



Westinghouse Electric Company
Nuclear Power Plants
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355
USA

U.S. Nuclear Regulatory Commission
ATTENTION: Document Control Desk
Washington, D.C. 20555

Direct tel: 412-374-6306
Direct fax: 412-374-5005
e-mail: sterdia@westinghouse.com

Your ref: Project Number 740
Our ref: DCP/NRC1862

April 13, 2007

Subject: AP1000 COL Standard Technical Report Submittal of APP-GW-GLR-102, Rev. 0

In support of Combined License application pre-application activities, Westinghouse is submitting Revision 0 of AP1000 Standard Combined License Technical Report Number 102. This report completes and documents, on a generic basis, probabilistic risk assessment activities required for COL Information Item 19.59.10-2 in the AP1000 Design Control Document. Changes to the Design Control Document identified in Technical Report 102 are intended to be incorporated into FSARs referencing the AP1000 design certification or incorporated into the design certification when Part 52 is revised to permit amendment of the design certification. This report is submitted as part of the NuStart Bellefonte COL Project (NRC Project Number 740). The information included in this report is generic and is expected to apply to all COL applications referencing the AP1000 Design Certification.

The purpose for submittal of this report was explained in a March 8, 2006 letter from NuStart to the U.S. Nuclear Regulatory Commission.

Pursuant to 10 CFR 50.30(b), APP-GW-GLR-102, Revision 0, "AP1000 Probabilistic Risk Assessment Update Report," Technical Report Number 102, is submitted as Enclosure 1 under the attached Oath of Affirmation.

It is expected that when the NRC review of Technical Report Number 102 is complete, COL Information Item 19.59.10-2 will be considered complete for COL applicants referencing the AP1000 Design Certification.

The AP1000 PRA will be available for NRC onsite review at the Westinghouse offices in Monroeville, Pennsylvania after April 30, 2007.

Questions or requests for additional information related to the content and preparation of this report should be directed to Westinghouse. Please send copies of such questions or requests to the prospective

applicants for combined licenses referencing the AP1000 Design Certification. A representative for each applicant is included on the cc: list of this letter.

Westinghouse requests the NRC to provide a schedule for review of this technical report within two weeks of its submittal.

Very truly yours,



A. Sterdis, Manager
Licensing and Customer Interface
Regulatory Affairs and Standardization

/Attachment

1. "Oath of Affirmation," dated April 13, 2007

/Enclosure

1. APP-GW-GLR-102, Revision 0, "AP1000 Probabilistic Risk Assessment Update Report," Technical Report Number 102, dated March 2007.

cc:	S. Bloom	-	U.S. NRC	1E	1A
	S. Coffin	-	U.S. NRC	1E	1A
	G. Curtis	-	TVA	1E	1A
	P. Grendys	-	Westinghouse	1E	1A
	P. Hastings	-	Duke Power	1E	1A
	C. Ionescu	-	Progress Energy	1E	1A
	D. Lindgren	-	Westinghouse	1E	1A
	A. Monroe	-	SCANA	1E	1A
	M. Moran	-	Florida Power & Light	1E	1A
	C. Pierce	-	Southern Company	1E	1A
	E. Schmiech	-	Westinghouse	1E	1A
	G. Zinke	-	NuStart/Entergy	1E	1A

ATTACHMENT 1

“Oath of Affirmation”

ATTACHMENT 1

UNITED STATES OF AMERICA
NUCLEAR REGULATORY COMMISSION

In the Matter of:)
NuStart Bellefonte COL Project)
NRC Project Number 740)

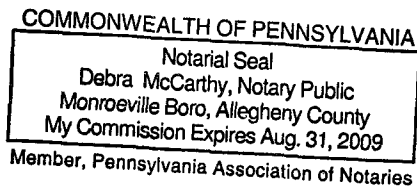
APPLICATION FOR REVIEW OF
"AP1000 GENERAL COMBINED LICENSE INFORMATION"
FOR COL APPLICATION PRE-APPLICATION REVIEW

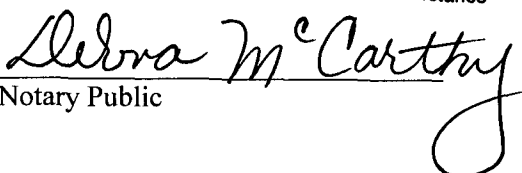
W. E. Cummins, being duly sworn, states that he is Vice President, Regulatory Affairs & Standardization, for Westinghouse Electric Company; that he is authorized on the part of said company to sign and file with the Nuclear Regulatory Commission this document; that all statements made and matters set forth therein are true and correct to the best of his knowledge, information and belief.



W. E. Cummins
Vice President
Regulatory Affairs & Standardization

Subscribed and sworn to
before me this 13th day
of April 2007.




Notary Public

ENCLOSURE 1

APP-GW-GLR-102, Revision 0

AP1000 Probabilistic Risk Assessment Update Report

Technical Report Number 102

AP1000 DOCUMENT COVER SHEET

TDC: _____ Permanent File: _____ APY _____
RFS#: _____ RFS ITEM #: _____

AP1000 DOCUMENT NO. APP-GW-GLR-102	REVISION NO. 0	Page 1 of 27	ASSIGNED TO WINTERS
---------------------------------------	-------------------	--------------	------------------------

ALTERNATE DOCUMENT NUMBER: TR-102

WORK BREAKDOWN #: GW

ORIGINATING ORGANIZATION: Westinghouse Electric Company

TITLE: AP1000 Probabilistic Risk Assessment Update Report

ATTACHMENTS: N/A	DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION: N/A
---------------------	--


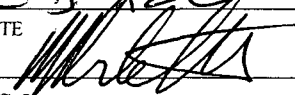
CALCULATION/ANALYSIS REFERENCE: N/A	
--	--

ELECTRONIC FILENAME APP-GW-GLR-102.doc	ELECTRONIC FILE FORMAT Microsoft Word	ELECTRONIC FILE DESCRIPTION AP1000 Probabilistic Risk Assessment Update Report
---	--	---

(C) WESTINGHOUSE ELECTRIC COMPANY LLC – 2007



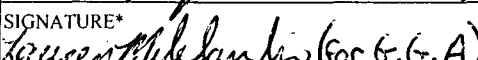
☒ WESTINGHOUSE CLASS 3 (NON PROPRIETARY)

Class 3 Documents being transmitted to the NRC require the following two review signatures in lieu of a Form 36.

LEGAL REVIEW Tom White E. Gillen	SIGNATURE/DATE  4-5-07
PATENT REVIEW Mike Corletti	SIGNATURE/DATE  4-5-07

☐ WESTINGHOUSE PROPRIETARY CLASS 2

This document is the property of and contains Proprietary Information owned by Westinghouse Electric Company LLC and/or its subcontractors and suppliers. It is transmitted to you in confidence and trust, and you agree to treat this document in strict accordance with the terms and conditions of the agreement under which it was provided to you.

ORIGINATOR D. T. McLaughlin	SIGNATURE/DATE  3/30/07	
REVIEWERS	SIGNATURE/DATE	
N/A		
VERIFIER R. G. Anderson	SIGNATURE/DATE  3/30/07	VERIFICATION METHOD Independent 3-Pass Review
API000 RESPONSIBLE MANAGER G. G. Ament	SIGNATURE*  (for G.G.A.)	APPROVAL DATE 3/30/07

* Approval of the responsible manager signifies that document is complete, all required reviews are complete, electronic file is attached and document is released for use.

