Lewis Sumner
Vice President
Hatch Project Support

Southern Nuclear Operating Company, Inc.
40 Inverness Parkway
Post Office Box 1295
Birmingham, Alabama 35201

Tel 205.992.7279
Fax 205.992.0341

SOUTHERN COMPANY
Energy to Serve Your World℠

August 31, 2001

Docket Nos. 50-321
50-366

HL-6080

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

Edwin I. Hatch Nuclear Plant
Request to Revise Technical Specifications:
Extension of Completion Times for Inoperable Emergency Diesel Generators

Ladies and Gentlemen:

In accordance with the provisions of 10 CFR 50.90, as required by 10 CFR 50.59(c)(1), Southern Nuclear Operating Company (SNC) is proposing changes to the Plant Hatch Unit 1 and Unit 2 Technical Specifications, Appendix A to Operating Licenses DPR-57 and NPF-5, respectively. The proposed changes to the Technical Specifications extend the Completion Times for the Required Actions associated with restoration of an inoperable Unit 1 or Unit 2 emergency diesel generator (DG). These proposed changes provide operational flexibility, allowing more efficient application of plant resources to safety significant activities. The proposed changes allow performance of periodic DG overhauls on line, reduce plant refueling outage duration, and improve DG availability during shutdown.

The justification for the change to the DG Completion Times is based upon a risk-informed, deterministic evaluation consisting of three main elements: 1) the availability of offsite power via the Startup Auxiliary Transformers, 2) verification that the other DGs and offsite power sources are operable, and 3) reliance on the site procedure for managing risk while a DG is in an extended Completion Time. These elements provide the basis for the requested Technical Specifications change by providing a high degree of assurance of the capability to provide power to the Engineered Safety Feature buses during the DG extended Completion Time. The NRC recently approved similar requests for several other stations including an Amendment to Perry Nuclear Plant, dated February 24, 1999 and Amendments to Byron Station and Braidwood Station, dated September 1, 2000.

Enclosures 1 and 2 include the justification for the change and the 10 CFR 50.92, no significant hazards evaluation. Enclosure 3 provides the page change instructions as well as the changed Technical Specifications and Bases pages. Attachments 1 and 2 are included as information. Attachment 1 describes the Hatch probabilistic safety assessment (PSA); Attachment 2 contains information regarding Hatch PSA quality.

SNC requests the NRC review and approve the amendments no later than March 1, 2002. SNC also requests that, once the amendments are approved, they be issued with an immediate effective date, with implementation no later than 30 days after issuance.

A001

In accordance with the requirements of 10 CFR 50.91, a copy of this letter and all applicable enclosures will be sent to the designated State official of the Environmental Protection Division of the Georgia Department of Natural Resources.

Mr. H. L. Sumner, Jr. states he is Vice President of Southern Nuclear Operating Company and is authorized to execute this oath on behalf of Southern Nuclear Operating Company, and to the best of his knowledge and belief, the facts set forth in this letter are true.

Respectfully submitted,

H. L. Sumner, Jr.

Sworn to and subscribed before me this 31 *day of* August, *2001.*

Notary Public MY COMMISSION EXPIRES JAN. 12, 2005

OCV/dlp

Enclosures:
1. Description of and Justification for Proposed Changes.
2. 10 CFR 50.92 No Significant Hazards Evaluation and Environmental Assessment.
3. Page Change Instructions, Revised Technical Specifications Pages, and Associated Marked-Up Pages.

Attachments:
1. Description of Plant Hatch Probabilistic Safety Assessment.
2. Probabilistic Safety Assessment Peer Certification Comments

cc: Southern Nuclear Operating Company
Mr. P. H. Wells, Nuclear Plant General Manager
Document Management - A2.001

U.S. Nuclear Regulatory Commission, Washington, D.C.
Mr. L. N. Olshan, Project Manager - Hatch

U.S. Nuclear Regulatory Commission, Region II
Mr. L. A. Reyes, Regional Administrator
Mr. J. T. Munday, Senior Resident Inspector - Hatch

State of Georgia
Mr. L. C. Barrett, Commissioner - Department of Natural Resources

Enclosure 1

Edwin I. Hatch Nuclear Plant
Request to Revise Technical Specifications:
Extension of Completion Times for Inoperable Emergency Diesel Generators

Description of and Justification for Proposed Changes

I. Introduction and Background

A. Summary of Proposed Changes

Southern Nuclear Operating Company (SNC) proposes to revise the Plant Hatch Unit 1 and Unit 2 Technical Specifications requirements for an inoperable emergency diesel generator (DG). The change extends the Completion Time for an inoperable 1A, 1C, 2A, or 2C DG from 72 hours to a maximum of 14 days and extends the Completion Time for an inoperable 1B DG (the swing DG) from 7 days to 14 days.

Additionally, the proposed extension of the Completion Time to 14 days for an inoperable DG results in a corresponding extension of the time period associated with discovery of failure to meet Limiting Condition for Operation (LCO) 3.8.1 from 10 days to 17 days.

The proposed changes will provide operational flexibility allowing more efficient application of plant resources to safety significant activities. The proposed changes will allow performance of periodic DG overhauls on line, reduce plant refueling outage duration and improve DG availability during shutdown.

The proposed changes are described below. The marked-up and proposed Technical Specifications pages and Bases pages are provided in Enclosure 3.

B. Description of the Current Requirements

Technical Specifications Section 3.8.1 addresses the requirements for alternating current (AC) sources including the DGs, when operating. Currently, each unit's Technical Specifications allow continued plant operation for 72 hours with an inoperable A or C DG, and 7 days for an inoperable 1B DG (the swing DG).

Additionally, Technical Specifications Section 3.8.1 limits continued plant operation to a maximum of 10 days from discovery of a failure to meet LCO 3.8.1.

C. Bases for the Current Requirements

The current Completion Times associated with inoperable A and C DGs are intended to minimize the time an operating plant is exposed to a reduction in the number of available AC power sources. Nuclear Regulatory Commission (NRC) Regulatory Guide 1.93, "Availability of Electric Power Sources," December 1974, provides operating guidance (i.e., Completion Times) that the NRC considers acceptable if the number of available AC power sources are less than the LCO. Specifically, "if the available ac power sources are one less than the number required by the LCO, power

operation may continue for a period that should not exceed 72 hours if the system stability and reserves are such that a subsequent single failure (including a trip of the unit's generator, but excluding an unrelated failure of the remaining offsite circuit if this degraded state was caused by the loss of an offsite source) would not cause total loss of offsite power." Regulatory Guide 1.93 also states the following: "The operating time limits delineated [in regulatory positions C.1 through C.5] are explicitly for corrective maintenance activities only. The operating time limits should not be construed to include preventive maintenance activities which require the incapacitation of any required electric power source." Therefore, per this guide, preventive maintenance for a DG should be scheduled for performance during cold shutdown and/or refueling periods.

The 72 hour Completion Time for an A or C DG takes into account the capacity and capability of the remaining AC sources, a reasonable time for repairs, and the low probability of a Design Basis Accident (DBA) occurring during this period. The 7 day Completion Time for the swing DG also takes into consideration the fact that the DG is common to both units, and that time must be provided to perform routine maintenance on the DG without requiring a dual unit shutdown.

The 10 day Completion Time establishes a limit on the maximum time allowed for any combination of required AC power sources to be inoperable during any single contiguous occurrence of failing to meet the Technical Specifications.

II. Proposed Technical Specifications Changes

A. Description of the Proposed Changes

The proposed Technical Specifications changes are as follows.

1. Change Specification 3.8.1, Required Action A.3, second Completion Time for restoration of a required offsite circuit to OPERABLE status from "10 days from discovery of failure to meet LCO 3.8.1.a, b, or c" to "17 days from discovery of failure to meet LCO 3.8.1.a, b, or c."

2. Change Specification 3.8.1, Required Action B.4, first Completion Time for restoration of a unit's A or C DG from "72 hours for a Unit 1[2] DG" to "72 hours for a Unit 1[2] DG with the swing DG not inhibited AND 14 days for a Unit 1[2] DG with the swing DG inhibited from automatically aligning to Unit 2[1]."

3. Change Specification 3.8.1, Required Action B.4, second Completion Time for restoration of the swing DG from "7 days for the swing DG" to "14 days for the swing DG."

4. Change Specification 3.8.1, Required Action B.4, third Completion Time for restoration of a unit's A or C DG or the swing DG from "10 days from discovery of failure to meet LCO 3.8.1.a, b, or c" to "17 days from discovery of failure to meet LCO 3.8.1.a, b, or c."

5. Change Specification 3.8.1, Required Action C.4, Completion Time for restoration of a required other unit's DG from "7 days" to "7 days with the swing DG not inhibited AND 14 days with the swing DG inhibited from automatically aligning to Unit 1[2]."

Additionally, the Bases for each of the Technical Specifications revisions are changed accordingly.

B. Need for Revision of the Requirements

The proposed changes are consistent with NRC policy and will continue to provide adequate protection of public health and safety and common defense and security as described below. The changes advance the objectives of the NRC's Probabilistic Risk Assessment (PRA) Policy Statement, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," Federal Register, Volume 60, p. 42622, August 16, 1995, for enhanced decision-making and result in a more efficient use of resources and reduction of unnecessary burden. Implementation of this proposed Completion Time extension will provide the following benefits.

1. Avert unplanned plant shutdowns and minimize the potential need for requests for Notice of Enforcement Discretion. Risks incurred by unexpected plant shutdowns can be comparable to and often exceed those associated with continued power operation.

2. Allow increased flexibility in the scheduling and performance of DG preventive maintenance.

3. Allow better control and allocation of resources. Allowing on-line preventive maintenance, including overhauls, provides the flexibility to focus more quality resources on any required or elected DG maintenance.

4. Improve DG availability during shutdown Modes or Conditions. This will reduce the risk associated with DG maintenance and the synergistic effects on risk due to DG unavailability occurring at the same time as other various activities and equipment outages that occur during a refueling outage.

5. Permit scheduling of DG overhauls within the requested 14-day Completion Time period.

The proposed Completion Time of 14 days for a DG is adequate to perform normal preventive DG inspections and maintenance requiring disassembly of the DG and to perform post-maintenance and operability tests required to return the DG to operable status. It is intended that the proposed 14 day Completion Time for performing a major overhaul of a DG be used at a frequency of no more than once per DG per operating cycle. The time periods to complete unplanned maintenance shall continue to be minimized. Plant configuration changes for planned and unplanned maintenance of the DGs as well as the maintenance of equipment having risk significance are managed by site procedure.

III. Evaluation of Proposed Changes

Plant Hatch, Units 1 and 2, have a total of five DGs, two per unit and one shared. There are three 4160 volt Class 1E safety buses on each unit. Each unit's 4160 volt buses E and G have a dedicated DG. The 4160 volt F bus on each unit share a common DG. The logic is preselected to a particular plant unit to cover simultaneous undervoltage conditions on both 4160 volt F buses. This accounts for the dual unit loss of offsite power (LOSP) case. The shared DG whether selected to that unit or not will go to the under voltage 4160 volt F bus during single unit LOSP or loss of an individual 4160 volt F bus. If during dual unit F bus undervoltage or LOSP, one plant unit also has a LOCA signal, the shared DG will go to that unit.

The proposed changes have been evaluated to determine that current regulations and applicable requirements continue to be met, that adequate defense-in-depth and sufficient safety margins are maintained, and that any increase in core damage frequency (CDF) and large early release frequency (LERF) is small and consistent with the NRC Safety Goal Policy Statement, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," Federal Register, Volume 60, p. 42622, August 16, 1995.

The justification for the use of an extended inoperable DG Completion Time is based upon a risk-informed and deterministic evaluation consisting of three main elements: 1) the availability of the normal and alternate offsite power sources via the startup auxiliary transformers (SATs), 2) verification that the other DGs and offsite power sources are operable, and 3) incorporation of the additional requirements in the existing site procedure for configuration risk management while a DG is in an extended Completion Time. This site procedure is used for DG work as well as other work and helps ensure that there is no significant increase in the risk of or consequences of an event while any DG maintenance is performed. These elements provide the bases for the proposed TS change by providing a high degree of assurance that power can be provided to the Engineered Safety Feature (ESF) buses during all DBAs and other analyzed events.

A. Defense-in-Depth

The impact of the proposed TS changes were evaluated and determined to be consistent with the defense-in-depth philosophy. The defense-in-depth philosophy in reactor design and operation results in multiple means to accomplish safety functions and prevent release of radioactive material.

Plant Hatch Units 1 and 2 are designed and operated consistent with the defense-in-depth philosophy. The Class 1E AC electrical power distribution system AC sources consist of the offsite power sources (preferred power sources, normal and alternate), and the onsite standby power sources (DGs). The design of the AC electrical power system provides independence and redundancy to ensure an available source of power to the ESF systems. The Class 1E AC distribution system is divided into redundant load groups, so loss of any one group does not prevent the minimum safety functions from being performed. Each load group has connections to two preferred offsite power supplies and a single DG. Since the Station has diverse power sources available to cope with a loss of the preferred AC, the overall availability of the AC power sources to the ESF buses will not be reduced significantly as a result of increased on-line

preventive maintenance activities. It is therefore acceptable, under controlled conditions, to extend the Completion Time and perform on-line maintenance intended to maintain the reliability of the onsite emergency power systems. A summary of defense-in-depth relative to station AC power sources is provided in the following table.

Summary of Defense-In-Depth for Plant Hatch, Units 1 and 2

Power Supplies	Station AC Power Available Sources		
	4160 v ESF bus 1[2]E	4160 v ESF bus 1[2]F	4160 v ESF bus 1[2]G
Normal preferred	SAT 1[2]D	SAT 1[2]D	SAT 1[2]D
Alternate preferred	SAT 1[2]C	SAT 1[2]C	SAT 1[2]C
Standby	DG 1[2]A	DG 1B	DG 1[2]C

While the proposed changes do increase the length of time a DG can be out-of-service during unit operation, it will also increase the availability of the DGs while either unit is shutdown. Even with one DG out-of-service during operation, the system is designed with adequate defense-in-depth. The increased availability of the DG while shutdown will increase the systems defense-in-depth during outages. Even with one DG out-of-service there are multiple means to accomplish safety functions and prevent release of radioactive material. The Hatch Nuclear Plant Probabilistic Safety Assessment (PSA) supports the results of the deterministic analysis (i.e., the adequacy of defense-in-depth). It also supports the contention that protection of the public health and safety is ensured.

System redundancy, independence, and diversity are maintained commensurate with the expected frequency and consequences of challenges to the system. As demonstrated below there are no risk outliers. Implementation of the proposed changes will be done in a manner consistent with the defense-in-depth philosophy. Station procedures will ensure consideration of prevailing conditions, including other equipment out-of-service, and implementation of compensatory actions to assure adequate defense-in-depth whenever the DGs are out-of-service. In addition, appropriate personnel are trained on the operation and maintenance of the DGs and the 4160 volt electrical distribution system.

No new potential common cause failure modes are introduced by these proposed changes, and protection against common cause failure modes previously considered is not compromised.

Independence of physical barriers to radionuclide release is not affected by these proposed changes.

B. Availability of the Offsite Power System

Offsite power is supplied to the 230 kV and 500 kV switchyards from the transmission network by eight transmission lines, four per high voltage switchyard. The switchyards are connected by an autobank transformer. From the 230 kV switchyard, two electrically and physically separated circuits provide AC power, through SATs 1[2]C and 1[2]D, to 4160 volt ESF buses 1[2]E, 1[2]F, and 1[2]G. SAT 1[2]D provides the normal source of power to the ESF buses 1[2]E, 1[2]F, and 1[2]G. If any 4160 volt ESF bus loses power, an automatic transfer from SAT 1[2]D to SAT 1[2]C occurs. At this time station service 4160 volt buses 1[2]A and 1[2]B supply breakers from SAT 1[2]C also trip open, if closed, disconnecting all nonessential loads from SAT 1[2]C to preclude overloading of the transformer.

SATs 1[2]C and 1[2]D are sized to accommodate the simultaneous starting of all required ESF loads on receipt of an accident signal without the need for load sequencing. However, ESF loads are sequenced when the associated 4160 volt ESF bus is supplied from SAT 1[2]C.

In summary, the offsite power system consists of independent transmission lines into the switchyard and two independent circuits into each unit. A single loss of an incoming transmission line, switchyard breaker, transmission tower, SAT or circuit into the plant will not result in unavailability of offsite power.

C. Availability of the On-Site Power System

Plant Hatch has a total of five DGs, one dedicated to each of the 1E, 1G, 2E, and 2G 4160 volt buses and a swing DG that can provide power to either 4160 volt bus 1F or 4160 volt bus 2F. A DG starts automatically on a loss of coolant accident (LOCA) signal (i.e., low reactor water level signal or high drywell pressure signal) or on an ESF bus loss of voltage signal. After the DG has started, it automatically ties to its respective bus as a consequence of ESF bus loss of voltage, independent of or coincident with a LOCA signal. The DGs also start and operate in the standby mode without tying to the ESF bus on a LOCA signal alone. Following the trip of offsite power, load shed relays strip nonpermanent loads from the ESF bus. When the DG is tied to the ESF bus, loads are then sequentially connected to its respective ESF bus by the automatic load sequence timing devices. The sequencing logic controls the permissive and starting signals to motor breakers to prevent overloading the DG.

In the event of a loss of preferred power, the ESF electrical loads are automatically connected to the DGs in sufficient time to provide for safe reactor shutdown and to mitigate the consequences of a DBA such as a LOCA.

Due to the redundancy of the unit's ESF divisions and DGs, the loss of any one of the DGs will not prevent the safe shutdown of the unit. The total standby power system, including DGs and electrical power distribution equipment, satisfies the single failure criterion.

D. Station Blackout DG Capacity

The Hatch Nuclear Plant is able to withstand and recover from a station blackout (SBO) event of four hours in accordance with 10 CFR 50.63, "Loss of all alternating current power." A SBO occurs as a result of a dual unit LOSP in conjunction with a loss of onsite AC power, failure of the 1A, 1C, 2A, and 2C DGs. The 1B DG is classified as "Alternate AC" power source, providing additional safety margin for Plant Hatch as compared to those plants with no alternate AC source. Since the allowed Completion Time for an out-of-service DG is not considered in the SBO analysis, the proposed changes do not effect the Hatch Nuclear Plant SBO analysis.

E. Other Considerations

As discussed in the previous section, conformance with relevant regulatory guidance is not affected by this proposed change, with the exception of Regulatory Guide 1.93. The proposed changes do not affect any assumptions or inputs to the safety analyses. The proposed changes have no impact on the availability of the two offsite sources of power. The effect on the Updated Final Safety Analysis Report (UFSAR) acceptance criteria has been assessed assuming that one DG is out-of-service and no additional failures on the maintenance unit occur. All safety functions continue to be available and acceptance criteria are met.

The enclosed PSA analysis does necessitate procedural changes that impact the operability of the 1B DG on the non-maintenance unit while utilizing the extended Completion Time for an A or C DG. To ensure the availability of two DGs per unit, when an A or C DG is to be inoperable in excess of 72 hours, the 1B DG must be affixed to that unit with the inoperable DG. This means that the 1B DG will be inhibited from an automatic swap to the opposite unit when that unit (the non-maintenance unit) experiences an undervoltage condition on its F 4160 volt bus, regardless of the presence or absence of a LOCA signal. Inhibiting the automatic transfer makes the 1B DG inoperable for the non-maintenance unit, with a Completion Time of 14 days. However, unavailability of a single DG on each unit does not reduce the number of DGs below the minimum required to mitigate all analyzed events.

F. Evaluation of Risk Impact

Risk informed input for these proposed changes is based on a Hatch Nuclear Plant PSA. The PSA is used to quantify the change in CDF and LERF produced by the extended Completion Time for the DGs. Other deterministic techniques are being implemented to minimize any risk impact. These deterministic techniques include: (1) implementation of the configuration risk management site procedure to control performance of other high risk tasks during the DG outage, and (2) consideration of specific compensatory measures to minimize risk.

The evaluation of quantitative risk was performed using the figures of merit from Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment In Risk-Informed Decisions On Plant-Specific Changes to the Licensing Basis," and Regulatory Guide 1.177, "An Approach for Plant-Specific, Risk-Informed Decision making: Technical Specifications." The Hatch PSA models CDF and LERF

separately, although LERF is actually a subset of the core damage cutsets, with the exception of interfacing systems LOCA and break outside containment. These cutsets are those that lead to reactor vessel failure and subsequent containment failure. The models are used to provide quantitative results to compare to the Regulatory Guide information.

For the analysis performed in support of this amendment request, the Regulatory Guide 1.174 criterion for low risk significance (less than or equal to 1E-06) is met for ΔCDF. The value for ΔLERF is slightly above the 1E-07 guidance, but with an average LERF value in the E-06 range, it is still considered acceptable. The guidance of Regulatory Guide 1.177 is easily met for Incremental Conditional Core Damage Probability (ICCDP). The Incremental Conditional Large Early Release Probability (ICLERP) values are slightly higher than the guidance of 5.0E-08; however, this should be considered acceptable because of the extremely small value that 5.0E-08 represents. A discussion of a significant reason for the LERF result follows.

Station blackout cutsets provide a significant contribution to LERF. Modeling for recovery of the offsite electric grid during blackout conditions is partially a function of station battery life, which is slightly greater than two hours without charging capability. This timing is consistent with the UFSAR and SBO coping analysis as well as very conservative battery load calculations. Battery load based on the PSA case, which primarily considers reactor core isolation cooling (RCIC) operation as the largest load, is not as extreme as the loading calculations consider. It is therefore possible that battery life under PSA model conditions could approximate four hours. The extra time for RCIC operation provides core coverage while decay heat subsides. Loss of RCIC due to battery depletion after a time frame longer than 2 hours will help to prolong the period prior to core uncovery. Prolonging the period prior to core uncovery allows more time for offsite electric grid recovery, which would ultimately reduce cutset worth. Battery life in general under actual blackout conditions would also depend on conservation measures. One example would be associated with the actual number of times that RCIC is started and shutdown. This in turn would depend on how high the water level was allowed to go initially. Present calculations use the conservative approach of RCIC cycling between its high level shutoff and its low level start point. The repeated cycling uses battery capacity and, in reality, could be controlled. This level of detail and its consequential affects on the battery system is not included in the PSA model. It is believed that it is proper in this case to follow the conservative analysis associated with the UFSAR. This is one reason that LERF values exceed the guidance criteria. The fact that two ICLERP values are still in the E-08 range shows, however, that the Hatch LERF PSA model is not overly conservative. In fact, the model is built on sound engineering basis consistent with pertinent plant analyses.

The proposed methods of evaluating risk during maintenance and the proposed revision to the site procedure for configuration risk management are designed to control and minimize the calculated risk involved with this Completion Time extension.

The overall risk evaluation for this proposed Completion Time extension for each inoperable Plant Hatch DG is based on the following three-tier approach described in Regulatory Guide 1.177:

- Tier 1: PSA Capability and Insights,
- Tier 2: Avoidance of Risk-Significant Plant Configurations, and
- Tier 3: Risk-Informed Configuration Risk Management.

1. Tier 1: PSA Capability and Insights

   The quantified risk impact associated with this proposed DG Completion Time extension was evaluated using the Plant Hatch Unit 1 Revision 1 PSA "At Power" model. Results from this model are directly applied to Unit 2 because of the high degree of similarity between the Hatch Plant units. A unit comparison follows with the associated PSA model impact discussed.

   The major differences in Plant Hatch units are that Unit 2 has one more feedwater heater than does Unit 1 and Unit 2 has an intermediate chill water system for drywell cooling whereas the Unit 1 drywell is cooled by plant service water. Drywell cooling ultimately provides the same general thermodynamic results on both plant units because the Unit 1 drywell coolers are twin-fan units as opposed to single fan units on Unit 2. Unit 1 has more circulating water cooling tower fans per tower than Unit 2, 12 versus 10. These items make little difference in the quantified risk values.

   There is a difference between units in the failure modes of the station service air compressor outlet valves in a loss of power event. It is insignificant in average risk because pertinent portions of instrument air are backed up by nitrogen. The main control room is shared between plant units and has a common three independent unit air-conditioning system. Both plant unit PSA models include this system for completeness. River water intake structure traveling water screens share plant unit plant service water spray wash supplies. This is likewise depicted in both PSA models. The swing diesel generator has its ability to seek undervoltage, as well as transfer to the plant unit with a LOCA signal during dual unit LOSP, referenced in both PSA models. Low pressure coolant injection (LPCI) buses are supplied normally from the opposite plant unit 600VAC emergency buses; this is likewise modeled in both PSAs. Actually, individual plant unit PSA models serve as a convenience for computerized on-line risk monitoring. For normal risk work it is common to use a single unit PSA model for representing both units because the results tend to be very close. This is the case for this analysis.

   The Hatch PSA models CDF and LERF as separate models. LERF is actually a subset of the core damage cutsets that are evaluated for leading to vessel failure and subsequent containment failure. The containment is bypassed prior to core damage, however, for interfacing systems LOCA and break outside containment events. These models are used to provide quantitative results to compare to the Regulatory Guide information.

Evaluations for the risk associated with this proposed amendment were therefore performed using the following:

- Internal Events using the Plant Hatch "At Power" PSA,
- Low Power / Shutdown Risk discussed qualitatively,
- Internal Flooding using the Plant Hatch "At Power" PSA,
- Seismic Events using qualitative discussion based on the Plant Hatch Seismic Margins Analysis, and
- Internal Fires using the Plant Hatch Fire PSA.

The Plant Hatch PSA is the second revision (Rev.1) to a Linked Fault Tree model based on CAFTA software. The original Individual Plant Examination (IPE) model was a Linked Event Tree model constructed with RISKMAN (trademark PLG, Inc.) software. The major differences between the revisions are in the way Success Paths and support systems are handled and the physical structure of the model. The Linked Fault Tree evaluates failure paths only and has all Top Events (i.e., Containment Heat Removal, Pressure Control, etc.) tied directly to all supporting features to form one large failure model. Several changes were made during the conversion from RISKMAN to CAFTA, primarily in the LERF model. The end result was a decrease in overall CDF and LERF values. Many changes are attributed to the ease in modeling support features in Linked Fault Tree Models, as opposed to using text rules in Linked Event Trees to describe the use of split fractions created for extra support features. In addition success terms are mathematically accounted for during quantification in Linked Event Tree models. Linked Fault Tree models accomplish this in initial construction such that only failure cutsets are quantified.

In theory both forms of modeling should yield similar results, and in the Plant Hatch initial conversion, CDF differences were not that large considering the addition of extra support for the CAFTA model (2.0E-5 versus 1.6E-5 for CAFTA).

Information regarding the CAFTA model and its comparison to the IPE model was sent to the NRC in response to Request for Additional Information (RAI) questions regarding the Severe Accident Mitigation Analysis (SAMA) portion of the License Renewal effort. Attachment 1 provides basic information regarding the Unit 1 Hatch Revision 1 PSA model construction and quantification. Changes between Revision 1 and Revision 0 were primarily to remove analysis flags, make additions to the Mutually Exclusive File for certain maintenance events that could not occur "on-line", and to add a Recovery Tree vice a text file. The reduction in CDF and LERF from Revision 0 (1.6E-5) to Revision 1(1.2E-5) is primarily attributed to an update of the Initiating Event data using NUREG/CR-5750, Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995. The Plant Hatch PSA is a very detailed model with very detailed electrical support structure. It includes many

options available to the plant for electrical alignment that will be used in this Completion Time extension model. A discussion of PSA quality is included in Attachment 2.

a.1 Internal Events Evaluation

a.1 Definitions

The guidance documented in Regulatory Guides 1.174 and 1.177 was used to evaluate the risk impact of the requested 14 day Completion Time for each Plant Hatch DG. The following information defines the terms used in the Plant Hatch calculation.

Regulatory Guide 1.174

ΔCDF = CDF(New Base) – CDF(Base)

ΔCDF

This value shows the difference or change in average quantified Core Damage Frequency based on conservative new values for DG maintenance unavailabilities as opposed to the presently used values. This value is designed to show the average risk difference in increasing the Completion Time for each DG from its present value to 14 days.

CDF(New Base)

This value is the quantified average Core Damage Frequency considering conservative versions of new DG maintenance unavailabilities. The new DG maintenance term considers the potential for DG work being done while the plant units are "At Power."

CDF(Base)

This value is the average Core Damage Frequency quantified using the present DG maintenance unavailabilities.

ΔLERF = LERF(New Base) – LERF(Base)

ΔLERF

This value shows the difference or change in average quantified Large Early Release Frequency based on conservative new values for DG maintenance unavailabilities as opposed to the presently used values. This value is designed to show the average risk difference in increasing the Completion Time for each DG from its present value to 14 days.

LERF(New Base)

This value is the same as CDF(New Base) except it is only for Large Early Release Frequency.

LERF(Base)

This value is the Large Early Release Frequency quantified using the present DG maintenance unavailabilities.

Regulatory Guide 1.177

ICCDP = [CDF(New AOT) – CDF(New Base)] × (14Days ÷365Days)

ICCDP

Incremental Conditional Core Damage Probability is designed to show the increase in probability for core damage under the condition that one DG is out of service for maintenance for 14 days.

CDF(New AOT-A Diesel)

This is the instantaneous Core Damage Frequency for either the Unit 1 or Unit 2 "A" DG being out of service. This value is quantified with certain stipulations that will become part of the configuration risk management plant procedure.

CDF(New Base)

This term was explained previously.

CDF(New AOT-B Diesel)

This is the instantaneous Core Damage Frequency for the "B" DG being out of service. This value is quantified with certain stipulations that will become part of the configuration risk management plant procedure.

CDF(New AOT-C Diesel)

This is the instantaneous Core Damage Frequency for either the Unit 1 or Unit 2 "C" DG being out of service. This value is quantified with certain stipulations that will become part of the configuration risk management plant procedure.

ICLERP = [LERF(New AOT) – LERF(New Base)] × (14Days ÷365Days)

ICLERP

Incremental Conditional Large Early Release Frequency is designed to show the increase in probability for Large Early Release Fraction under the condition that one DG is out of service for maintenance for 14 days.

LERF(New AOT-A Diesel)

This is the instantaneous Large Early Release Frequency for either the Unit 1 or Unit 2 "A" DG being out of service. This value is quantified with certain stipulations that will become part of the configuration risk management plant procedure.

LERF(New Base)

This term was explained previously.

LERF(New AOT-B Diesel)

This is the instantaneous Large Early Release Frequency for the "B" DG being out of service. This value is quantified with certain stipulations that will become part of the configuration risk management plant procedure.

LERF(New AOT-C Diesel)

This is the instantaneous Large Early Release Frequency for either the Unit 1 or Unit 2 "C" DG being out of service. This value is quantified with certain stipulations that will become part of the configuration risk management plant procedure.

a.2 Methodology

In order to perform these calculations Plant Hatch PSA was evaluated for its ability to strictly support the DG Completion Time extension. The present overall CDF and LERF numbers are sufficient to support the now-in-use Completion Times as well as typical maintenance. These numbers are based on Revision 1 to the Unit 1 PSA model.

Revision 1 to the PSA removed a DG non-recovery factor and also combined selected electric power grid non-recovery factors to simplify calculations. This was and still is considered conservative and useful for all present applications. Consideration of the extremely low LERF values in Regulatory Guide 1.177 forced a reinstatement of the original DG non-recovery factor. In addition, it necessitated using electric power grid non-recovery factors as they were originally used in the IPE. This in effect allows for a more reasonable calculation for the specifics of a DG extended Completion Time. The present LERF model is considered adequate

and a good representation of such conditions for Hatch, but it functions with data based on shorter Completion Times (i.e., 3 days for either DG A or C and 7 days for the B DG). The additions of a DG non-recovery factor and reinstatement of separated electric power grid non-recovery factors are considered to be an appropriate approach for this proposed Completion Time extension.

The DG non-recovery factor is based on actual review of the DG failure data and has procedural backup. There is proceduralized operator direction for emergency recovery of diesels which fail to start. This, as well as data history, support the probability of recovering a DG start failure.

