree; and
- *References* - documents materials used in the system analysis.

5.1.2.3 Spatial Interactions Analysis - Scope and Overview

Internal plant hazards (e.g., internal floods, plant fire, or seismic response) are highly dependent on the location of risk-significant equipment relative to the hazard. Due to this dependence on plant geometry, the identification and screening of scenarios caused by internal plant hazards is referred to as Spatial Interactions Analysis. To perform this analysis, the sources of hazards within the plant and the available hazard mitigative features are tabulated. Then, by starting with the hazard sources and taking the potential propagation paths and mitigative feature into account, environmental hazard scenarios are constructed for each location¹. Computerized methods are used to analyze this data and to determine the frequencies of the scenarios occurring. Finally, a list is generated of scenarios ranked by their contribution to the occurrence of various impact vectors². The STP spatial interactions analysis is documented in the Level 1 PSA (Reference 1), the Level 2 PSA/IPE (Reference 2), and in the Fire PSA update (Reference 3).

5.1.2.4 System Success Criteria

System success criteria are generally based on analyses performed to determine plant response to a UFSAR Chapter 15 accident (e.g., Large LOCA, with single failure assumed) or a scenario defined in the Fire Safe Shutdown Report. Any analyses which modify the system success criteria are documented in the success criteria section of each system notebook.

5.1.2 Data Analysis - Scope and Overview

Data used in the PSA consists of generic data and plant-specific data. The generic data used in the Level 1 STP PSA quantifications performed in 1988 and 1989 was provided by PLG. Inc. Since then, selected plant-specific data has been incorporated into the PSA. In 1993, a successful comprehensive effort was made to perform a full scope update of plant-specific failure data. Future updates are planned for each

¹ A "location" means a well-defined volume in the plant that does not overlap another location. In general, fire zones as defined in a Fire Hazards Analysis are a good starting point for locations used in Spatial Interaction Analysis.

² Impact vectors are combinations of system success/failure, initiating events, and event tree top events.

DRAFT

	0aaaann-aa-0000	Rev. 0	Page 7 of 12
PROBABILISTIC SAFETY ASSESSMENT PROGRAM			

Unit 1 refueling outage, and these updates will also be used as an input for Maintenance Rule (10CFR50.65) compliance. The types of data which can be updated include:

- equipment failure rates;
- human performance assumptions;
- initiating event frequencies (internal and external events);
- planned and unplanned maintenance frequencies;
- planned and unplanned maintenance durations;
- testing frequencies and durations;
- common cause failure rates; and
- other performance data (e.g., fraction of time supplemental purge valves are open; fraction of time PORV block valves are closed, etc.)

5.1.3 PSA Methodology

Probabilistic methods and techniques used in the original STP PSA are documented in the Level 1 PSA, the Level 2 PSA/IPE, and the Risk Based Evaluation of Technical Specifications (Reference 4). New PSA methodology will be incorporated on a case-by-case basis depending upon its applicability to STP.

5.1.4 PSA Assumptions

Assumptions made in the Level 1 PSA and Level 2 PSA/IPE range from those concerning construction of plant systems/equipment to those associated with plant transient and accident response. Documentation of assumptions made in the PSA are individually documented in the Level 1 PSA, Level 2 PSA/IPE, event tree notebooks, plant system notebooks, or other documents, as appropriate.

5.2 PSA Software Control

5.2.1 Scope and Overview

Only the software used to quantify and document quality risk-based calculations is included within the scope of this procedure.

The at-power (Mode 1) risk analysis performed at STP uses RISKMAN, a proprietary software program developed by PLG, Inc. A site license is maintained for RISKMAN in order to perform plant level event tree and system level fault tree quantifications.

DRAFT

	0aaaann-aa-0000	Rev. 0	Page 8 of 12
PROBABILISTIC SAFETY ASSESSMENT PROGRAM			

The probabilistic safe shutdown analysis (PSSA) at STP uses the EPRI code ORAM (Outage Risk Assessment Module). ORAM is used for PSA analyses when the STP units are in Modes 4, 5, 6, or defueled. Plant conditions during shutdown configurations are evaluated by ORAM using qualitative and quantitative analyses. Documentation of STP's PSSA models is contained in Reference 6. ORAM software control is provided by EPRI and Erin Engineering, Inc.