AP1000 Standard Combined License Technical Report

AP1000 Probabilistic Risk Assessment Update Report

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

© 2007 Westinghouse Electric Company LLC
All Rights Reserved

1.0 INTRODUCTION

This technical report addresses AP1000 Design Control Document (DCD) (Reference 1) Combined Operating License (COL) Information Item 19.59.10-2 on page 19.59-37.

DCD Paragraph 19.59.10.5 Combined License Information 19.59.10-2 states:

“The Combined License applicant referencing the AP1000 certified design will review differences between the as-built plant and the design used as the basis for the AP1000 PRA and Table 19.59-18. If the effects of the differences are shown, by a screening analysis, to potentially result in a significant increase in core damage frequency or large release frequency, the PRA will be updated to reflect these differences”

This technical report is necessary to assist COL applicants close this COL information item with respect to updating the PRA to be consistent with the as-to-be-built plant design. The AP1000 PRA has been updated to include the most recent Instrumentation and Controls design information. Additionally, to facilitate future updates, the PRA software package was converted from the Westinghouse Proprietary WesSAGE software package, to the CAFTA software package, which is widely accepted as a capable PRA modeling software. COL applicants may now have the ability to use the updated PRA model, with the results, conclusions and insights from the AP1000 DCD, to provide a resolution to the COL item named above.

The AP1000 PRA is available for NRC onsite review at Westinghouse offices in Monroeville, Pennsylvania after April 30, 2007.

2.0 AP1000 PROBABILISTIC RISK ASSESSMENT SOFTWARE

The AP1000 PRA, as submitted as part of the AP1000 Design Certification Applications, was analyzed using the Westinghouse Proprietary software package, WesSAGE. This software package is capable of accurately and precisely performing probabilistic risk assessment. It is recognized that there are other industry PRA software packages with greater analysis capability.

WesSAGE was initially created to support Individual Plant Examination (IPE) development in the late 1980's and early 1990's. WesSAGE was developed to competently quantify a PRA model, using fault tree linking techniques with defined boundary conditions. As computer software and quantification technology advanced in other industry codes, it is appropriate to replace WesSAGE with CAFTA.

To improve ease of use, to take advantage of technological improvements in computer programming and to conform to the analytical techniques employed by other U.S. utilities, Westinghouse selected CAFTA for use on the AP1000 PRA.

CAFTA is similar to WesSAGE in that it utilizes the fault tree linking with boundary conditions approach. The CAFTA software package allows the AP1000 event trees to be created in CAFTA and converted to fault tree format; thus, maintaining the sequence structure of the AP1000 PRA model. CAFTA is an integrated software package, where the fault trees and database automatically interact with each other. CAFTA provides a function to perform sensitivity studies and calculate risk importance measures. CAFTA provides an automatic filter for the conversion of WesSAGE (GRAFTER) fault trees to CAFTA format with minimal human actions. As the introduction of human actions often contributes as an error precursor, heavy weight was placed

on the automatic conversion criterion. CAFTA is a software package available to EPRI members.

3.0 AP1000 INSTRUMENTATION AND CONTROLS PROBABILISTIC RISK ASSESSMENT MODELS

Because of the rapid changes that are taking place in the digital computer and graphic display technologies employed in a modern human system interface, design certification of the AP1000 focused upon the process used to design and implement Instrumentation and Control (I&C) systems for the AP1000, rather than on the specific implementation. In order to address the need for a plant specific PRA to support Combined Construction and Operating License (COL), it became necessary to revise the AP1000 PRA to reflect the to-be-built design. The platform for the Protection and Safety Monitoring System (PMS) and Plant Control System (PLS) has been selected and is designed in accordance with the design process described in Chapter 7 of the AP1000 Design Control Document. The purpose of this section is to discuss the revision to the AP1000 PRA I&C models that reflect the new PMS and PLS architecture.

This task coincides with the work performed in Section 2.0 of this report. The models are created using the CAFTA software.

3.1 Protection and Safety Monitoring System

This section evaluates the reliability of the PMS and its ability to initiate the safety-related functions necessary to shut down the plant and to maintain the plant in a safe condition. Included in the assessed functions are the PMS's capability to control safety-related components in the plant that are operated from the main control room or remote shutdown workstation and to monitor the plant safety-related functions during and following an accident. The assessed functions of the PMS include the availability of the system to:

- Automatically initiate operation of appropriate systems, including reactivity control systems and ensure that acceptable reactor core design limits of the reactor coolant and moderator pressure boundaries, are not exceeded as a result of anticipated operational occurrences, maintenance, and testing
- Sense accident conditions and initiate operation of systems and components important to safety

A description of the PMS function is provided in Chapter 7 of the AP1000 DCD.

The AP1000 instrumentation and control architecture contains the following three major components: 1) the protection and safety monitoring system, 2) the plant control system, and 3) the diverse actuation system. This section focuses on the assessment of the PMS; the PLS and DAS are discussed in Sections 3.2 and 3.3, respectively.

The details of the AP1000 PRA I&C model followed the AP600 design. Fault trees for the AP1000 system were documented in the AP1000 PRA Document. The Common Q hardware and software has been selected for the PMS platform in the AP1000.

The scope of the system analyses includes the following equipment:

- Bistable Logic Processors (BLP)
- Local Coincidence Logic Cabinets (LCL)
- Integrated Logic Processors/Cabinets (ILP/ILC)
- AF100 bus
- Reactor trip switchgear (RTS)
- Qualified Display Processing System (QDPS)
- Operator controls

The following systems are also addressed in this section:

- Control rod drive mechanisms (CRDM)
- Sensors

The analysis of the PMS is divided into the following functional groupings:

- Reactor trip
 - Automatic – sensors through breakers and CRDMs
 - Manual – control inputs through breakers and CRDMs
- Engineered safety features (ESF) actuation
 - Automatic – sensors through output driver modules
 - Manual – control inputs through output driver modules
- Indication – QDPS, PMS/PLS/data display system (DDS), DAS
- Reactor coolant pump trip – sensors through breakers (Note that while the reactor coolant pump trip is a function of the engineered safety features, system level trees are developed. The reactor coolant pump trip is treated separately from the engineered safety features)

The following paragraphs discuss the general approach taken for the modeling of each of the functional groupings.

Reactor Trip

Three reactor-trip-signal-related trees from the AP1000 PRA are maintained. These are RTPMS, RTPMS1, and RTSTP. These trees are simplified and do not reflect the detailed system architecture.