Hatch PSA grid non-recovery factors, GRA2&3 and GRB2&3, were reexamined for this extended Completion Time application. Originally these factors were separated into GRA2, GRA3, GRB2, and GRB3. The numbers associated with the GR terms refer to a RISKMAN multi-state top event that partitioned sequences as to when the offsite power grid would be recovered. State 1 or 1 referred to the conditions that allowed offsite power recovery prior to core damage (i.e., Success); State 2 or 2 referred to recovery of offsite power after core damage had occurred but prior to vessel failure (i.e., this helped to separate CDF and LERF sequences during LOSP). State 3 or 3 referred to non-recovery of offsite power prior to core damage and subsequent vessel failure (i.e., this helped define LERF sequences). The GR values were calculated as a function of time, DG availability, generic off-site grid recovery data, and reactor vessel water level inventory using (or not using) the battery powered RCIC system. During the conversion from RISKMAN Event Tree modeling to CAFTA Fault Tree modeling, it was convenient to add the GRA 2 and 3 numbers together and add the GRB 2 and 3 numbers together as well. This conservatism was carried over to the LERF model because the difference in values for GRA2&3 and GRB2&3, vice GRA3 and GRB3, was not very large. The simplification in quantification and recovery rules, especially in using a Recovery Tree to provide quantification speed, was well worth the small conservatism. In addition the LERF overall values were still in the low E-06 range. In order to revert back to the original non-recovery factor separation, the values for GRA3 and GRB3 were applied in the LERF cutset files in place of GRA2&3 and GRB2&3 for LOSP events. LERF cutsets are a subset of CDF cutsets that go to State 3 or vessel failure and from this point containment failure (i.e., offsite power recovery is not addressed until after vessel failure).

The DG non-recovery factor and the grid non-recovery factors were applied in base cases as well as new Completion Time cases in order to make like comparisons of frequency values.

The third item used in the methodology was a modified maintenance unavailability for each DG. These numbers allowed for previewing the change in average risk due strictly to an extended DG out of service time considered over an operating cycle. The ICCDP and ICLERP calculations used the new maintenance unavailabilities in the CDF(New Base) and LERF(New Base) portions of the equations. The CDF(New AOT) and LERF(New AOT) are obtained by setting maintenance to True on the specific DG in question and False on the other two, and

as a result, did not require the new maintenance unavailabilities. The calculation for the new maintenance unavailabilities will be discussed later in this report.

Additionally, risk significant maintenance (i.e., evaluated to a cutset frequency of 5E-10) was removed in the specific cases for CDF (New AOT) and LERF (New AOT) which addressed individual DGs being removed from service for the new Completion Time. This was accomplished in the specific cutset reports by setting these maintenance terms to 0.0. Maintenance regarding battery charger swapping and Analog Transmitter Trip System (ATTS) surveillance was left as is. This models the changes to the configuration risk management plant procedure that will ensure no risk significant planned maintenance is in progress on a plant unit when a DG on either unit is scheduled to be out for planned maintenance.

In order to perform the calculations the following key assumptions are made:

- The swing DG is aligned to one plant unit. Normal conditions allow, if aligned to one unit, the swing DG to go to the opposite unit if there is undervoltage on the opposite unit's F 4160VAC Bus. If there is undervoltage on both units' buses, it will go to the 4160VAC F bus on the plant unit to which the B DG Mode Selection switch is selected. Its ability to align on undervoltage is affixed for purposes of this Completion Time to a single unit. The ability of the B DG to transfer to an opposite plant unit during dual unit LOSP when the opposite unit has a LOCA signal is likewise impaired. This means that when A or C DG is out for planned maintenance on a plant unit, the B DG is affixed for the undervoltage condition to that unit. The opposite unit's LOCA signal, which could cause the B DG to transfer during a dual unit LOSP, is likewise inoperative for the transfer only. These requirements to affix the B DG to the maintenance unit and to inhibit the auto transfer to the other unit will be included in the configuration risk management plant procedure.

- The Reactor Protection System (RPS) Alternate Power "Throwover" switch controls the location of the alternate source of AC power for the RPS system. It can be aligned to essential bus 1R25S036 or 1R25S037, which are ultimately powered from 600 volt emergency buses C and D respectively. The PSA models are sensitive to loss of 600 volt emergency bus initiators, and as such, location of the Throwover Switch can easily modify CDF and LERF. For CDF and LERF average cases (Base and New Base), the Throwover Switch is set to be on one side 50% of the time and the other side for the remainder. There is procedural guidance for side selection, but considering various other maintenance and the possibility of new on-line maintenance affiliated with the DGs, the 50/50 selection is appropriate. For the cases of CDF(New AOT) and LERF(New AOT), the "Throwover Switch" is selected to the opposite side from the 600 volt buses powered by the DG in maintenance. This particular switch alignment will also be part of the configuration risk management plant procedure.

a. Maintenance Probability Calculation

The basic change in risk for this proposed DG Completion Time concerns the potential for a DG being out of service with the plant units "At Power" for a time frame longer than is presently allowed. This out of service time is presumed to be affiliated with planned maintenance. Random failure probabilities were not adjusted for these calculations. In order to calculate the differential risk associated with this potential maintenance, a conservative evaluation of a new set of maintenance probabilities for each DG was performed. These probabilities are used only for calculational purposes for this extended Completion Time and are expected to actually be lower; however, actual evaluation will not be possible until some time after implementation of the extended Completion Time. The methodology is based on an 18/24 month operating cycle with an average of 1500 hours per cycle allotted for forced and planned plant outages. (Basing the methodology on 18 month cycles is conservative with respect to 24 month cycles, which are currently under consideration at Hatch.)

Presently, a conservative value allotted for plant outage maintenance on either plant unit's A or C DG is 7 days per outage per DG. Due to the differences in Technical Specification allotments for the B DG as compared to the other DGs, allotted plant outage maintenance on the B DG is 4 days.

This information is applied as follows to produce the new maintenance terms.

Present Maintenance Probabilities for Units 1 and 2 DGs
A DG = 5.51E-03
B DG = 7.205E-03
C DG = 5.51E-03

For an 18 Month (1.5 Years) Operating Cycle
1500 hours allotted for forced and planned outages during the operating cycle.
(365Days÷1Year) × (1Year) × (24Hours÷1Day) = 8760Hours
[1.5Years ×(8760Hours÷1Year)] – 1500Hours = **1.164E+04Hours**

7 Day Outage Time is allotted for A DG and C DG during present planned outages.
4 Day Outage Time is allotted for B DG during present planned outages.
7 Days × (24Hours÷1Day) = 168Hours
4 Days × (24Hours÷1Day) = 96Hours

168Hours÷1.164E+04Hours = 1.44E-02
96Hours÷1.164E+04Hours = 8.247E-03

Proposed Maintenance Term for A DG
5.51E-03 + 1.44E-02 = 2.0E-02
Proposed Maintenance Term for B DG
7.205E-03 + 8.247E-03 = 1.545E-02
Proposed Maintenance Term for C DG
2.0E-02

Note: Availability is addressed as follows:
A and C DGs $1 - 2.0E\text{-}02 \cong 98\%$
B DG $1 - 1.545E\text{-}02 \cong 98.5\%$

These numbers are considered conservative since on-line maintenance is completed as expeditiously as possible.

a.4 Calculation Results

Table 1 provides the maintenance unavailability values, present and proposed, used in this calculation.

Table 2 provides the values for each defined term under the Evaluation Approach, Definitions section of this proposal.

Table 3 shows the calculations.

Table 4 shows the results of the calculations with comparison to the Regulatory Guide metrics.

Table 1: DG Unavailabilities

DG	Present Unavailability	Completion Time Unavailability
Unit 1 A (1R43S001A)	5.51E-03	2.0E-02
Unit 1 C (1R43S001C)	5.51E-03	2.0E-02
Unit1/2 B (1R43S001B)	7.2E-03	1.545E-02
Unit 2 A (2R43S001A)	5.51E-03	2.0E-02
Unit 2 C (2R43S001C)	5.51E-03	2.0E-02

Table 2: Values of Calculation Terms

Term	Value
CDF (Base)	1.11E-05
CDF (New Base)	1.14E-05
LERF (Base)	1.42E-06
LERF (New Base)	1.602E-06
CDF (New AOT-A DG)	1.137E-05
CDF (New AOT-B DG)	1.249E-05
CDF (New AOT-C DG)	1.455E-05
LERF (New AOT-A DG)	3.94E-06
LERF (New AOT-B DG)	4.02E-06
LERF (New AOT-C DG)	4.61E-06

Table 3 Calculations

ΔCDF = CDF(New Base) – CDF(Base)
ΔCDF = 1.14E-05 – 1.11E-05
ΔCDF = 3.0E-07

ΔLERF = LERF(New Base) – LERF(Base)
ΔLERF = 1.602E-06 – 1.423E-06
ΔLERF= 1.79E-07

A DG in maintenance
ICCDP = [1.14E-05 – 1.14E-05] × (14÷365)
ICCDP < 1.0E-08
Note: This result is expected because DG worth for CDF is limited. In reality it is unnecessary to remove maintenance terms from the cutsets representing CDF(New AOT-A DG).

B DG in maintenance
ICCDP = [1.249E-05– 1.14E-05] × (14÷365)
ICCDP = 4.18E-08

C DG in maintenance
ICCDP = [1.455E-05 – 1.14E-05] × (14÷365)
ICCDP = 1.208E-07

A DG in maintenance
ICLERP = [3.94E-06 – 1.602E-06] × (14÷365)
ICLERP = 8.967E-08

B DG in maintenance
ICLERP = [4.02E-06 – 1.602E-06] × (14÷365)
ICLERP = 9.27E-08

C DG in maintenance
ICLERP = [4.61E-06 – 1.602E-06] × (14÷365)
ICLERP = 1.15E-07

Table 4: Results	
Regulatory Guide 1.174 Comparison	
Reg. Guide 1.174 Guidance	**Actual Value for AOT**
ΔCDF = 1.0E-06	**ΔCDF = 3.0E-07**
ΔLERF = 1.0E-07	**ΔLERF = 1.79E-07**
Regulatory Guide 1.177 Comparison	
Reg. Guide 1.177 Guidance	**Actual Value for AOT**
ICCDP = 5.0E-07	**ICCDP (A DG) < 1.0E-08**
	ICCDP (B DG) = 4.18E-08
	ICCDP (C DG) = 1.208E-07
ICLERP = 5.0E-08	**ICLERP (A DG) = 8.967E-08**
	ICLERP (B DG) = 9.27E-08
	ICLERP (C DG) = 1.15E-07

a.5 Discussion of Results

The end result of these calculations shows that LERF values (ΔLERF and ICLERP) exceed the first level regulatory metrics (see Table 4). This in itself, however, does not make the results unacceptable. The guidance allows not only a range for consideration but also evaluates the applicants average CDF and average LERF, both of which are low for Plant Hatch.

Plant Hatch LERF numbers are heavily weighted to the LOSP initiator. LOSP places significant worth on DG availability and as a consequence, LERF values tend to increase when a DG is removed from service. Station blackout scenarios are the risk drivers in these cases. Recovery of offsite power for the blackout case in the PSA model is considered in conjunction with the availability of a high pressure steam driven injection source. If this battery powered source can keep the core covered, core damage and potential radioactive release are delayed. The Hatch model considers RCIC as that source. Like its counterpart, high pressure coolant injection (HPCI), it is powered from the Station Service Battery System. As mentioned in the FSAR SBO Analysis, as well as the description of the battery systems, approximately two hours are allotted for battery operation without chargers. The potential, however, for extended battery life (up to two hours longer) under PSA model circumstances exists because of the uncertainties associated with repeated RCIC operation and the conservatism applied to the battery loading calculations.

Another part of the weighting considers that Hatch uses two DGs per plant unit with a swing DG that ties to one unit or the other based on certain conditions. The probability of the swing DG maneuvering between units tends to support conservative LERF results because of the inability to absolutely assign it to one specific electrical bus. The dual unit LOSP initiator at Hatch is 1.89E-02 despite the fact that Hatch has never had such an event in many years of operation. The Hatch off site electric grid ties essentially consists of four offsite sources per plant unit connected by an autobank transformer. This particular arrangement is considered a very robust source of power.

ΔCDF and ICCDP are below the risk metrics discussed in the regulatory guidance. The CDF (New Base) numbers which reflect the conservative estimates for DG maintenance based on the proposed extended Completion Time, and the CDF (Base) numbers which reflect present DG maintenance numbers, are compared in Table 5. The end result of this comparison is that there is very little effect on initiating event contributions. Table 6 shows the comparison of LERF (New Base) and LERF (Base). The changes are minor.

Table 5

CDF (New Base) Initiator Contribution			
EVENT	**%CONTRIBUTION**	**FREQUENCY**	**EVENT DESCRIPTION**
%FL-LODC	26.5%	3.03E-06	Loss of Station Battery A
%LOSP	20.7%	2.36E-06	Loss of Site Power
%LOFW-CO	9.8%	1.11E-06	Loss of Feedwater Due to Loss of Condensate
%FL-BUSC	7.3%	8.28E-07	Loss of 600V Bus C
%FL-LOPSW	6.4%	7.28E-07	Loss of Plant Service Water
%TTRIP	4.2%	4.74E-07	Turbine Trip
%FL-DISCH	2.6%	3.01E-07	PSW Discharge Flowpath Failed
%FL-BUSD	2.5%	2.87E-07	Loss of 600V Bus D
%FL-LOMCHV	2.2%	2.5E-07	Loss of Main Control Room Air Conditioning
%SCRAM	2.1%	2.38E-07	Reactor Scram
%IORV	2.0%	2.26E-07	Inadvertently Opened SRV
Other Events	13.7%	1.6E-06	
Total	100%	1.14E-5	
CDF (Base) Initiator Contribution			
EVENT	**%CONTRIBUTION**	**FREQUENCY**	**EVENT DESCRIPTION**
%FL-LODC	27.4%	3.03E-06	Loss of Station Battery A
%LOSP	18.4%	2.04E-06	Loss of Site Power
%LOFW-CO	10.1%	1.11E-06	Loss of Feedwater Due to Loss of Condensate
%FL-BUSC	7.4%	8.19E-07	Loss of 600V Bus C
%FL-LOPSW	6.6%	7.28E-07	Loss of Plant Service Water
%TTRIP	4.3%	4.7E-07	Turbine Trip
%FL-DISCH	2.7%	3.01E-07	PSW Discharge Flowpath Failed
%FL-BUSD	2.6%	2.86E-07	Loss of 600V Bus D
%FL-LOMCHV	2.3%	2.5E-07	Loss of Main Control Room Air Conditioning
%SCRAM	2.0%	2.18E-07	Reactor Scram
%IORV	2.0%	2.26E-07	Inadvertently Opened SRV
Other Events	14.2%	1.60E-06	
Total	100%	1.11E-5	

Table 6 shows similar sensitivity results for LERF.

Table 6

LERF (New Base) Initiator Contribution			
EVENT	**%CONTRIBUTION**	**FREQUENCY**	**EVENT DESCRIPTION**
%LOSP	**56.7%**	**9.08E-07**	**Loss of Site Power**
%FL-BUSC	**10.8%**	**1.73E-07**	**Loss of 600V Bus C**
%FL-LOPSW	**6.6%**	**1.06E-07**	**Loss of Plant Service Water**
%VSEQ	**5.3%**	**8.50E-08**	**Interfacing Systems LOCA**
%FL-LODC	**4.8%**	**7.69E-08**	**Loss of Station Battery A**
%SCRAM	**4.6%**	**7.39E-08**	**Reactor Scram**
Other Events	**11.2%**	**1.79E-07**	
Total	**100%**	**1.602E-06**	
LERF (Base) Initiator Contribution			
EVENT	**%CONTRIBUTION**	**FREQUENCY**	**EVENT DESCRIPTION**
%LOSP	**52.2%**	**7.4E-07**	**Loss of Site Power**
%FL-BUSC	**11.9%**	**1.70E-07**	**Loss of 600V Bus C**
%FL-LOPSW	**7.4%**	**1.06E-07**	**Loss of Plant Service Water**
%VSEQ	**6.0%**	**8.50E-08**	**Interfacing Systems LOCA**
%FL-LODC	**5.4%**	**7.69E-08**	**Loss of Station Battery A**
%SCRAM	**4.5%**	**6.34E-08**	**Reactor Scram**
Other Events	**12.6%**	**1.787E-07**	
Total	**100%**	**1.42E-06**	

b. Low Power / Shutdown Risk

This amendment request is not applicable to operational Mode 4 (cold shutdown) and Mode 5 (refuel). Therefore, these operational conditions will not be evaluated.

The Internal Events review, although it considers Mode 1 or the "At Power" case, bounds Mode 2 (Startup/Hot Standby) and Mode 3 (Hot Shutdown). In these cases the reactor can be cold (just above 212°F) or in excess of 500 psig; each case, however, considers a shutdown reactor. Shutdown reactor water supply systems such as condensate are abundant. Their redundancy, required to keep an operating reactor at 100% power, makes this so. Consideration of the low pressure cases shows that there are several motor driven pumps capable of supplying the vessel with water. For the high pressure cases, there is an extra reactor feed pump, HPCI, RCIC, or the condensate booster pumps--the service of which depends on the particular reactor pressure. The transition from high pressure to low pressure sources is by normal means and is the same

as that modeled in the PSA for Mode 1. The overall difference is that there is a longer time frame allowed for depressurization because power or decay heat is not as demanding as in the "At Power" model. Level control is an important consideration for shutdown as well as for the operating reactor. The shutdown cases tend to be less severe, however, because decay heat (or even the potential for approximately 5% reactor power in Mode 2) does not demand the full function of the systems under consideration as in the "At Power" case.

LOCAs, which tend to pose the most restrictive level control problems, are normally evaluated for a pressurized system which means that most of the time the consideration is for the "At Power" condition. The time a shutdown reactor is pressurized is short compared to the time at power. LOCA is possible during a depressurized condition, but it would tend to be caused by valve misalignment or operator error more so than actual pipe rupture. This type of event typically has more evaluation time and a longer time frame for recovery than at-power LOCAs, and the problem is corrected prior to catastrophic core damage. The overall LOCA initiating event frequencies are reasonably small (E-04 to E-05) for the range of LOCAs considered and are not a significant contribution during the shutdown or full power case.

The LERF condition is not as significant in Modes 2 and 3 because of the low reactor power. In order to have LERF, there needs to be core damage as well as a release of the damaged core to primary containment and ultimately to the environs. The availability of sources to cover the core in the low power condition has previously been discussed. The next phase of the LERF condition should water sources fail, however, is release of this damaged product to primary containment or out via a failed isolation pathway. If the material does get into primary containment, the capability to penetrate the containment via some failure mode such as overpressure is such that the time frame involved would no longer make it an Early Release. This does not take into account the availability of sources for containment cooling or pressure control.

In consideration of failed containment isolation, it is possible that the main steam isolation values (MSIVs) may be closed already due to the operational variations involved with startup and hot shutdown; therefore, in these states their probability of failure to close would be less. HPCI and RCIC steam line isolations could be treated in a similar fashion as the MSIVs; however, as soon as the steam line low pressure alarms cleared, they would be opened. Their failure to close would provide a high energy pathway. If, however, all sources of core coverage failed and a HPCI or RCIC steam line failed to isolate, the actual release rate would decrease rapidly because the motive force (i.e., the steam pressure attributed to low power or decay heat) would not last. This plus the holdup time involved with the reactor building would severely retard the LERF capabilities of such scenarios.

In the shutdown or startup conditions, not only are more physical attributes available to prevent core damage, the number of initiating events contributing are less. One such example is the case with the Anticipated Transient Without

Scram (ATWS). Losses of condenser vacuum and feedwater or MSIV closure are not as severe as they would be at power. These accidents have their most significant contributions when these Balance Of Plant (BOP) systems are required to keep the unit operating. Failure of these systems limits the use of the condenser as a heat sink and the use of high pressure feedwater injection. During the shutdown or startup condition, failure of these systems or functions would tend to be more of an inconvenience to operation than a threat to core damage. Reactor scram is not considered for the Mode 3 case but is for Mode 2, but even this would be a very low power event. The main events to consider would be LOSP or Loss of Electrical Bus cases. These events tend to take away the redundancy associated with extra systems during the non "At Power" case.

The removal of a DG for extended maintenance during this time (Modes 2 or 3) would tend to add to the problems with losses of power. Typically this would not be done unless planned DG maintenance was in progress during Mode 1 and the unit was forced to enter Mode 3. However, the risk increase from this would be much smaller than that associated with Mode 1, essentially for the reasons previously discussed.

In general, Modes 2 and 3 are not normally sustained. Mode 2 is the startup case. Transition through this mode can certainly be more than a few hours, but it is not designed as a convenient holding point to perform various activities without going to cold shutdown. It is an allowance for the physical restrictions of control rod manipulation during startup (and certain Refuel Mode cases) and goes from simple to rather complex transitional plant operation where planned maintenance on DGs would be an administrative hindrance. Use of Mode 2 is controlled by Technical Specifications and procedures.

Mode 3 is a unique end state that accounts for any requirements to end full power operation. It is convenient to perform certain required maintenance in this condition in order to save time restoring the unit to full power operation from cold (Mode 4). It is possible to enter this condition by necessity during the time that a DG is undergoing planned maintenance on an extended Completion Time. The transition into Mode 3 for those unique times when a DG is already in planned maintenance in Mode 1 are still low risk as discussed previously.

c. Internal Flooding

Flooding initiators are included in the Plant Hatch PSA model and as such were evaluated in the Internal Events section of this document. Their contribution to CDF and LERF are negligible. Increasing the allowed Completion Time for restoration of an inoperable DG does not create any new flooding problems. This proposed amendment does not change any of the previous flooding analyses.

d. Seismic Events

Plant Hatch uses a Seismic Margins Analysis (SMA). This analysis was conducted as a pilot study for the Electric Power Research Institute (EPRI) and the NRC in order to evaluate the EPRI SMA methodology (EPRI NP-6041-SL "A Methodology for Assessment of Nuclear Power Plant Seismic Margin" Revision 1) from 1988 to 1989. Unit 2 had similar work performed in the 1993 to 1994 time frame. The results of the Unit 1 study are documented in EPRI NP-7217-SL. Extended allowed Completion Time for restoration of an inoperable DG does not affect the results of the SMA evaluation for Hatch. Shutdown for the LOSP case is provided by primary and alternate pathways that cover the effect of a single DG being out of service for maintenance.

e. Internal Fires

A Fire PSA was performed for Plant Hatch in response to the NRC Generic Letter 88-20, Supplement 4, "Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities – 10 CFR 50.54(f). This analysis was performed using the RISKMAN Event Tree software by PLG Inc. In order to evaluate the DG extended Completion Time with regards to fire risk, it was determined that the most appropriate comparison between present conditions and proposed Completion Time conditions would be to use the appropriate fire initiators in the CDF and LERF models. This is not intended to be a permanent model change but was done only to show the delta (Δ) between fire risk under the present Completion Time and the proposed Completion Time.

Addition of fire initiators to the CDF and LERF models is considered very conservative because of the conditions postulated for these initiators. The fire areas under consideration for this proposed Completion Time extension are those that may challenge the availability of the DGs. These involve the 4160VAC emergency switchgear rooms; therefore, these rooms are evaluated for this analysis. Not only are the switchgear and affiliated DG battery systems considered lost for a fire in each room; but, a LOSP is postulated from potential fire damage as well. This damage is due to transient combustible fires as well as fire in the switchgear itself. The end results are conservative because if there was doubt that these failures would or would not occur, they were assumed 100% failed.

The results for the DG extended Completion Time calculations are as follows.

ΔCDF (Due to Fire) = 6.0E-07
ΔLERF (Due to Fire) = 3.9E-07

These values show that the differential due to fire is still small, even considering the conservatism of the fire analysis. ΔCDF is less than 1E-06 and ΔLERF is still within the 1E-07 range.

2. Tier 2: Avoidance of Risk-Significant Plant Configurations

   Based on the configuration risk management site procedure and the conservative risk analysis used for evaluation of this Completion Time extension, there exists a reasonable level of assurance that risk-significant plant configurations will not exist. The dedication of the 1B DG to the plant unit with a DG in planned maintenance ensures the presence of two DGs per plant unit in the event of an accident situation.

3. Tier 3: Risk-Informed Configuration Risk Management Program

   The following discussion focuses on a description of and necessary changes to this 10 CFR 50.65(a)(4) program to support the requested diesel AOT. A formal Configuration Risk Management Program (CRMP) is not proposed.

   Edwin I. Hatch Nuclear Plant presently manages risk with a procedurally controlled program that governs the scheduling of maintenance activities. This program involves review from a probabilistic and/or deterministic standpoint of all, planned and unplanned, maintenance activities. The program is effective for all modes of operation including forced and planned outages.

   Maintenance is normally assessed from a probabilistic standpoint using a computerized On-Line Risk Monitor. This monitor uses the EPRI sponsored software developed by Data Systems and Solutions called Equipment Out Of Service (EOOS). There is an EOOS system for each plant unit. The system uses the actual PSA model for that unit to quantify results. In simplified cases, a more conservative equipment out of service matrix, applicable for only two items at a time, can be used. This matrix, however, is being phased out as EOOS training and usage progresses. In cases where quantitative solution is not possible because the functions or systems under consideration are not modeled, a qualitative assessment is used. Under certain risk significant conditions both quantitative and qualitative assessments are required.

   Risk is related for evaluation purposes to a color code with specific managerial levels of approval for the work in question. The following chart describes this concept.

Risk Action Level	On-Line Maintenance	Forced Outage	Refueling Outage
Green (None)	Shift Supervisor	Shift Supervisor	Shift Supervisor
Yellow (Low Risk)	Superintendent of Shift or Unit Superintendent	Superintendent of Shift or Unit Superintendent	Outage Director
Orange (Medium Risk)	Manager-Operations or Assistant General Manager-Plant Operations	Manager-Operations or Assistant General Manager-Plant Operations	Outage and Maintenance Manager or Assistant General Manager-Plant Operations
Red (High Risk)	General Manager-Nuclear Plant	General Manager-Nuclear Plant	General Manager-Nuclear Plant

Maintenance rule functions are evaluated to the component level either by matrix or EOOS. Removal of a redundant portion of a function will typically provide a Yellow color on EOOS or a Low Risk identification on the matrix. A single Yellow color or one Low Risk maintenance item will typically not require a documented evaluation of risk. The Scheduling Maintenance procedure documents the need for this as well as the need for the quantitative evaluation. If planned maintenance, unplanned maintenance, or a combination of both produces an Orange color, a documented evaluation of the situation is necessary. The same documentation is required for Red color situations, but, typically, these are not approved as planned maintenance. If unplanned events place the plant in this situation, all maintenance activities focus on exiting the situation as soon as possible. All attempts are made to address all maintenance rule functions from either a direct quantification standpoint or one that is less direct. Certain functions are not specifically part of the EOOS/PSA quantitative model but are modeled for equipment out of service purposes on the EOOS Operator's Screen. Depending on the color codes generated when portions of or all of one or more of these specific functions are removed from service, selected Initiating Event frequencies are increased by a factor of 10 to account for the degraded condition. This is conservative, yet it allows for evaluating these situations against modeled components that likewise may be removed from service.

Additionally, selected Initiating Event frequencies are increased by a factor of 10 with the aid of EOOS software based on selected external conditions. Examples of such events are described in the following:

- severe weather –Loss of Offsite Power,
- switchyard work—Loss of Offsite Power, and
- items affiliated with increased probability of reactor scram—Scram.

The Risk Management Actions associated with the color codes discussed previously are listed within the procedure and are paraphrased in the following list.

- Hold shift briefings to increase involvement and cooperation between Operations, Engineering, and Management personnel.

- Take actions such as pre-staging parts and materials, perform pre-job walkdowns and mock-up training, plan for around-the-shift work, and set up contingencies for rapid restoration if necessary.

- Take actions to minimize risk by limiting other work being done.

- Follow established approval levels.

- Use compensatory measures as necessary to minimize risk and adverse operational effects. These include temporary modifications, shielding, lighting, temporary jumpers or lifted wires. Each is proceduralized in its application.

The actual qualitative assessment form addresses the previously mentioned items and is normally used to ensure such measures are taken. DG maintenance falls

under the previously mentioned process at present. In order to manage the risk activities associated with this Completion Time extension, the configuration risk management site procedure will be revised. It will contain the following limitations for planned maintenance while in Mode 1 on one DG utilizing the Completion Time extension to 14 days.

1. Only one DG of the five DGs for both plant units will be removed for planned maintenance at a time.

2. No planned risk significant activities or maintenance will be performed during the time on either plant unit when maintenance on 1A (1R43S001A), 1C (1R43S001C), 2A (2R43S002A), 2C (2R43S002C), or 1B (1R43S001B) DG is in progress. Analog Transmitter Trip System Functional Test and Calibrations as well as Battery Charger Swapping is allowed.

3. Planned DG maintenance will not coincide with planned work in the High Voltage Switchyard.

4. Planned maintenance that will exceed 72 hours on 1A, 1C, 2A, or 2C DG will involve the following requirement.

   a) DG 1B will be aligned for supplying emergency power to the F 4160VAC Bus of the plant unit that has a DG in planned maintenance.

   b) This alignment will be such that the 1B DG cannot "swing" to the opposite unit on F bus undervoltage or dual unit LOSP with an opposite unit LOCA signal.

   c) The intent is to provide two DGs per plant unit during this time.

   d) Forced alignment of the 1B DG will limit alternate LPCI Bus (1R24S018A, 1R24S018B, 2R24S018A, and 2R24S018B) power alignment to the plant unit assigned the 1B diesel.

5. The selection or "throwover" switch that determines the alternate source of power for the Reactor Protection System, 1R25S036 (2R25S036) or 1R25S037 (2R25S037) will be placed accordingly:

   a) 1A or 2A DG Maintenance –1R25S037 or 2R25S037,

   b) 1C or 2C DG Maintenance –1R25S036 or 2R25S036, and

   c) 1B DG Maintenance – Either Essential Bus.

IV. Conclusion

The proposed extension of the DG Completion Times is based upon both a deterministic evaluation and a risk-informed assessment. The deterministic evaluation consisted of the following elements: 1) availability of offsite power via the startup transformers, 2) verification that the other DGs and offsite power sources are operable, and 3) reliance on the site procedure for managing risk, consistent with 10 CFR 50.65(a)(4), while a DG is in an extended Completion Time. This evaluation concluded that an extended allowed outage time for the DGs is consistent with the defense-in-depth philosophy and that sufficient safety margins are maintained. The risk-informed assessment concluded that the increase in plant risk is small and consistent with the NRC "Safety Goals for the Operations of Nuclear Power Plants; Policy Statement," Federal Register, Vol. 51, p. 30028 (51 FR 30028), August 4, 1986, as further described by NRC Regulatory Guides 1.174 and 1.177. Together these analyses provide high assurance of the capability to provide power to the ESF buses during the proposed extension of the DG Completion Times.

The proposed changes are consistent with NRC policy and will continue to provide adequate protection of public health. The changes advance the objectives of the NRC's Probabilistic Risk Assessment Policy Statement, "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," Federal Register, Volume 60, p. 42622, August 16, 1995 for enhanced decision-making and result in a more efficient use of resources and reduction of unnecessary burden.

Maintenance during power operation should improve overall DG availability which, in turn, should result in reducing shutdown risk by increasing the availability of emergency power during refueling outages. The proposed changes in DG Completion Times in conjunction with the availability of offsite power via the startup transformers and use of the site configuration risk management procedure during the proposed extended DG Completion Time will provide adequate assurance of the capability to provide power to the ESF buses. The equipment required to mitigate design basis events will not be reduced below the required level by performance of the DG on-line maintenance.

The proposed changes are consistent with the applicable regulatory requirements and guidelines. The proposed deviation from NRC Regulatory Guide 1.93 (i.e., extending the allowed outage time to 14 days for each DG) has been evaluated to be acceptable. The resultant slight increases in CDF and LERF are consistent with the intent of the NRC Safety Goal Policy Statement.

Therefore, the proposed changes are acceptable.

Enclosure 2

Edwin I. Hatch Nuclear Plant
Request to Revise Technical Specifications:
Extension of Completion Times for Inoperable Emergency Diesel Generators

10 CFR 50.92 No Significant Hazards Evaluation and Environmental Assessment

Basis for no significant hazards consideration determination

1. *Does the change involve a significant increase in the probability or consequences of an accident previously evaluated?*

The proposed changes extend the Technical Specifications required Completion Times for restoration of an inoperable emergency diesel generator (DG) to a maximum of 14 days. Additionally, the proposed extension of the Completion Time to 14 days results in a corresponding extension of the time period associated with discovery of failure to meet Limiting Condition for Operation 3.8.1 to 17 days. (This provides a maximum time limit for overlapping inoperabilities of DGs and offsite sources.)

For both Plant Hatch units A and C DGs, to utilize the 72 hours to 14 day period of the proposed extended Completion Time, compensatory action is required to ensure two DGs per unit remain available. This action consists of dedicating the 1B DG to that unit with the inoperable DG. This means that the 1B DG will be inhibited from an automatic swap to the opposite unit when that unit (the non-maintenance unit) experiences an undervoltage condition on its F 4160 volt bus, regardless of the presence or absence of a loss of coolant accident (LOCA) signal. Inhibiting the automatic transfer makes the 1B DG inoperable (with a Completion Time of 14 days) for the non-maintenance unit.