5.2.2 Software Configuration Control

Configuration control of RISKMAN and verification and validation (V&V) requirements are maintained by PLG, Inc., pursuant to 10CFR50, Appendix B. The STP PSA program takes credit for PLG's Appendix B program with respect to software configuration control and V&V (Reference 5). To ensure that RISKMAN properly performs risk-based calculations at STP, a test case with a known input and output is run to document the accurate installation and performance of RISKMAN on STP PC workstations. Performance of the test case is documented per QA document in the RISKMAN Software.

5.2.3 Software Development and Enhancement

STP is also a member of the RISKMAN Technology Group (RTG), which is a user group comprised of utilities and national laboratories who use RISKMAN. Further development and application of RISKMAN and RISKMAN code maintenance are directed by the RTG. By participating in the RTG, STP is involved in the identification and correction of software errors as well as other RISKMAN enhancements.

5.3 PSA Application Control

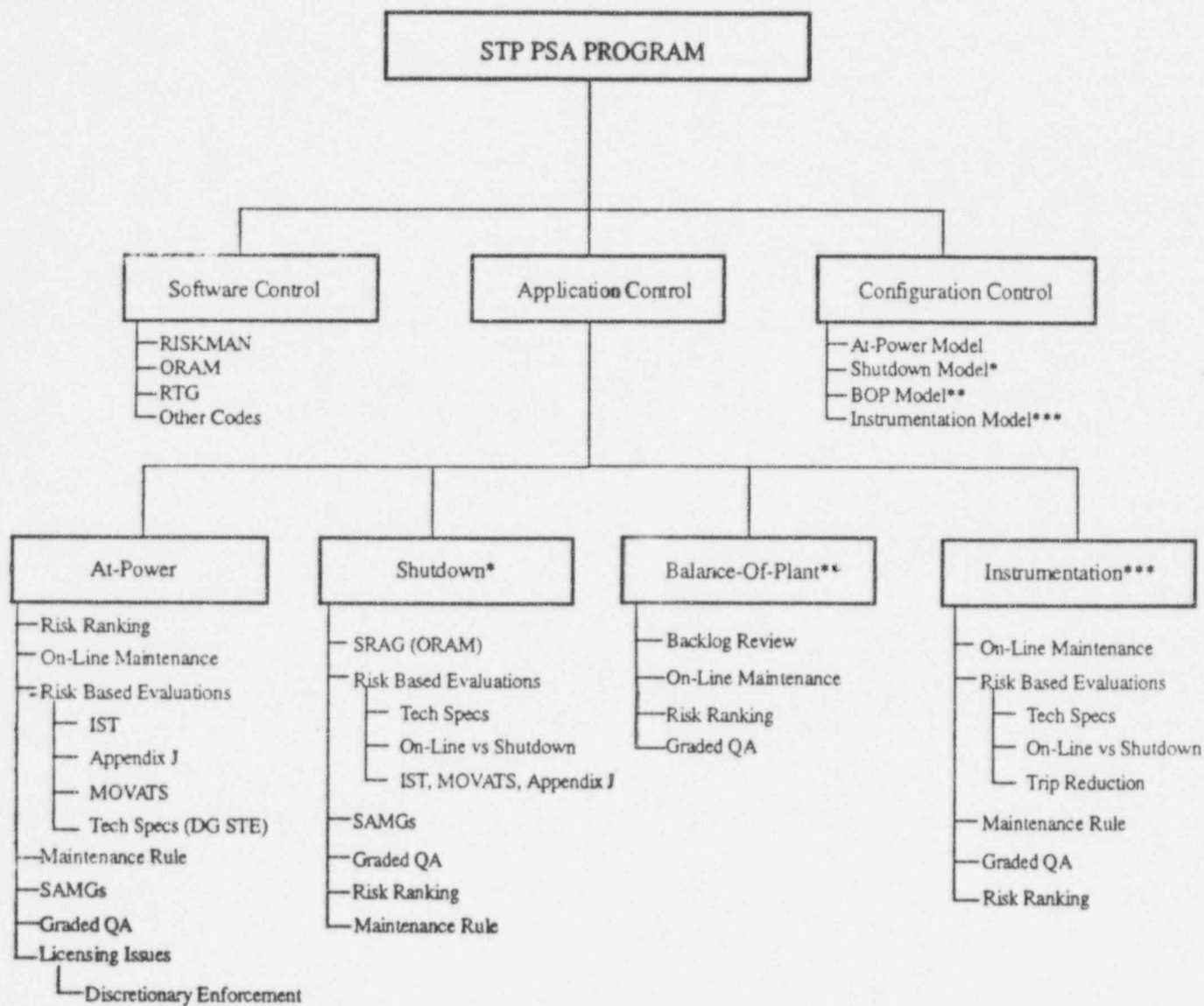
Control of PSA applications at STP is accomplished by ensuring that the PSA model and required changes used for the application are appropriate. The technical basis and changes required by the analysis are reviewed, approved, and documented. This provides adequate traceability and control.