Engineered Safety Features Actuation

As part of the system trees, an engineered safety features actuation signal is typically needed as one of the inputs to a system tree to model actuation of an ESF-related component. For each of these actuation signals, an instrumentation and control subtree is developed to model the unavailability of the engineered safety features to provide the actuation signal upon demand. The assigned systems/functions that they support in the models are:

- Automatic depressurization system (ADS)
- Containment isolation system (CIS)
- Core makeup tank (CMT)

- Chemical volume and control system (CVS – valves only)
- IRWST/gravity feed (IRW)
- Passive containment cooling (PCS)
- Passive residual heat removal (PRHR)
- Normal residual heat removal (RNS)
- Reactor coolant pump trip (RPT)
- Steam generator system (SGS)

Indication

Wherever a human action is credited in the successful operation of the PMS, the unavailability of systems that collect and provide the appropriate information to be displayed as indications to the operator are modeled. These models are meant only to provide an input to the human reliability analysis and do not contribute to the failure probability of the system itself. A conservative simplified model is applied generically to the PMS assessments to bound the unavailability of the indication functions. That model is developed as follows:

There are three basic paths that are assumed to be normally available to provide indication to the operator. These are:

- Data display system (DDS)
- Qualified display processing system (QDPS)
- Diverse actuation system (DAS)

The assigned unavailability of each of these systems to provide a particular indication is $1.0\text{E-}02$ failures/demand. While it is expected that the actual unavailabilities of each of these systems to provide indication would be substantially better than the assigned value, there is not an overlap of indication functions provided across all of the systems, and the conservative assigned value reflects the consideration of that limitation. These values are also consistent with the assigned unavailability of $1.0\text{E-}02$ failures/demand for the DAS in general. It is assumed that each of the systems is capable of providing the essential indications required for the PMS functions being modeled at that assigned rate. Therefore, failure of all three systems must occur before total loss of indication to the operator is achieved. This gives a total unavailability for the combinational loss of all indication systems of $1.0\text{E-}06$ failures/demand. Contribution of common cause failure is minimized in this evaluation as the DAS design is diverse, where common cause failure is considered most significant, from the DDS and QDPS, and hence, does not have a dominant contribution in this model.

Application of these results in the PMS models is achieved by implementing a node representing the failure of all indication, which has the resultant contribution of $1.0\text{E-}06$, wherever a human action is credited. It should be noted that wherever the failure-of-all-indication node is applied, a failure node representing the common cause failure of the associated instrumentation, namely sensors, is also applied. This is done to reflect the fact that while the cabinetry and functions of the DAS versus the PMS may be diverse, the sensors, although independent, are conservatively expected to be of the same type, and hence, susceptible to a common cause failure that could inhibit the availability of an accurate indication across all systems. But relying on a single indication type is considered conservative, as multiple queues are usually available to the

operator as indications relating to various plant parameters being monitored. The models of the PMS generally consider the most direct sensor/queue path and do not credit alternate paths.

Reactor Coolant Pump Trip

Three fault trees are developed to address reactor coolant pump trip function in the assessment. These are the RCL, RCN and RCT fault trees. Note that these trees represent system level fault trees and are supported by a number of instrumentation and control subtrees, all of which were developed in the previous PRA revision.

The RCL fault tree addresses the unavailability of the PMS to trip all four reactor coolant pumps following a small LOCA, while the RCT fault tree addresses the unavailability of the PMS to trip all four reactor coolant pumps following a transient. The RCN fault tree addresses the unavailability of the PMS to trip all four reactor coolant pumps following an intermediate LOCA.

3.2 Plant Control System

This section evaluates the reliability of the PLS. The analyses presented in this section assess the unavailability of the plant control system to provide the nonsafety-related functions necessary to control the plant during normal operation and to maintain the plant in a desired condition. Included in the assessed functions are the plant control system capability to control nonsafety components in the plant that are operated automatically and remotely from the main control room or remote shutdown workstation, and the plant control system capability to monitor the plant functions during and following an accident. The assessed functions of the plant control system include the unavailability of the system to:

- Automatically initiate the appropriate systems to provide control of the reactor and other key components in response to load changes, and monitor margins to plant safety limits and the plant's transient performance
- Sense accident conditions and initiate the operation of mitigating systems and components.

A description of the plant control system is provided in Chapter 7 of the AP1000 DCD.

The AP1000 instrumentation and control architecture contains the following three major components: 1) protection and safety monitoring system, 2) plant control system, and 3) diverse actuation system. This section focuses on the assessment of the plant control system. The protection and safety monitoring system and diverse actuation system are discussed in Section 3.1 and 3.3 respectively.

The I&C functional requirements and the degree of redundancy modeled in the PRA are representative of the expected I&C design. Therefore, analyses are based on the Ovation platform.

The scope of the system analyses includes the following equipment:

- Control cabinets
- Input/Output (I/O) Modules
- Data highway
- Sensors

- Operator controls

An assessment of the rod control system is also developed in chapter 7 of the AP1000 DCD.

The analysis of the plant control system is divided into the following functional groups:

- Control
 - Automatic – Sensors through output driver modules
 - Manual – Control inputs through output driver modules
- Indication – Qualified data processing system (QDPS), data display and processing system (DDS), and diverse actuation system (DAS) (These systems, although not included formally in the plant control system, are evaluated to form a generic indication model in chapter 7 of the AP1000 DCD.)

The following paragraphs discuss the general approach taken for the modeling of each of the functional groupings.

Control

As part of the system fault trees, developed in other sections of this document, an actuation signal is typically needed as one of the inputs to a system fault tree to model the actuation and control of a component. For each of these required actuation signals, an I&C subtree is developed to model the unavailability of the plant control system to provide the actuation signal upon demand. The assigned systems/functions that they support in the models are:

- Compressed and instrument air system (CAS)
- Containment cooling system (CCS)
- Condenser system (CDS)
- Chemical volume and control system (CVS – pumps only)
- Main ac power system (ECS)
- Main feedwater system (MFS)
- Main steam system (MSS)
- Normal residual heat removal system (RNS)
- Rod cluster control system (RCCS)
- Startup feedwater system (SFW)
- Service water system (SWS)
- Turbine building closed cooling water system (TCS)
- Hydrogen control system (VLS)
- Chilled water system (VWS)

Indication

Wherever a human action is credited in the assessment of the plant control system the operator displays are modeled. These models are meant only to provide an input to the human reliability analysis and do not contribute to the failure probability of the system itself. A conservative

simplified model is applied generically to the plant control system to bound the availability of the indication functions. That model is developed as follows:

Three basic paths are assumed to be normally available to provide indication to the operator. These are:

- Data display and processing system
- Qualified data processing system
- Diverse actuation system

The unavailability of each of these systems to provide a particular indication is assigned at $1.0\text{E-}02$ failures/demand. While it is expected that the actual unavailability of each of these systems to provide indication would be substantially better than the assigned value, there is not a total overlap of indication functions provided across the systems. The conservative assigned value reflects the consideration of that limitation. These values are also consistent with the assigned unavailability of $1.0\text{E-}02$ failures/demand for the diverse actuation system in general. It is assumed that each of the systems is capable of providing the essential indications required for the plant control system functions being modeled at that assigned rate. Failure of all three systems must occur before total loss of indication to the operator is achieved. This gives a total unavailability for the combinational loss of all indication systems of $1.0\text{E-}06$ failures/demand. Due to diversity between the systems, the contribution of common cause failure is minimized in this evaluation and, does not have a dominant contribution in this model.