Completion Times are not an initial condition or assumption of any analyzed event. DGs are not initiators of any analyzed event. No event mitigation assumes more than two DGs per unit. The consequences of an accident are independent of the time the DGs are out of service provided adequate DG availability is assured. Compensatory actions are proposed in this amendment request that ensure adequate DG availability for both Plant Hatch units. Therefore, the assumptions regarding DG availability are maintained.

To fully evaluate the effect of the proposed DG Completion Time extension, Probabilistic Safety Assessment methods and a deterministic analysis were utilized. The results of the analyses show no significant increase in Core Damage Frequency (CDF) and Large Early Release Frequency (LERF).

Therefore, the proposed changes do not involve a significant increase in the probability or consequences of an event previously analyzed.

2. *Do the proposed changes create the possibility of a new or different type of accident from any previously evaluated.*

The proposed changes do involve a change to the plant configuration when either unit's A or C DG is utilizing the extended Completion Time (i.e., inoperable in excess of 72 hours). That configuration change ensures that both units have two dedicated DGs. Futhermore, affixing the 1B DG to one unit will cause it (1B DG) to be inoperable with respect to the Technical Specifications. Ensuring two DGs available to each unit for event mitigation in no way creates the possibility of a new or different type of accident.

No other change in the design, configuration, or method of operation of the plant is introduced by the proposed change. The changes do not alter any assumptions made in the safety analyses. No new failure modes are introduced.

Therefore, the proposed changes do not create the possibility of a new or different type of accident from any previously evaluated.

3. *Do the proposed changes involve a significant reduction in the margin of safety?*

Since all assumptions of the plant event analyses are maintained, there is no effect on the margin of safety in any safety analyses. If there is any margin of safety ascribed to DG availability and plant risk, it has been determined that such a margin of safety is not significantly reduced, as the proposed changes have been evaluated both deterministically and using a risk-informed approach. These evaluations concluded the following with respect to the proposed changes:

Applicable regulatory requirements will continue to be met, adequate defense-in-depth will be maintained, sufficient safety margins will be maintained, and any increases in CDF and LERF are small and consistent with the NRC Safety Goal Policy Statement (Federal Register, Vol. 51, p. 30028 (51 FR 30028), August 4, 1986, as interpreted by NRC Regulatory Guides 1.174 and 1.177). Furthermore, increases in risk posed by potential combinations of equipment out of service during the proposed DG extended Completion Time will be managed by the site configuration risk management procedure, consistent with 10 CFR 50.65, "Requirements for Monitoring the Effectiveness of Maintenance at Nuclear Power Plants," paragraph (a)(4).

The availability of offsite power together with the availability of the other DGs and the use of on-line risk assessment tools provide adequate compensation for the potential small incremental increase in plant risk of the extended DG Completion Time. In addition, the increased availability of the DGs during refueling outages offsets the small increase in plant risk during operation. The proposed extended DG Completion Times, in conjunction with the availability of the other DGs continues to provide adequate assurance of the capability to provide power to the engineered safety features buses. Therefore, implementation of the proposed changes will not involve a significant reduction in the margin of safety.

Summary

Based on the above analysis, the proposed changes will not increase the probability or consequences of any accident previously evaluated, create the possibility of a new or different kind of accident from any accident previously evaluated, or involve a significant reduction in the margin of safety. Therefore, the proposed changes meet the criteria of 10 CFR 50.92(c) and involve no significant hazard consideration.

Environmental Assessment

10 CFR 51.22(c) (9) provides criterion for identification of licensing and regulatory actions eligible for categorical exclusion from performing an environmental assessment. A proposed amendment to an operating license for a facility requires no environmental assessment if operation of the facility in accordance with the proposed license amendment would not:

1. Involve a significant hazards consideration,

2. Result in a significant change in the types or significant increase in the amounts of any effluents that may be released off-site, or

3. Result in a significant increase in individual or cumulative occupational radiation exposure.

Southern Nuclear Operating Company (SNC) has determined that the proposed Technical Specifications changes described in Enclosure 1 meet the eligibility criteria for categorical exclusion set forth in 10 CFR 51.229(c) (9). Accordingly, pursuant to 10 CFR 51.22, no environmental impact statement needs to be prepared in connection with the issuance of the license amendment for the proposed changes. The basis for this determination using the above criteria follows:

1. As demonstrated in this enclosure, the proposed changes do not involve a significant hazards consideration.

2. The proposed changes do not result in a significant change to the types of effluents or in the amounts of effluents released offsite. These proposed changes involve extending the Completion Time for an inoperable DG. They do not involve changes to the radioactive waste processing systems or to radioactive waste effluent monitors. Accordingly, the changes do not require the radioactive waste processing systems to perform any different function than they are designed to perform nor do they change the operation or testing of any such system.

3. The proposed changes do not result in a significant increase in occupational radiation exposure. The proposed changes impact the allowed Completion Time for an inoperable DG. The DGs are not located in a radiation area. The proposed changes do not require any additional time to be spent in a radiation area and do not impact dose rates or shielding.

Enclosure 3

Edwin I. Hatch Nuclear Plant
Request to Revise Technical Specifications:
Extension of Completion Times for Inoperable Emergency Diesel Generators

Page Change Instructions

Unit 1

Page	Instruction
3.8-2	Replace
3.8-3	Replace
3.8-4	Replace
3.8-5	Replace
3.8-6	Replace
B 3.8-8	Replace
B 3.8-11	Replace
B 3.8-12	Replace
B 3.8-13	Replace
B 3.8-14	Replace
B 3.8-15	Replace
B 3.8-16	Replace
B 3.8-17	Replace
B 3.8-18	Replace
B 3.8-19	Replace

Unit 2

Page	Instruction
3.8-2	Replace
3.8-3	Replace
3.8-4	Replace
3.8-5	Replace
3.8-6	Replace
B 3.8-8	Replace
B 3.8-11	Replace
B 3.8-12	Replace
B 3.8-13	Replace
B 3.8-14	Replace
B 3.8-15	Replace
B 3.8-16	Replace
B 3.8-17	Replace
B 3.8-18	Replace
B 3.8-19	Replace
B 3.8-20	Replace
B 3.8-21	Replace
B 3.8-22	Replace

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
A. One required offsite circuit inoperable.	A.1	Perform SR 3.8.1.1 for OPERABLE required offsite circuits.	1 hour AND Once per 8 hours thereafter
	AND		
	A.2	Declare required feature(s) with no offsite power available inoperable when the redundant required feature(s) are inoperable.	24 hours from discovery of no offsite power to one 4160 V ESF bus concurrent with inoperability of redundant required feature(s)
	AND		
	A.3	Restore required offsite circuit to OPERABLE status.	72 hours AND 17 days from discovery of failure to meet LCO 3.8.1.a, b, or c
B. One Unit 1 or the swing DG inoperable.	B.1	Perform SR 3.8.1.1 for OPERABLE required offsite circuit(s).	1 hour AND Once per 8 hours thereafter
	AND		

(continued)

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
B. (continued)	B.2	Declare required feature(s), supported by the inoperable DG, inoperable when the redundant required feature(s) are inoperable.	4 hours from discovery of Condition B concurrent with inoperability of redundant required feature(s)
	AND		
	B.3.1	Determine OPERABLE DG(s) are not inoperable due to common cause failure.	24 hours
	OR		
	B.3.2	Perform SR 3.8.1.2.a for OPERABLE DG(s).	24 hours
	AND		
	B.4	Restore DG to OPERABLE status.	72 hours for a Unit 1 DG with the swing DG not inhibited AND 14 days for a Unit 1 DG with the swing DG inhibited from automatically aligning to Unit 2 AND 14 days for the swing DG AND

(continued)

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
B. (continued)	B.4 (continued)	17 days from discovery of failure to meet LCO 3.8.1.a, b, or c
C. One required Unit 2 DG inoperable.	C.1 Perform SR 3.8.1.1 for OPERABLE required offsite circuit(s).	1 hour AND Once per 8 hours thereafter
	AND	
	C.2 Declare required feature(s), supported by the inoperable DG, inoperable when the redundant required feature(s) are inoperable.	4 hours from discovery of Condition C concurrent with inoperability of redundant required feature(s)
	AND	
	C.3.1 Determine OPERABLE DG(s) are not inoperable due to common cause failure.	24 hours
	OR	
	C.3.2 Perform SR 3.8.1.2.a for OPERABLE DG(s).	24 hours
	AND	
	C.4 Restore required DG to OPERABLE status.	7 days with the swing DG not inhibited AND (continued)

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
C. (continued)	C.4 (continued)	14 days with the swing DG inhibited from automatically aligning to Unit 1
D. Two or more required offsite circuits inoperable.	D.1 Declare required feature(s) with no offsite power available inoperable when the redundant required feature(s) are inoperable. AND D.2 Restore all but one required offsite circuit to OPERABLE status.	12 hours from discovery of Condition D concurrent with inoperability of redundant required feature(s) 24 hours
E. One required offsite circuit inoperable. AND One required DG inoperable.	----------NOTE---------- Enter applicable Conditions and Required Actions of LCO 3.8.7, "Distribution Systems — Operating," when Condition E is entered with no AC power source to one 4160 V ESF bus. ---------- E.1 Restore required offsite circuit to OPERABLE status. OR E.2 Restore required DG to OPERABLE status.	 12 hours 12 hours

(continued)

ACTIONS (continued)

CONDITION	REQUIRED ACTION	COMPLETION TIME
F. Two or more (Unit 1 and swing) DGs inoperable.	F.1 Restore all but one Unit 1 and swing DGs to OPERABLE status.	2 hours
G. No DGs capable of supplying power to any Unit 1 LPCI valve load center.	G.1 Restore one DG capable of supplying power to Unit 1 LPCI valve load center to OPERABLE status.	2 hours
H. Required Action and Associated Completion Time of Condition A, B, C, D, E, F, or G not met.	H.1 Be in MODE 3. AND H.2 Be in MODE 4.	12 hours 36 hours
I. One or more required offsite circuits and two or more required DGs inoperable. OR Two or more required offsite circuits and one required DG inoperable.	I.1 Enter LCO 3.0.3.	Immediately

BASES

ACTIONS

A.3 (continued)

reliability of the offsite system is degraded, and the potential for a loss of offsite power is increased, with attendant potential for a challenge to the plant safety systems. In this condition, however, the remaining OPERABLE offsite circuit and DGs are adequate to supply electrical power to the onsite Class 1E Distribution System.

The 72 hour Completion Time takes into account the capacity and capability of the remaining AC sources, reasonable time for repairs, and the low probability of a DBA occurring during this period.

The second Completion Time for Required Action A.3 establishes a limit on the maximum time allowed for any combination of required AC power sources to be inoperable during any single contiguous occurrence of failing to meet LCO 3.8.1.a, b, or c. If Condition A is entered while, for instance, the swing DG is inoperable, and that DG is subsequently returned OPERABLE, LCO 3.8.1.a, b, or c may already have been not met for up to 14 days. This situation could lead to a total of 17 days, since initial failure to meet LCO 3.8.1.a, b, and c, to restore the offsite circuit. At this time, the swing DG could again become inoperable, the circuit restored OPERABLE, and an additional 14 days (for a total of 31 days) allowed prior to complete restoration of LCO 3.8.1.a, b, and c. The 17 day Completion Time provides a limit on the time allowed in a specified condition after discovery of failure to meet LCO 3.8.1.a, b, or c. This limit is considered reasonable for situations in which Conditions A and B are entered concurrently. The "AND" connector between the 72 hours and 17 day Completion Times means that both Completion Times apply simultaneously, and the more restrictive Completion Time must be met.

As in Required Action A.2, the Completion Time allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." This exception results in establishing the "time zero" at the time LCO 3.8.1.a, b, or c was initially not met, instead of at the time that Condition A was entered.

(continued)

BASES

ACTIONS

B.3.1 and B.3.2 (continued)

According to Generic Letter 84-15 (Ref. 7), 24 hours is a reasonable time to confirm that the OPERABLE DGs are not affected by the same problem as the inoperable DG.

B.4

Regulatory Guide 1.93 (Ref. 6) provides guidance that operation in Condition B may continue for 72 hours. A risk-informed, deterministic evaluation performed for Plant Hatch justifies operation in Condition B for 14 days, provided action is taken to ensure two DGs are dedicated to each Hatch unit. This is accomplished for an inoperable A or C DG by inhibiting the automatic alignment (on a LOCA or LOSP signal) of the swing DG to the other unit. If the inoperable DG is the swing DG, each unit has two dedicated DGs and a 14 day Completion Time is allowed. In Condition B for each defined Completion Time and restriction (if applicable), the remaining OPERABLE DGs and offsite circuits are adequate to supply electrical power to the onsite Unit 1 Class 1E Distribution System. The Completion Times take into account the capacity and capability of the remaining AC sources, reasonable time for maintenance, and low probability of a DBA occurring during this period. Entry into Condition B for the purpose of planned maintenance, subject to additional restrictions controlled by plant procedures, is allowed.

The "AND" connector between the 72 hour and 14 day Completion Times means that both Completion Times apply simultaneously. That is, the 14 day Completion Time for an A or C DG with the swing DG inhibited applies from the time of entry into Condition B, not from the time the swing DG is inhibited.

The fourth Completion Time for Required Action B.4 establishes a limit on the maximum time allowed for any combination of required AC power sources to be inoperable during any single contiguous occurrence of failing to meet LCO 3.8.1.a, b, or c. If Condition B is entered while, for instance, an offsite circuit is inoperable and that circuit is subsequently restored OPERABLE, LCO 3.8.1.a, b, or c may already have been not met for up to 72 hours. This situation could lead to a total of 17 days, since initial failure to meet LCO 3.8.1.a, b, and c, to restore the DG.

(continued)

BASES

ACTIONS

B.4 (continued)

At this time, an offsite circuit could again become inoperable, the DG restored OPERABLE, and an additional 72 hours (for a total of 20 days) allowed prior to complete restoration of LCO 3.8.1.a, b, and c. The 17 day Completion Time provides a limit on the time allowed in a specified condition after discovery of failure to meet LCO 3.8.1.a, b, or c. This limit is considered reasonable for situations in which Conditions A and B are entered concurrently. The "AND" connectors between the Completion Times mean that all Completion Times apply simultaneously, and the more restrictive must be met.

As in Required Action B.2, the Completion Time allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." This exception results in establishing the "time zero" at the time that LCO 3.8.1.a, b, or c was initially not met, instead of the time that Condition B was entered.

C.1

To ensure a highly reliable power source remains with one required Unit 2 DG inoperable, it is necessary to verify the availability of the required offsite circuits on a more frequent basis. Since the Required Action only specifies "perform," a failure of SR 3.8.1.1 acceptance criteria does not result in a Required Action being not met. However, if a circuit fails to pass SR 3.8.1.1, it is inoperable. Upon offsite circuit inoperability, additional Conditions must then be entered.

C.2

Required Action C.2 is intended to provide assurance that a loss of offsite power, during the period that one required Unit 2 DG is inoperable, does not result in a complete loss of safety function of critical systems. These features are designed with redundant safety related divisions (i.e., single division systems are not included). Redundant required features failures consist of inoperable features associated with a division redundant to the division that has an inoperable DG.

(continued)

BASES

ACTIONS

C.2 (continued)

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." In this Required Action the Completion Time only begins on discovery that both:

a. An inoperable required Unit 2 DG exists; and

b. A redundant required feature on the other division (Division 1 or 2), or divisions in the case of the Unit 1 and 2 SGT System, is inoperable.

If, at any time during the existence of this Condition (required Unit 2 DG inoperable), a redundant required feature subsequently becomes inoperable, this Completion Time begins to be tracked.

Discovering one required Unit 2 DG inoperable coincident with one or more inoperable redundant required support or supported features, or both, that are associated with the OPERABLE DGs results in starting the Completion Time for the Required Action. Four hours from the discovery of these events existing concurrently is acceptable because it minimizes risk while allowing time for restoration before subjecting the unit to transients associated with shutdown.

The remaining OPERABLE DGs and offsite circuits are adequate to supply electrical power to the onsite Class 1E Distribution System. Thus, on a component basis, single failure protection for the required feature's function may have been lost; however, function has not been lost. The 4 hour Completion Time takes into account the component OPERABILITY of the redundant counterpart to the inoperable required feature. Additionally, the 4 hour Completion Time takes into account the capacity and capability of the remaining AC sources, reasonable time for repairs, and low probability of a DBA occurring during this period.

C.3.1 and C.3.2

Required Action C.3.1 provides an allowance to avoid unnecessary testing of OPERABLE DGs. If it can be

(continued)

BASES

ACTIONS

C.3.1 and C.3.2 (continued)

determined that the cause of the inoperable DG does not exist on the OPERABLE DG, SR 3.8.1.2.a does not have to be performed. If the cause of inoperability exists on other DG(s), they are declared inoperable upon discovery, and Condition F of LCO 3.8.1 is entered. Once the failure is repaired, and the common cause failure no longer exists, Required Action C.3.1 is satisfied. If the cause of the initial inoperable DG cannot be confirmed not to exist on the remaining DG(s), performance of SR 3.8.1.2.a suffices to provide assurance of continued OPERABILITY of those DGs. In the event the inoperable DG is restored to OPERABLE status prior to completing either C.3.1 or C.3.2, the deficiency control program, as appropriate, will continue to evaluate the common cause possibility. This continued evaluation, however, is no longer under the 24 hour constraint imposed while in Condition C.

According to Generic Letter 84-15 (Ref. 7), 24 hours is a reasonable time to confirm that the OPERABLE DGs are not affected by the same problem as the inoperable DG.

C.4

In Condition C, the remaining OPERABLE offsite circuit is adequate to supply electrical power to the required onsite Unit 2 Class 1E Distribution System. The 7 day Completion Time is based on the shortest restoration time allowed for the systems affected by the inoperable DG in the individual system LCOs. A risk-informed, deterministic evaluation performed for Plant Hatch justifies operation in Condition C for 14 days, provided action is taken to ensure two DGs are dedicated to each Hatch unit. This is accomplished for an inoperable A or C DG by inhibiting the automatic alignment (on a LOCA or LOSP signal) of the swing DG to the other unit. The Completion Times take into account the capacity and capability of the remaining AC sources, reasonable time for maintenance, and low probability of a DBA occurring during this period. Entry into Condition C for the purpose of planned maintenance, subject to additional restrictions controlled by plant procedures, is allowed.

(continued)

BASES

ACTIONS (continued)

D.1 and D.2

Required Action D.1 addresses actions to be taken in the event of inoperability of redundant required features concurrent with inoperability of two or more required offsite circuits. Required Action D.1 reduces the vulnerability to a loss of function. The Completion Time for taking these actions is reduced to 12 hours from that allowed with one 4160 V ESF bus without offsite power (Required Action A.2). The rationale for the reduction to 12 hours is that Regulatory Guide 1.93 (Ref. 6) allows a Completion Time of 24 hours for two required offsite circuits inoperable, based upon the assumption that two complete safety divisions are OPERABLE. (While this ACTION allows more than two circuits to be inoperable, Regulatory Guide 1.93 assumed two circuits were all that were required by the LCO, and a loss of those two circuits resulted in a loss of all offsite power to the Class 1E AC Electrical Power Distribution System. Thus, with the Plant Hatch design, a loss of more than two required offsite circuits results in the same conditions assumed in Regulatory Guide 1.93.) When a concurrent redundant required feature failure exists, this assumption is not the case, and a shorter Completion Time of 12 hours is appropriate. These features are designed with redundant safety related divisions, (i.e., single division systems are not included in the list). Redundant required features failures consist of any of these features that are inoperable because any inoperability is on a division redundant to a division with inoperable offsite circuits.

The Completion Time for Required Action D.1 is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." In this Required Action, the Completion Time only begins on discovery that both:

a. All required offsite circuits are inoperable; and

b. A redundant required feature is inoperable.

If, at any time during the existence of this Condition (two or more required offsite circuits inoperable), a redundant required feature subsequently becomes inoperable, this Completion Time begins to be tracked.

(continued)

BASES

ACTIONS

D.1 and D.2 (continued)

According to Regulatory Guide 1.93 (Ref. 6), operation may continue in Condition D for a period that should not exceed 24 hours. This level of degradation means that the offsite electrical power system does not have the capability to effect a safe shutdown and to mitigate the effects of an accident; however, the onsite AC sources have not been degraded. This level of degradation generally corresponds to a total loss of the immediately accessible offsite power sources.

Because of the normally high availability of the offsite sources, this level of degradation may appear to be more severe than other combinations of two AC sources inoperable that involve one or more DGs inoperable. However, two factors tend to decrease the severity of this degradation level:

a. The configuration of the redundant AC electrical power system that remains available is not susceptible to a single bus or switching failure; and

b. The time required to detect and restore an unavailable offsite power source is generally much less than that required to detect and restore an unavailable onsite AC source.

With two or more of the required offsite circuits inoperable, sufficient onsite AC sources are available to maintain the unit in a safe shutdown condition in the event of a DBA or transient. In fact, a simultaneous loss of offsite AC sources, a LOCA, and a worst case single failure were postulated as a part of the design basis in the safety analysis. Thus, the 24 hour Completion Time provides a period of time to effect restoration of one of the offsite circuits commensurate with the importance of maintaining an AC electrical power system capable of meeting its design criteria.

According to Regulatory Guide 1.93 (Ref. 6), with the available offsite AC sources two less than required by the LCO (which as stated earlier, generally corresponds to a total loss of the immediately accessible offsite power

(continued)

BASES

ACTIONS

D.1 and D.2 (continued)

sources; this is the condition experienced by Plant Hatch when two or more required circuits are inoperable), operation may continue for 24 hours. If all required offsite sources are restored within 24 hours, unrestricted operation may continue. If all but one required offsite sources are restored within 24 hours, power operation continues in accordance with Condition A.

E.1 and E.2

Pursuant to LCO 3.0.6, the Distribution System ACTIONS would not be entered even if all AC sources to it were inoperable, resulting in de-energization. Therefore, the Required Actions of Condition E are modified by a Note to indicate that when Condition E is entered with no AC source to any ESF bus, ACTIONS for LCO 3.8.7, "Distribution Systems — Operating," must be immediately entered. This allows Condition E to provide requirements for the loss of the offsite circuit and one DG without regard to whether a division is de-energized. LCO 3.8.7 provides the appropriate restrictions for a de-energized ESF bus.

According to Regulatory Guide 1.93 (Ref. 6), operation may continue in Condition E for a period that should not exceed 12 hours. In Condition E, individual redundancy is lost in both the offsite electrical power system and the onsite AC electrical power system. However, since power system redundancy is provided by two diverse sources of power, the reliability of the power systems in this Condition may appear higher than that in Condition D (loss of two or more required offsite circuits). This difference in reliability is offset by the susceptibility of this power system configuration to a single bus or switching failure.

The 12 hour Completion Time takes into account the capacity and capability of the remaining AC sources, reasonable time for repairs, and the low probability of a DBA occurring during this period.

(continued)

BASES

ACTIONS (continued)

F.1

With two or more Unit 1 and swing DGs inoperable, with an assumed loss of offsite electrical power, insufficient standby AC sources are available to power the minimum required ESF functions. Since the offsite electrical power system is the only source of AC power for the majority of ESF equipment at this level of degradation, the risk associated with continued operation for a very short time could be less than that associated with an immediate controlled shutdown. (The immediate shutdown could cause grid instability, which could result in a total loss of AC power.) Since any inadvertent unit generator trip could also result in a total loss of offsite AC power, the time allowed for continued operation is severely restricted. The intent here is to avoid the risk associated with an immediate controlled shutdown and to minimize the risk associated with this level of degradation.

According to Regulatory Guide 1.93 (Ref. 6), with two or more DGs inoperable, operation may continue for a period that should not exceed 2 hours. (Regulatory Guide 1.93 assumed the unit has two DGs. Thus, a loss of both DGs results in a total loss of onsite power. Therefore, a loss of more than two DGs, in the Plant Hatch design, results in degradation no worse than that assumed in Regulatory Guide 1.93. In addition, the loss of a required Unit 2 DG concurrent with the loss of a Unit 1 or swing DG, is analogous to the loss of a single DG in the Regulatory Guide 1.93 assumptions, thus, entry into this Condition is not required in this case.)

G.1

With both Unit 2 DGs and the swing DG inoperable (or otherwise incapable of supplying power to the LPCI valve load centers), and an assumed loss of offsite electrical power, insufficient standby AC sources are available to power the LPCI valve load centers. Since the offsite electrical power system is the only source of AC power for the LPCI valve load centers at this level of degradation, the risk associated with operation for a very short time could be less than that associated with an immediate controlled shutdown. (The immediate shutdown could cause grid instability, which could result in a total loss of AC power.) Since any inadvertent unit generator trip could

(continued)

BASES

ACTIONS

G.1 (continued)

also result in a total loss of offsite AC power, the time allowed for continued operation is severely restricted. The intent here is to avoid the risk associated with an immediate controlled shutdown and minimize the risk associated with an immediate controlled shutdown and minimize the risk associated with this level of degradation.

According to Regulatory Guide 1.93 (Ref. 6), with two or more DGs inoperable, operation may continue for a period that should not exceed 2 hours. (Regulatory Guide 1.93 assumed the unit had two DGs. Thus, a loss of both DGs results in a total loss of onsite power.) Therefore, a loss of both Unit 2 DGs and the swing DG results in degradation no worse than that assumed in Regulatory Guide 1.93, and the 2 hour Completion Time is acceptable.

H.1 and H.2

If the inoperable AC electrical power sources cannot be restored to OPERABLE status within the associated Completion Time, the unit must be brought to a MODE in which the LCO does not apply. To achieve this status, the unit must be brought to at least MODE 3 within 12 hours and to MODE 4 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

I.1

Condition I corresponds to a level of degradation in which all redundancy in the AC electrical power supplies has been lost. At this severely degraded level, any further losses in the AC electrical power system will cause a loss of function. Therefore, no additional time is justified for continued operation. The unit is required by LCO 3.0.3 to commence a controlled shutdown.

SURVEILLANCE REQUIREMENTS

The AC sources are designed to permit inspection and testing of all important areas and features, especially those that have a standby function, in accordance with

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

10 CFR 50, GDC 18 (Ref. 8). Periodic component tests are supplemented by extensive functional tests during refueling outages under simulated accident conditions. The SRs for demonstrating the OPERABILITY of the DGs are generally consistent with the recommendations of Regulatory Guide 1.9 (Ref. 9), Regulatory Guide 1.108 (Ref. 10), and Regulatory Guide 1.137 (Ref. 11), although Plant Hatch Unit 1 is not committed to these Regulatory Guides. Specific commitments relative to DG testing are described in FSAR section 8.4 (Ref. 2).

Where the SRs discussed herein specify voltage and frequency tolerances, the following summary is applicable. The allowable values for achieving steady state voltage are specified within a range of minus 10 percent (3740 V) and plus 2 percent (4243 V) of 4160 V. The Allowable Value of 3740 V is consistent with Regulatory Guide 1.9 for demonstrating that the diesel generator is capable of attaining the required voltage. A more limiting value of 4243 V is specified as the allowable value for overvoltage due to overvoltage limits on the 600 V buses. The plus 2 percent value maintains the required overvoltage limits. The specified minimum and maximum frequencies of the DG are 58.8 Hz and 61.2 Hz, respectively. These values are equal to ± 2% of the 60 Hz nominal frequency and are derived from the recommendations found in Regulatory Guide 1.9 (Ref. 9).

The SRs are modified by a NOTE to indicate that SR 3.8.1.1 through SR 3.8.1.18 apply only to the Unit 1 AC sources, and that SR 3.8.1.19 applies only to the Unit 2 AC sources.

SR 3.8.1.1

This SR ensures proper circuit continuity for the offsite AC electrical power supply to the onsite distribution network and availability of offsite AC electrical power. The breaker alignment verifies that each breaker is in its correct position to ensure that distribution buses and loads are connected to their preferred power source and that appropriate independence of offsite circuits is maintained. The 7 day Frequency is adequate since breaker position is not likely to change without the operator being aware of it and because its status is displayed in the control room.

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.2

This SR helps to ensure the availability of the standby electrical power supply to mitigate DBAs and transients and maintain the unit in a safe shutdown condition, and verifies that the DGs are capable of proper startup, synchronizing, and accepting a load approximately 50% of the continuous load rating. This demonstrates DG capability while minimizing the mechanical stress and wear on the engine. A minimum run time of 60 minutes is required to stabilize engine temperatures, while minimizing the time that the DG is connected to the offsite source.

Although no power factor requirements are established by this SR, the DG is normally operated at a power factor between 0.8 lagging and 1.0. The 0.8 value is the design rating of the machine, while 1.0 is an operational limitation.

To minimize the wear on moving parts that do not get lubricated when the engine is not running, this SR has been modified by a Note (Note 2) to indicate that all DG starts for this Surveillance may be preceded by an engine prelube period and followed by a warmup prior to loading.

For the purposes of this testing, the DGs are started from standby conditions. Standby conditions for a DG mean that the diesel engine coolant and oil are being continuously circulated and temperature is being maintained consistent with manufacturer recommendations.

In order to reduce stress and wear on diesel engines, the DG manufacturer recommends a modified start in which the starting speed of DGs is limited, warmup is limited to this lower speed, and the DGs are gradually accelerated to synchronous speed prior to loading. These start procedures are the intent of Note 3. Once voltage and frequency requirements are demonstrated, the DG may be tied to its respective 4160 V emergency bus, as directed by SR 3.8.1.2.b. When the DG is tied to its bus, the electrical grid, due to its much larger size compared to the DG, will dictate DG voltage and frequency. The DG operator cannot adjust either parameter. Therefore, the voltage and frequency requirements of SR 3.8.1.2.a no longer apply while the DG is tied to its bus and need not be met to satisfy the requirements of SR 3.8.1.2.b. Other SRs, notably

(continued)

BASES

SURVEILLANCE REQUIREMENTS

SR 3.8.1.2 (continued)

SR 3.8.1.9, require that voltage and frequency requirements can be met while the DG is supplying load.

SR 3.8.1.5.a requires that, at a 184 day Frequency, the DG starts from standby conditions and achieves required voltage and frequency within 12 seconds. The 12 second start requirement supports the assumptions in the design basis LOCA analysis of FSAR, Chapter 6 (Ref. 4). The 12 second start requirement is not applicable to SR 3.8.1.2 (see Note 3), when a modified start procedure as described above is used. If a modified start is not used, the 12 second start voltage and frequency requirements of SR 3.8.1.5.a apply.

Since SR 3.8.1.5.a does require a 12 second start, it is more restrictive than SR 3.8.1.2, and it may be performed in lieu of SR 3.8.1.2. This procedure is the intent of Note 1.

To minimize testing of the swing DG, this SR is modified by a note (Note 4) to allow a single test (instead of two tests, one for each unit) to satisfy the requirements for both units, using the starting circuitry of one unit for one periodic test and the starting circuitry of the other unit during the next periodic test. This is allowed since the main purpose of the Surveillance, to ensure DG OPERABILITY, is still being verified on the proper frequency, the starting circuits historically have a very low failure rate, as compared to the DG itself, and that, while each starting circuit is only being tested every second test (due to the staggering of the tests), some portions of the starting circuits are common to both units. If the swing DG fails one of these Surveillance, the DG should be considered inoperable on both units, unless the cause of the failure can be directly related to only one unit.

Note 5 modifies this Surveillance to indicate that diesel engine runs for this Surveillance may include gradual loading, as recommended by the manufacturer, so that mechanical stress and wear on the diesel engine are minimized.

Note 6 modifies the Surveillance by stating that starting transients above the upper voltage limit do not invalidate this test.