6.0 Documentation

- 6.1 Selected Stand-Alone Reports or other risk based analyses, as required, are submitted to requesting organizations and to STP Records Management Services.
- 6.2 Periodic Reports updates to existing applications, as required, are submitted to client organizations and to STP Record Management Services.

DRAFT

FIGURE 1
PSA CONTROL ELEMENTS



* Presently Underway
 ** Part of Graded QA
 *** Business Plan Initiative

DRAFT

DRAFT

MLP, SEC. 3.1A PFE

3.1.1-3

REV. 0 (06-23-92)

STP PSA PLANT EVENT TREE MODEL

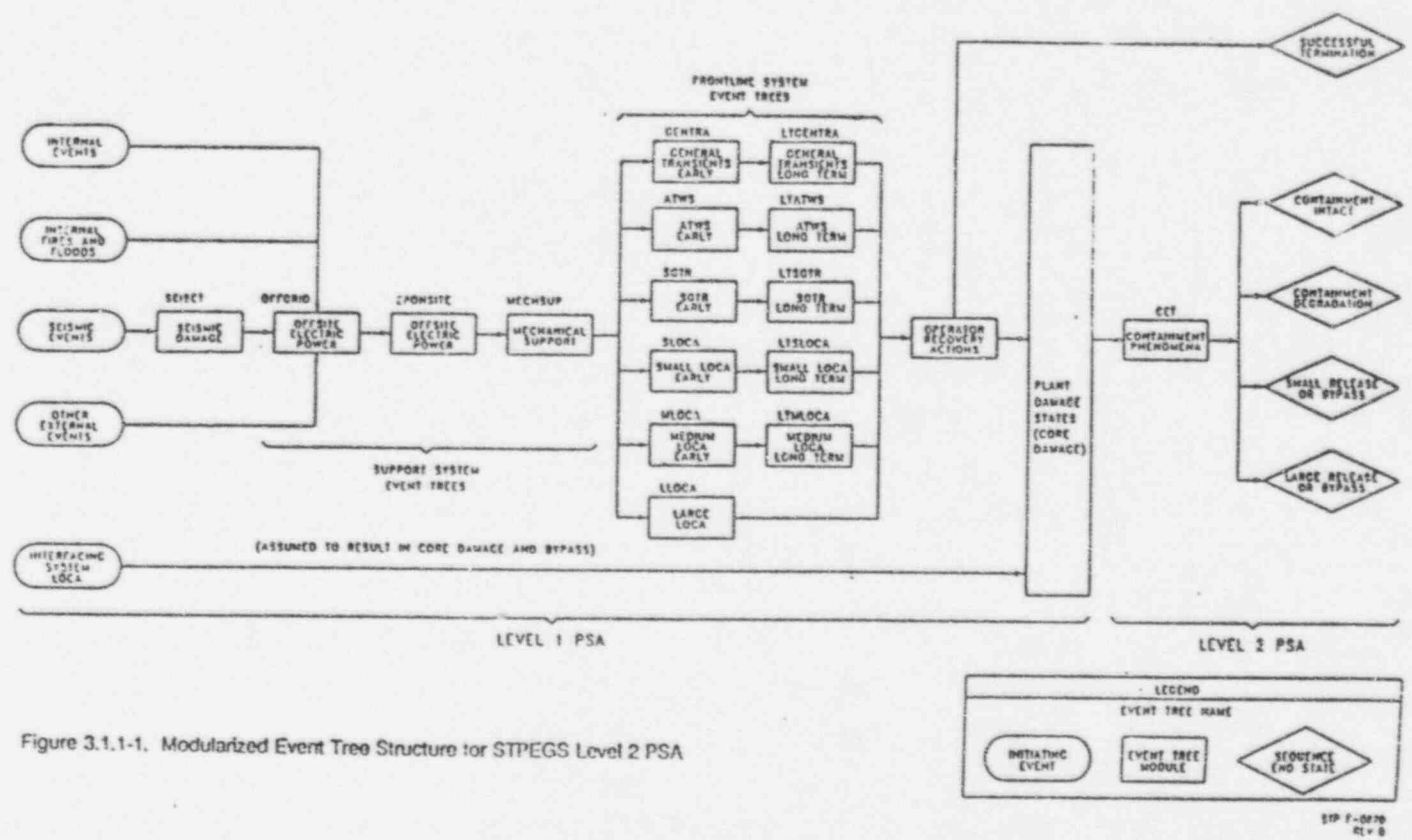


FIGURE 2
PSA EVENT TREES

**FIGURE 3
SYSTEMS MODELED IN THE PSA**

AC	Closed Loop Auxiliary Cooling Water	Select components modeled
AF	Auxiliary Feedwater System	Explicitly modeled
AM03	QDPS	Select components modeled
CC	Component Cooling Water	Explicitly modeled
CH	Essential Chilled Water System	Explicitly modeled
CS	Containment Spray	Explicitly modeled
CT	Condensate Storage & Transfer	Select components modeled
CV	Chemical Volume and Control System	Explicitly modeled
DB	Diesel Generator (BOP, TSC, & EOF)	Select components modeled
DC	250V DC Non-class 1E	Select components modeled
DG	Diesel Generator System	Explicitly modeled
DI	Standby Diesel Combustion Air Intake	Implicitly modeled in DG
DJ	125V DC Class 1E	Explicitly modeled
DO	Standby DG Fuel Oil Storage & Transfer	Implicitly modeled in DG
DX	Standby Diesel Generator Exhaust	Implicitly modeled in DG
ED	Radioactive Vents & Drains	Containment Isolation only
EH	Electro-Hydraulic Controls	Select components modeled
EW	Essential Cooling Water	Explicitly modeled