The application of the result in the plant control system models is achieved by implementing a node representing the failure of all indication, which has the resultant contribution of $1.0\text{E-}06$, wherever a human action is credited. Wherever the "failure of all indication" node is applied, a failure node representing the common cause failure of the associated instrumentation, namely sensors, is also applied. This is done to reflect the fact that the sensors, although independent, are conservatively expected to be of the same type. Therefore, they are susceptible to a common cause failure that could inhibit the availability of an accurate indication across all systems. But relying on a single indication type is considered conservative because multiple queues are usually available to the operator as indications relating to the various plant parameters. The models of the plant control system generally consider the most direct sensor/queue path and do not credit alternate paths.

3.3 Diverse Actuation System

The Diverse Actuation System design had not been selected at the time of this analysis. The DAS PRA model as documented in Chapter 27 of the AP1000 PRA Report APP-GW-GL-022 is maintained as a representative model of the DAS. Refer to Chapter 27 of the AP1000 PRA Report APP-GW-GL-022 for description and probabilistic analysis of the DAS.

4.0 PROBABILISTIC RISK ASSESSMENT RESULTS

4.1 Introduction

The AP1000 PRA model consists of fault trees and accident sequences that are quantified using a fault tree linking process.

The result of the fault tree linking quantification is a core damage frequency and large release frequency and a listing of dominant cutsets.

The fault tree linking process involves the following steps:

1. Create Fault Tree Top Logic

Use the CAFTA software package to convert the AP1000 event tree accident sequence structure into a fault tree logic structure, with one top event serving to capture the core damage frequency cutsets and a separate top event, linked to CDF sequences, to capture large release frequency cutsets. The AP1000 event tree accident sequence structure is not modified from that documented in AP1000 PRA Report APP-GW-GL-022 (Reference 2).

2. Convert Fault Trees

This step involves using the system fault trees from the WesSAGE model, and utilizing the CAFTA conversion filter. The fault trees documented in AP1000 PRA Report APP-GW-GL-022 are not modified during this process.

3. Quantify the event tree models to obtain a core damage frequency.

The output of this step is a listing of dominate cutsets. Fault tree quantification is performed using the PRAQuant program as part of the CAFTA software suite. PRAQuant allows a batch quantification using flag files to modify basic event or gate probability, and recovery files to apply operator action dependencies. This step must be performed any time PRA quantification is necessary.

4.2 Accident Sequence Model Quantification

In this section, documentation of the quantification of plant core damage frequency for internal initiating events at power and shutdown is provided.

The method utilized for core damage calculation is discussed in Section 4.2.1. Input files and data used in the core damage quantification are provided in Section 4.2.2. The implementation of the consequential event modeling is described in Section 4.2.3. The incorporation of the operator action dependency into core damage frequency quantification is discussed in Section 4.2.4.

The core damage frequency is reported for each initiating event in Section 4.3. The large release frequency results are provided in Section 4.4. The core damage frequency for the Sensitivity to Standby Non-Safety Systems is reported in Section 4.5. The core damage frequency for

shutdown events is reported in Section 4.6.

The core damage frequency calculation was performed using the fault tree linking method.

4.2.1 Core Damage Quantification Method

The accident sequences for each initiating event category are defined in terms of event trees in Chapter 4 of the AP1000 PRA Report APP-GW-GL-022. The core damage sequences for each event tree are modeled in CAFTA using the fault tree linking method. Consequential event sequences are considered in the linked fault tree.

Each core damage event sequence contains a set of top events (including the initiating event) which are either scalars or are a set of cutsets representing a fault tree. These top events are assigned symbols that have specific prefixes. These prefixes are:

1. IEV-AAA

This symbol refers to an initiating event frequency that is a scalar quantity for the initiating event category symbolized by AAA.

2. OTH-CCC

This symbol refers to the failure probability of a top event (other than an initiating event) which is a scalar.

3. Failure and Success

Failure logic is modeled in failure gates ("AND" and "OR"). Success logic is modeled using the "A and not B" ("ANOTB") gates in CAFTA. The use of the NOT gate is important to eliminate successful cutsets.

The capability to quantify each core damage sequence exists, but is not used to streamline the quantification process. If required, the dominant core damage sequences, once identified, may be individually quantified to capture specific information.

After the accident sequences are quantified, the results are added to find the plant core damage frequency and to identify the dominant core damage sequences and cutsets. The fractional contribution of each initiating event category to the total plant core damage frequency is also determined.

The core damage quantification process can be summarized as follows:

1. Create an accident sequence model using fault tree linking methods for each initiating event and each consequential event.
2. Quantify the linked fault tree, calculating core damage frequencies and identify cutsets.
3. Add all core damage results from individual initiating events to calculate plant core damage frequency, and identify dominant cutsets.

4.2.2 Core Damage Quantification Input Files and Data

This section documents both the scalar input data and the fault trees that are used in the core damage quantification for AP1000.

4.2.2.1 Scalar Inputs

Scalar inputs are modeled in one of two forms; initiating event frequencies (IEVs) and events not modeled in the system fault tree models. The scalar inputs are documented in Chapter 2 of the AP1000 PRA. Chapter 2 of the AP1000 PRA documents the development of the initiating event frequencies used in the core damage quantification.

4.2.2.2 System Fault Tree Inputs

The following PRA chapters document the AP1000 system fault tree models.

Chapter 8	Passive Residual Heat Removal
Chapter 9	Core Makeup Tank
Chapter 10	Accumulator
Chapter 11	Automatic Depressurization System
Chapter 12	In-Containment Refueling Water Storage Tank
Chapter 13	Passive Containment Cooling System
Chapter 14	Main and Startup Feedwater System
Chapter 15	Chemical and Volumen control System
Chapter 16	Containment Hydrogen Control System
Chapter 17	Normal Residual Heat Removal System
Chapter 18	Component Cooling Water System
Chapter 19	Service Water System
Chapter 20	Central Chilled Water System
Chapter 21	AC Power System
Chapter 22	Class 1E DC and Uninterruptible Power Supply
Chapter 23	Non-Class 1E and UPS System
Chapter 24	Containment Isolation
Chapter 25	Compressed and Instrument Air System
Chapter 26	Protection and Safety Monitoring System
Chapter 27	Diverse Actuation System
Chapter 28	Plant Control System.

There were several PRA model changes made in addition to the I&C revision. These changes were made to maintain consistency with the AP1000 Design. Section 7.0 documents the markup to AP1000 DCD Appendix 19C to reflect implementation of these changes.

- Eliminate common cause event IWX-MV-GO, CCF to open of 2/2 Recirc MOVs (117A/B). In the current design, these valves are normally open. The previous revision of the AP1000 PRA is considered conservative.
- Consider allowable time for multiple divisions of 1E DC (IDS) power system to be unavailable. Per Technical Specifications, two divisions of 1E DC power are permitted to be unavailable for 2 hours. If one of the divisions cannot be made available in that

time, the operators must shutdown the plant in 6 hours. Therefore, cutsets containing two divisions of 1E DC power unavailable due to maintenance do consider a mission time of 8 hours.