(continued)

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
A. One required offsite circuit inoperable.	A.1 Perform SR 3.8.1.1 for OPERABLE required offsite circuits.	1 hour AND Once per 8 hours thereafter
	AND	
	A.2 Declare required feature(s) with no offsite power available inoperable when the redundant required feature(s) are inoperable.	24 hours from discovery of no offsite power to one 4160 V ESF bus concurrent with inoperability of redundant required feature(s)
	AND	
	A.3 Restore required offsite circuit to OPERABLE status.	72 hours AND 17 days from discovery of failure to meet LCO 3.8.1.a, b, or c
B. One Unit 2 or the swing DG inoperable.	B.1 Perform SR 3.8.1.1 for OPERABLE required offsite circuit(s).	1 hour AND Once per 8 hours thereafter
	AND	

(continued)

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
B. (continued)	B.2 Declare required feature(s), supported by the inoperable DG, inoperable when the redundant required feature(s) are inoperable.	4 hours from discovery of Condition B concurrent with inoperability of redundant required feature(s)
	AND	
	B.3.1 Determine OPERABLE DG(s) are not inoperable due to common cause failure.	24 hours
	OR	
	B.3.2 Perform SR 3.8.1.2.a for OPERABLE DG(s).	24 hours
	AND	
	B.4 Restore DG to OPERABLE status.	72 hours for a Unit 2 DG with the swing DG not inhibited AND 14 days for a Unit 2 DG with the swing DG inhibited from automatically aligning to Unit 1 AND 14 days for the swing DG AND

(continued)

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
B. (continued)	B.4 (continued)	17 days from discovery of failure to meet LCO 3.8.1.a, b, or c
C. One required Unit 1 DG inoperable.	C.1 Perform SR 3.8.1.1 for OPERABLE required offsite circuit(s).	1 hour AND Once per 8 hours thereafter
	AND	
	C.2 Declare required feature(s), supported by the inoperable DG, inoperable when the redundant required feature(s) are inoperable.	4 hours from discovery of Condition C concurrent with inoperability of redundant required feature(s)
	AND	
	C.3.1 Determine OPERABLE DG(s) are not inoperable due to common cause failure.	24 hours
	OR	
	C.3.2 Perform SR 3.8.1.2.a for OPERABLE DG(s).	24 hours
	AND	
	C.4 Restore required DG to OPERABLE status.	7 days with the swing DG not inhibited AND (continued)

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
C. (continued)	C.4 (continued)	14 days with the swing DG inhibited from automatically aligning to Unit 2
D. Two or more required offsite circuits inoperable.	D.1 Declare required feature(s) with no offsite power available inoperable when the redundant required feature(s) are inoperable. AND D.2 Restore all but one required offsite circuit to OPERABLE status.	12 hours from discovery of Condition D concurrent with inoperability of redundant required feature(s) 24 hours
E. One required offsite circuit inoperable. AND One required DG inoperable.	----------NOTE---------- Enter applicable Conditions and Required Actions of LCO 3.8.7, "Distribution Systems — Operating," when Condition E is entered with no AC power source to one 4160 V ESF bus. ---------- E.1 Restore required offsite circuit to OPERABLE status. OR E.2 Restore required DG to OPERABLE status.	 12 hours 12 hours

(continued)

ACTIONS (continued)

CONDITION	REQUIRED ACTION	COMPLETION TIME
F. Two or more (Unit 1 and swing) DGs inoperable.	F.1 Restore all but one Unit 1 and swing DGs to OPERABLE status.	2 hours
G. No DGs capable of supplying power to any Unit 2 LPCI valve load center.	G.1 Restore one DG capable of supplying power to Unit 2 LPCI valve load center to OPERABLE status.	2 hours
H. Required Action and Associated Completion Time of Condition A, B, C, D, E, F, or G not met.	H.1 Be in MODE 3. AND H.2 Be in MODE 4.	12 hours 36 hours
I. One or more required offsite circuits and two or more required DGs inoperable. OR Two or more required offsite circuits and one required DG inoperable.	I.1 Enter LCO 3.0.3.	Immediately

BASES

ACTIONS

A.3 (continued)

reliability of the offsite system is degraded, and the potential for a loss of offsite power is increased, with attendant potential for a challenge to the plant safety systems. In this condition, however, the remaining OPERABLE offsite circuit and DGs are adequate to supply electrical power to the onsite Class 1E Distribution System.

The 72 hour Completion Time takes into account the capacity and capability of the remaining AC sources, reasonable time for repairs, and the low probability of a DBA occurring during this period.

The second Completion Time for Required Action A.3 establishes a limit on the maximum time allowed for any combination of required AC power sources to be inoperable during any single contiguous occurrence of failing to meet LCO 3.8.1.a, b, or c. If Condition A is entered while, for instance, the swing DG is inoperable, and that DG is subsequently returned OPERABLE, LCO 3.8.1.a, b, or c may already have been not met for up to 14 days. This situation could lead to a total of 17 days, since initial failure to meet LCO 3.8.1.a, b, and c, to restore the offsite circuit. At this time, the swing DG could again become inoperable, the circuit restored OPERABLE, and an additional 14 days (for a total of 31 days) allowed prior to complete restoration of LCO 3.8.1.a, b, and c. The 17 day Completion Time provides a limit on the time allowed in a specified condition after discovery of failure to meet LCO 3.8.1.a, b, or c. This limit is considered reasonable for situations in which Conditions A and B are entered concurrently. The "AND" connector between the 72 hours and 17 day Completion Times means that both Completion Times apply simultaneously, and the more restrictive Completion Time must be met.

As in Required Action A.2, the Completion Time allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." This exception results in establishing the "time zero" at the time LCO 3.8.1.a, b, or c was initially not met, instead of at the time that Condition A was entered.

(continued)

BASES

ACTIONS

B.3.1 and B.3.2 (continued)

According to Generic Letter 84-15 (Ref. 7), 24 hours is a reasonable time to confirm that the OPERABLE DGs are not affected by the same problem as the inoperable DG.

B.4

Regulatory Guide 1.93 (Ref. 6) provides guidance that operation in Condition B may continue for 72 hours. A risk-informed, deterministic evaluation performed for Plant Hatch justifies operation in Condition B for 14 days, provided action is taken to ensure two DGs are dedicated to each Hatch unit. This is accomplished for an inoperable A or C DG by inhibiting the automatic alignment (on a LOCA or LOSP signal) of the swing DG to the other unit. If the inoperable DG is the swing DG, each unit has two dedicated DGs and a 14 day Completion Time is allowed. In Condition B for each defined Completion Time and restriction (if applicable), the remaining OPERABLE DGs and offsite circuits are adequate to supply electrical power to the onsite Unit 2 Class 1E Distribution System. The Completion Times take into account the capacity and capability of the remaining AC sources, reasonable time for maintenance, and low probability of a DBA occurring during this period. Entry into Condition B for the purpose of planned maintenance, subject to additional restrictions controlled by plant procedures, is allowed.

The "AND" connector between the 72 hour and 14 day Completion Times means that both Completion Times apply simultaneously. That is, the 14 day Completion Time for an A or C DG with the swing DG inhibited applies from the time of entry into Conditon B, not from the time the swing DG is inhibited.

The fourth Completion Time for Required Action B.4 establishes a limit on the maximum time allowed for any combination of required AC power sources to be inoperable during any single contiguous occurrence of failing to meet LCO 3.8.1.a, b, or c. If Condition B is entered while, for instance, an offsite circuit is inoperable and that circuit is subsequently restored OPERABLE, LCO 3.8.1.a, b, or c may already have been not met for up to 72 hours. This situation could lead to a total of 17 days, since initial failure to meet LCO 3.8.1.a, b, and c, to restore the DG.

(continued)

BASES

ACTIONS

B.4 (continued)

At this time, an offsite circuit could again become inoperable, the DG restored OPERABLE, and an additional 72 hours (for a total of 20 days) allowed prior to complete restoration of LCO 3.8.1.a, b, and c. The 17 day Completion Time provides a limit on the time allowed in a specified condition after discovery of failure to meet LCO 3.8.1.a, b, or c. This limit is considered reasonable for situations in which Conditions A and B are entered concurrently. The "AND" connectors between the Completion Times mean that all Completion Times apply simultaneously, and the more restrictive must be met.

As in Required Action B.2, the Completion Time allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." This exception results in establishing the "time zero" at the time that LCO 3.8.1.a, b, or c was initially not met, instead of the time that Condition B was entered.

C.1

To ensure a highly reliable power source remains with one required Unit 1 DG inoperable, it is necessary to verify the availability of the required offsite circuits on a more frequent basis. Since the Required Action only specifies "perform," a failure of SR 3.8.1.1 acceptance criteria does not result in a Required Action being not met. However, if a circuit fails to pass SR 3.8.1.1, it is inoperable. Upon offsite circuit inoperability, additional Conditions must then be entered.

C.2

Required Action C.2 is intended to provide assurance that a loss of offsite power, during the period that one required Unit 1 DG is inoperable, does not result in a complete loss of safety function of critical systems. These features are designed with redundant safety related divisions (i.e., single division systems are not included). Redundant required features failures consist of inoperable features associated with a division redundant to the division that has an inoperable DG.

(continued)

BASES

ACTIONS

C.2 (continued)

The Completion Time is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." In this Required Action the Completion Time only begins on discovery that both:

a. An inoperable required Unit 1 DG exists; and

b. A redundant required feature on the other division (Division 1 or 2), or divisions in the case of the Unit 1 and 2 SGT System, is inoperable.

If, at any time during the existence of this Condition (required Unit 1 DG inoperable), a redundant feature subsequently becomes inoperable, this Completion Time begins to be tracked.

Discovering one required Unit 1 DG inoperable coincident with one or more inoperable redundant required support or supported features, or both, that are associated with the OPERABLE DGs results in starting the Completion Time for the Required Action. Four hours from the discovery of these events existing concurrently is acceptable because it minimizes risk while allowing time for restoration before subjecting the unit to transients associated with shutdown.

The remaining OPERABLE DGs and offsite circuits are adequate to supply electrical power to the onsite Class 1E Distribution System. Thus, on a component basis, single failure protection for the required feature's function may have been lost; however, function has not been lost. The 4 hour Completion Time takes into account the component OPERABILITY of the redundant counterpart to the inoperable required feature. Additionally, the 4 hour Completion Time takes into account the capacity and capability of the remaining AC sources, reasonable time for repairs, and low probability of a DBA occurring during this period.

C.3.1 and C.3.2

Required Action C.3.1 provides an allowance to avoid unnecessary testing of OPERABLE DGs. If it can be

(continued)

BASES

ACTIONS

C.3.1 and C.3.2 (continued)

determined that the cause of the inoperable DG does not exist on the OPERABLE DG, SR 3.8.1.2.a does not have to be performed. If the cause of inoperability exists on other DG(s), they are declared inoperable upon discovery, and Condition F of LCO 3.8.1 is entered. Once the failure is repaired, and the common cause failure no longer exists, Required Action C.3.1 is satisfied. If the cause of the initial inoperable DG cannot be confirmed not to exist on the remaining DG(s), performance of SR 3.8.1.2.a suffices to provide assurance of continued OPERABILITY of those DGs. In the event the inoperable DG is restored to OPERABLE status prior to completing either C.3.1 or C.3.2, the deficiency control program, as appropriate, will continue to evaluate the common cause possibility. This continued evaluation, however, is no longer under the 24 hour constraint imposed while in Condition C.

According to Generic Letter 84-15 (Ref. 7), 24 hours is a reasonable time to confirm that the OPERABLE DGs are not affected by the same problem as the inoperable DG.

C.4

In Condition C, the remaining OPERABLE offsite circuit is adequate to supply electrical power to the required onsite Unit 1 Class 1E Distribution System. The 7 day Completion Time is based on the shortest restoration time allowed for the systems affected by the inoperable DG in the individual system LCOs. A risk-informed, deterministic evaluation performed for Plant Hatch justifies operation in Condition C for 14 days, provided action is taken to ensure two DGs are dedicated to each Hatch unit. This is accomplished for an inoperable A or C DG by inhibiting the automatic alignment (on a LOCA or LOSP signal) of the swing DG to the other unit. The Completion Times take into account the capacity and capability of the remaining AC sources, reasonable time for maintenance, and low probability of a DBA occurring during this period. Entry into Condition C for the purpose of planned maintenance, subject to additional restrictions controlled by plant procedures, is allowed.

(continued)

BASES

ACTIONS (continued)

D.1 and D.2

Required Action D.1 addresses actions to be taken in the event of inoperability of redundant required features concurrent with inoperability of two or more required offsite circuits. Required Action D.1 reduces the vulnerability to a loss of function. The Completion Time for taking these actions is reduced to 12 hours from that allowed with one 4160 V ESF bus without offsite power (Required Action A.2). The rationale for the reduction to 12 hours is that Regulatory Guide 1.93 (Ref. 6) allows a Completion Time of 24 hours for two required offsite circuits inoperable, based upon the assumption that two complete safety divisions are OPERABLE. (While this ACTION allows more than two circuits to be inoperable, Regulatory Guide 1.93 assumed two circuits were all that were required by the LCO, and a loss of those two circuits resulted in a loss of all offsite power to the Class 1E AC Electrical Power Distribution System. Thus, with the Plant Hatch design, a loss of more than two required offsite circuits results in the same conditions assumed in Regulatory Guide 1.93.) When a concurrent redundant required feature failure exists, this assumption is not the case, and a shorter Completion Time of 12 hours is appropriate. These features are designed with redundant safety related divisions, (i.e., single division systems are not included in the list). Redundant required features failures consist of any of these features that are inoperable because any inoperability is on a division redundant to a division with inoperable offsite circuits.

The Completion Time for Required Action D.1 is intended to allow the operator time to evaluate and repair any discovered inoperabilities. This Completion Time also allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." In this Required Action, the Completion Time only begins on discovery that both:

a. All required offsite circuits are inoperable; and

b. A redundant required feature is inoperable.

If, at any time during the existence of this Condition (two or more required offsite circuits inoperable), a redundant required feature subsequently becomes inoperable, this Completion Time begins to be tracked.

(continued)

BASES

ACTIONS

D.1 and D.2 (continued)

According to Regulatory Guide 1.93 (Ref. 6), operation may continue in Condition D for a period that should not exceed 24 hours. This level of degradation means that the offsite electrical power system does not have the capability to effect a safe shutdown and to mitigate the effects of an accident; however, the onsite AC sources have not been degraded. This level of degradation generally corresponds to a total loss of the immediately accessible offsite power sources.

Because of the normally high availability of the offsite sources, this level of degradation may appear to be more severe than other combinations of two AC sources inoperable that involve one or more DGs inoperable. However, two factors tend to decrease the severity of this degradation level:

a. The configuration of the redundant AC electrical power system that remains available is not susceptible to a single bus or switching failure; and

b. The time required to detect and restore an unavailable offsite power source is generally much less than that required to detect and restore an unavailable onsite AC source.

With two or more of the required offsite circuits inoperable, sufficient onsite AC sources are available to maintain the unit in a safe shutdown condition in the event of a DBA or transient. In fact, a simultaneous loss of offsite AC sources, a LOCA, and a worst case single failure were postulated as a part of the design basis in the safety analysis. Thus, the 24 hour Completion Time provides a period of time to effect restoration of one of the offsite circuits commensurate with the importance of maintaining an AC electrical power system capable of meeting its design criteria.

According to Regulatory Guide 1.93 (Ref. 6), with the available offsite AC sources two less than required by the LCO (which as stated earlier, generally corresponds to a total loss of the immediately accessible offsite power

(continued)

BASES

ACTIONS

D.1 and D.2 (continued)

sources; this is the condition experienced by Plant Hatch when two or more required circuits are inoperable), operation may continue for 24 hours. If all required offsite sources are restored within 24 hours, unrestricted operation may continue. If all but one required offsite sources are restored within 24 hours, power operation continues in accordance with Condition A.

E.1 and E.2

Pursuant to LCO 3.0.6, the Distribution System ACTIONS would not be entered even if all AC sources to it were inoperable, resulting in de-energization. Therefore, the Required Actions of Condition E are modified by a Note to indicate that when Condition E is entered with no AC source to any ESF bus, ACTIONS for LCO 3.8.7, "Distribution Systems — Operating," must be immediately entered. This allows Condition E to provide requirements for the loss of the offsite circuit and one DG without regard to whether a division is de-energized. LCO 3.8.7 provides the appropriate restrictions for a de-energized ESF bus.

According to Regulatory Guide 1.93 (Ref. 6), operation may continue in Condition E for a period that should not exceed 12 hours. In Condition E, individual redundancy is lost in both the offsite electrical power system and the onsite AC electrical power system. However, since power system redundancy is provided by two diverse sources of power, the reliability of the power systems in this Condition may appear higher than that in Condition D (loss of two or more required offsite circuits). This difference in reliability is offset by the susceptibility of this power system configuration to a single bus or switching failure.

The 12 hour Completion Time takes into account the capacity and capability of the remaining AC sources, reasonable time for repairs, and the low probability of a DBA occurring during this period.

(continued)

BASES

ACTIONS (continued)

F.1

With two or more Unit 2 and swing DGs inoperable, with an assumed loss of offsite electrical power, insufficient standby AC sources are available to power the minimum required ESF functions. Since the offsite electrical power system is the only source of AC power for the majority of ESF equipment at this level of degradation, the risk associated with continued operation for a very short time could be less than that associated with an immediate controlled shutdown. (The immediate shutdown could cause grid instability, which could result in a total loss of AC power.) Since any inadvertent unit generator trip could also result in a total loss of offsite AC power, the time allowed for continued operation is severely restricted. The intent here is to avoid the risk associated with an immediate controlled shutdown and to minimize the risk associated with this level of degradation.

According to Regulatory Guide 1.93 (Ref. 6), with two or more DGs inoperable, operation may continue for a period that should not exceed 2 hours. (Regulatory Guide 1.93 assumed the unit has two DGs. Thus, a loss of both DGs results in a total loss of onsite power. Therefore, a loss of more than two DGs, in the Plant Hatch design, results in degradation no worse than that assumed in Regulatory Guide 1.93. In addition, the loss of a required Unit 1 DG concurrent with the loss of a Unit 2 or swing DG, is analogous to the loss of a single DG in the Regulatory Guide 1.93 assumptions, thus, entry into this Condition is not required in this case.)

G.1

With both Unit 1 DGs and the swing DG inoperable (or otherwise incapable of supplying power to the LPCI valve load centers), and an assumed loss of offsite electrical power, insufficient standby AC sources are available to power the LPCI valve load centers. Since the offsite electrical power system is the only source of AC power for the LPCI valve load centers at this level of degradation, the risk associated with operation for a very short time could be less than that associated with an immediate controlled shutdown. (The immediate shutdown could cause grid instability, which could result in a total loss of AC power.) Since any inadvertent unit generator trip could

(continued)

BASES

ACTIONS

G.1 (continued)

also result in a total loss of offsite AC power, the time allowed for continued operation is severely restricted. The intent here is to avoid the risk associated with an immediate controlled shutdown and minimize the risk associated with an immediate controlled shutdown and minimize the risk associated with this level of degradation.

According to Regulatory Guide 1.93 (Ref. 6), with two or more DGs inoperable, operation may continue for a period that should not exceed 2 hours. (Regulatory Guide 1.93 assumed the unit had two DGs. Thus, a loss of both DGs results in a total loss of onsite power.) Therefore, a loss of both Unit 1 DGs and the swing DG results in degradation no worse than that assumed in Regulatory Guide 1.93, and the 2 hour Completion Time is acceptable.

H.1 and H.2

If the inoperable AC electrical power sources cannot be restored to OPERABLE status within the associated Completion Time, the unit must be brought to a MODE in which the LCO does not apply. To achieve this status, the unit must be brought to at least MODE 3 within 12 hours and to MODE 4 within 36 hours. The allowed Completion Times are reasonable, based on operating experience, to reach the required plant conditions from full power conditions in an orderly manner and without challenging plant systems.

I.1

Condition I corresponds to a level of degradation in which all redundancy in the AC electrical power supplies has been lost. At this severely degraded level, any further losses in the AC electrical power system will cause a loss of function. Therefore, no additional time is justified for continued operation. The unit is required by LCO 3.0.3 to commence a controlled shutdown.

SURVEILLANCE REQUIREMENTS

The AC sources are designed to permit inspection and testing of all important areas and features, especially those that have a standby function, in accordance with

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

10 CFR 50, GDC 18 (Ref. 8). Periodic component tests are supplemented by extensive functional tests during refueling outages under simulated accident conditions. The SRs for demonstrating the OPERABILITY of the DGs are generally consistent with the recommendations of Regulatory Guide 1.9 (Ref. 3), Regulatory Guide 1.108 (Ref. 9), and Regulatory Guide 1.137 (Ref. 10), although Plant Hatch Unit 2 is not committed to Regulatory Guides 1.108 or 1.137. Specific commitments relative to DG testing is described in FSAR Section 8.3 (Ref. 2).

Where the SRs discussed herein specify voltage and frequency tolerances, the following summary is applicable. The allowable values for achieving steady state voltage are specified within a range of minus 10 percent (3740 V) and plus 2 percent (4243 V) of 4160 V. The Allowable Value of 3740 V is consistent with Regulatory Guide 1.9 for demonstrating that the diesel generator is capable of attaining the required voltage. A more limiting value of 4243 V is specified as the allowable value for overvoltage due to overvoltage limits on the 600 V buses. The plus 2 percent value maintains the required overvoltage limits. The specified minimum and maximum frequencies of the DG are 58.8 Hz and 61.2 Hz, respectively. These values are equal to ± 2% of the 60 Hz nominal frequency and are derived from the recommendations found in Regulatory Guide 1.9 (Ref. 3).

The SRs are modified by a Note to indicate that SR 3.8.1.1 through SR 3.8.1.18 apply only to the Unit 2 AC sources, and that SR 3.8.1.19 applies only to the Unit 1 AC sources.

SR 3.8.1.1

This SR ensures proper circuit continuity for the offsite AC electrical power supply to the onsite distribution network and availability of offsite AC electrical power. The breaker alignment verifies that each breaker is in its correct position to ensure that distribution buses and loads are connected to their preferred power source and that appropriate independence of offsite circuits is maintained. The 7 day Frequency is adequate since breaker position is not likely to change without the operator being aware of it and because its status is displayed in the control room.

(continued)

BASES

SURVEILLANCE REQUIREMENTS (continued)

SR 3.8.1.2

This SR helps to ensure the availability of the standby electrical power supply to mitigate DBAs and transients and maintain the unit in a safe shutdown condition, and verifies that the DGs are capable of proper startup, synchronizing, and accepting a load approximately 50% of the continuous load rating. This demonstrates DG capability while minimizing the mechanical stress and wear on the engine. A minimum run time of 60 minutes is required to stabilize engine temperatures, while minimizing the time that the DG is connected to the offsite source.

Although no power factor requirements are established by this SR, the DG is normally operated at a power factor between 0.8 lagging and 1.0. The 0.8 value is the design rating of the machine, while 1.0 is an operational limitation.

To minimize the wear on moving parts that do not get lubricated when the engine is not running, this SR has been modified by a Note (Note 2) to indicate that all DG starts for this Surveillance may be preceded by an engine prelube period and followed by a warmup prior to loading.

For the purposes of this testing, the DGs are started from standby conditions. Standby conditions for a DG mean that the diesel engine coolant and oil are being continuously circulated and temperature is being maintained consistent with manufacturer recommendations.

In order to reduce stress and wear on diesel engines, the DG manufacturer recommends a modified start in which the starting speed of DGs is limited, warmup is limited to this lower speed, and the DGs are gradually accelerated to synchronous speed prior to loading. These start procedures are the intent of Note 3. Once voltage and frequency requirements are demonstrated, the DG may be tied to its respective 4160 V emergency bus, as directed by SR 3.8.1.2.b. When the DG is tied to its bus, the electrical grid, due to its larger size compared to the DG, will dictate DG voltage and frequency. The DG operator cannot adjust either parameter. Therefore, the voltage and frequency requirements of SR 3.8.1.2.a no longer apply while the DG is tied to its bus and need not be met to satisfy the requirements of SR 3.8.1.2.b. Other SRs, notably

(continued)

BASES

SURVEILLANCE REQUIREMENTS

SR 3.8.1.2 (continued)

SR 3.8.1.9, require that voltage and frequency requirements can be met while the DG is supplying load.

SR 3.8.1.5.a requires that, at a 184 day Frequency, the DG starts from standby conditions and achieves required voltage and frequency within 12 seconds. The 12 second start requirement supports the assumptions in the design basis LOCA analysis of FSAR, Chapter 6 (Ref. 4). The 12 second start requirement is not applicable to SR 3.8.1.2 (see Note 3), when a modified start procedure as described above is used. If a modified start is not used, the 12 second start voltage and frequency requirements of SR 3.8.1.5.a apply.

Since SR 3.8.1.5.a does require a 12 second start, it is more restrictive than SR 3.8.1.2, and it may be performed in lieu of SR 3.8.1.2. This procedure is the intent of Note 1.

To minimize testing of the swing DG, this SR is modified by a note (Note 4) to allow a single test (instead of two tests, one for each unit) to satisfy the requirements for both units, using the starting circuitry of one unit for one periodic test and the starting circuitry of the other unit during the next periodic test. This is allowed since the main purpose of the Surveillance, to ensure DG OPERABILITY, is still being verified on the proper frequency, the starting circuits historically have a very low failure rate, as compared to the DG itself, and that, while each starting circuit is only being tested every second test (due to the staggering of the tests), some portions of the starting circuits are common to both units. If the swing DG fails one of these Surveillance, the DG should be considered inoperable on both units, unless the cause of the failure can be directly related to only one unit.

Note 5 modifies this Surveillance to indicate that diesel engine runs for this Surveillance may include gradual loading, as recommended by the manufacturer, so that mechanical stress and wear on the diesel engine are minimized.

Note 6 modifies the Surveillance by stating that starting transients above the upper voltage limit do not invalidate this test.

(continued)

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
A. One required offsite circuit inoperable.	A.1	Perform SR 3.8.1.1 for OPERABLE required offsite circuits.	1 hour AND Once per 8 hours thereafter
	AND		
	A.2	Declare required feature(s) with no offsite power available inoperable when the redundant required feature(s) are inoperable.	24 hours from discovery of no offsite power to one 4160 V ESF bus concurrent with inoperability of redundant required feature(s)
	AND		
	A.3	Restore required offsite circuit to OPERABLE status.	72 hours AND 17 ~~10~~ days from discovery of failure to meet LCO 3.8.1.a, b, or c
B. One Unit 1 or the swing DG inoperable.	B.1	Perform SR 3.8.1.1 for OPERABLE required offsite circuit(s).	1 hour AND Once per 8 hours thereafter
	AND		

(continued)

ACTIONS

CONDITION	REQUIRED ACTION	COMPLETION TIME
B. (continued)	B.2 Declare required feature(s), supported by the inoperable DG, inoperable when the redundant required feature(s) are inoperable.	4 hours from discovery of Condition B concurrent with inoperability of redundant required feature(s)
	AND	
	B.3.1 Determine OPERABLE DG(s) are not inoperable due to common cause failure.	24 hours
	OR	
	B.3.2 Perform SR 3.8.1.2.a for OPERABLE DG(s).	24 hours
	AND	
	B.4 Restore DG to OPERABLE status.	72 hours for a Unit 1 DG with the swing DG not inhibited AND 14 days for the swing DG AND 17 days from discovery of failure to meet LCO 3.8.1.a, b, or c

(continued)

ACTIONS (continued)

CONDITION	REQUIRED ACTION	COMPLETION TIME
C. One required Unit 2 DG inoperable.	C.1 Perform SR 3.8.1.1 for OPERABLE required offsite circuit(s).	1 hour AND Once per 8 hours thereafter
	AND	
	C.2 Declare required feature(s), supported by the inoperable DG, inoperable when the redundant required feature(s) are inoperable.	4 hours from discovery of Condition C concurrent with inoperability of redundant required feature(s)
	AND	
	C.3.1 Determine OPERABLE DG(s) are not inoperable due to common cause failure.	24 hours
	OR	
	C.3.2 Perform SR 3.8.1.2.a for OPERABLE DG(s).	24 hours
	AND	
	C.4 Restore required DG to OPERABLE status.	~~7 days~~

(continued)

7 days with the swing DG not inhibited

AND

14 days with the swing DG inhibited from automatically aligning to Unit 1

BASES

ACTIONS

A.3 (continued)

reliability of the offsite system is degraded, and the potential for a loss of offsite power is increased, with attendant potential for a challenge to the plant safety systems. In this condition, however, the remaining OPERABLE offsite circuit and DGs are adequate to supply electrical power to the onsite Class 1E Distribution System.

The 72 hour Completion Time takes into account the capacity and capability of the remaining AC sources, reasonable time for repairs, and the low probability of a DBA occurring during this period.

The second Completion Time for Required Action A.3 establishes a limit on the maximum time allowed for any combination of required AC power sources to be inoperable during any single contiguous occurrence of failing to meet LCO 3.8.1.a, b, or c. If Condition A is entered while, for instance, the swing DG is inoperable, and that DG is subsequently returned OPERABLE, LCO 3.8.1.a, b, or c may already have been not met for up to 7 days. This situation could lead to a total of 10 days, since initial failure to meet LCO 3.8.1.a, b, and c, to restore the offsite circuit. At this time, the swing DG could again become inoperable, the circuit restored OPERABLE, and an additional 7 days (for a total of 17 days) allowed prior to complete restoration of LCO 3.8.1.a, b, and c. The 10 day Completion Time provides a limit on the time allowed in a specified condition after discovery of failure to meet LCO 3.8.1.a, b, or c. This limit is considered reasonable for situations in which Conditions A and B are entered concurrently. The "AND" connector between the 72 hours and 10 day Completion Times means that both Completion Times apply simultaneously, and the more restrictive Completion Time must be met.

As in Required Action A.2, the Completion Time allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." This exception results in establishing the "time zero" at the time LCO 3.8.1.a, b, or c was initially not met, instead of at the time that Condition A was entered.

(continued)

BASES

ACTIONS

B.3.1 and B.3.2 (continued)

According to Generic Letter 84-15 (Ref. 7), 24 hours is a reasonable time to confirm that the OPERABLE DGs are not affected by the same problem as the inoperable DG.

B.4 <Replace with Insert 1>

According to Regulatory Guide 1.93 (Ref. 6), operation may continue in Condition B for a period that should not exceed 72 hours. However, if the inoperable DG is the swing DG, operation may continue in Condition B for a period that should not exceed 7 days. In Condition B, the remaining OPERABLE DGs and offsite circuits are adequate to supply electrical power to the onsite Unit 1 Class 1E Distribution System. The 72 hour Completion Time takes into account the capacity and capability of the remaining AC sources, reasonable time for repairs, and low probability of a DBA occurring during this period. The 7 day Completion Time for the swing DG also takes into consideration the fact that the DG is common to both units, and that time must be provided to perform routine maintenance on the DG without requiring a dual unit shutdown.

fourth

The third Completion Time for Required Action B.4 establishes a limit on the maximum time allowed for any combination of required AC power sources to be inoperable during any single contiguous occurrence of failing to meet LCO 3.8.1.a, b, or c. If Condition B is entered while, for instance, an offsite circuit is inoperable and that circuit is subsequently restored OPERABLE, LCO 3.8.1.a, b, or c may already have been not met for up to 72 hours. This situation could lead to a total of 10 days, since initial failure to meet LCO 3.8.1.a, b, and c, to restore the DG. At this time, an offsite circuit could again become inoperable, the DG restored OPERABLE, and an additional 72 hours (for a total of 13 days) allowed prior to complete restoration of LCO 3.8.1.a, b, and c. The 10 day Completion Time provides a limit on the time allowed in a specified condition after discovery of failure to meet LCO 3.8.1.a, b, or c. This limit is considered reasonable for situations in which Conditions A and B are entered concurrently. The "AND" Connector between the 72 hour and 10 day Completion Times means that both Completion Times apply simultaneously, and the more restrictive must be met.

17

20

17

connectors

all

(continued)

INSERT 1

Regulatory Guide 1.93 (Ref. 6) provides guidance that operation in Condition B may continue for 72 hours. A risk-informed, deterministic evaluation performed for Plant Hatch justifies operation in Condition B for 14 days, provided action is taken to ensure two DGs are dedicated to each Hatch unit. This is accomplished for an inoperable A or C DG by inhibiting the automatic alignment (on a LOCA or LOSP signal) of the swing DG to the other unit. If the inoperable DG is the swing DG, then each unit has two dedicated DGs and a 14 day Completion Time is allowed. In Condition B for each defined Completion Time and restriction (if applicable), the remaining OPERABLE DGs and offsite circuits are adequate to supply electrical power to the onsite Unit 1 Class 1E Distribution System. The Completion Times take into account the capacity and capability of the remaining AC sources, reasonable time for maintenance, and low probability of a DBA occurring during this period. Entry into Condition B for the purpose of planned maintenance, subject to additional restrictions controlled by plant procedures, is allowed.

The "AND" connector between the 72 hour and 14 day Completion Times means that both Completion Times apply simultaneously. That is, the 14 day Completion Time for an A or C DG with the swing DG inhibited applies from the time of entry into Condition B, not from the time that the swing DG is inhibited.

BASES

ACTIONS

C.3.1 and C.3.2 (continued)

initial inoperable DG cannot be confirmed not to exist on the remaining DG(s), performance of SR 3.8.1.2.a suffices to provide assurance of continued OPERABILITY of those DGs. In the event the inoperable DG is restored to OPERABLE status prior to completing either C.3.1 or C.3.2, the deficiency control program, as appropriate, will continue to evaluate the common cause possibility. This continued evaluation, however, is no longer under the 24 hour constraint imposed while in Condition C.