HC	HVAC - Containment Building	Explicitly modeled
HE	HVAC - Electrical Auxiliary Building	Explicitly modeled
HG	HVAC - Standby DG Bldg	Select components modeled
HM	HVAC - MAB	Select components modeled
HZ	HVAC - Miscellaneous	Select components modeled
IA	Instrument Air	Select components modeled
JW	Standby DG Jacket Water	Implicitly modeled in DG
LU	Standby DG Lube Oil	Implicitly modeled in DG
MS	Main Steam System	Explicitly modeled
PA	Standby Transformer	Explicitly modeled
PB	Main & Auxiliary Transformers	Explicitly modeled
PC	13.8 kV AC Auxiliary	Explicitly modeled
PE	480 V AC Non-class 1E Load Centers	Select components modeled
PF	480 V AC Non-class 1E	Select components modeled
PG	13.8 KV Emergency Power	Explicitly modeled
PK	4 kV AC Class 1E Power	Explicitly modeled
PL	480 V AC Class 1E Load Center	Explicitly modeled
PM	480 V AC Class 1E MCC & Distribution Panels	Explicitly modeled
RA	Radiation Monitoring	Containment Isolation only
RC	Reactor Coolant System	Explicitly modeled
RH	Residual Heat Removal System	Explicitly modeled

DRAFT

	0aaann-aa-0000	Rev. 0	Page 12 of 12
PROBABILISTIC SAFETY ASSESSMENT PROGRAM			

FIGURE 3
SYSTEMS MODELED IN THE PSA

SB	Steam Generator Blowdown	Select components modeled
SD	Standby DG Starting Air	Implicitly modeled in DG
SF	Engineered Safety Features Actuation	Explicitly modeled
SI	Safety Injection System	Explicitly modeled
SP	Solid State Protection System	Explicitly modeled
VA	120 V AC Class 1E Vital Power	Explicitly modeled
WL	Liquid Waste Processing	Containment Isolation only
XS	Switchyard	Select components modeled

DRAFT