- The PRHR and CMT subsystems automatically actuate on loss of 1E DC (IDS) power. As such, the IDS dependency is removed from the fault trees for these subsystems.
- Removal of the need for I&C to open IRWST injection MOVs V121A/B during shutdown conditions. These valves are normally open and thus do not require an actuation signal (shutdown only).
- Update Electric Power dependencies per latest design information (from Revision 2 of the AP1000 PRA).
- Removal of AOV001B from the compressed air system fault trees (from Revision 2 of the AP1000 PRA).
- Quantification of loss-of-offsite power event sequences with a low cutoff probability to collect more cutsets for the station blackout event ($1.0\text{E-}14$ cutoff) (from Revision 2 of the AP1000 PRA).
- Addition of the third main feedwater pump to the main feedwater fault trees (from Revision 2 of the AP1000 PRA).

4.2.3 Definition of Consequential Event Categories

Five consequential event categories are modeled in the AP1000 PRA study. They are: consequential medium LOCA, consequential medium LOCA following a LOSP event, consequential medium LOCA following a LCCW event, consequential stuck open secondary side safety valve, and consequential steam generator tube rupture. The following subsections describe the implementation of the consequential event modeling.

4.2.3.1 Consequential Medium LOCA

Consequential medium LOCA can occur, depending upon subsequent system failures, after the following initiating events:

IEV-TRANS	Transients with main feedwater
IEV-LRCS	Transients with loss of RCS flow
IEV-LMFW-P	Transients with loss of main feedwater to 1 SG
IEV-POWEX	Transients with core power excursion
IEV-LCOND	Transients with loss of condenser
IEV-LMFW-T	Loss of main feedwater
IEV-LCAS	Loss of main compressed air
IEV-LCCW	Loss of CCW/SW
IEV-LOSP	Loss of offsite power

The appropriate sequences of the above initiating events are treated similarly as medium LOCA initiating events in the medium LOCA accident sequence model.

4.2.3.2 Consequential Stuck Open Secondary Side Safety Valve

Consequential stuck open secondary side safety valve can occur, depending upon subsequent system failures, after the following initiating events:

IEV-TRANS	Transients with main feedwater
IEV-LRCS	Transients with loss of RCS flow
IEV-LMFW-P	Transients with loss of main feedwater to 1 SG
IEV-POWEX	Transients with core power excursion
IEV-LCCW	Transients with loss of CCW/SW
IEV-LMFW-T	Loss of main feedwater
IEV-LCOND	Loss of main condenser
IEV-LCAS	Loss of main compressed air
IEV-LOSP	Loss of offsite power
IEV-SLB-U	Main steam line break upstream of MSIVs

4.2.3.3 Consequential Steam Generator Tube Rupture

Consequential steam generator tube rupture can occur, depending upon subsequent system failures, after the following initiating events:

IEV-SLB-D	Main steam line break downstream of MSIVs
IEV-SLB-U	Main steam line break upstream of MSIVs
IEV-SLB-V	Stuck open secondary side safety valve

Consequential stuck open secondary side safety valve event, as stated above, can also lead to a consequential steam generator tube rupture event.

4.2.4 Incorporate Operator Action Dependencies Into Plant Core Damage / Large Release Frequency Quantification

The PRA quantification incorporated dependencies among operator actions introduced during the level 1 core damage quantification. The dependency relationship among operator actions is referred to as human reliability conditional probability evaluation. The method of deducing the HRA conditionals and results of the dependency evaluation are provided in Chapter 30 of the AP1000 PRA Report APP-GW-GL-022.

4.3 Core Damage Frequency Results

The results of the AP1000 plant core damage quantification indicate a plant core damage frequency of 2.30E-07 events per reactor year. The core damage frequency quantified in the previous revision of the AP1000 PRA was 2.41E-07 events per reactor year. When qualitatively considering PRA uncertainties, the results of these two quantifications are statistically equivalent, indicating at least equivalent reliability in the newly modeled I&C designs. Cutsets from the internal events PRA revision were compared to those of the previous revision. All cutsets reviewed are equivalent (in cutset contributors and frequency) with the exception of the cutsets containing I&C contributors. The top 10 cutsets are found to be identical. This is expected and is acceptable. The similarity in the cutsets indicates that the PRA software conversion was performed properly, with the only changes due to the revision to the I&C PRA model. More

detailed results of the core damage quantification are presented in the Table 4.3-1 and Table 4.3-2.

Table 4.3-1 presents the initiating event contribution to core damage frequency. The values of the initiating event contributions have changed as a result of the PRA model revision, as expected. Many of the initiating event contribution changes are due to the I&C model revision; however, many are due to the updated Electrical Power dependencies. One such example is the RCS Leak initiating event. The RCS Leak initiator progresses to a Small LOCA if Chemical and Volume Control (CVS) is failed or unavailable. In the previous revision, there was a cutset in which CVS was unavailable due to AC Power Bus Unavailability (Train A) and CVS Pump B Unavailability. With the updated Electrical Power dependencies, the AC Power Bus Unavailability directly results in the unavailability of the CVS. The RCS Leak cutset then becomes more important. However, the changes are not so significant to result in a change to PRA results and insights. Major contributors to risk in the previous revision are still major contributors to risk in this revision of the AP1000 PRA.

Table 4.3-2 documents relative system importances. This analysis was performed by failing the respective systems in the PRA model to determine the subsequent increase in core damage frequency. The table indicates that the PMS is less important for this I&C design. As PMS reliability has increased, the Risk Achievement Worth has decreased. It should be noted that this decrease is smaller than indicated by the Table 4.3-2. The CDF with PMS failed in the old model was 1.59E-02 /yr, whereas it is 8.73E-03 /yr in this updated model. This is a small change in risk importance.

Table 4.3-1: Initiating Event Contribution to CDF				
	Initiating Event Category*	Current DCD PRA Contribution to CDF from Table 19.59-1 of Reference 1 (/yr)	Updated Contribution to CDF (/yr)	Updated Percent Contribution to CDF
1	SAFETY INJECTION LINE BREAK INITIATING EVENT	9.50E-08	9.33E-08	40.5%
2	LARGE LOCA INITIATING EVENT	4.50E-08	4.42E-08	19.2%
3	SPURIOUS ADS INITIATING EVENT	2.96E-08	2.18E-08	9.5%
4	SMALL LOCA INITIATING EVENT	1.81E-08	1.61E-08	7.0%
5	MEDIUM LOCA INITIATING EVENT	1.61E-08	1.44E-08	6.2%
6	REACTOR VESSEL RUPTURE INITIATING EVENT	1.00E-08	1.00E-08	4.3%
7	STEAM GENERATOR TUBE RUPTURE INITIATING EVENT	6.79E-09	9.29E-09	4.0%
8	RCS LEAK INITIATING EVENT	1.71E-09	6.31E-09	2.7%
9	TRANSIENT WITH MFW INITIATING EVENT	8.70E-10	3.55E-09	1.5%
10	CMT LINE BREAK INITIATING EVENT	3.08E-09	3.30E-09	1.4%
11	CORE POWER EXCURSION INITIATING EVENT	3.68E-09	1.48E-09	0.6%
12	LOSS OF CONDENSER INITIATING EVENT	1.66E-09	1.21E-09	0.5%