According to Generic Letter 84-15 (Ref. 7), 24 hours is a reasonable time to confirm that the OPERABLE DGs are not affected by the same problem as the inoperable DG.

C.4

In Condition C, the remaining OPERABLE offsite circuit is adequate to supply electrical power to the required onsite Unit 2 Class 1E Distribution System. The 7 day Completion Time takes into account the capacity and capability of the remaining AC source, reasonable time for repairs, and low probability of a DBA occurring during this period. In addition, the shortest restoration time allowed for the systems affected by the inoperable DG is 7 days in the individual system's LCOs.

Replace with Insert 2

D.1 and D.2

Required Action D.1 addresses actions to be taken in the event of inoperability of redundant required features concurrent with inoperability of two or more required offsite circuits. Required Action D.1 reduces the vulnerability to a loss of function. The Completion Time for taking these actions is reduced to 12 hours from that allowed with one 4160 V ESF bus without offsite power (Required Action A.2). The rationale for the reduction to 12 hours is that Regulatory Guide 1.93 (Ref. 6) allows a Completion Time of 24 hours for two required offsite circuits inoperable, based upon the assumption that two complete safety divisions are OPERABLE. (While this ACTION allows more than two circuits to be inoperable, Regulatory Guide 1.93 assumed two circuits were all that were required

(continued)

INSERT 2

The 7 day Completion Time is based on the shortest restoration time allowed for the systems affected by the inoperable DG in the individual system LCOs. A risk-informed, deterministic evaluation performed for Plant Hatch justifies operation in Condition C for 14 days, provided action is taken to ensure two DGs are dedicated to each Hatch unit. This is accomplished for an inoperable A or C DG by inhibiting the automatic alignment (on a LOCA or LOSP signal) of the swing DG to the other unit. The Completion Times take into account the capacity and capability of the remaining AC sources, reasonable time for maintenance, and low probability of a DBA occurring during this period. Entry into Condition C for the purpose of planned maintenance, subject to additional restrictions controlled by plant procedures, is allowed.

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
A. One required offsite circuit inoperable.	A.1	Perform SR 3.8.1.1 for OPERABLE required offsite circuits.	1 hour AND Once per 8 hours thereafter
	AND		
	A.2	Declare required feature(s) with no offsite power available inoperable when the redundant required feature(s) are inoperable.	24 hours from discovery of no offsite power to one 4160 V ESF bus concurrent with inoperability of redundant required feature(s)
	AND		
	A.3	Restore required offsite circuit to OPERABLE status.	72 hours AND 17 18 days from discovery of failure to meet LCO 3.8.1.a, b, or c
B. One Unit 2 or the swing DG inoperable.	B.1	Perform SR 3.8.1.1 for OPERABLE required offsite circuit(s).	1 hour AND Once per 8 hours thereafter
	AND		

(continued)

ACTIONS

CONDITION	REQUIRED ACTION		COMPLETION TIME
B. (continued)	B.2	Declare required feature(s), supported by the inoperable DG, inoperable when the redundant required feature(s) are inoperable.	4 hours from discovery of Condition B concurrent with inoperability of redundant required feature(s)
	AND		
	B.3.1	Determine OPERABLE DG(s) are not inoperable due to common cause failure.	24 hours
	OR		
	B.3.2	Perform SR 3.8.1.2.a for OPERABLE DG(s).	24 hours
	AND		
	B.4	Restore DG to OPERABLE status.	72 hours for a Unit 2 DG with the swing DG not inhibited AND 14 days for a Unit 2 DG with the swing DG inhibited from automatically aligning to Unit 1.
			AND (14) 0 days for the swing DG AND (17) 10 days from discovery of failure to meet LCO 3.8.1.a, b, or c

(continued)

ACTIONS (continued)

CONDITION	REQUIRED ACTION		COMPLETION TIME
C. One required Unit 1 DG inoperable.	C.1	Perform SR 3.8.1.1 for OPERABLE required offsite circuit(s).	1 hour AND Once per 8 hours thereafter
	AND		
	C.2	Declare required feature(s), supported by the inoperable DG, inoperable when the redundant required feature(s) are inoperable.	4 hours from discovery of Condition C concurrent with inoperability of redundant required feature(s)
	AND		
	C.3.1	Determine OPERABLE DG(s) are not inoperable due to common cause failure.	24 hours
	OR		
	C.3.2	Perform SR 3.8.1.2.a for OPERABLE DG(s).	24 hours
	AND		
	C.4	Restore required DG to OPERABLE status.	7 ~~days~~

(continued)

7 days with the swing DG not inhibited

AND

14 days with the swing DG inhibited from automatically aligning to Unit 2

BASES

ACTIONS

A.3 (continued)

reliability of the offsite system is degraded, and the potential for a loss of offsite power is increased, with attendant potential for a challenge to the plant safety systems. In this condition, however, the remaining OPERABLE offsite circuit and DGs are adequate to supply electrical power to the onsite Class 1E Distribution System.

The 72 hour Completion Time takes into account the capacity and capability of the remaining AC sources, reasonable time for repairs, and the low probability of a DBA occurring during this period.

The second Completion Time for Required Action A.3 establishes a limit on the maximum time allowed for any combination of required AC power sources to be inoperable during any single contiguous occurrence of failing to meet LCO 3.8.1.a, b, or c. If Condition A is entered while, for instance, the swing DG is inoperable, and that DG is subsequently returned OPERABLE, LCO 3.8.1.a, b, or c may already have been not met for up to 7 days. This situation could lead to a total of 10 days, since initial failure to meet LCO 3.8.1.a, b, and c, to restore the offsite circuit. At this time, the swing DG could again become inoperable, the circuit restored OPERABLE, and an additional 7 days (for a total of 17 days) allowed prior to complete restoration of LCO 3.8.1.a, b, and c. The 10 day Completion Time provides a limit on the time allowed in a specified condition after discovery of failure to meet LCO 3.8.1.a, b, or c. This limit is considered reasonable for situations in which Conditions A and B are entered concurrently. The "AND" connector between the 72 hours and 10 day Completion Times means that both Completion Times apply simultaneously, and the more restrictive Completion Time must be met.

As in Required Action A.2, the Completion Time allows for an exception to the normal "time zero" for beginning the allowed outage time "clock." This exception results in establishing the "time zero" at the time LCO 3.8.1.a, b, or c was initially not met, instead of at the time that Condition A was entered.

(continued)

BASES

ACTIONS

B.3.1 and B.3.2 (continued)

According to Generic Letter 84-15 (Ref. 7), 24 hours is a reasonable time to confirm that the OPERABLE DGs are not affected by the same problem as the inoperable DG.

B.4 <Replace with Insert 3>

According to Regulatory Guide 1.93 (Ref. 6), operation may continue in Condition B for a period that should not exceed 72 hours. However, if the inoperable DG is the swing DG, operation may continue in Condition B for a period that should not exceed 7 days. In Condition B, the remaining OPERABLE DGs and offsite circuits are adequate to supply electrical power to the onsite Unit 2 Class 1E Distribution System. The 72 hour Completion Time takes into account the capacity and capability of the remaining AC sources, reasonable time for repairs, and low probability of a DBA occurring during this period. The 7 day Completion Time for the swing DG also takes into consideration the fact that the DG is common to both units, and that time must be provided to perform routine maintenance on the DG without requiring a dual unit shutdown.

fourth

The third Completion Time for Required Action B.4 establishes a limit on the maximum time allowed for any combination of required AC power sources to be inoperable during any single contiguous occurrence of failing to meet LCO 3.8.1.a, b, or c. If Condition B is entered while, for instance, an offsite circuit is inoperable and that circuit is subsequently restored OPERABLE, LCO 3.8.1.a, b, or c may

17

already have been not met for up to 72 hours. This situation could lead to a total of 10 days, since initial failure to meet LCO 3.8.1.a, b, and c, to restore the DG.

20

At this time, an offsite circuit could again become inoperable, the DG restored OPERABLE, and an additional 72 hours (for a total of 12 days) allowed prior to complete

17

restoration of LCO 3.8.1.a, b, and c. The 10 day Completion Time provides a limit on the time allowed in a specified condition after discovery of failure to meet LCO 3.8.1.a, b, or c. This limit is considered reasonable for situations in

connectors

which Conditions A and B are entered concurrently. The "AND" connector between the 72 hour and 10 day Completion

all

Times means that both Completion Times apply simultaneously, and the more restrictive must be met.

(continued)

INSERT 3

Regulatory Guide 1.93 (Ref. 6) provides guidance that operation in Condition B may continue for 72 hours. A risk-informed, deterministic evaluation performed for Plant Hatch justifies operation in Condition B for 14 days, provided action is taken to ensure two DGs are dedicated to each Hatch unit. This is accomplished for an inoperable A or C DG by inhibiting the automatic alignment (on a LOCA or LOSP signal) of the swing DG to the other unit. If the inoperable DG is the swing DG, then each unit has two dedicated DGs and a 14 day Completion Time is allowed. In Condition B for each defined Completion Time and restriction (if applicable), the remaining OPERABLE DGs and offsite circuits are adequate to supply electrical power to the onsite Unit 2 Class 1E Distribution System. The Completion Times take into account the capacity and capability of the remaining AC sources, reasonable time for maintenance, and low probability of a DBA occurring during this period. Entry into Condition B for the purpose of planned maintenance, subject to additional restrictions controlled by plant procedures, is allowed.

The "AND" connector between the 72 hour and 14 day Completion Times means that both Completion Times apply simultaneously. That is, the 14 day Completion Time for an A or C DG with the swing DG inhibited applies from the time of entry into Condition B, not from the time that the swing DG is inhibited.

BASES

ACTIONS

C.3.1 and C.3.2 (continued)

initial inoperable DG cannot be confirmed not to exist on the remaining DG(s), performance of SR 3.8.1.2.a suffices to provide assurance of continued OPERABILITY of those DGs. In the event the inoperable DG is restored to OPERABLE status prior to completing either C.3.1 or C.3.2, the deficiency control program, as appropriate, will continue to evaluate the common cause possibility. This continued evaluation, however, is no longer under the 24 hour constraint imposed while in Condition C.

According to Generic Letter 84-15 (Ref. 7), 24 hours is a reasonable time to confirm that the OPERABLE DGs are not affected by the same problem as the inoperable DG.

C.4

In Condition C, the remaining OPERABLE offsite circuit is adequate to supply electrical power to the required onsite Unit 1 Class 1E Distribution System. The 7 day Completion Time takes into account the capacity and capability of the remaining AC source, reasonable time for repairs, and low probability of a DBA occurring during this period. In addition, the shortest restoration time allowed for the systems affected by the inoperable DG is 7 days in the individual system's LCOs.

Replace with Insert 2

D.1 and D.2

Required Action D.1 addresses actions to be taken in the event of inoperability of redundant required features concurrent with inoperability of two or more required offsite circuits. Required Action D.1 reduces the vulnerability to a loss of function. The Completion Time for taking these actions is reduced to 12 hours from that allowed with one 4160 V ESF bus without offsite power (Required Action A.2). The rationale for the reduction to 12 hours is that Regulatory Guide 1.93 (Ref. 6) allows a Completion Time of 24 hours for two required offsite circuits inoperable, based upon the assumption that two complete safety divisions are OPERABLE. (While this ACTION allows more than two circuits to be inoperable, Regulatory Guide 1.93 assumed two circuits were all that were required

(continued)

INSERT 2

The 7 day Completion Time is based on the shortest restoration time allowed for the systems affected by the inoperable DG in the individual system LCOs. A risk-informed, deterministic evaluation performed for Plant Hatch justifies operation in Condition C for 14 days, provided action is taken to ensure two DGs are dedicated to each Hatch unit. This is accomplished for an inoperable A or C DG by inhibiting the automatic alignment (on a LOCA or LOSP signal) of the swing DG to the other unit. The Completion Times take into account the capacity and capability of the remaining AC sources, reasonable time for maintenance, and low probability of a DBA occurring during this period. Entry into Condition C for the purpose of planned maintenance, subject to additional restrictions controlled by plant procedures, is allowed.

Attachment 1

Edwin I. Hatch Nuclear Plant
Request to Revise Technical Specifications:
Extension of Completion Times for Inoperable Emergency Diesel Generators

Description of Plant Hatch Probabilistic Safety Assessment

Description of Plant Hatch Probabilistic Safety Assessment

Attachment 1

Description of Plant Hatch Probabilistic Safety Assessment

This information is used to describe the Unit 1 Revision 1 Probabilistic Safety Assessment (PSA) "At Power" model. This documentation allows for a general understanding of how the conversion from the RISKMAN Event Tree Linking model to the CAFTA Fault Tree Linking model was accomplished.

The following information describes the formation of the sequences which comprise the event trees that were used to construct the Hatch PSA model. This information is divided into two parts. The first part describes sequence formation and definitions. The second part describes how the sequences are used to build the CAFTA model as well as quantification results.

PART 1 Sequence Development and RISKMAN to CAFTA Conversion

Table of Contents

1.0 INTRODUCTION

This report documents the development of the Plant Hatch core damage sequences and their associated event trees. The purpose of the project was to convert the RISKMAN event trees to Windows ETA event trees. This effort is part of a larger project to convert the Hatch RISKMAN model to a CAFTA "linked fault tree" model. This document describes the resultant core damage event trees and sequences. Development of the plant damage model that carries the events out to plant damage states for release category classification is not discussed at this time.

1.1 Event Tree Conversion

As part of the conversion process, Hatch documents prepared during the IPE were reviewed. The document review included the reports identified above as well as fault trees, event trees, and the Hatch IPE submittal. In addition to providing the original event trees, these reports also provided the list of assumptions and success criteria used in the original analysis. Additional insight was provided from the review of the IPE submittal. Since the basic assumptions and success criteria remain true, they will not be reiterated in this report.

During the conversion process, every attempt was made to maintain the fidelity of the IPE model and achieve simplification by combining mitigation systems into similar event tree functions. For each initiator, multiple, linked event trees were consolidated into one event tree. In addition, event trees for initiators with similar plant response are grouped and represented by the same, converted event trees. The conversion was achieved as follows:

First, all event trees associated with each specific initiator were identified. The frontline system event trees were reviewed and evaluated for similarity in plant response characterized by top events and sequence logic. Initiators with similar plant response and RISKMAN event trees were grouped together for the purpose of developing ETA event trees. For example, all of the transient initiators are grouped under the category of "Transients."

RISKMAN initiators LOSPAC, LOSPDC, LOSPPS, LOSPVM, LOSPLL, LOSPML, and LOSPSL are not needed since loss of offsite power following each of the corresponding initiators (i.e., LOBUSE, LOBUSF, and LOBUSG for LOSPAC, LODC for LOSPDC, LOPSW for LOSPPS, LOMCHV for LOSPVM, LLOCA for LOSPLL, MLOCA for LOSPML, and SLOCA for LOSPSL) is accounted for in the linked fault tree for the corresponding initiators.

Break outside containment and V sequence initiators lead to core damage directly. No event trees were developed in this conversion.

It is noted that the ETA event trees encompass only the RISKMAN frontline systems event trees. The RISKMAN support systems event trees (ELEC1, MECH1, ELEC2, and MECH2) do not need to be represented in the ETA trees since support systems are linked directly through the fault tree models. Separate support systems event trees are not necessary for a linked fault tree model.

In addition, top events within the linked, RISKMAN event trees for each of the initiator groups were merged or collapsed as appropriate. If separate top events represented different elements of a function, the top events were combined into one ETA event tree heading with multiple inputs.

For example, RISKMAN top events CO (condensate initially unavailable for injection), FW (feedwater pumps not available or tripped following transient), FR (feedwater/condensate not recovered before Level 2 reached), and MC (MSIVs fail to remain open/Main condenser not available) could be collapsed into an ETA event tree heading named PCS representing the unavailability of the power conversion system. All of the nodes under this heading in the ETA event tree for "Transient" are represented by a fault tree designated as #PCS. The pound sign serves as an indicator that multiple inputs exist at that node.

In the discussion that follows, each of the event tree groups will be discussed. For each case, the modifications, node headings and sequences will be identified and documented.

2.0 EVENT TREES

The following sections will provide a detailed description of the accident sequences.

2.1 The Transient Event Tree

This sections contains information regarding the core damage event tree developed for all of the transient initiators, including &LOSUTD, %TTRIP, &LOMCHV, &DCPAN, &LODC, %MSIVC, %SLOCA, &BUSC, &BUSD, &LOBUSE, &LOBUSF, &LOBUSG, &LODWC, %SCRAM, %LOFW, %LOCV, &DISCH, &INTAKE, and &LOPSW. Note that initiators with "&" in the first character of their designators are, in general, support system failure initiating events. Each of these initiators (or called special initiators) is modeled by a system fault tree. The remaining initiators are signified by "%" in the first character of their designators.

This transient event tree covers transient-induced LOCAs and loss of offsite power (LOSP) following transient initiators. This tree does not include core damage sequences associated with the LOSP initiator and the corresponding Station Blackout (SBO) scenarios. Core damage sequences induced by Anticipated Transient Without Scram (ATWS) following transient initiators are modeled separately with the ATWS initiators.

EVENT TREE MODIFICATION

In the IPE, the frontline system core damage sequences for each of the transient initiators were obtained by linking together 5 RISKMAN frontline systems event trees. For example, event trees TTRIP, INTER1, REC0, RHRCS, and LTC1 were linked together to model the core damage sequences for initiator TTRIP. In IPE for this group of initiators, the first RISKMAN event tree used in the string of linked event trees is TTRIP, MSIVC, SCRAM, LOFW, or LOCV, depending on the initiator. These 5 RISKMAN event trees have identical tree structure. The only differences between these 5 event trees are the split fraction assignments for selected top events. These split fraction assignments vary as a function of the initiator considered. With the exception of initiators DISCH, INTAKE, and LOPSW, the remaining 4 RISKMAN event trees linked together for the quantification of this group of initiators are identical (i.e., INTER1, REC0, RHRCS, and LTC1). Initiators DISCH, INTAKE, and LOPSW use the following set of RISKMAN event trees linked together: TTRIP, INTER1, REC1, RHRCS, and LTC1. The tree structures for RISKMAN event trees REC0 and REC1 are identical and the only differences between these two trees are split fraction assignments.

After reviewing the RISKMAN event trees developed for the previously mentioned group of initiating events, the following key changes were made:

- The initiators were combined into a single transient initiator heading GT (with a node designated by IEGGT).

- Top events modeled in RISKMAN event trees TTRIP/MSIVC/SCRAM/LOFW/LOCV are combined according to the functions provided by the individual systems.

- With the exception of RP, most of the top events in RISKMAN event tree INTER1 are incorporated into lower level fault tree models for LOCA signal, operator restoration following a LOCA signal, automatic/emergency depressurization, main condenser availability, recovery of HPCI/RCIC, etc.

- Recovery top events modeled in REC0 or REC1 are incorporated into the appropriate system fault trees throughout the model.

- Most top events listed in RISKMAN event trees RHRCS and LTC1 are incorporated into the lower level fault trees for ETA headings DE, LO, and QR. RISKMAN top events Z5, DESC2, DESC1, CFF, and IN2 were determined to be not functional requirements for core damage.

The initiators included in the ETA transient initiator heading GT are:

General:	%TTRIP, %MSIVC, %SLOCA, %SCRAM, %LOFW, and %LOCV
Special initiators:	&LOSUTD, &LOMCHV, &DCPAN, &LODC, &BUSC, &BUSD, &LOBUSE, &LOBUSF, &LOBUSG, &LODWC, &DISCH, &INTAKE, and &LOPSW

For the new ETA event tree GT, nodes under each heading may be represented by one or more fault tree gates. The multiple RISKMAN system models were combined into one fault tree gate with additional compression achieved by combining similar functions into one final fault tree gate with multiple inputs. Listed below are the new top logic gates developed for the ETA event tree nodes and the original inputs associated with each (i.e., RISKMAN event tree top events combined into the gate):

#BVPR	BV, PR
#SORV0/1/2/3	SORV
#PCS	CO, FW, FR, MC, MS
#HP-1	RCIC, HPCI, HI, CW, RD
#ADED	VC, V18, LOCA, L1OP, DWTC, OW
#RP	RP, RPOP
#DEHICO1	DE, HI, CO
#LO	CO, CS, RA, RB, JS, VA, VB, VOP, NS, NSREC, LC
#QRIN1REC/#QRQRA/ #QR/#QT	OL, QC, QS, QT, RA, RB, VA, VB, VOP, HA, HB, QV, IN1, QR

EVENT TREE HEADINGS & BRANCHES

The following event tree headings and nodes appear on the tree in the approximate chronological order that would be expected during a transient.

GT General Transient Initiating Events. This heading (Branch ID IEGGT) includes all general transient and special initiators.

BVPR Pressure Relief. This heading models the pressure control function performed by the turbine bypass valves and SRVs during the initial pressure transient following a plant trip. For transient events with MSIVs open, both the turbine bypass valves and the SRVs may be available. Failure of this event (Branch ID #BVPR) is modeled as resulting in a medium-break LOCA.

SORV SORV Reclosure. This is a multistate heading. It models the reclosure status of SRVs (i.e., the number of stuck open SRVs). The four states applicable to this heading are: all SRVs successfully reclose (Branch ID #SORV0); one SRV fails to reclose (Branch ID #SORV1); two SRVs fail to reclose (Branch ID #SORV2); and three or more SRVs fail to reclose (Branch ID #SORV3).

PCS Power Conversion System. This heading models the availability or unavailability of the power conversion system to provide the core cooling function. Condensate system, feedwater system, and main condenser are included in this heading. One condensate pump and one condensate booster pump are required to support operation of a single feedwater pump when the plant unit is shut down. Only one reactor feed pump is required to provide feedwater flow to the reactor for level control. If the feedwater is initially unavailable following a reactor trip, restoration of feedwater prior to initiation of HPCI, or RCIC on Level 2 is also considered in this heading.

Success of this event implies that condensate, feedwater, and main condenser are available for plant response following the reactor trip. For the main condenser to remain available, the MSIVs must remain open, turbine bypass valves must continue to function and all support for the electrohydraulic control system must be available. Failure of this event (Branch ID #PCS) implies that RCIC/HPCI will be demanded to operate to provide the high pressure level control function. Due to the rapid vessel depressurization, PCS is not asked in sequences involving three or more stuck open SRVs (Branch ID #SORV3).

HPI High Pressure Level Control by RCIC/HPCI. This heading models the high pressure level control function provided by the RCIC and HPCI systems. Both automatic and manual actuations are considered in this heading. Also included in this heading are the operator actions to control HPCI and RCIC to prevent multiple Level 8 trips. For any stuck-open SRVs and medium LOCAs, RCIC is inadequate for vessel level control. For three or more stuck-open SRVs, HPCI is inadequate, and for one or two SRVs stuck open HPCI recovery is not credited. This event is only asked in this event tree when PCS is unsuccessful. Success of this event implies that RCIC or HPCI is available to provide the high pressure level control function. Failure of this event (Branch ID #HP-1) implies that both RCIC and HPCI are unavailable for the vessel level control function and vessel depressurization is required.

ADED Automatic and Emergency Depressurization Conditions. This heading models the automatic and emergency depressurization conditions. The automatic depressurization condition is modeled by generation of the LOCA signal and failure of the operators to inhibit ADS actuation. LOCA signals include Level 1 and high drywell pressure signals. In addition, it was assumed that loss of MCR cooling would result in generation of a LOCA signal. Failure of drywell cooling (RISKMAN Top Event VC) and failure of the operators to vent via the 18" vents to prevent a LOCA signal (RISKMAN Top Event V18) were assumed to lead to generation of a high drywell pressure signal.

Emergency vessel depressurization is required by the Plant Hatch procedures if the drywell temperature limit is exceeded. Drywell temperature would increase if drywell cooling fails and the operators fail to initiate drywell spray (RISKMAN Top Event OW), or if the operators fail to restore drywell cooling following a LOCA signal.

Success of this event implies that there are no automatic and emergency depressurization conditions, or the operators successfully inhibit ADS and restore drywell cooling given a LOCA signal. Failure of this event (Branch ID #ADED) implies that ADS would be actuated or the operators are required to initiate emergency vessel depressurization. It is assumed in sequences involving failure of this heading that vessel is depressurized and downstream heading DE is not asked. This heading is not asked if both PCS and HPI fail requiring a vessel depressurization (downstream heading DE).

RP Return to Power Operation. This heading models the success path with the reactor returning to power operation without proceeding to cold shutdown. This heading is only asked if the pressure relief function performed by the turbine bypass valves/SRVs is successful, there is no stuck-open SRV, RCIC/HPCI is successful in controlling vessel level, and there is no automatic/emergency vessel depressurization condition. Success of this event implies that the transient has been terminated and plant returns to power operation. Loss of the main condenser or failure of any support system would cause failure of this event (Branch ID #RP).

DE Depressurization of Vessel Before Core Damage. This heading models the reduction of vessel pressure to permit level recovery. This heading includes the manual emergency depressurization actions required when all high pressure injection sources are lost. Also included in this heading is the controlled cooldown and pressure reduction to allow the use of condensate and condensate booster pumps. This heading is only asked when both PCS and HPI fail. Success of this event implies that operators successfully depressurize the reactor vessel to allow injection by the low pressure systems. Failure of this event (Branch ID #DEHICO1) implies that reactor vessel remains at high pressure and core damage would result. #DEHICO1 also accounts for a condensate/condensate booster pump injection at a lower reactor pressure, approximately 500 psig, following vessel pressure reduction using the turbine bypass valves or the SRVs. This is, when available, an alternative way to vessel depressurization followed by low pressure injection. It can be performed without exceeding the cooldown rate. If the operators fail to reduce pressure for condensate injection, it is considered likely that it is because their attention is focused on recovery of other injection systems and restoration of the vessel level, not because they are unaware of the decreasing vessel level. However, the action to emergency depressurize is called for in the

EOPs at a specific vessel level. Therefore, the action for controlled cooldown is relatively independent of emergency depressurization.

LO Low Pressure Injection. This heading models the low pressure injection function provided by the condensate, core spray, and low pressure coolant injection (LPCI) systems. Both automatic and manual actions are considered for core spray and LPCI. Success of this event implies that low pressure injection is available. Failure of this event (Branch ID #LO) implies that low pressure injection is unsuccessful.

QR Decay Heat Removal. This heading models decay heat removal by shutdown cooling, suppression pool cooling, main condenser, torus vent, etc. A number of different top logic gates have been developed to model the nodes under this heading. They include #QRIN1REC, #QRQRA, #QR, and #QT.

Top logic gate #QRIN1REC models failure of decay heat removal with consideration of recovery of decay heat removal during the period prior to failure of the containment or ECCS. After decay heat removal is lost, the low pressure injection systems would become ineffective due to reactor repressurization. For successful recovery of decay heat removal, HPCI must be available after repressurization of the reactor vessel. The RISKMAN event tree top events associated with the recovery of decay heat removal include IN1 and QR. Top gate #QRIN1REC is used for nodes where high pressure injection is available, reactor pressure is reduced, there is no stuck-open SRV (or no failure of pressure relief), and low pressure injection is successful. Success implies that decay heat removal is available or is recovered before containment or ECCS is failed. Failure (Branch ID #QRIN1REC) implies that decay heat removal is not recovered, the reactor is repressurized, and the containment fails subsequently.

For sequences in which RCIC or HPCI is successful, there is no stuck-open SRV (or no failure of pressure relief), return to power has failed, and low pressure injection is unavailable, decay heat removal can be achieved by suppression pool cooling (modeled by top logic gate #QT). Success implies that, with suppression pool cooling, the long term operation of RCIC or HPCI can be successful. The reactor would remain at pressure long enough to support HPCI or RCIC injection allowing adequate time to recover low pressure injection. Failure (Branch ID #QT) implies that high pressure injection would also be lost due to loss of heat removal.

Top logic gate #QR is used in sequences in which there is no stuck-open SRV (no failure of pressure relief) and high pressure injection is unavailable. Success implies that the decay heat removal function is successful. Failure (Branch ID #QR) implies that no decay heat removal is available.

For sequences in which a stuck-open SRV is present or the initial pressure relief has failed, top logic gate #QRQRA is used. Recovery of decay heat removal during the period prior to containment or ECCS failure is considered.

SEQUENCES

The following sequence descriptions use a "/" prior to the branch designation to denote the success path of the branch and the branch name alone to designate the failure path.

GT_3: IEGGT /#BVPR #SORV0 /#PCS #ADED /#LO #QRIN1REC

A transient event occurs (IEGGT). After the reactor trip, the initial pressure relief is successful (/#BVPR) followed by successful SRV reclosure (#SORV0). Condensate, feedwater, and main condenser operate successfully following the plant trip (/#PCS). Since the power conversion system is successful, high pressure injection by RCIC or HPCI is not necessary. Reactor vessel depressurizes due to automatic depressurization conditions or emergency depressurization requirements (#ADED). The hardware response for vessel depressurization (modeled in #DE) is assumed successful. Due to vessel depressurization, return to power operation is not asked in this sequence. Low pressure injection is successful (/#LO). The decay heat removal function is unavailable (#QRIN1REC) resulting in eventual core damage.

GT_4: IEGGT /#BVPR #SORV0 /#PCS #ADED #LO

Similar to Sequence GT_3 except that low pressure injection is unsuccessful (#LO) resulting in eventual core damage. The decay heat removal function is not asked in this sequence.

GT_7: IEGGT /#BVPR #SORV0 #PCS /#HP-1 /#ADED #RP /#LO #QRIN1REC

A transient event occurs (IEGGT). After reactor trip, the initial pressure relief is successful (/#BVPR) followed by successful SRV reclosure (#SORV0). The power conversion system (condensate, feedwater, and main condenser) fails to operate following the plant trip (#PCS). High pressure injection by RCIC or HPCI is successful (/#HP-1). There are no automatic depressurization conditions or emergency depressurization requirements to cause vessel depressurization (/#ADED). Therefore, hardware response for the vessel depressurization is not asked in this sequence. Return to power operation has been unsuccessful (#RP). Vessel pressure is reduced due to the cooldown operation provided by RCIC/HPCI. Low pressure injection is successful (/#LO). The decay heat removal function is unavailable (#QRIN1REC) resulting in eventual core damage.

GT_9: IEGGT /#BVPR #SORV0 #PCS /#HP-1 /#ADED #RP #LO #QT

Similar to Sequence GT_7 except that low pressure injection is unsuccessful (#LO). Core cooling can only be achieved by high pressure injection provided by RCIC/HPCI (/#HP-1). To permit long term RCIC/HPCI operation, suppression pool cooling must be successful. However, in this sequence, suppression pool cooling is unavailable (#QT) resulting in eventual core damage.

GT_11: IEGGT /#BVPR #SORV0 #PCS /#HP-1 #ADED /#LO #QRIN1REC

Same as Sequence GT_3 except that the power conversion system is unavailable (#PCS). High pressure injection is provided by RCIC or HPCI (/#HP-1). Compared to Sequence GT_3, this sequence is not minimal since it involves the additional failure of the power conversion system (#PCS).

GT_12: IEGGT /#BVPR #SORV0 #PCS /#HP-1 #ADED #LO

Same as Sequence GT_4 except that the power conversion system is unavailable (#PCS). High pressure injection is provided by RCIC or HPCI (/#HP-1). Compared to Sequence GT_4, this sequence is not minimal since it involves the additional failure of the power conversion system (#PCS).

GT_14: IEGGT /#BVPR #SORV0 #PCS #HP-1 /#DEHICO1 /#LO #QR

A transient event occurs (IEGGT). After reactor trip, the initial pressure relief is successful (/#BVPR) followed by successful SRV reclosure (#SORV0). The power conversion system (condensate, feedwater, and main condenser) fails to operate following the plant trip (#PCS). High pressure injection by RCIC or HPCI is also unavailable (#HP-1). Vessel pressure is successfully reduced by the use of either condensate booster pumps or SRVs/turbine bypass valves (/#DEHICO1). Low pressure injection is successful (/#LO). However, decay heat removal has failed resulting in eventual core damage.

GT_15: IEGGT /#BVPR #SORV0 #PCS #HP-1 /#DEHICO1 #LO

Similar to Sequence GT_14 except that low pressure injection is unsuccessful (#LO) leading to eventual core damage.

GT_16: IEGGT /#BVPR #SORV0 #PCS #HP-1 #DEHICO1

Similar to Sequence GT_14 except that vessel pressure reduction is unsuccessful (#DEHICO1) resulting in eventual core damage.

GT_18: IEGGT /#BVPR #SORV1 /#PCS #QRQRA

A transient event occurs (IEGGT). After reactor trip, the initial pressure relief is successful (/#BVPR). However, one SRV fails to reclose (#SORV1). The power conversion system (condensate, feedwater, and main condenser) operates successfully following the plant trip (#PCS). Due to the stuck-open SRV, vessel pressure will continue to decrease after the initial pressure response. As the vessel pressure reduces, feedwater and condensate booster pumps can be gradually turned off. In this sequence, the decay heat removal function is unavailable (#QRQRA) resulting in eventual core damage.

GT_20: IEGGT /#BVPR #SORV1 #PCS /#HP-1 /#LO #QRQRA

Similar to Sequence GT_18 except that the power conversion system is unavailable (#PCS) and high pressure injection is provided by RCIC or HPCI (/#HP-1). Due to the stuck-open SRV, vessel pressure will continue to decrease to the low pressure system shutoff head. Low pressure injection is successful (/#LO). Decay heat removal is unavailable (#QRQRA) resulting in eventual core damage. Compared to Sequence GT_18, this sequence is non-minimal.

GT_21: IEGGT /#BVPR #SORV1 #PCS /#HP-1 #LO

Similar to Sequence GT_20 except that low pressure injection is unavailable (#LO) resulting in eventual core damage.

GT_23: IEGGT /#BVPR #SORV1 #PCS #HP-1 /#DEHICO1 /#LO #QRQRA

Similar to Sequence GT_20 except that high pressure injection by RCIC/HPCI is unavailable (#HP-1) and vessel pressure reduction by the use of SRVs/turbine bypass valves is successful (/#DEHICO1). Compared to Sequence GT_18, this sequence is non-minimal.

GT_24: IEGGT /#BVPR #SORV1 #PCS #HP-1 /#DEHICO1 #LO

Similar to Sequence GT_21 except that high pressure injection by RCIC/HPCI is unavailable (#HP-1) and vessel pressure reduction by the use of SRVs/turbine bypass valves is successful (/#DEHICO1). Compared to Sequence GT_21, this sequence is non-minimal.

GT_25: IEGGT /#BVPR #SORV1 #PCS #HP-1 #DEHICO1

Similar to Sequence GT_24 except that vessel pressure reduction has failed (#DEHICO1) resulting in eventual core damage.

GT_27: IEGGT /#BVPR #SORV2 /#PCS #QRQRA

Same as Sequence GT_18 except that two SRVs stick open (#SORV2).

GT_29: IEGGT /#BVPR #SORV2 #PCS /#HP-1 /#LO #QRQRA

Similar to Sequence GT_20 except that two SRVs stick open (#SORV2). Compared to Sequence GT_27, this sequence is non-minimal.

GT_30: IEGGT /#BVPR #SORV2 #PCS /#HP-1 #LO

Similar to Sequence GT_21 except that two SRVs stick open (#SORV2).

GT_32: IEGGT /#BVPR #SORV2 #PCS #HP-1 /#DEHICO1 /#LO #QRQRA

Similar to Sequence GT_23 except that two SRVs stick open (#SORV2). Compared to Sequence GT_27, this sequence is non-minimal.

GT_33: IEGGT /#BVPR #SORV2 #PCS #HP-1 /#DEHICO1 #LO

Similar to Sequence GT_24 except that two SRVs stick open (#SORV2). Compared to Sequence GT_30, this sequence is non-minimal.

GT_34: IEGGT /#BVPR #SORV2 #PCS #HP-1 #DEHICO1

Similar to Sequence GT_25 except that two SRVs stick open (#SORV2).

GT_36: IEGGT /#BVPR #SORV3 /#LO #QRQRA

A transient event occurs (IEGGT). After reactor trip, the initial pressure relief is successful (/#BVPR). However, three or more SRVs fail to reclose (#SORV3). All high pressure injection sources are lost due to vessel depressurization caused by the stuck-open SRVs. Following vessel depressurization, low pressure injection is successful (/#LO). However, the decay heat removal function is unavailable resulting in eventual core damage (#QRQRA).

GT_37: IEGGT /#BVPR #SORV3 #LO

Similar to Sequence GT_36 except that low pressure injection is unavailable (#LO) resulting in eventual core damage.

GT_39: IEGGT #BVPR /#PCS #QRQRA

Similar to Sequence GT_27 except that the initial pressure relief has failed (#BVPR). It was assumed that a medium-break LOCA resulted. SRVs are not challenged.

GT_41: IEGGT #BVPR #PCS /#HP-1 /#LO #QRQRA

Similar to Sequence GT_29 except that the initial pressure relief has failed (#BVPR). It was assumed that a medium-break LOCA resulted. SRVs are not challenged. Compared to Sequence GT_39, this sequence is non-minimal.

GT_42: IEGGT #BVPR #PCS /#HP-1 #LO

Similar to Sequence GT_30 except that the initial pressure relief has failed (#BVPR). It was assumed that a medium-break LOCA resulted. SRVs are not challenged.

GT_44: IEGGT #BVPR #PCS #HP-1 /#DEHICO1 /#LO #QRQRA

Similar to Sequence GT_32 except that the initial pressure relief has failed (#BVPR). It was assumed that a medium-break LOCA resulted. SRVs are not challenged. Compared to Sequence GT_39, this sequence is non-minimal.

GT_45: IEGGT #BVPR #PCS #HP-1 /#DEHICO1 #LO

Similar to Sequence GT_33 except that the initial pressure relief has failed (#BVPR). It was assumed that a medium-break LOCA resulted. SRVs are not challenged. Compared to Sequence GT_42, this sequence is non-minimal.

GT_46: IEGGT #BVPR #PCS #HP-1 #DEHICO1

Similar to Sequence GT_34 except that the initial pressure relief has failed (#BVPR). It was assumed that a medium-break LOCA resulted. SRVs are not challenged.

2.2 The Anticipated Transient Without Scram (ATWS) Event Tree

This section contains information regarding the ATWS core damage event tree. This event tree models core damage event sequences associated with those "ATWS initiators" included in the RISKMAN IPE model. In principal, ATWS is not an initiator. It is a plant condition following transient initiating events. For modeling convenience, however, event sequences involving failure of the reactor scram function following plant transients are treated as initiators in both IPE and this CAFTA model. Of all the transient events, the most significant initiating events for ATWS mitigation are turbine trip, loss of feedwater, and MSIV closure because of their frequency of occurrence and impact on plant response during the progression of the ATWS events. Therefore, the event tree model described in this section is characterized by three ATWS initiators: turbine trip, loss of feedwater, and MSIV closure. The MSIV closure ATWS initiator, however, really represents event sequences involving failure of the reactor scram function following both the MSIV closure and the loss of condenser vacuum events.

EVENT TREE MODIFICATIONS

In the IPE, the core damage sequences for each of the ATWS initiators were obtained by linking together the following 7 RISKMAN frontline systems event trees: ATWSSUP, ATWS, ATWSBIT, INTER3, REC0, RHRCS, and LTC3. The same set of event trees were linked together for all three initiators in this group. After reviewing the RISKMAN event trees developed for this group of initiating events, the following key changes were made:

- The initiators were combined into a single ATWS initiator heading ATWS (with a node designated by IEGATWS).

- Top events modeled in RISKMAN event trees ATWSSUP, ATWS, and ATWSBIT are combined according to the functions provided by the individual systems.

- With the exception of V18, CW, RD, and RP, top events in RISKMAN event tree INTER3 are incorporated into lower level fault tree models for LOCA signal, operator restoration following a LOCA signal, automatic/emergency depressurization, main condenser availability, etc. RISKMAN Top Events V18, CW, RD, and RP were determined to not be ATWS functional requirements for core damage.

- Recovery top events modeled in REC0 are incorporated into the appropriate system fault trees.

- Most top events listed in RISKMAN event trees RHRCS and LTC3 are incorporated into the lower level fault trees for ETA headings DE, LO, and QR. RISKMAN Top Events Z5, DESC2, DESC1, IN1, QR, CFF, and IN2 were determined to not be ATWS functional requirements for core damage.

The initiators included in the ETA ATWS initiator heading ATWS are: %ATWSTT, %ATWSFW, and %ATWSMS.

For the new ETA event tree ATWS, nodes under each heading may be represented by one or more fault tree gates. The multiple RISKMAN system models were combined into one fault tree gate with additional compression achieved by combining similar functions into one final fault tree gate with multiple inputs. Listed below are the new top logic gates developed for the ETA ATWS event tree nodes and the original inputs associated with each (i.e., RISKMAN event tree top events combined into the gate):

#RSCRAM	HCU, ARIA, ARIB, RPS, ARI, MT
RPT	RPT
#BVPR	BV, PR
#SORV0/1/2/3	SORV
#PCS	CO, FW, FC, MC, MS
HPCI-1	HPCI
#BI	BIIT, SL, OS
#TINJ	TINJ, HO
#HR	TINJ, HR
#ADEDWS/ADWS	VC, LOCA, L1OP, DWTC, OW/VC, LOCA, L1OP
#DEWS/#DE	VC, LOCA, L1OP, DWTC, OW, DE/DE
#LOWS	CO, CS, RA, RB, JS, VA, VB, VOP, NS, NSREC, LC, LO
#QR/#QT	OL, QC, QS, QT, RA, RB, VA, VB, VOP, HA, HB, QV

EVENT TREE HEADINGS & BRANCHES

The following event tree headings and nodes appear on the tree in the approximate chronological order that would be expected during an ATWS.

ATWS ATWS Initiating Events. The ATWS initiator is defined as a transient (including support system failure) or small LOCA initiating event followed by failure of the automatic and manual reactor trip. Since failure of the reactor trip is modeled under heading RSCRAM, the ATWS heading just includes transient initiators without consideration of the status of reactor scram. For ATWS core damage, the most important and highest frequency transient initiators are turbine trip, loss of feedwater, MSIV closure, and loss of condenser vacuum. MSIV closure and loss of condenser vacuum also present severe impact on ATWS mitigation. The impact of MSIV closure and loss of condenser vacuum are very similar, therefore, these two initiators are combined and represented by the MSIV closure initiator. As such, the top logic gate IEGATWS developed for this heading (Branch ID IEGATWS) includes the following 3 initiators: turbine trip with ATWS (%ATWSTT), loss of feedwater with ATWS (%ATWSFW), and MSIV closure with ATWS (%ATWSMS).

RSCRAM Reactor Shutdown. This heading models the scram function provided by the reactor protection system (RPS), alternate rod insertion (ARI) system, and manual operator scram. The reactor can be brought to a shutdown condition by inserting a sufficient number of control rods. Scram signals from the RPS would deenergize the scram pilot valves causing control rod insertion. An ARI scram signal would open the ARI valves to depressurize the scram air header causing control rod insertion. The scram pilot valves can also be deenergized by the manual RPS scram signal. Success of this event implies that reactivity control is established by inserting the control rods via automatic RPS scram, automatic ARI actuation, or manual operator trip. Failure of this event (Branch ID #RSCRAM) implies that reactivity control function is unsuccessful.

RPT Recirculation Pump Trips (RPT). This heading models the RPT logic required for successful pressure control under ATWS conditions. The ATWS high pressure and the end-of-cycle trip are modeled. No credit is taken for the ATWS low level trip signal. Successful RPT requires that both recirculation pumps trip automatically given an ATWS event. Success of this event implies that both recirculation pumps are tripped, RCS pressure is decreased, and reactor power is reduced. Failure of this event implies that the RPT and RCS pressure control are unsuccessful. It is conservatively assumed in this ATWS event tree model that failure of RPT would result in core damage.

BVPR Pressure Relief. This heading models the pressure control function performed by the turbine bypass valves and SRVs during the initial pressure transient. For transient events with MSIVs open, both the turbine bypass valves and the SRVs may be available. Failure of this event (Branch ID #BVPR) is conservatively modeled as resulting in core damage.

SORV SORV Reclosure. This is a multistate heading. It models the reclosure status of SRVs (i.e., the number of stuck open SRVs). All open SRVs must close after the vessel pressure falls below the SRV setpoints. The four states applicable to this

heading are: all SRVs successfully reclose (Branch ID #SORV0); one SRV fails to reclose (Branch ID #SORV1); two SRVs fail to reclose (Branch ID #SORV2); and three or more SRVs fail to reclose (Branch ID #SORV3). Failure of three or more SRVs to reclose is conservatively modeled as resulting in core damage.

PCS Power Conversion System. This heading models the availability or unavailability of the power conversion system to provide the core cooling function. Condensate system, feedwater system, and main condenser are included in this heading. One condensate pump and one condensate booster pump are required to support operation of a single feedwater pump when the plant unit is shut down. One reactor feed pump is required to provide feedwater flow to the reactor for level control. If feedwater is initially unavailable, no credit for restoration of feedwater is considered in this heading.

Success of this event implies that condensate, feedwater, and main condenser are available for plant response following the transient. For main condenser to remain available, the MSIVs must remain open, turbine bypass valves must continue to function, and all support for the electrohydraulic control system must be available. Failure of this event (Branch ID #PCS) implies that HPCI will be demanded to operate to provide the high pressure level control function.

HPI High Pressure Level Control by HPCI. This heading models the high pressure level control provided by the HPCI system. HPCI must initiate on vessel low water Level 2 and provides makeup to the reactor. Only automatic actuation is considered in this heading. Success of this heading implies that HPCI is available to provide the high pressure level control function. Failure of this heading (Branch ID HPCI-1) implies that HPCI is unavailable for the vessel level control function and vessel depressurization is required. This event is only asked in this event tree when PCS fails.

BI Boron Injection. This heading models the injection of cold shutdown boron concentration into the reactor by the standby liquid control system (SLCS) during an ATWS event. It includes the conditions under which boron injection must be initiated (i.e., exceeding the boron injection initiation temperature [BIIT]), availability or unavailability of SLCS, and the operator action to initiate the SLCS. Success of this event implies that either the BIIT is not exceeded, or BIIT is exceeded and SLCS is successful. Failure of this event (Branch ID #BI) implies that the BIIT is exceeded and SLCS injection is unsuccessful.

TINJ Termination of High Pressure Injection. This heading models the operator action to terminate all high pressure injection to lower vessel level as rapidly as possible to near top of active fuel (TAF). This event also includes conditions under which high pressure injection must be terminated. Conditions which direct the operators to terminate all high pressure injection are 1) reactor power above 5%, 2) torus temperature exceeding the BIIT, and 3) one or more SRVs discharging to the torus or drywell pressure above 1.85 psig, and level above TAF. Success of this event implies that either termination of high pressure injection is not required or the operators have successfully terminated all high pressure injection when required. Failure of this event (Branch ID #TINJ) implies that there is a need to terminate high pressure injection and the operators have failed in terminating high pressure injection.

HR Failure of HPCI to Restart following Termination of Injection to Lower Water Level. This heading (Branch ID #HR) models the restart of HPCI following termination of high pressure injection for ATWS scenarios.

ADED Automatic and Emergency Depressurization Conditions. This heading models the automatic and emergency depressurization conditions. The automatic depressurization condition is modeled by generation of the LOCA signal and failure of the operators to inhibit the ADS actuation. LOCA signals include Level 1 and high drywell pressure signals. In addition to a loss of all high pressure injection, it was assumed that a Level 1 signal would be generated if there is a requirement for termination of all high pressure injection. Furthermore, failure of the operators to control feedwater, RCIC, and HPCI to lower and control vessel level and thus to reduce reactor power was assumed to cause generation of a Level 1 signal. Failure of drywell cooling (RISKMAN Top Event VC) was assumed to lead to generation of a high drywell pressure signal.

Emergency vessel depressurization is required by the Plant Hatch procedures if the drywell temperature limit is exceeded. Drywell temperature would increase if drywell cooling fails and the operators fail to initiate drywell spray (RISKMAN Top Event OW). Drywell cooling would also be lost if the operators fail to restore drywell cooling following a LOCA signal.

Success of this event implies that there are no automatic and emergency depressurization conditions, or the operators successfully inhibit ADS and restore drywell cooling given a LOCA signal. Failure of this event (Branch IDs #ADEDWS) implies that ADS would be actuated (gate ADWS is true) or the operators are required to initiate emergency vessel depressurization (gate EDWS is true). If gate ADWS is true, the downstream heading DE will also be true since gate ADWS is also included under top logic gate #DEWS. This implies that, if ADS would be actuated (i.e., ADS condition exists and the operators fail to inhibit), the reactor vessel is assumed to successfully depressurize (i.e., no failure in depressurization). Top logic gate ADWS is used in sequences in which a Level 1 condition has occurred (i.e., failure of #BI, #TINJ, #HR, or #PCS and HPCI-1). Failure of top gate ADWS in these sequences (Brach ID ADWS) implies that the operators have failed to inhibit ADS. It is therefore assumed in sequences involving failure of top gate ADWS that vessel is depressurized and downstream heading DE is not asked.

DE Depressurization of Vessel Before Core Damage. This heading models the reduction of vessel pressure to allow low pressure injection. Two top logic gates (#DE and #DEWS) are used under this heading. Top gate #DE includes the manual emergency depressurization actions required when all high pressure injection sources are lost or power reduction by all other methods is unsuccessful. This top logic gate is only asked in sequences in which top gate ADWS is successful (i.e., no ADS actuation) or #ADEDWS is successful. Success of this event implies that the operators successfully depressurize the reactor vessel to allow injection by the low pressure systems. Failure of this event (Branch ID #DE) implies that reactor vessel remains at high pressure.

In addition to those modeled for #DE, also included in top gate ID #DEWS for sequences involving failure of top logic gate #ADEDWS (i.e., ADS would be actuated or emergency depressurization is required) are logic gates ADWS (i.e.,

ADS would be actuated) and EDWS (i.e., emergency depressurization is required). Top logic gate #DEWS is only asked when gate #ADEDWS is used and fails. Under top gate #DEWS, gate EDWS is "anded" with gate #DE. Therefore, if gate ADWS under top gate #ADEDWS is true, this event (#DEWS) is also true. It is assumed that the reactor vessel would be successfully depressurized if the ADS actuation has occurred. In other words, automatic vessel depressurization is assumed to occur when both gates ADWS (under #ADEDWS) and #DEWS fail. Success of this event implies that there is no automatic vessel depressurization and the operators have successfully depressurized the vessel given a requirement for emergency depressurization. Failure of this event (Branch ID #DEWS) implies that either an automatic vessel depressurization has occurred, or emergency depressurization is required and the operators fail to manually depressurize.

LO Low Pressure Injection. This heading models the low pressure injection function provided by the condensate, core spray, and low pressure coolant injection (LPCI) systems. Manual control of low pressure injection following vessel depressurization (i.e., control the rate of cold water injection and thus reactivity increase) is also considered in this heading. Success of this event implies that low pressure injection is successful. Failure of this event (Branch ID #LOWS) implies that low pressure injection is unsuccessful.

QR Decay Heat Removal. This heading models decay heat removal by shutdown cooling, suppression pool cooling, main condenser, or torus vent. Two different top logic gates were used to model the nodes under this heading. They include #QR and #QT.

In general, top gate #QR is used for decay heat removal which considers main condenser, suppression pool cooling, shutdown cooling, and torus vent. Success implies that the decay heat removal function is successful. Failure (Branch ID #QR) implies that no decay heat removal is available.

For sequences in which HPCI is successful, there is no stuck-open SRV (or no failure of pressure relief), and low pressure injection is unavailable, decay heat removal can be achieved by suppression pool cooling (modeled by top logic gate #QT). Success implies that, with suppression pool cooling, the long term operation of HPCI can be successful. The reactor vessel would remain at high pressure. Failure (Branch ID #QT) implies that high pressure injection would also be lost due to loss of heat removal.

SEQUENCES

The following sequence descriptions use a "/" prior to the branch designation to denote the success path of the branch and the branch name alone to designate the failure path.

ATWS_3: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 /#PCS /#ADEDWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). All SRVs that open have reclosed successfully (#SORV0). The power conversion system is successful in providing core cooling (/#PCS). No ADS actuation occurs and no emergency depressurization is required (/#ADEDWS). Reactor vessel remains at high pressure. However, heat removal function is

unsuccessful (#QR) resulting in eventual core damage. Note that #QR is conservatively assumed to be required for long term cooling even though heat removal via main condenser as part of the PCS is successful

ATWS_5: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 /#PCS #ADEDWS /#DEWS /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (#BVPR). All SRVs that open have reclosed successfully (#SORV). Core cooling is initially provided by the power conversion system (/#PCS). The reactor is successfully depressurized due to an emergency depressurization requirement (#ADEDWS, /#DEW). The low pressure injection system successfully provides vessel level control function following vessel depressurization, but heat removal function is unavailable resulting in eventual core damage. Compared to Sequence ATWS_3, this is a non-minimal sequence.

ATWS_6: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 /#PCS #ADEDWS /#DEWS #LOWS

Similar to Sequence ATWS_5 except that low pressure injection is unsuccessful (#LOWS) resulting in eventual core damage.

ATWS_7: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 /#PCS #ADEDWS #DEWS

Similar to Sequence ATWS_5 except that automatic vessel depressurization has occurred or vessel depressurization has failed given an emergency depressurization requirement (#ADEDWS and #DEWS). Core damage is conservatively assumed in this sequence due to the uncontrolled injection of cold water following vessel depressurization or due to failure to depressurize when required.

ATWS_9: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI /#TINJ /#HR /#ADEDWS /#DE /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). All SRVs that open have reclosed successfully (#SORV0). The power conversion system is unsuccessful in providing core cooling (#PCS). HPCI is successful in providing high pressure vessel water level control (/HPCI-1). BIIT is exceeded (due to loss of the PCS and possible discharging through the SRVs) and SLCS injection is successful (/#BI). To reduce reactor power, the operators have successfully terminated all high pressure injection (since SRVs may be discharging) and lowered water level to top of active fuel (/#TINJ). HPCI is successfully restarted (/#HR). However, heat removal function is unsuccessful (#QR) resulting in eventual core damage. Without the heat removal function, eventual depressurization will be required due to Heat Capacity Temperature Limit. Despite successful depressurization (/#DE) and low pressure injection, low pressure injection will be lost due to an overheated or failed suppression pool.

In this sequence, vessel depressurization to allow low pressure injection is not initially needed since HPCI is available. However, failure of suppression pool cooling would cause vessel depressurization due to HCTL concerns as well as failure of the long term HPCI operation. But, vessel depressurization and low pressure injection would be successful (/#DE and /#LOWS). Note

that successful lowering of level and subsequently power will put the heat load within bypass capacity thus relieving the load on the torus, if the power conversion system is available.

Compared to Sequence ATWS_3, this is a non-minimal sequence.

ATWS_10B: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI /#TINJ /#HR /#ADEDWS /#DE #LOWS #QT

Similar to Sequence ATWS_9 except that low pressure injection would be unavailable if needed (#LOWS). For HPCI to continue to operate and provide long term core cooling, suppression pool cooling must be available. However, suppression pool cooling is unavailable in this sequence (#QT) resulting in eventual core damage.

ATWS_12: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI /#TINJ /#HR /#ADEDWS #DE #QT

Similar to Sequence ATWS_9 except that vessel depressurization would be unavailable if needed (#DE). For HPCI to continue to operate and provide long term core cooling, suppression pool cooling must be available. However, suppression pool cooling is unavailable in this sequence (#QT) resulting in eventual core damage.

ATWS_14: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI /#TINJ /#HR #ADEDWS /#DEWS /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). All SRVs that open have reclosed successfully (#SORV0). The power conversion system is unsuccessful in providing core cooling (#PCS). HPCI is successful in providing high pressure vessel water level control (/HPCI-1). BIIT is exceeded (due to loss of the PCS and possible discharging through the SRVs) and SLCS injection is successful (/#BI). To reduce reactor power, the operators have successfully terminated all high pressure injection (since SRVs may be discharging) and lowered water level to top of active fuel (/#TINJ). HPCI is successfully restarted (/#HR). However, an emergency vessel depressurization is required and has been successfully achieved. The low pressure systems are successful in providing controlled injection of cold water for vessel inventory makeup. However, the heat removal function is unsuccessful (#QR) resulting in eventual core damage. Compared to Sequence ATWS_3, this is a non-minimal sequence.

ATWS_15: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI /#TINJ /#HR #ADEDWS /#DEWS #LOWS

Similar to Sequence ATWS_14 except that controlled low pressure injection is unsuccessful (#LOWS) resulting in eventual core damage. Compared to Sequence ATWS_6, this is a non-minimal sequence.

ATWS_16: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI /#TINJ /#HR #ADEDWS #DEWS

Similar to Sequence ATWS_14 except that an ADS actuation has occurred or vessel depressurization has failed given an emergency depressurization requirement (#ADEDWS, #DEWS). Core damage is assumed. Compared to Sequence ATWS_7, this is a non-minimal sequence.

ATWS_18: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI /#TINJ #HR /ADWS /#DE /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). All SRVs that open have reclosed successfully (#SORV0). The power conversion system is unsuccessful in providing core cooling (#PCS). HPCI is successful in providing high pressure vessel water level control (/HPCI-1). BIIT is exceeded (due to loss of the PCS and possible discharging through the SRVs) and SLCS injection is successful (/#BI). To reduce reactor power, the operators have successfully terminated all high pressure injection (since SRVs may be discharging) and lowered water level to top of active fuel (/#TINJ). However, HPCI restart is unsuccessful (#HR). Manual depressurization is therefore required to permit low pressure injection for vessel level control. Vessel depressurization (required due to unavailability of all high pressure injection sources) and low pressure injection are successful (/#DE, /LOWS). Heat removal function is unsuccessful (#QR) resulting in eventual core damage. Compared to Sequence ATWS_3, this is a non-minimal sequence.

ATWS_19: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI /#TINJ #HR /ADWS /#DE #LOWS

Similar to Sequence ATWS_18 except that controlled low pressure injection is unsuccessful (#LOWS) resulting in eventual core damage.

ATWS_20: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI /#TINJ #HR /ADWS #DE

Similar to Sequence ATWS_18 except that vessel depressurization has failed resulting in eventual core damage.

ATWS_21: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI /#TINJ #HR ADWS

Similar to Sequence ATWS_18 except that automatic vessel depressurization has occurred. Core damage is assumed due to the uncontrolled cold water injection from the low pressure injection systems.

ATWS_23: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI #TINJ /ADWS /#DE /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). All SRVs that open have reclosed successfully (#SORV0). The power conversion system is unsuccessful in providing core cooling (#PCS). HPCI is successful in providing high pressure vessel water level control (/HPCI-1). BIIT is exceeded (due to loss of the PCS and possible discharging through the SRVs) and SLCS injection is successful (/#BI). The operators fail to terminate high pressure injection (since SRVs may be discharging) and lower water level to top of active fuel (#TINJ). High pressure injection from HPCI is not sufficient to maintain operating water level for a full power ATWS. As such, reactor water level will decrease to a point where power matches flowrate: around 20% for HPCI. This is getting close to the Top of Active Fuel (TAF). Based on the torus approaching the HCTL, manual depressurization is conservatively assumed to be required in this sequence to

prevent containment and core damage. Vessel depressurization and controlled low pressure injection are successful (/#DE, /LOWS). Heat removal function is unsuccessful (#QR) resulting in eventual core damage due to loss of suction source for low pressure injection. Note that reactor power at lowered water level should be within bypass capacity which would serve to remove the heat load from containment, if available.

Compared to Sequence ATWS_3, this is a non-minimal sequence.

ATWS_24: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI #TINJ /ADWS /#DE #LOWS

Similar to Sequence ATWS_23 except that controlled low pressure injection is unsuccessful (#LOWS) resulting in eventual core damage.

ATWS_25: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI #TINJ /ADWS #DE

Similar to Sequence ATWS_23 except that vessel depressurization has failed (#DE), following failure to reduce power by lowering vessel level to TAF when needed. Core damage therefore conservatively results from fuel being uncovered from lack of low pressure injection.

ATWS_26: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 /#BI #TINJ ADWS

Similar to Sequence ATWS_23 except that automatic vessel depressurization has occurred (ADWS). Core damage is assumed due to the uncontrolled cold water injection from the low pressure injection systems.

ATWS_28: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 #BI /#TINJ /#HR /ADWS /#DE /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). All SRVs that open have reclosed successfully (#SORV0). The power conversion system is unsuccessful in providing core cooling (#PCS). HPCI is successful in providing high pressure vessel water level control (/HPCI-1). BIIT is exceeded (due to loss of the PCS and possible discharging through the SRVs) and SLCS injection is unsuccessful (#BI). To reduce reactor power, the operators have successfully terminated all high pressure injection (since SRVs may be discharging) and lowered water level to top of active fuel (/#TINJ). Manual depressurization is performed to further reduce reactivity. Vessel depressurization and controlled low pressure injection are successful (/#DE, /LOWS). However, the heat removal function is unsuccessful (#QR). Operation of HPCI will lead to the need for depressurization due to HCTL being approached. Without long term cooling, the torus will be lost as a suction source to low pressure systems. Without low pressure injection, the core will become uncovered and damage will occur. Compared to Sequence ATWS_3, this is a non-minimal sequence.

ATWS_29: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 #BI /#TINJ /#HR /ADWS /#DE #LOWS

Similar to Sequence ATWS_28 except that controlled low pressure injection is unsuccessful resulting in eventual core damage.

ATWS_31: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 #BI /#TINJ /#HR /ADWS #DE #QT

Similar to Sequence ATWS_28 except that vessel depressurization is not performed and suppression pool fails resulting in eventual core damage. In this sequence, HPCI is the only source for vessel water level control. Long term operation of HPCI requires successful suppression pool cooling. Compared to Sequence ATWS_12, this is a non-minimal sequence.

ATWS_32: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 #BI /#TINJ /#HR ADWS

Similar to Sequence ATWS_28 except that automatic vessel depressurization has occurred. Core damage is assumed due to the uncontrolled injection of cold water from the low pressure systems.

ATWS_34: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 #BI /#TINJ #HR /ADWS /#DE /#LOWS #QR

Similar to Sequence ATWS_18 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_3, this is a non-minimal sequence.

ATWS_35: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 #BI /#TINJ #HR /ADWS /#DE #LOWS

Similar to Sequence ATWS_19 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_19, this is a non-minimal sequence.

ATWS_36: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 #BI /#TINJ #HR /ADWS #DE

Similar to Sequence ATWS_20 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_20, this is a non-minimal sequence.

ATWS_37: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 #BI /#TINJ #HR ADWS

Similar to Sequence ATWS_21 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_21, this is a non-minimal sequence.

ATWS_39: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 #BI #TINJ /ADWS /#DE /#LOWS #QR

Similar to Sequence ATWS_23 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_3, this is a non-minimal sequence.

ATWS_40: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 #BI #TINJ /ADWS /#DE #LOWS

Similar to Sequence ATWS_24 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_24, this is a non-minimal sequence.

ATWS_41: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 #BI #TINJ /ADWS #DE

Similar to Sequence ATWS_25 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_25, this is a non-minimal sequence.

ATWS_42: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS /HPCI-1 #BI #TINJ ADWS

Similar to Sequence ATWS_26 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_26, this is a non-minimal sequence.

ATWS_44: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS HPCI-1 /ADWS /#DE /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). All SRVs that open have reclosed successfully (#SORV0). The power conversion system is unsuccessful in providing core cooling (#PCS). HPCI is unavailable in providing high pressure vessel water level control (/HPCI-1). Manual depressurization is required to allow vessel inventory control by the low pressure injection systems. Vessel depressurization and controlled low pressure injection are successful (/ADWS, /#DE, /LOWS). However, the heat removal function is unsuccessful (#QR) resulting in eventual core damage. Note that, at this point, the power level is within bypass valve capacity. If the power conversion system is available, it can limit the energy being dumped to the suppression pool. Compared to Sequence ATWS_3, this is a non-minimal sequence.

ATWS_45: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS HPCI-1 /ADWS /#DE #LOWS

Similar to Sequence ATWS_44 except that controlled low pressure injection is unsuccessful resulting in eventual core damage.

ATWS_46: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS HPCI-1 /ADWS #DE

Similar to Sequence ATWS_44 except that vessel depressurization has failed resulting in eventual core damage.

ATWS_47: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS HPCI-1 ADWS

Similar to Sequence ATWS_44 except that an ADS actuation has occurred. Core damage is assumed due to the uncontrolled injection of cold water by the low pressure systems.

ATWS_49: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI /#TINJ /#HR /#ADEDWS /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). One SRV sticks open after opening (#SORV1). The power conversion system is successful in providing core cooling (/#PCS). BIIT is exceeded (due to the stuck-open SRV) and SLCS injection is successful (/#BI). To reduce reactor power, the operators have successfully terminated all high pressure injection and lowered water level to top of active fuel (/#TINJ). HPCI is successfully started (/#HR). There are no ADS

actuation and emergency depressurization requirement. Due to the stuck-open SRV, reactor vessel is eventually depressurized and low pressure injection is successful. The heat removal function is unsuccessful (#QR) resulting in eventual core damage. Similar to Sequence ATWS_3, this is a conservative assumption since main condenser as part of the power conversion system is available.