Table 4.3-1: Initiating Event Contribution to CDF

	Initiating Event Category*	Current DCD PRA Contribution to CDF from Table 19.59-1 of Reference 1 (/yr)	Updated Contribution to CDF (/yr)	Updated Percent Contribution to CDF
13	TOTAL LOSS OF MAIN FEEDWATER INITIATING EVENT	1.24E-09	9.36E-10	0.4%
14	ATWS PRECURSOR WITHOUT MFW INITIATING EVENTS	3.61E-09	8.09E-10	0.4%
15	LOSS OF OFFSITE POWER INITIATING EVENT	9.58E-10	8.00E-10	0.3%
16	LOSS OF COMPRESSED AIR	6.72E-10	6.61E-10	0.3%
17	PASSIVE RHR TUBE RUPTURE INITIATING EVENT	5.02E-10	5.58E-10	0.2%
18	LOSS OF MAIN FEEDWATER TO ONE SG INITIATING EVENT	4.53E-10	5.39E-10	0.2%
19	MAIN STEAM LINE SAFETY VALVE STUCK-OPEN INITIATING EVENT	6.06E-10	4.77E-10	0.2%
20	LOSS OF COMPONENT COOLING WATER / SERVICE WATER	3.23E-10	3.78E-10	0.2%
21	ATWS PRECURSOR WITH SI	1.11E-10	1.34E-10	0.1%
22	MAIN STEAM LINE BREAK UPSTREAM OF MSIV INITIATING EVENT	1.31E-10	5.05E-11	0.02%
23	INTERFACING SYSTEM LOCA INITIATING EVENT	5.00E-11	5.00E-11	0.02%
24	LOSS OF RCS FLOW INITIATING EVENT	3.52E-11	4.17E-11	0.02%
25	MAIN STEAM LINE BREAK DOWNSTREAM OF MSIV INITIATING EVENT	9.15E-12	6.25E-12	0.003%
26	ATWS PRECURSOR WITH MFW OCCURS	7.12E-10	2.35E-12	0.001%
	Totals	2.41E-07	2.33E-07	100%
*Initiating Event Frequencies were not modified in this revision of the AP1000 PRA.				

Table 4.3-2 Updated Summary of System Importance					
Important			Medium Importance (*)	Marginally Important	
1E-02 /yr	1E-03 /yr	1E-04 /yr	1E-05 /yr	1E-06 /yr	1E-07 /yr
	PMS	IRW-INJ	CMT	AC POWER	SG OVERFILL PROTECTION
	ADS		ACC	DAS	NRHR
	IRW-RECIRC		PRHR		MFW
	DC-1E		PLS		SFW
			NON DC-1E		DG
					SWS
					CCS
					CAS
Current DCD PRA Summary of System Importance (From Reference 2 AP1000 PRA Chapter 50)					
Important			Medium Importance (*)	Marginally Important	
1E-02 /yr	1E-03 /yr	1E-04 /yr	1E-05 /yr	1E-06 /yr	1E-07 /yr
PMS	ADS	IRW-INJ	CMT	AC Power	SG Overfill Protection
	IRW-RECIRC		ACC	DAS	NRHR
	DC-1E		PRHR		MFW
			PLS		SFW
			NON DC-1E		DG
					SWS
					CCS
					CAS

(*) = core melt values greater than 5.0E-06 are conservatively classified in this column, since this column contains transition from marginally important category to important category.

4.4 Large Release Frequency Results

The AP1000 plant large release frequency was requantified for this revision of the AP1000 PRA and the quantification results indicate a plant large release frequency of 1.80E-08 events per reactor year. The large release frequency quantified in the previous revision of the AP1000 PRA was 1.95E-08 events per reactor year. The small change in large release frequency is a result of the improved reliability of the Instrumentation and Controls systems. Containment effectiveness, the ratio of the frequency of core damage sequences ending in "Intact Containment" (IC) end state to the plant CDF, is maintained at approximately 92%. Table 4.4-2 presents plant damage state (PDS) frequencies used in the AP1000 PRA Level 2 analysis. This table indicates that the PDS frequencies, while they may differ in value due to PRA modeling changes, they are similar in percent contribution.

Table 4.4-1: Internal Events Summary		
CDF (/yr)	LRF (/yr)	$C_{eff} = 1 - \frac{LRF}{CDF}$
2.30E-07	1.80E-08	92%

Table 4.4-2: Summary of Plant Damage State Frequencies					
PDS	Description	Current DCD PRA AP1000 (Reference 2)		Updated AP1000	
		Frequency (/yr)	%	Frequency (/yr)	%
1A	High RCS Pressure (Transient or SLOCA)	5.01E-09	2.1%	5.28E-09	2.3%
1P	High RCS Pressure (P-RHR operating)	1.48E-09	0.6%	1.77E-09	0.8%
2E	RCS Depressurized	8.06E-08	33.4%	8.26E-08	35.9%
2L	RCS Depres.(Gravity Injection succ.; Sump Recirc. fails)	2.40E-08	9.9%	1.73E-08	7.5%
2R	RCS Depressurized (CMT and ACC fail)	4.63E-08	19.2%	4.76E-08	20.7%
3A	High RCS Pressure and ATWS	4.43E-09	1.8%	9.07E-10	0.4%
3C	Vessel Failure	1.00E-08	4.2%	1.00E-08	4.3%
3D	Partial RCS Depressurization	5.97E-08	24.8%	5.34E-08	23.2%
6	Containment Bypass by SGTR or ISLOCA	9.52E-09	4.0%	8.74E-09	3.8%
Others	All Others	Not Reported	Not Reported	2.40E-09	1.0%
CDF =		2.41E-07	100.0%	2.30E-07	100.0%

4.5 Shutdown PRA

This section provides an assessment of the risk to the AP1000 during low-power and shutdown conditions. In the AP1000 PRA, an evaluation of the risk associated with low-power and shutdown conditions was provided in Chapter 54 of the AP1000 PRA.

The evaluation, which covers shutdown and low-power operation, encompasses operation when the reactor is in a subcritical state or is in transition between subcriticality and power operation up to 5 percent of rated power. The evaluation addresses conditions for which there is fuel in the reactor vessel and includes aspects of nuclear steam supply, the containment, and systems that support the nuclear steam supply and containment. The evaluation does not address events involving fuel handling outside of the containment and fuel storage in the fuel storage building.

The AP1000 shutdown PRA was performed in accordance with the requirements outlined in the EPRI ALWR Utility Requirements Document, which specified that a simplified assessment of the risk of the plant should be performed for shutdown conditions. The AP1000 Shutdown PRA results demonstrate that the risk to the AP1000 plant during shutdown was very low. The AP1000 shutdown PRA model documented in Chapter 54 of the AP1000 PRA was created using the AP600 shutdown CDF cutset file. Modifications were made to the AP600 cutset file to reflect AP1000 design and operating cycle changes, as documented in Chapter 54 of the AP1000 PRA. In the analysis performed for this report, the AP600 fault trees were converted to the CAFTA software and modifications were made to the fault trees, as necessary. In the AP1000 shutdown PRA report, the events during hot/cold shutdown conditions are grouped and referred to as non-drained events and drained events. The drained events include events during drain down of the RCS and events when the plant is at mid-loop.