ATWS_50: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI /#TINJ /#HR /#ADEDWS #LOWS

Similar to Sequence ATWS_49 except that low pressure injection is unsuccessful (#LOWS) resulting in eventual core damage.

ATWS_52: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI /#TINJ /#HR #ADEDWS /#DEWS /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). One SRV sticks open after opening (#SORV1). The power conversion system is successful in providing core cooling (/#PCS). BIIT is exceeded (due to the stuck-open SRV) and SLCS injection is successful (/#BI). To reduce reactor power, the operators have successfully terminated all high pressure injection and lowered water level to top of active fuel (/#TINJ). HPCI is successfully started (/#HR). An emergency depressurization is required and manual operator depressurization is successful. Low pressure injection is successful following vessel depressurization. The heat removal function is unsuccessful (#QR) resulting in eventual core damage. Without torus cooling, a part of #QR, the low pressure injection systems would lose their suction source. The loss of low pressure injection would cause core damage due to core uncovery. Similar to Sequence ATWS_49, this is a conservative assumption since main condenser as part of the power conversion system is available. Compared to Sequence ATWS_49, this is a non-minimal sequence.

ATWS_53: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI /#TINJ /#HR #ADEDWS /#DEWS #LOWS

Similar to Sequence ATWS_52 except that low pressure injection is unavailable. Compared to Sequence ATWS_50, this is a non-minimal sequence.

ATWS_54: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI /#TINJ /#HR #ADEDWS #DEWS

Similar to Sequence ATWS_52 except that an ADS actuation has occurred or emergency depressurization is required and the operators fail to depressurize. Core damage is assumed for this sequence.

ATWS_56: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI /#TINJ #HR /ADWS /#DE /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). One SRV sticks open (#SORV1). The power conversion system is successful in providing core cooling (/#PCS). BIIT is exceeded (due to the stuck-open SRV) and SLCS injection is successful (/#BI). To reduce reactor power, the operators have successfully terminated all high pressure injection and lowered water level to top of active fuel (/#TINJ). HPCI start is unsuccessful (#HR). Vessel depressurization and

low pressure injection are successful (/#DE, /LOWS). Heat removal function is unsuccessful (#QR) resulting in eventual core damage. Compared to Sequence ATWS_49, this is a non-minimal sequence.

ATWS_57: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI /#TINJ #HR /ADWS /#DE #LOWS

Similar to Sequence ATWS_56 except that low pressure injection is unavailable (#LOWS) resulting in eventual core damage. Compared to Sequence ATWS_50, this is a non-minimal sequence.

ATWS_58: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI /#TINJ #HR /ADWS #DE

Similar to Sequence ATWS_56 except that vessel depressurization has failed resulting in eventual core damage due to core uncovery.

ATWS_59: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI /#TINJ #HR ADWS

Similar to Sequence ATWS_56 except that automatic vessel depressurization has occurred. Core damage is assumed due to the uncontrolled cold water injection.

ATWS_61: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI #TINJ /ADWS /#DE /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). One SRV sticks open (#SORV1). The power conversion system is successful in providing core cooling (/#PCS). BIIT is exceeded (due to the stuck-open SRV) and SLCS injection is successful (/#BI). The operators fail to terminate high pressure injection and lower water level to top of active fuel (#TINJ). Manual depressurization is assumed to be required to reduce reactivity. Manual vessel depressurization and low pressure injection are successful (/#DE, /LOWS). Heat removal function is unsuccessful (#QR) resulting in eventual core damage. Compared to Sequence ATWS_49, this is a non-minimal sequence.

ATWS_62: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI #TINJ /ADWS /#DE #LOWS

Similar to Sequence ATWS_61 except that low pressure injection is unsuccessful (#LOWS) resulting in eventual core damage. Compared to Sequence ATWS_50, this is a non-minimal sequence.

ATWS_63: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI #TINJ /ADWS #DE

Similar to Sequence ATWS_61 except that manual vessel depressurization has failed (#DE) resulting in eventual core damage.

ATWS_64: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI #TINJ ADWS

Similar to Sequence ATWS_61 except that automatic vessel depressurization has occurred (ADWS). Core damage is assumed due to uncontrolled injection.

ATWS_66: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS #BI /#TINJ /#HR /#ADEDWS /#LOWS #QR

Similar to Sequence ATWS_49 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_49, this is a non-minimal sequence.

ATWS_67: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS #BI /#TINJ /#HR /#ADEDWS #LOWS

Similar to Sequence ATWS_50 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_50, this is a non-minimal sequence.

ATWS_69: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS #BI /#TINJ /#HR #ADEDWS /#DEWS /#LOWS #QR

Similar to Sequence ATWS_52 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_49, this is a non-minimal sequence.

ATWS_70: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS #BI /#TINJ /#HR #ADEDWS /#DEWS #LOWS

Similar to Sequence ATWS_53 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_50, this is a non-minimal sequence.

ATWS_71: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS #BI /#TINJ /#HR #ADEDWS #DEWS

Similar to Sequence ATWS_54 except that boron injection is unsuccessful (#BI). Compared to Sequence ATWS_54, this is a non-minimal sequence.

ATWS_73: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS #BI /#TINJ #HR /ADWS /#DE /#LOWS #QR

Similar to Sequence ATWS_56 except that boron injection has failed (#BI). Compared to Sequence ATWS_49, this is a non-minimal sequence.

ATWS_74: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI /#TINJ #HR /ADWS /#DE #LOWS

Similar to Sequence ATWS_57 except that boron injection has failed (#BI). Compared to Sequence ATWS_50, this is a non-minimal sequence.

ATWS_75: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS #BI /#TINJ #HR /ADWS #DE

Similar to Sequence ATWS_58 except that boron injection has failed (#BI). Compared to Sequence ATWS_58, this is a non-minimal sequence.

ATWS_76: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS #BI /#TINJ #HR ADWS

Similar to Sequence ATWS_59 except that boron injection has failed (#BI). Compared to Sequence ATWS_59, this is a non-minimal sequence.

ATWS_78: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS #BI #TINJ /ADWS /#DE /#LOWS #QR

Similar to Sequence ATWS_61 except that boron injection has failed (#BI). Compared to Sequence ATWS_49, this is a non-minimal sequence.

ATWS_79: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS #BI #TINJ /ADWS /#DE #LOWS

Similar to Sequence ATWS_62 except that boron injection has failed (#BI). Compared to Sequence ATWS_50, this is a non-minimal sequence.

ATWS_80: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI #TINJ /ADWS #DE

Similar to Sequence ATWS_63 except that boron injection has failed (#BI). Compared to Sequence ATWS_63, this is a non-minimal sequence.

ATWS_81: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI #TINJ ADWS

Similar to Sequence ATWS_64 except that boron injection has failed (#BI). Compared to Sequence ATWS_64, this is a non-minimal sequence.

ATWS_83: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 /#BI /#TINJ /#HR /#ADEDWS /#LOWS #QR

Similar to Sequence ATWS_49 except that the power conversion system is unavailable (#PCS) and HPCI is successful in providing core cooling initially following the transient (/HPCI-1). Compared to Sequence ATWS_49, this is a non-minimal sequence.

ATWS_84: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 /#PCS /#BI /#TINJ /#HR /#ADEDWS #LOWS

Similar to Sequence ATWS_50 except that the power conversion system is unavailable (#PCS) and HPCI is successful in providing core cooling initially following the transient (/HPCI-1). Compared to Sequence ATWS_50 this is a non-minimal sequence.

ATWS_86: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 /#BI /#TINJ /#HR #ADEDWS /#DEWS /#LOWS #QR

Similar to Sequence ATWS_52 except that the power conversion system is unavailable (#PCS) and HPCI is successful in providing core cooling initially following the transient (/HPCI-1). Compared to Sequence ATWS_52 this is a non-minimal sequence.

ATWS_87: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 /#BI /#TINJ /#HR #ADEDWS /#DEWS #LOWS

Similar to Sequence ATWS_53 except that the power conversion system is unavailable (#PCS) and HPCI is successful in providing core cooling initially following the transient (/HPCI-1). Compared to Sequence ATWS_53 this is a non-minimal sequence

ATWS_88: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 /#BI /#TINJ /#HR #ADEDWS #DEWS

Similar to Sequence ATWS_54 except that the power conversion system is unavailable (#PCS) and HPCI is successful in providing core cooling initially following the transient (/HPCI-1). Compared to Sequence ATWS_54 this is a non-minimal sequence.

ATWS_90: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 /#BI /#TINJ #HR /ADWS /#DE /#LOWS #QR

Similar to Sequence ATWS_56 except that power conversion system is unavailable (#PCS) and HPCI is successful in providing core cooling initially following the transient (/HPCI-1). Compared to Sequence ATWS_49 this is a non-minimal sequence.

ATWS_91: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 /#BI /#TINJ #HR /ADWS /#DE #LOWS

Similar to Sequence ATWS_57 except that power conversion system is unavailable and HPCI is successful in providing core cooling initially following the transient. Compared to Sequence ATWS_50 this is a non-minimal sequence.

ATWS_92: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 /#BI /#TINJ #HR /ADWS #DE

Similar to Sequence ATWS_58 except that power conversion system is unavailable (#PCS) and HPCI is successful in providing core cooling initially following the transient (/HPCI-1). Compared to Sequence ATWS_58 this is a non-minimal sequence.

ATWS_93: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 /#BI /#TINJ #HR ADWS

Similar to Sequence ATWS_59 except that power conversion system is unavailable (#PCS) and HPCI is successful in providing core cooling initially following the transient (/HPCI-1). Compared to Sequence ATWS_59 this is a non-minimal sequence.

ATWS_95: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 /#BI #TINJ /ADWS /#DE /#LOWS #QR

Similar to Sequence ATWS_61 except that the power conversion system is unavailable (#PCS) and HPCI is successful in providing core cooling initially following the transient (/HPCI-1). Compared to Sequence ATWS_49 this is a non-minimal sequence.

ATWS_96: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 /#BI #TINJ /ADWS /#DE #LOWS

Similar to Sequence ATWS_62 except that the power conversion system is unavailable (#PCS) and HPCI is successful in providing core cooling initially following the transient (/HPCI-1). Compared to Sequence ATWS_50 this is a non-minimal sequence.

ATWS_97: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 /#BI #TINJ /ADWS #DE

Similar to Sequence ATWS_63 except that the power conversion system is unavailable (#PCS) and HPCI is successful in providing core cooling initially following the transient (/HPCI-1). Compared to Sequence ATWS_63 this is a non-minimal sequence.

ATWS_98: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 /#BI #TINJ ADWS

Similar to Sequence ATWS_64 except that the power conversion system is unavailable (#PCS) and HPCI is successful in providing core cooling initially following the transient (/HPCI-1). Compared to Sequence ATWS_64 this is a non-minimal sequence.

ATWS_100: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 #BI /ADWS /#DE /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). One SRV sticks open (#SORV1). The power conversion system is unsuccessful in providing core cooling (#PCS). HPCI-1 is successful in providing core cooling during the initial period following the transient (/HPCI-1). BIIT is exceeded (due to the stuck-open SRV) and SLCS injection is unsuccessful (#BI). No ADS actuation has occurred. Manual vessel depressurization and low pressure injection are successful (/#DE, /LOWS). Heat removal function is unsuccessful (#QR) resulting in eventual core damage. Compared to Sequence ATWS_49, this is a non-minimal sequence.

ATWS_101: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 #BI /ADWS /#DE #LOWS

Similar to Sequence ATWS_100 except that low pressure injection is unavailable (#LOWS) resulting in eventual core damage. Compared to Sequence ATWS_50, this is a non-minimal sequence.

ATWS_102: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 #BI /ADWS #DE

Similar to Sequence ATWS_100 except that manual vessel depressurization has failed resulting in eventual core damage.

ATWS_103: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS /HPCI-1 #BI ADWS

Similar to Sequence ATWS_100 except that automatic vessel depressurization has occurred. Core damage is assumed due to the uncontrolled injection of cold water from low pressure systems.

ATWS_105: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS HPCI-1 /ADWS /#DE /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). One SRV sticks open (#SORV1). Both the power conversion system and HPCI are unsuccessful in providing core cooling (#PCS, HPCI-1). Manual vessel depressurization is required to allow low pressure

injection for core cooling. No ADS actuation has occurred. Vessel depressurization and low pressure injection are successful (/#DE, /LOWS). The heat removal function is unsuccessful (#QR) resulting in eventual core damage. Compared to Sequence ATWS_49, this is a non-minimal sequence.

ATWS_106: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS HPCI-1 /ADWS /#DE #LOWS

Similar to Sequence ATWS_105 except that low pressure injection is unavailable resulting in eventual core damage. Compared to Sequence ATWS_50, this is a non-minimal sequence.

ATWS_107: IEGATWS #RSCRAM /RPT /#BVPR #SORV1 #PCS HPCI-1 /ADWS #DE

Similar to Sequence ATWS_105 except that manual vessel depressurization is unsuccessful resulting in eventual core damage due to lack of low pressure injection.

ATWS_108: IEGATWS #RSCRAM /RPT /#BVPR #SORV0 #PCS HPCI-1 ADWS

Similar to Sequence ATWS_105 except that ADS actuation has occurred. Core damage is assumed due to the uncontrolled injection of cold water from low pressure systems.

ATWS_110: IEGATWS #RSCRAM /RPT /#BVPR #SORV2 /ADWS /#DE /#LOWS #QR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). Two SRVs stick open (#SORV2). Both the power conversion system and HPCI will eventually become ineffective due to the vessel pressure decrease through the stuck-open SRVs. Manual vessel depressurization (conservatively assumed to be required) and low-pressure injection are successful (/ADWS, #DE, #LOWS). However, the heat removal function is unavailable (#QR) resulting in eventual core damage.

ATWS_111 IEGATWS #RSCRAM /RPT /#BVPR #SORV2 /ADWS /#DE #LOWS

Similar to Sequence ATWS_110 except that low pressure injection is unavailable (#LOWS) resulting in eventual core damage.

ATWS_112 IEGATWS #RSCRAM /RPT /#BVPR #SORV2 /ADWS #DE

Similar to Sequence ATWS_110 except that manual depressurization (#DE) is unsuccessful resulting in eventual core damage.

ATWS_113 IEGATWS #RSCRAM /RPT /#BVPR #SORV2 ADWS

Similar to Sequence ATWS_110 except that automatic vessel depressurization has occurred. Core damage is assumed due to the uncontrolled injection of cold water by the low pressure systems.

ATWS_114 IEGATWS #RSCRAM /RPT /#BVPR #SORV3

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief is provided by the turbine bypass valves and SRVs (/#BVPR). Three or more SRVs stick

open (#SORV3). Rapid vessel depressurization occurs. It is assumed that core damage results due to uncontrolled injection.

ATWS_115 IEGATWS #RSCRAM /RPT #BVPR

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Both recirculation pumps trip (/RPT). Initial vessel pressure relief by the turbine bypass valves and SRVs is unsuccessful (#BVPR). Core damage is assumed.

ATWS_116 IEGATWS #RSCRAM RPT

Following the occurrence of a transient, reactor shutdown by the RPS, ARI, and manual operator action is unsuccessful (#RSCRAM). Recirculation pump trip fails (RPT). Core damage is assumed.

2.3 The Loss of Offsite Power Event Tree

This LOSP event tree covers core damage sequences associated with the LOSP initiator and the corresponding Station Blackout (SBO) scenarios.

EVENT TREE MODIFICATION

In the IPE, the frontline system core damage sequences for the LOSP initiator was obtained by linking together 6 RISKMAN frontline systems event trees (LOSP, INTER2, REC3, REC2, RHRCS and LTC1). After reviewing the RISKMAN event trees developed for the LOSP initiating event, the following key changes were made:

- Top events RCIC, HPCI and HP modeled in the RISKMAN event tree LOSP are combined according to the function provided by the individual systems, high pressure injection (HPI). Similarly, other top events modeled in the RISKMAN event trees are also combined according to the functions provided by the systems.

- With the exception of RP (which is guaranteed to fail during an LOSP event), many of the top events in RISKMAN event tree INTER2 are incorporated into lower level fault tree models for LOCA signal, operator restoration following a LOCA signal, automatic/emergency depressurization, diesel generator availability, etc. Top events V18, CW, and RD are also guaranteed to fail.

- Recovery top events modeled in REC3 are incorporated into the recovery rule file, as necessary, and the appropriate system fault trees (e.g., plant service water).

- Recovery top events modeled in REC2 are incorporated into the appropriate system fault trees.

- Most of the top events modeled in RISKMAN event trees RHRCS and LTC1 are incorporated into the lower level fault trees for ETA headings DE, LO, and QR. RISKMAN top events Z5, DESC2, RPOP, DESC1, CFF, and IN2 were determined to be not functional requirements for core damage.

For the new ETA event tree, LOSP, nodes under each heading may be represented by one or more fault tree gates. The multiple RISKMAN system models were combined into one fault tree gate with additional compression achieved by combining similar functions into one final fault tree gate with multiple inputs. Listed below are the new top logic gates developed for the ETA event tree

nodes and the original inputs associated with each (i.e., RISKMAN event tree top events combined into the gate):

#BVPR	(BV failed by LOSP), PR
#SORV0/1/2/3	SORV
#HP-1	RCIC, HPCI, HP, HI, (CW, RD failed by LOSP)
#ADED	VC, V18 (failed by LOSP), LOCA, L1OP, DWTC, OW
#DE	DE
#LO	(CO failed by LOSP), CS, RA, RB, JS, VA, VB, VOP, NS, NSREC, LC
#QR/#QT	OL, QS, QT, RA, RB, VA, VB, VOP, HA, HB, QV, IN1, QR
#HP-B	RCIC, HPCI, HP
FL-HPI-B-S	N/A

EVENT TREE HEADINGS & BRANCHES

The following event tree headings and nodes appear on the tree in the approximate chronological order that would be expected during an LOSP event.

%LOSP Loss of Offsite Power Initiating Event.

PR Pressure Relief. This heading models the pressure control function performed by the SRVs during the initial pressure transient following a plant trip due to an LOSP event. The bypass valves are unavailable due to closure of the MSIVs during an LOSP event. Failure of this event (Branch ID #BVPR) is modeled as resulting in a medium-break LOCA.

SORV SORV Reclosure. This is a multistate heading. It models the reclosure status of SRVs (i.e., the number of stuck open SRVs). The four states applicable to this heading are: all SRVs successfully reclose (Branch ID #SORV0); one SRV fails to reclose (Branch ID #SORV1); two SRVs fail to reclose (Branch ID #SORV2); and three or more SRVs fail to reclose (Branch ID #SORV3).

HPI High Pressure Level Control by RCIC/HPCI. This heading models the high-pressure level control function provided by the RCIC and HPCI systems. Both automatic and manual actuations are considered in this heading. Also included in this heading are the operator actions to control HPCI and RCIC to prevent multiple Level 8 trips. For any stuck-open SRVs and medium LOCAs, RCIC is inadequate for vessel level control. For three or more stuck-open SRVs, HPCI is inadequate, and for one or two SRVs stuck open HPCI recovery is not credited. Success of this event implies that RCIC or HPCI is available to provide the high-pressure level control function. Failure of this event (Branch ID #HP-1) implies that both RCIC and HPCI are unavailable for the vessel level control function and vessel depressurization is required.

ADED Automatic and Emergency Depressurization Conditions. This heading models the automatic and emergency depressurization conditions. The automatic depressurization condition is modeled by generation of the LOCA signal and failure of the operators to inhibit the ADS actuation. LOCA signals include Level 1 and high drywell pressure signals. In addition, it was assumed that loss of the MCR cooling would result in generation of a LOCA signal. Failure of drywell cooling (RISKMAN Top Event VC) and failure of the operators to vent via the 18"

vents to prevent a LOCA signal (RISKMAN Top Event V18) were assumed to lead to generation of a high drywell pressure signal.

Emergency vessel depressurization is required by the Plant Hatch procedures if the drywell temperature limit is exceeded. Drywell temperature would increase if drywell cooling fails and the operators fail to initiate drywell spray (RISKMAN Top Event OW). Drywell cooling would also be lost if the operators fail to restore drywell cooling following a LOCA signal.

Success of this event implies that there are no automatic and emergency depressurization conditions, or the operators successfully inhibit ADS and restore drywell cooling given a LOCA signal. Failure of this event (Branch ID #ADED) implies that ADS would be actuated or the operators are required to initiate emergency vessel depressurization. It is assumed in sequences involving failure of this heading that the vessel is depressurized and downstream heading DE is not asked. This heading is not asked if HPI fails requiring a vessel depressurization (downstream heading DE).

DE Depressurization of Vessel before Core Damage. This heading models the reduction of vessel pressure to permit level recovery. This heading includes the manual emergency depressurization actions required when all high-pressure injection sources are lost. This heading is only asked when HPI fails. Success of this event implies that operators successfully depressurize the reactor vessel to allow injection by the low-pressure systems. Failure of this event (Branch ID #DE) implies that reactor vessel remains at high pressure and core damage will result.

LO Low Pressure Injection. This heading models the low pressure injection function provided by the condensate, core spray, and low pressure coolant injection (LPCI) systems. Both automatic and manual actions are considered for core spray and LPCI. Success of this event implies that low-pressure injection is available. Failure of this event (Branch ID #LO) implies that low-pressure injection is unsuccessful.

QR Decay Heat Removal. This heading models decay heat removal by shutdown cooling, suppression pool cooling, and the containment hardened vent. Two different top logic gates have been developed to model the nodes under this heading, #QR and #QT.

For sequences in which RCIC or HPCI is successful, there is no stuck-open SRV (or no failure of pressure relief), and low pressure injection is unavailable, decay heat removal can be achieved by suppression pool cooling (modeled by top logic gate #QT). Success implies that, with suppression pool cooling, the long-term operation of RCIC or HPCI can be successful. Failure (Branch ID #QT) implies that high-pressure injection would also be lost due to loss of heat removal.

Top logic gate #QR is used in sequences in which #LO is successful. Success implies that the decay heat removal function is successful due to the success of torus or shutdown cooling or the containment hardened vent. Heat removal via the main condenser is failed by an LOSP event. Failure (Branch ID #QR) implies that no decay heat removal is available.

HPI-B High Pressure Injection until Battery Depletion. This heading models high-pressure injection for the life of the station batteries without AC power for charging. Only RCIC is involved because it can operate without room cooling which depends on AC power. The heading HPI-B is only addressed in sequences in which #BVPR is successful and no SRVs fail to reclose (#SORV0). This heading helps to define the power recovery timing, based on whether HPI is successful for the duration of the battery life, for the Station Blackout cutsets obtained from the integrated model.

SEQUENCES

The following sequence descriptions use a "/" prior to the branch designation to denote the success path of the branch and the branch name alone to designate the failure path.

LOSP_2: %LOSP /#BVPR #SORV0 /#HP-1 /#ADED /#LO #QR

An LOSP event occurs which causes a reactor trip. The initial pressure relief is successful (/#BVPR) followed by successful SRV reclosure (#SORV0). High pressure injection by RCIC or HPCI is successful. No automatic or emergency depressurization occurs (/#ADED); therefore, hardware response for the vessel depressurization is not asked in this sequence. Vessel pressure is reduced due to the cooldown operation provided by RCIC/HPCI. Low pressure injection is successful (/#LO). The decay heat removal function is unavailable (#QR) resulting in eventual core damage. Since #HP-1 is successful, RCIC would operate until the batteries are depleted, if an SBO event occurs. (Rev 1 change removes FL-HPI-B-S flag which indicated RCIC success on battery power.)

LOSP_4: %LOSP /#BVPR #SORV0 /#HP-1 /#ADED #LO #QT

Similar to Sequence LOSP_2 except that low pressure injection is unsuccessful (#LO). Core cooling can only be achieved by high pressure injection provided by RCIC/HPCI (/#HP-1). To permit long term RCIC/HPCI operation, suppression pool cooling must be successful. However, in this sequence, suppression pool cooling is unavailable (#QT) resulting in eventual core damage. Since #HP-1 is successful, RCIC would operate until the batteries are depleted, if an SBO event occurs. (Rev 1 model removes FL-HPI-B-S flag.)

LOSP_6: %LOSP /#BVPR #SORV0 /#HP-1 #ADED /#LO #QR

Same as Sequence LOSP_2 except that the reactor vessel is depressurized by actuation of ADS or the operators were required to initiate emergency vessel depressurization (#ADED). Compared to Sequence LOSP_2, this sequence is not minimal since it involves the additional failure of #ADED.

LOSP_7: %LOSP /#BVPR #SORV0 /#HP-1 #ADED #LO

An LOSP event occurs which causes a reactor trip. The initial pressure relief is successful (/#BVPR) followed by successful SRV reclosure (#SORV0). High pressure injection by RCIC or HPCI is successful (/#HP-1), but the reactor vessel depressurizes due to automatic depressurization conditions or emergency depressurization requirements (#ADED). The hardware response for vessel depressurization (modeled in #DE) is assumed successful. Low pressure injection is unsuccessful (#LO) resulting in eventual core damage due to loss of all high and low pressure injection sources . The decay heat removal function is not asked in this sequence. Since #HP-1 is successful, RCIC would operate until the batteries are depleted, if an SBO event occurs. (Rev 1)

LOSP_9A: %LOSP /#BVPR #SORV0 #HP-1 /#DE /#LO #QR /#HP-B

Same as Sequence LOSP_2 except long term high pressure injection by RCIC or HPCI is unavailable (#HP-1) and vessel pressure is successfully reduced by the SRVs (/#DE). In the event of an SBO, RCIC would operate successfully until the batteries are depleted (/#HP-B). Compared to Sequence LOSP_2, this sequence is not minimal since it involves the additional failure of high pressure injection (#HP-1). Since #HP-B is successful, RCIC would be available for the duration of the battery life. (Rev 1)

LOSP_9B: %LOSP /#BVPR #SORV0 #HP-1 /#DE /#LO #QR #HP-B

Same as Sequence LOSP_2 except long term high pressure injection by RCIC or HPCI is unavailable (#HP-1) and vessel pressure is successfully reduced by the SRVs (/#DE). Failure of the heat removal function leads to eventual core damage. In the event of an SBO, RCIC would be unavailable for the duration of the battery life (#HP-B).

LOSP_10A: %LOSP /#BVPR #SORV0 #HP-1 /#DE #LO /#HP-B

An LOSP event occurs which causes a reactor trip. The initial pressure relief is successful (/#BVPR) followed by successful SRV reclosure (#SORV0). High pressure injection by RCIC or HPCI fails (#HP-1). Vessel depressurization occurs (/#DE) but low pressure injection fails (#LO). If an SBO event occurs, RCIC would operate until the batteries are depleted .

LOSP_10B: %LOSP /#BVPR #SORV0 #HP-1 /#DE #LO #HP-B

Same as Sequence LOSP_10A except, in the event of an SBO, RCIC would not operate until the batteries are depleted (#HP-B).

LOSP_11A: %LOSP /#BVPR #SORV0 #HP-1 #DE /#HP-B

An LOSP event occurs which causes a reactor trip. The initial pressure relief is successful (/#BVPR) followed by successful SRV reclosure (#SORV0). Long term high-pressure injection by RCIC or HPCI fails (#HP-1) and vessel depressurization fails (#DE). If an SBO occurs, RCIC would operate until the batteries are depleted .

LOSP_11B: %LOSP /#BVPR #SORV0 #HP-1 #DE #HP-B

Same as Sequence LOSP_11A except, in the event of an SBO, RCIC would not operate until the batteries are depleted (#HP-B).

LOSP_13: %LOSP /#BVPR #SORV1 /#HP-1 /#LO #QR

An LOSP event occurs which causes a reactor trip. The initial pressure relief is successful (/#BVPR) followed by one SRV failing to reclose (#SORV1). High-pressure injection by HPCI is successful (/#HP-1). Vessel pressure continues to decrease due to the SRV failing to reclose, so ADED is bypassed. Low-pressure injection is successful (/#LO). The decay heat removal function is unavailable (#QR). Because low pressure injection would lose its suction source (i.e., the suppression pool) due to excessive temperature, the eventual overpressure failure would result in eventual core damage.

LOSP_14: %LOSP /#BVPR #SORV1 /#HP-1 #LO

An LOSP event occurs which causes a reactor trip. The initial pressure relief is successful (/#BVPR) followed by one SRV failing to reclose (#SORV1). High-pressure injection by HPCI is successful (/#HP-1). Vessel pressure continues to decrease due to the SRV failing to reclose, so ADED is bypassed. Low pressure injection is unsuccessful (#LO) resulting in eventual core damage due to loss of all high and low pressure injection sources. The decay heat removal function is not asked in this sequence.

LOSP_16: %LOSP /#BVPR #SORV1 #HP-1 /#DE /#LO #QR

Similar to Sequence LOSP_13 except high-pressure injection by HPCI is unavailable (#HP-1). Manual vessel depressurization is successful. Compared to Sequence LOSP_13, this sequence is not minimal since it involves the additional failure of high-pressure injection (#HP-1).

LOSP_17: %LOSP /#BVPR #SORV1 #HP-1 /#DE #LO

Similar to Sequence LOSP_14 except high-pressure injection by HPCI is unavailable (#HP-1). Manual vessel depressurization is successful. Compared to Sequence LOSP_14, this sequence is not minimal since it involves the additional failure of high-pressure injection (#HP-1).

LOSP_18: %LOSP /#BVPR #SORV1 #HP-1 #DE

Similar to Sequence LOSP_17 except that vessel pressure reduction has failed (#DE), given failure of high-pressure injection. This results in eventual core damage due to the inability to inject low pressure water to the vessel.

LOSP_20: %LOSP /#BVPR #SORV2 /#HP-1 /#LO #QR

Similar to Sequence LOSP_13 except that two SRVs stick open (#SORV2).

LOSP_21: %LOSP /#BVPR #SORV2 /#HP-1 #LO

Similar to Sequence LOSP_14 except that two SRVs stick open (#SORV2).

LOSP_23: %LOSP /#BVPR #SORV2 #HP-1 /#DE /#LO #QR

Similar to Sequence LOSP_16 except that two SRVs stick open (#SORV2). Compared to Sequence LOSP_20, this sequence is non-minimal.

LOSP_24: %LOSP /#BVPR #SORV2 #HP-1 /#DE #LO

Similar to Sequence LOSP_17 except that two SRVs stick open (#SORV2). Compared to Sequence LOSP_21, this sequence is non-minimal.

LOSP_25: %LOSP /#BVPR #SORV2 #HP-1 #DE

Similar to Sequence LOSP_18 except that two SRVs stick open (#SORV2).

LOSP_27: %LOSP /#BVPR #SORV3 /#LO #QR

An LOSP event occurs which causes a reactor trip. The initial pressure relief is successful (/#BVPR) followed by three or more SRVs failing to reclose (#SORV3). All high-pressure injection sources are lost due to vessel depressurization caused by the stuck-open SRVs. Following vessel depressurization, low-pressure injection is successful (/#LO). However, the decay heat removal function is unavailable (#QR). Due to the loss of the low-pressure injection suction source (i.e., the suppression pool), overpressure resulting in eventual core damage.

LOSP_28: %LOSP /#BVPR #SORV3 #LO

Similar to Sequence LOSP_27 except low-pressure injection is unsuccessful (#LO) resulting in eventual core damage due to loss of all high and low pressure injection sources. The decay heat removal function is not asked in this sequence.

LOSP_30: %LOSP #BVPR /#HP-1 /#LO #QR

Similar to Sequence LOSP_20 except that the initial pressure relief has failed (#BVPR). It was assumed that a medium-break LOCA resulted. SRVs are not challenged.

LOSP_31: %LOSP #BVPR /#HP-1 #LO

Similar to Sequence LOSP_21 except that the initial pressure relief has failed (#BVPR). It is assumed that a medium-break LOCA has resulted with failed low-pressure injection. The SRVs are not challenged.

LOSP_33: %LOSP #BVPR #HP-1 /#DE /#LO #QR

Similar to Sequence LOSP_23 except that the initial pressure relief has failed (#BVPR). It was assumed that a medium-break LOCA resulted. Compared to Sequence LOSP_30, this sequence is non-minimal.

LOSP_34: %LOSP #BVPR #HP-1 /#DE #LO

Similar to Sequence LOSP_24 except that the initial pressure relief has failed (#BVPR). It was assumed that a medium-break LOCA resulted. Compared to Sequence LOSP_31, this sequence is non-minimal.

LOSP_35: %LOSP #BVPR #HP-1 #DE

Similar to Sequence LOSP_25 except that the initial pressure relief has failed (#BVPR). It is assumed that a medium-break LOCA has resulted.