The CDF for Shutdown events is 1.01E-07 events per year. This value is a reduction in risk compared to 1.23E-07 events per year quantified previously in Chapter 54 of the AP1000 PRA. The results of the AP1000 Shutdown PRA quantification are summarized in the Table 4.5-1. The results indicate a change in initiator contributions to Core Damage Frequency. This is due to two changes. First, the revision to the I&C model does have an impact on system response and does modify contributions to core damage. Second, the removal of the IWN-MAN00 operator failure as a valid failure mode does impact system response. The IWN-MAN00 operator action evaluates the probability of failure to recognize the need and failure to open the in-containment refueling water storage tank motor-operated valves during shutdown conditions, given that the normal residual heat removal system is unavailable. As these motor operated valves are now designed to be normally open, this operator action is no longer necessary. The changes are not significant enough to indicate a change in the Reference 2 AP1000 PRA Chapter 54 conclusions.

Additionally, the Large Release Frequency calculation is provided. The AP600 shutdown level 2 model is applicable to the AP1000 design for estimating plant LRF; moreover, the dominant sequences contributing to AP1000 shutdown risk are the same as those of AP600. The conditional containment failure probability (CCFP=LRF/CDF) for AP600 was calculated to be 1.5E-08/9.0E-08 = 0.1667. Thus, the containment effectiveness is 83.3 percent. This conditional probability is used to estimate the AP1000 LRF as follows:

$$\text{LRF}(\text{AP1000, shutdown}) = 0.1667 * 1.01\text{E-}07 = 1.68\text{E-}08/\text{yr.}$$

Table 4.5-1: Initiating Event Contribution to Shutdown CDF

Initiating Event	Description	Initiating Event Frequency (/yr)	Current DCD PRA (Reference 2) CDF From Initiator (/yr)	Updated CDF From Initiator (/yr)
IEV-CCWD	LOSS OF CCW/SW DURING DRAINED CONDITION SEQUENCES	7.16E-04	8.43E-08	7.73E-08
IEV-RNSD	LOSS OF RNS OPERATION DURING DRAINED CONDITION SEQUENCES	9.69E-05	1.14E-08	1.05E-08
IEV-LOSPD	LOSS OF OFFSITE POWER DURING DRAINED CONDITION SEQUENCES	5.28E-03	1.74E-08	8.45E-09
IEV-LOCA24ND	LOCA THROUGH RNS-V024 DURING NON-DRAINED CONDITION SEQUENCES	1.73E-05	2.03E-09	2.44E-09
IEV-LOCA24D	LOCA THROUGH RNS-V024 DURING DRAINED CONDITION SEQUENCES	1.15E-05	1.35E-09	1.24E-09
IEV-RCSOD	RCS OVERDRAINING DURING DRAINDOWN TO MID-LOOP	5.28E-06	3.75E-09	5.70E-10
IEV-CCWND	LOSS OF CCW/SW DURING NON-DRAINED CONDITION SEQUENCES	3.99E-03	1.77E-09	1.99E-10
IEV-LOCAPRND	RNS PIPE REPUTURE DURING NON-DRAINED RCS SEQUENCES	1.61E-05	1.17E-10	1.25E-10
IEV-LOSPND	LOSS OF OFFSITE POWER DURING NON-DRAINED CONDITION SEQUENCES	1.82E-02	5.10E-10	5.65E-11
IEV-RNSND	LOSS OF RNS OPERATION DURING NON-DRAINED CONDITION SEQUENCES	1.02E-03	4.52E-10	5.07E-11
	Totals	2.94E-02	1.23E-07	1.01E-07

4.6 Sensitivity to Standby Non-Safety Systems

This section documents the non-safety systems sensitivity analysis performed on the core damage frequency results of the AP1000 PRA internal events at-power. The objective of this analysis is to estimate the core damage frequency (CDF) for internal events at-power when no credit is taken for five standby systems which may not be available following an initiating event. These five systems (which are taken credit for in the base AP1000 PRA) are:

1. Chemical and Volume Control System (CVS),
2. Startup Feedwater System (SFW),
3. Normal Residual Heat Removal System (RNS),
4. Diverse Actuation System (DAS),
5. Diesel Generators (DG).

The calculations are performed on a personal computer using the CAFTA code. The results of the sensitivity analysis are given in Table 4.6-1. Table 4.6-1 shows the contribution of the initiating events when no credit is taken for the above standby systems. This table was not presented in previous revisions; thus, no comparison is made.

This sensitivity analysis estimates that the CDF increases from $2.30\text{E-}07$ /year to $2.00\text{E-}06$ /year when no credit is taken for the standby systems CVS, SFW, RNS, automatic DAS, and DGs. This value is comparable to the value from Chapter 50 of the AP1000 PRA, $2.12\text{E-}06$ /year.

These results are intended to replicate the AP1000 PRA Chapter 50 analysis, which performed a modification of the AP1000 internal events CDF cutset file. However, unlike that analysis, a flag file is applied to the entire model in this revision, not just a limited set of cutsets. Therefore, a more realistic risk assessment is now provided.

Table 4.6-1: Sensitivity to Standby Non-Safety Systems Contribution of Initiating Events to CDF

Event Name	Description	Frequency (/yr)	Updated Percent Contribution	Updated CDF Contribution (/yr)
IEV-RCSLK	RCS LEAK INITIATING EVENT	6.20E-03	54.20%	1.08E-06
IEV-ATWS	ATWS PRECURSOR WITHOUT MFW INITIATING EVENTS	4.81E-01	8.86%	1.77E-07
IEV-LMFW-T	TOTAL LOSS OF MAIN FEEDWATER INITIATING EVENT	3.35E-01	6.77%	1.35E-07
IEV-SI-LB	SAFETY INJECTION LINE BREAK INITIATING EVENT	2.12E-04	4.66%	9.32E-08
IEV-SLOCA	SMALL LOCA INITIATING EVENT	5.00E-04	4.37%	8.74E-08
IEV-MLOCA	MEDIUM LOCA INITIATING EVENT	4.36E-04	3.82%	7.64E-08
IEV-TRANS	TRANSIENT WITH MFW INITIATING EVENT	1.40E+00	3.13%	6.26E-08
IEV-LCOND	LOSS OF CONDENSER INITIATING EVENT	1.12E-01	2.49%	4.98E-08
IEV-ATW-T	ATWS PRECURSOR WITH MFW OCCURS	1.17E+00	2.36%	4.72E-08
IEV-LLOCA	LARGE LOCA INITIATING EVENT	5.00E-06	2.21%	4.42E-08
IEV-SGTR	STEAM GENERATOR TUBE RUPTURE INITIATING EVENT	3.88E-03	1.47%	2.94E-08
IEV-PRSTR	PASSIVE RHR TUBE RUPTURE INITIATING EVENT	1.34E-04	1.17%	2.34E-08
IEV-SPADS	SPURIOUS ADS INITIATING EVENT	5.40E-05	1.09%	2.18E-08
IEV-CMTLB	CMT LINE BREAK INITIATING EVENT	9.31E-05	0.83%	1.66E-08
IEV-RV-RP	REACTOR VESSEL RUPTURE INITIATING EVENT	1.00E-08	0.50%	9.98E-09
IEV-LMFW-P	LOSS OF MAIN FEEDWATER TO ONE SG INITIATING EVENT	1.92E-01	0.46%	9.14E-09
IEV-POWEX	CORE POWER EXCURSION INITIATING EVENT	4.50E-03	0.40%	8.08E-09
IEV-LCCW	LOSS OF COMPONENT COOLING WATER / SERVICE WATER	1.44E-01	0.32%	6.42E-09
IEV-ATW-S	ATWS PRECURSOR WITH SI	1.48E-02	0.27%	5.44E-09
IEV-LOSP	LOSS OF OFFSITE POWER INITIATING EVENT	1.20E-01	0.25%	4.90E-09
IEV-LCAS	LOSS OF COMPRESSED AIR	3.48E-02	0.19%	3.82E-09
IEV-SLB-V	MAIN STEAM LINE SAFETY VALVE STUCK-OPEN INITIATING EVENT	1.21E-03	0.13%	2.68E-09
IEV-LRCS	LOSS OF RCS FLOW INITIATING EVENT	1.80E-02	0.04%	7.96E-10
IEV-SLB-U	MAIN STEAM LINE BREAK UPSTREAM OF MSIV INITIATING EVENT	3.72E-04	0.01%	2.68E-10
IEV-SLB-D	MAIN STEAM LINE BREAK DOWNSTREAM OF MSIV INITIATING EVENT	5.96E-04	0.01%	1.80E-10
IEV-ISLOC	INTERFACING SYSTEM LOCA INITIATING EVENT	5.00E-11	0.00%	5.00E-11
	Total		100%	2.00E-06

5.0 REGULATORY IMPACT

AP1000 is expected to achieve a higher standard of severe accident safety performance than current pressurized water reactor operating plants, because both prevention and mitigation of severe accidents have been addressed during the design stage, taking advantage of PRA insights, PRA success criteria analysis, severe accident research, and severe accident analysis. Since PRA considerations have been integrated into the AP1000 design process from the beginning, many of the traditional PRA insights relating to current pressurized water reactor operating plants are not an issue for the AP1000. The Level 1, and Level 2 results show that addressing PRA issues in the design process leads to a low level of risk. The PRA results indicate that the AP1000 design meets the higher expectations and goals for new generation passive pressurized water reactors (PWRs).

The core damage frequency (CDF) and large release frequency (LRF) for at-power internal events (excluding seismic, fire, and flood events) are $2.30\text{E-}07$ events per reactor-year and $1.80\text{E-}08$ events per reactor-year, respectively. These frequencies are at least two orders of magnitude less than a typical pressurized water reactor plant currently in operation. This reduction in risk is due to many plant design features, with the dominant reduction coming from highly reliable and redundant passive safety-related systems that impact both at-power and shutdown risks. These passive systems are much less dependent on operator action and support systems than plant systems in current operating plants. The CDF cutset results indicate a reduction in importance of the key CDF cutset contributors, as illustrated below.

- The 100 highest-frequency at-power cutsets together contribute approximately 85 percent of the total core damage frequency, compared to 86% from Reference 1. (approximately $2.0\text{E-}07$ events per year).
- The top 200 at-power cutsets contribute approximately 90 percent, compared to 91% from Reference 1 ($2.1\text{E-}07$ events per year).
- The top 500 at-power cutsets contribute approximately 94 percent, compared to 95% from Reference 1 ($2.2\text{E-}07$ events per year).
- The top 1,000 at-power cutsets contribute approximately 97 percent, compared to 97% from Reference 1 ($2.23\text{E-}07$ events per year).
- The top 2,000 at-power cutsets contribute approximately 98 percent, compared to 98% from Reference 1 ($2.27\text{E-}07$ events per year).

The CDF for Shutdown events is $1.01\text{E-}07$ events per year. This value is a reduction in risk compared to $1.23\text{E-}07$ events per year quantified previously.

The above values are consistent with those presented in the previous revision to the AP1000 PRA. As such, the internal events evaluations, conclusions and insights documented in AP1000 DCD Chapter 19 remains representative of the AP1000 design and will not be revised. The sensitivity of standby non-safety systems is provided as additional justification that the PRA model revisions and software change further reinforce that the results and conclusions documented in AP1000 DCD Chapter 19 are valid and applicable to the AP1000 standard design.

Conservative, bounding fire and flood assessments show the core damage risk from these events is small compared to the core damage risk from at-power and shutdown events. As such, the

conservative bounding fire and flood assessment results documented in AP1000 DCD Chapter 19 are considered representative of the AP1000 design.

As this report concludes the revision to the AP1000 Probabilistic Risk Assessment, the AP1000 Design Control Document Chapter 19, Appendix 19C may be revised to remove reference to planned model revisions (See Section 7.0 of this report).

The AP1000 PRA will be available for NRC review at the Westinghouse offices in Monroeville, PA after April 30, 2007.

6.0 REFERENCES

1. APP-GW-GL-700, AP1000 Design Control Document, Revision 15.
2. APP-GW-GL-022, AP1000 Probabilistic Risk Assessment, Revision 5.

7.0 DCD MARKUP

Revise Chapter 19, Appendix 19C.

APPENDIX 19C ADDITIONAL ASSESSMENT OF AP1000 DESIGN FEATURES

The AP1000 PRA model, like many other conventional PRA models, is an evolving model. It is revised, as needed, to keep up with design changes and to implement revisions identified by various reviews, applications, and related analyses. Due to the iterative nature of the interface between the PRA analysts and the plant designers, it is not always possible to incorporate all differences identified between the plant design and the PRA model in a timely manner. This appendix is intended to summarize known differences between the two, and identify any future changes planned to the current PRA model to address these differences.

Planned Revisions to AP1000 PRA Model

~~A review of the bus assignments by the AP1000 designers for the AP1000 PRA model identified that some bus assignments needed to be revised. A systematic investigation of the support system buses in the fault trees has been made and the fault trees are revised as needed. This also includes the replacement of the 4.16 KVAC bus with the 6.9 KVAC bus in fault trees. This revision is the basis for Revision 2 of the plant core damage frequency (CDF) for internal events at power. While this revision is being made, other revisions identified by either the PRA team or the AP1000 designers during the review of the AP1000 PRA sections is also incorporated into the plant CDF revision. Several changes to the PRA were previously considered by preliminary evaluations indicated they are of low importance to the PRA results. These changes are reproduced here for future consideration. These additional revisions are:~~

1. Containment isolation event trees.
- ~~2. Removal of AOV001B from the compressed air system fault trees.~~
- ~~3. Quantification of loss of offsite power (LOSP) event sequences with a lower cutoff probability to collect more cutsets for the station blackout (SBO) event (1.0E-14 cutoff by removal of the /m:25000 cutset restriction during LOSP quantification).~~
- ~~4.2. Correction of ADR fault tree top logic to reflect the success criteria (logic was conservative).~~
- ~~5. Addition of the third pump main feedwater pump to the main feedwater (MFW) fault trees.~~
- ~~6.3. The success criteria for medium LOCA (including CMT and DVI line breaks) will be modified to credit the PRHR heat exchanger for those instances when the accumulators are assumed to fail. The impact on the overall PRA results for this change is not expected to be significant.~~

| Preliminary quantification shows that the plant CDF is not affected by this revision. The large release frequency (LRF) is not expected to be affected either. The next revision of the AP1000 PRA Report will incorporate these changes to the PRA model.