2.4 The Large LOCA Event Tree

This sections contains information regarding the core damage event tree developed for the large LOCA initiators, including %ALOCA and %LLOCA.

EVENT TREE MODIFICATION

In the IPE, the frontline system core damage sequences for both of the large LOCA initiators were obtained by linking together 5 RISKMAN frontline systems event trees; i.e., event trees LOCA, INTER1, REC0, RHRCS, and LTC1. This same set of linked event trees is also used for the medium LOCA initiator. The only differences are the split fraction assignments for selected top events.

After reviewing the RISKMAN event trees developed for the previously mentioned group of initiating events, the following key changes were made:

- The initiators were combined into a single transient initiator heading LLOCA (with a node designated by IEGALLOCA).
- Top events modeled in RISKMAN event trees are combined according to the functions provided by the individual systems.
- With some (e.g., RP), many of the top events in RISKMAN event tree INTER1 are incorporated into lower level fault tree models for LOCA signal, operator restoration following a LOCA signal, etc.
- Recovery top events modeled in REC0 are incorporated into the appropriate system fault trees throughout the model.
- Most top events listed in RISKMAN event trees RHRCS and LTC1 are incorporated into the lower level fault trees for ETA headings LO and QR. RISKMAN top events Z5, HI, DWTC, OW, DE, DESC2, RPOP, QS, QC, DESC1, IN1, CFF, and IN2 were determined to not be functional requirements for core damage mitigation in this case.

The initiators included in the ETA transient initiator heading LLOCA are %ALOCA and %LLOCA.

For the new ETA event tree LLOCA, nodes under each heading may be represented by one or more fault tree gates. The multiple RISKMAN system models were combined into one fault tree gate with additional compression achieved by combining similar functions into one final fault tree gate with multiple inputs. Listed below are the new top logic gates developed for the ETA event tree nodes and the relevant, original inputs associated with each (i.e., RISKMAN event tree top events combined into the gate):

#LO	CS, RA, RB, JS, VA, VB, VOP, NS, NSREC, LC
#QRQRA	OL, QT, RA, RB, VA, VB, VOP, HA, HB, QV, QR

EVENT TREE HEADINGS & BRANCHES

The following event tree headings and nodes appear on the tree in the approximate chronological order that would be expected during a transient.

LLOCA Large LOCA Initiating Events. This heading (Branch ID IEGALLOCA) includes both large LOCA initiators.

LO Low Pressure Injection. This heading models the low pressure injection function provided by the core spray and low pressure coolant injection (LPCI) systems. Only automatic actions are considered for core spray and LPCI. Success of this event implies that low pressure injection is available. Failure of this event (Branch ID #LO) implies that low pressure injection is unsuccessful.

QR Decay Heat Removal. This heading models decay heat removal by suppression pool cooling, torus vent, etc. Top logic gate #QRQRA has been developed to model the node under this heading. Recovery of decay heat removal during the period prior to containment or ECCS failure is also considered.

SEQUENCES

The following sequence descriptions use a "/" prior to the branch designation to denote the success path of the branch and the branch name alone to designate the failure path.

LLOCA_2: IEGALLOCA /#LO #QRQRA

A large LOCA event occurs (IEGALLOCA). Due to the LOCA break flow, the reactor is shut down and the vessel pressure decreases to the low pressure system shutoff head. Low pressure injection is successful (/#LO). However, the decay heat removal function is unavailable (#QRQRA) resulting in eventual core damage.

LLOCA_3: IEGALLOCA #LO

Similar to Sequence LLOCA_2, a large LOCA event occurs (IEGALLOCA). Due to the LOCA break flow, the reactor is shut down and the vessel pressure decreases to the low pressure system shutoff head. Low pressure injection is unsuccessful (#LO) resulting in eventual core damage. The decay heat removal function is not asked in this sequence.

2.5 The Medium LOCA Event Tree

This sections contains information regarding the core damage event tree developed for the medium LOCA initiator; i.e., %MLOCA.

EVENT TREE MODIFICATION

In the IPE, the frontline system core damage sequences for the medium LOCA initiator were obtained by linking together 5 RISKMAN frontline systems event trees; i.e., event trees LOCA, INTER1, REC0, RHRCS, and LTC1.

After reviewing the RISKMAN event trees developed for this initiating event, the following key changes were made:

- Top events modeled in RISKMAN event trees are combined according to the functions provided by the individual systems.

- With some exceptions (e.g., RP), many top events in RISKMAN event tree INTER1 are incorporated into lower level fault tree models for LOCA signal, operator restoration following a LOCA signal, etc.

- Recovery top events modeled in REC0 are incorporated into the appropriate system fault trees throughout the model.

- Most top events listed in RISKMAN event trees RHRCS and LTC1 are incorporated into the lower level fault trees for ETA headings DE, LO, and QR. RISKMAN top events Z5, DWTC, OW, DESC2, RPOP, QS, QC, DESC1, IN1, CFF, and IN2 were determined to not be functional requirements for core damage mitigation.

For the new ETA event tree MLOCA, nodes under each heading may be represented by one or more fault tree gates. The multiple RISKMAN system models were combined into one fault tree gate with additional compression achieved by combining similar functions into one final fault tree gate with multiple inputs. Listed below are the new top logic gates developed for the ETA event tree nodes and the relevant, original inputs associated with each (i.e., RISKMAN event tree top events combined into the gate):

#HP-1	HPCI
#DEHICO1	DE, HI, CO
#LO	CO, CS, RA, RB, JS, VA, VB, VOP, NS, NSREC, LC
#QRQRA	OL, QT, RA, RB, VA, VB, VOP, HA, HB, QV, QR

EVENT TREE HEADINGS & BRANCHES

The following event tree headings and nodes appear on the tree in the approximate chronological order that would be expected during a transient.

%MLOCA Medium LOCA Initiating Event. This heading includes only one initiator; i.e., %MLOCA.

HPI High Pressure Level Control by HPCI. This heading models the high pressure level control as well as cooldown and depressurization functions provided by the HPCI system. For medium LOCA, RCIC is inadequate for vessel level control. Only automatic actuation is considered in this heading and HPCI recovery is not credited for this initiator. Also included in this heading are the operator actions to control HPCI to prevent multiple Level 8 trips. Success of this event implies that HPCI is available to provide the high pressure level control, cooldown, and depressurization functions. Failure of this event (Branch ID #HP-1) implies that HPCI is unavailable for the vessel level control and cooldown functions and vessel depressurization is required.

DE Depressurization of Vessel Before Core Damage. This heading models the reduction of vessel pressure to permit level recovery. This heading includes the manual emergency depressurization actions required when all high pressure injection sources are lost. Also included in this heading is the controlled cooldown and pressure reduction with the use of condensate booster pumps. This heading is only asked when HPI fails. Success of this event implies that operators successfully depressurize the reactor vessel to allow injection by the low pressure systems. Failure of this event (Branch ID #DEHICO1) implies that reactor vessel remains at high pressure and core damage would result. #DEHICO1 also accounts

for a condensate/condensate booster pump injection at a lower reactor pressure, approximately 500 psig.

LO Low Pressure Injection. This heading models the low pressure injection function provided by the condensate, core spray, and low pressure coolant injection (LPCI) systems. Only automatic actions are considered for core spray and LPCI. Success of this event implies that low pressure injection is available. Failure of this event (Branch ID #LO) implies that low pressure injection is unsuccessful.

QR Decay Heat Removal. This heading models decay heat removal by suppression pool cooling, torus vent, etc. Top logic gate #QRQRA has been developed to model the node under this heading. Recovery of decay heat removal during the period prior to containment or ECCS failure is also considered.

SEQUENCES

The following sequence descriptions use a "/" prior to the branch designation to denote the success path of the branch and the branch name alone to designate the failure path.

MLOCA_2: %MLOCA /#HP-1 /#LO #QRQRA

A medium LOCA event occurs (%MLOCA). After reactor trip, high pressure injection by HPCI is successful (/#HP-1). Vessel pressure is reduced due to the cooldown operation provided by HPCI. Low pressure injection is successful (/#LO). However, the decay heat removal function is unavailable (#QRQRA) resulting in eventual core damage.

MLOCA_3: %MLOCA /#HP-1 #LO

Similar to Sequence MLOCA_2, a medium LOCA event occurs (%MLOCA). After reactor trip, high pressure injection by HPCI is successful (/#HP-1). Vessel pressure is reduced to the low pressure system shutoff head due to the cooldown operation provided by HPCI. Low pressure injection is unsuccessful (#LO) resulting in eventual core damage. The decay heat removal function is not asked in this sequence.

MLOCA_5: %MLOCA #HP-1 /#DEHICO1 /#LO #QRQRA

A medium LOCA event occurs (%MLOCA). After reactor trip, high pressure injection by HPCI fails (#HP-1). Vessel pressure is successfully reduced either by the cooldown operation of condensate/condensate booster pumps or by the manual initiation of SRV pressure relief (/#DEHICO1). Low pressure injection is successful (/#LO). However, the decay heat removal function is unavailable (#QRQRA) resulting in eventual core damage. Compared to Sequence MLOCA_2, this sequence is not minimal since it involves the additional failure of HPCI (#HP-1).

MLOCA_6: %MLOCA #HP-1 /#DEHICO1 #LO

A medium LOCA event occurs (%MLOCA). After reactor trip, high pressure injection by HPCI fails (#HP-1). Vessel pressure is successfully reduced to the low pressure system shutoff head either by the cooldown operation of condensate/condensate booster pumps or by the manual initiation of SRV pressure relief (/#DEHICO1). Low pressure injection is unsuccessful (#LO) resulting in eventual core damage. The decay heat removal function is not asked in this sequence. Compared to Sequence MLOCA_3, this sequence is not minimal since it involves the additional failure of HPCI (#HP-1).

MLOCA_7: %MLOCA #HP-1 #DEHICO1

A medium LOCA event occurs (%MLOCA). After reactor trip, high pressure injection by HPCI fails (#HP-1). In addition, vessel pressure reduction is unsuccessful (#DEHICO1) resulting in eventual core damage.

2.6 The Inadvertent Opening of Relief Valve Event Tree

This sections contains information regarding the core damage event tree developed for the inadvertent opening of relief valve initiator; i.e., %IORV.

EVENT TREE MODIFICATION

In the IPE, the frontline system core damage sequences for the inadvertent opening of relief valve initiator were obtained by linking together 5 RISKMAN frontline systems event trees; i.e., event trees IORV, INTER1, REC0, RHRCS, and LTC1.

After reviewing the RISKMAN event trees developed for this initiating event, the following key changes were made:

- Top events modeled in RISKMAN event trees are combined according to the functions provided by the individual systems.
- With the exception of RP, most of the top events in RISKMAN event tree INTER1 are incorporated into lower level fault tree models for LOCA signal, operator restoration following a LOCA signal, automatic/emergency depressurization, main condenser availability, etc.
- Recovery top events modeled in REC0 are incorporated into the appropriate system fault trees throughout the model.
- Most top events listed in RISKMAN event trees RHRCS and LTC1 are incorporated into the lower level fault trees for ETA headings DE, LO, and QR. RISKMAN top events Z5, DWTC, OW, DESC2, RPOP, QS, QC, DESC1, IN1, CFF, and IN2 were determined to not be functional requirements for core damage.

For the new ETA event tree IORV, nodes under each heading may be represented by one or more fault tree gates. The multiple RISKMAN system models were combined into one fault tree gate with additional compression achieved by combining similar functions into one final fault tree gate with multiple inputs. Listed below are the new top logic gates developed for the ETA event tree nodes and the relevant, original inputs associated with each (i.e., RISKMAN event tree top events combined into the gate):

BVA	BV
#PCS	CO, FW, FR, MC, MS
#HP-1	HPCI
#DEHICO1	DE, HI, CO
#LO	CO, CS, RA, RB, JS, VA, VB, VOP, NS, NSREC, LC
#QRQRA	OL, QT, RA, RB, VA, VB, VOP, HA, HB, QV, QR

EVENT TREE HEADINGS & BRANCHES

The following event tree headings and nodes appear on the tree in the approximate chronological order that would be expected during a transient.

%IORV Inadvertent Opening of Relief Valve Initiating Event. This heading includes only one initiator.

BV Pressure Relief. This heading models the pressure control function performed by the turbine bypass valves following a plant trip. Failure of this event (Branch ID BVA) would render the Power Conversion System unavailable.

PCS Power Conversion System. This heading models the availability or unavailability of the power conversion system to provide the core cooling function. Condensate system, feedwater system, and main condenser are included in this heading. One condensate pump and one condensate booster pump are required to support operation of a single feedwater pump. Only one reactor feed pump is required to provide feedwater flow to the reactor for level control. If the feedwater is initially unavailable following a reactor trip, restoration of feedwater prior to initiation of HPCI on Level 2 is also considered in this heading.

Success of this event implies that condensate, feedwater, and main condenser are available for plant response following the reactor trip. For the main condenser to remain available, the MSIVs must remain open, turbine bypass valves must continue to function and all support for the electrohydraulic control system must be available. Turbine bypass valves are modeled in the preceding heading (BV). Failure of this event (Branch ID #PCS) implies that HPCI will be demanded to operate to provide the high pressure level control function.

HPI High Pressure Level Control by HPCI. This heading models the high pressure level control function provided by the HPCI system. Only automatic actuation is considered in this heading and HPCI recovery is not credited for this initiator. Also included in this heading are the operator actions to control HPCI to prevent multiple Level 8 trips. RCIC is inadequate for vessel level control. This event is only asked in this event tree when turbine bypass valves or PCS is unsuccessful. Success of this event implies that HPCI is available to provide the high pressure level control function. Failure of this event (Branch ID #HP-1) implies that HPCI is unavailable for the vessel level control function and vessel depressurization is required.

ADED No branches are included for this heading.

DE Depressurization of Vessel Before Core Damage. This heading models the reduction of vessel pressure to permit level recovery. This heading includes the manual emergency depressurization actions required when all high pressure

injection sources are lost. Also included in this heading is the controlled cooldown and pressure reduction with the use of condensate booster pumps. This heading is only asked when both PCS and HPI fail. Success of this event implies that operators successfully depressurize the reactor vessel to allow injection by the low pressure systems. Failure of this event (Branch ID #DEHICO1) implies that reactor vessel remains at high pressure and core damage would result. #DEHICO1 also accounts for a condensate/condensate booster pump injection at a lower reactor pressure, approximately 500 psig.

LO Low Pressure Injection. This heading models the low pressure injection function provided by the condensate, core spray, and low pressure coolant injection (LPCI) systems. Both automatic and manual actions are considered for core spray and LPCI. Success of this event implies that low pressure injection is available. Failure of this event (Branch ID #LO) implies that low pressure injection is unsuccessful.

QR Decay Heat Removal. This heading models decay heat removal by suppression pool cooling, torus vent, etc. Top logic gate #QRQRA has been developed to model the nodes under this heading. Recovery of decay heat removal during the period prior to containment or ECCS failure is considered.

SEQUENCES

The following sequence descriptions use a "/" prior to the branch designation to denote the success path of the branch and the branch name alone to designate the failure path.

IORV_2: %IORV /BVA /#PCS #QRQRA

An inadvertent opening of relief valve event occurs (%IORV). After reactor trip, vessel pressure is successfully maintained by the turbine bypass valves (/BVA). In addition, condensate, feedwater, and main condenser operate successfully (/#PCS). Since the power conversion system is successful, high pressure injection by HPCI is not necessary. The decay heat removal function is unavailable (#QRQRA) resulting in eventual core damage.

IORV_4: %IORV /BVA #PCS /#HP-1 /#LO #QRQRA

An inadvertent opening of relief valve event occurs (%IORV). After reactor trip, vessel pressure is successfully maintained by the turbine bypass valves (/BVA). The power conversion system (condensate, feedwater, and main condenser) fails to operate (#PCS). High pressure injection by HPCI is successful (/#HP-1). Vessel pressure is reduced due to the cooldown operation provided by HPCI. Low pressure injection is successful (/#LO). However, the decay heat removal function is unavailable (#QRQRA) resulting in eventual core damage. Compared to Sequence IORV_2, this sequence is not minimal since it involves the additional failure of the power conversion system.

IORV_5: %IORV /BVA #PCS /#HP-1 #LO

Similar to Sequence IORV_4, an inadvertent opening of relief valve event occurs (%IORV). vessel pressure is successfully maintained by the turbine bypass valves (/BVA). The power conversion system (condensate, feedwater, and main condenser) fails to operate (#PCS). High pressure injection by HPCI is successful (/#HP-1). Vessel pressure is reduced due to the cooldown operation provided by HPCI. Low pressure injection is unsuccessful (#LO) resulting in eventual core damage. The decay heat removal function is not asked in this sequence.

IORV_7: %IORV /BVA #PCS #HP-1 /#DEHICO1 /#LO #QRQRA

An inadvertent opening of relief valve event occurs (%IORV). After reactor trip, vessel pressure is successfully maintained by the turbine bypass valves (/BVA). Both the power conversion system and high pressure injection by HPCI fail (#PCS and #HP-1). Vessel pressure is successfully reduced either by the controlled cooldown with the use of condensate/condensate booster pumps or by the manual initiation of SRV pressure relief (/#DEHICO1). Low pressure injection is successful (/#LO). However, the decay heat removal function is unavailable (#QRQRA) resulting in eventual core damage.

Compared to Sequence IORV_2, this sequence is not minimal since it involves the additional failures of the power conversion system and HPCI (#PCS and #HP-1).

IORV_8: %IORV /BVA #PCS #HP-1 /#DEHICO1 #LO

An inadvertent opening of relief valve event occurs (%IORV). After reactor trip, vessel pressure is successfully maintained by the turbine bypass valves (/BVA). Both the power conversion system and high pressure injection by HPCI fail (#PCS and #HP-1). Vessel pressure is successfully reduced either by the controlled cooldown with the use of condensate/condensate booster pumps or by the manual initiation of SRV pressure relief (/#DEHICO1). Low pressure injection is unsuccessful (#LO) resulting in eventual core damage. The decay heat removal function is not asked in this sequence. Compared to Sequence IORV_5, this sequence is not minimal since it involves the additional failure of HPCI (#HP-1).

IORV_9: %IORV /BVA #PCS #HP-1 #DEHICO1

An inadvertent opening of relief valve event occurs (%IORV). After reactor trip, vessel pressure is successfully maintained by the turbine bypass valves (/BVA). Both the power conversion system and high pressure injection by HPCI fail (#PCS and #HP-1). In addition, vessel pressure reduction is unsuccessful (#DEHICO1) resulting in eventual core damage.

IORV_11: %IORV BVA /#HP-1 /#LO #QRQRA

An inadvertent opening of relief valve event occurs (%IORV). After reactor trip, vessel pressure control by the turbine bypass valves fails (BVA). This also renders the long term heat removal via the main condenser unavailable. Power conversion system is therefore conservatively modeled as unavailable. High pressure injection by HPCI is successful (/#HP-1). Vessel pressure is reduced due to the cooldown operation provided by HPCI. Low pressure injection is successful (/#LO). However, the decay heat removal function is unavailable (#QRQRA) resulting in eventual core damage. Compared to Sequence IORV_2, this sequence is not minimal since it involves the additional failure of the turbine bypass valves (BVA).

IORV_12: %IORV BVA /#HP-1 #LO

An inadvertent opening of relief valve event occurs (%IORV). After reactor trip, vessel pressure control by the turbine bypass valves fails (BVA). This also renders the long term heat removal via the main condenser unavailable. Power conversion system is therefore conservatively modeled as unavailable. High pressure injection by HPCI is successful (/#HP-1). Vessel pressure is reduced due to the cooldown operation provided by HPCI. Low pressure injection is unavailable (#LO) resulting in eventual core damage.

IORV_14: %IORV BVA #HP-1 /#DEHICO1 /#LO #QRQRA

An inadvertent opening of relief valve event occurs (%IORV). After reactor trip, vessel pressure control by the turbine bypass valves fails (BVA). This also renders the long term heat removal via the main condenser unavailable. Power conversion system is therefore conservatively modeled as unavailable. High pressure injection by HPCI fails (#HP-1).

Vessel pressure is successfully reduced either by the controlled cooldown with the use of condensate/condensate booster pumps or by the manual initiation of SRV pressure relief (/#DEHICO1). Low pressure injection is successful (/#LO). However, the decay heat removal function is unavailable (#QRQRA) resulting in eventual core damage. Compared to Sequence IORV_2, this sequence is not minimal since it involves the additional failures of the turbine bypass valves and HPCI (BVA and #HP-1).

IORV_15: %IORV BVA #HP-1 /#DEHICO1 #LO

An inadvertent opening of relief valve event occurs (%IORV). After reactor trip, vessel pressure control by the turbine bypass valves fails (BVA). This also renders the long term heat removal via the main condenser unavailable. Power conversion system is therefore conservatively modeled as unavailable. High pressure injection by HPCI fails (#HP-1). Vessel pressure is successfully reduced either by the controlled cooldown with the use of condensate/condensate booster pumps or by the manual initiation of SRV pressure relief (/#DEHICO1). Low pressure injection is unsuccessful (#LO) resulting in eventual core damage. The decay heat removal function is not asked in this sequence. Compared to Sequence IORV_5, this sequence is not minimal since it involves the additional failure of HPCI (#HP-1).

IORV_16: %IORV BVA #HP-1 #DEHICO1

An inadvertent opening of relief valve event occurs (%IORV). After reactor trip, vessel pressure control by the turbine bypass valves fails (BVA). This also renders the long term heat removal unavailable. Power conversion system is therefore conservatively modeled as unavailable. High pressure injection by HPCI fails (#HP-1). In addition, vessel pressure reduction is unsuccessful (#DEHICO1) resulting in eventual core damage.

2.7 The Containment Release Event Tree

This section contains information regarding the containment release event tree.

EVENT TREE MODIFICATION

In the IPE model, each core damage sequence was first assigned an accident class. This assignment of the Level I core damage sequences dictated the path through the containment event tree (CET). The CET evaluates the characteristics of the containment response to the core damage sequences. It includes top events modeling those functions needed to support debris coolability and containment heat removal. The plant damage states are assigned to the CET outputs. They are based on the reactor status, the containment status, and the state of debris cooling. In addition, a release mode defining the type and the timing of release is also assigned to the CET outputs.

Due to the desire to collapse the number of unique plant damage states in the converted CAFTA model, it was decided to apply a simplified process of assigning core damage sequences to appropriate end states. SNC contracted Fauske and Associates (FAI) to develop the simplified Level II model.

The primary purpose of the containment event tree is to identify those sequences resulting in a Large Early Release from the containment (i.e., rapid, unscrubbed release of airborne aerosols within 6 hours or prior to effective implementation of offsite emergency response).

EVENT TREE HEADINGS & BRANCHES

The following event tree headings appear on the tree in the approximate chronological order that would be expected to lead to a release of fission products from the containment.

@H1CDFTOP Core Damage. This event includes all sequences leading to core damage. Since core damage is a prerequisite to the release of fission products, this is the starting point for the release categorization.

BYPASS Containment Bypass. This event represents those core damage sequences resulting in the direct bypass of the containment fission product boundary and a direct release to the environment. This includes all Interfacing Systems LOCA (V sequences) and break outside containment sequences.

VINJEC Vessel Injection. This heading models the availability or unavailability of the vessel injection source. This heading is asked if the containment is not bypassed. If the injection source is available, it would continue until either the vessel pressure increases to above the injection shutoff head or the containment fails due to overpressure since no containment heat removal is available (note that containment heat removal is unavailable if vessel injection is available since a core damage has occurred). In either case (whether the containment failure occurs prior to vessel failure), the containment and vessel failure times would be close with injection available. This would lead to a large release from the containment. If the injection source is unavailable, the containment response would be dependent on the containment heat removal asked in the next heading.

CHR Containment Heat Removal. This heading models the containment heat removal by the combination of drywell spray and suppression pool cooling. This heading is asked when the vessel injection is unavailable. If vessel injection is available, loss of containment heat removal is implied since core damage has already occurred. If the containment heat removal is available, the containment would remain intact. The drywell would be maintained at a relatively low pressure (with drywell spray available) minimizing the driving force for the release of fission products through leakage paths. The result is a small release from the containment. With no containment heat removal, venting would be required to limit the containment pressure rise.

VENT Containment Venting. This heading models containment venting via the drywell vent line or the wetwell vent line. It is asked when both the vessel injection and containment heat removal are unavailable. This is a multi-branch heading. The top branch represents successful containment venting via the wetwell vent line. The middle branch models successful venting via the drywell vent line. The bottom branch reflects unsuccessful venting.

Venting through the wetwell will provide fission product scrubbing and venting from the drywell will result in an unscrubbed release. If the containment venting is unsuccessful, the containment pressure will continue to rise until the containment

fails. However, the timing between the failure of the vessel and that of the containment is affected by the vessel pressure and drywell spray.

VDPR Vessel Depressurization. This heading models the reduction of vessel pressure. The status of this heading affects the timing between the failure of the vessel and that of the containment. This heading is asked when vessel injection, containment heat removal, and containment venting are all unavailable. If the vessel is not depressurized at the time of its failure, the drywell pressure would rise rapidly until the containment fails at time close to that of vessel failure. If the vessel is depressurized at the time of its failure, the rate of drywell pressure increase would not be sufficiently high to result in a containment failure occurring soon after vessel failure. As such, this scenario would not be an early release. Due to the elevated temperature in the containment caused by heatup from the debris bed (radiant heat) and concrete ablation, the containment failure pressure is reduced in this case. There is a long time between the vessel and containment failures. In the event of no vessel depressurization, drywell spray can also limit the pressure increase in the containment.

DWSP Drywell Spray. This heading models the availability or unavailability of drywell spray to limit the rate of containment pressure rise. This heading is asked when vessel injection, containment heat removal, containment venting, and vessel depressurization are all unavailable. If drywell spray is available, it can suppress the initial steam mass and reduce containment pressure rise. The drywell gas space temperature would increase. However, containment fails due to overpressure (not at a reduced pressure) caused by the spray water steaming from contact with the debris bed. This leads to an OPD end state. If drywell spray is unavailable, the drywell pressure rises quickly. Due to the lack of decay heat removal, the drywell gas temperature increases to the point where there is a reduced containment failure pressure due to the escalated temperature. An OT end state results in this case.

CNMT Containment Overpressure Failure. This heading models the containment overpressure failure location. This heading is asked when vessel injection is available and containment heat removal is unavailable. Failure of this heading includes drywell failure and wetwell water space failure. This would result in an unscrubbed release. Success of this heading implies a wetwell airspace failure.

SEQUENCES

The following sequence descriptions use a "/" prior to the branch designation to denote the success path of the branch and the branch name alone to designate the failure path.

LER_OPD: @H1CDFTOP /BYPASS /VINJEC CNMT

In LER_OPD, vessel injection is available with no containment heat removal following a core damage. Due to overpressure, the containment fails either prior to or soon after the vessel failure. The containment failure location is either in the drywell or in the wetwell water space. As a result, an unscrubbed release occurs.

LER_VD: @H1CDFTOP /BYPASS VINJEC CHR DWVENT

Following the core damage, vessel injection and containment heat removal are unavailable. To reduce the containment pressure, venting via the drywell vent line is performed. This provides no scrubbing.

LER_OT: @H1CDFTOP /BYPASS QV VDPR DWSP

Following the core damage, vessel injection, containment heat removal, containment venting, vessel depressurization, and drywell spray are all unavailable. The drywell pressure rises rapidly. The containment fails at a pressure lower than the design pressure due to the increased temperature in the drywell gas space caused by the loss of containment heat removal.

LER_CB: @H1CDFTOP BYPASS

This sequence involves the occurrence of either a break outside containment or an interfacing systems LOCA.

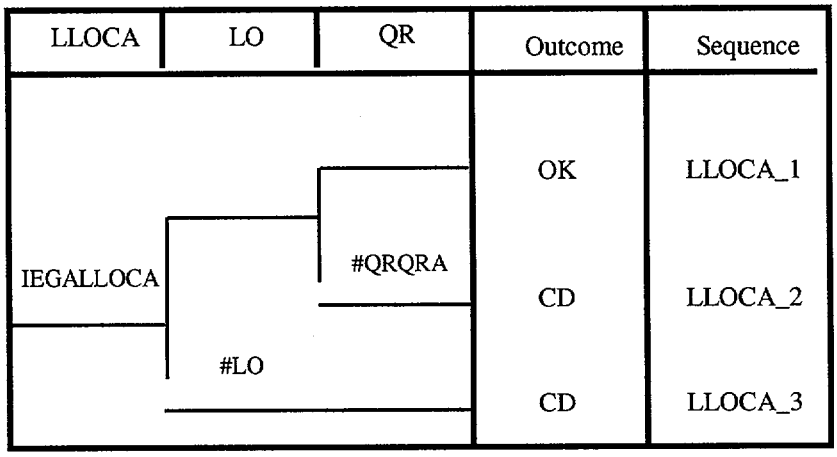
PART 2 Model Construction and Quantification Results

TABLE OF CONTENTS

1.0 GENERAL OVERVIEW

The methodology employed in the model integration and quantification task is based on a fault tree-linking approach. As shown in Figure 1.1, the methodology utilizes event trees to define the progression of an accident sequence from an initiating event to an undesirable state such as core damage. Appendix A contains definitions for many key terms used throughout this document.

Figure 1.1 Large LOCA Accident Sequence Event Tree



The status of mitigation functions (i.e., 'up' branch is success and 'down' branch is failure) along an event tree path determines the final outcome of the accident sequence. Therefore, failure sequences can be obtained by *ANDing* the down branch of successive mitigation functions, while success sequences can be obtained by *ANDing* the up branch of mitigation functions. In this example, the core damage sequence LLOCA_3 represents the occurrence of a large LOCA initiating event (i.e., event %LLOCA or %ALOCA designated as IEGALLOCA) and subsequent failures of the low pressure injection systems for inventory control (i.e., event #LO).

Since the fault tree linking methodology involves the solution of large fault tree models, it is necessary to translate the event tree logic to equivalent fault tree models called the accident sequence logic. The accident sequence logic models represent combinations of the initiating event with the top logic fault trees.

The top logic represents a set of fault tree models that provide the primary interface between the event tree model and frontline system fault tree models. The top logic models failures of mitigation functions. For example, in Figure 1.2, top logic model LLOCA_3 includes the Large LOCA event and failure of the low pressure injection mitigation function. The frontline fault tree models represent failures of systems that directly support a mitigation function. In Figure 1.2, the frontline system model LPCI represents failure of the Residual Heat Removal System in the low pressure coolant injection mode.

The support system fault tree models represent failures of systems that support the function of the frontline systems. In Figure 1.2, support system fault tree model ELEC represents failure of Electric Power to RHR pumps and valves. As shown on this figure, the accident sequence logic, top logic, frontline system, and support system fault tree models are linked together within CAFTA to form an integrated fault tree model. This fault tree contains all the necessary logic required to quantify the accident sequences defined by the event trees.

For accident sequences that do not involve the success of any mitigation functions, only one accident sequence logic fault tree model is required for quantification.

In Figure 1.2, core damage sequence LLOCA_3 is represented by the ***AND*** of initiating event IEGALLOCA (i.e., %LLOCA or %ALOCA) and the top logic model #LO for the low pressure injection function. Core damage sequence LLOCA_3 is quantified by solving the fault tree model for initiating events %LLOCA and %ALOCA and top logic model #LO. The results are in the form of ***CUTSETS*** that are combinations of failure events that result in core damage.

For accident sequences that contain successful mitigation functions, the fault tree models for the success functions are also required for quantification. For sequence LLOCA_2, function #QRQRA has *failed,* but function #LO has *succeeded.* To account for the success of #LO, the "delete-term" (DELTERM) procedure is used which removes cutsets from the failed function(s) containing events that fail the success function. For the LLOCA_2 sequence in Figure 1.2, the delete-term procedure is implemented by the following steps:

1. Solve the fault tree model for #QRQRA.

2. Solve the fault tree model for #LO.

3. Compare the cutsets for #LO with #QRQRA.

4. Delete any cutsets in #QRQRA that contain event combinations that are identical or are a superset of combinations already appearing in #LO.

The details of the overall quantification methodology, and its implementation using the CAFTA software, are described in the subsequent sections of this document. An overview of the quantification process is provided in Figure 1.3, where one can follow the original fault tree file through quantification, cutset manipulation, and output of final cutsets. Also, Figure 1.3 specifies the codes required to perform the quantification, and details the content and purpose of each input to the process. The left side of Figure 1.3 describe the inputs and the actual quantification is performed in PRAQUANT which is the software used by the CAFTA model for this purpose.

Figure 1.2 Overview of the Master Fault Tree Structure.

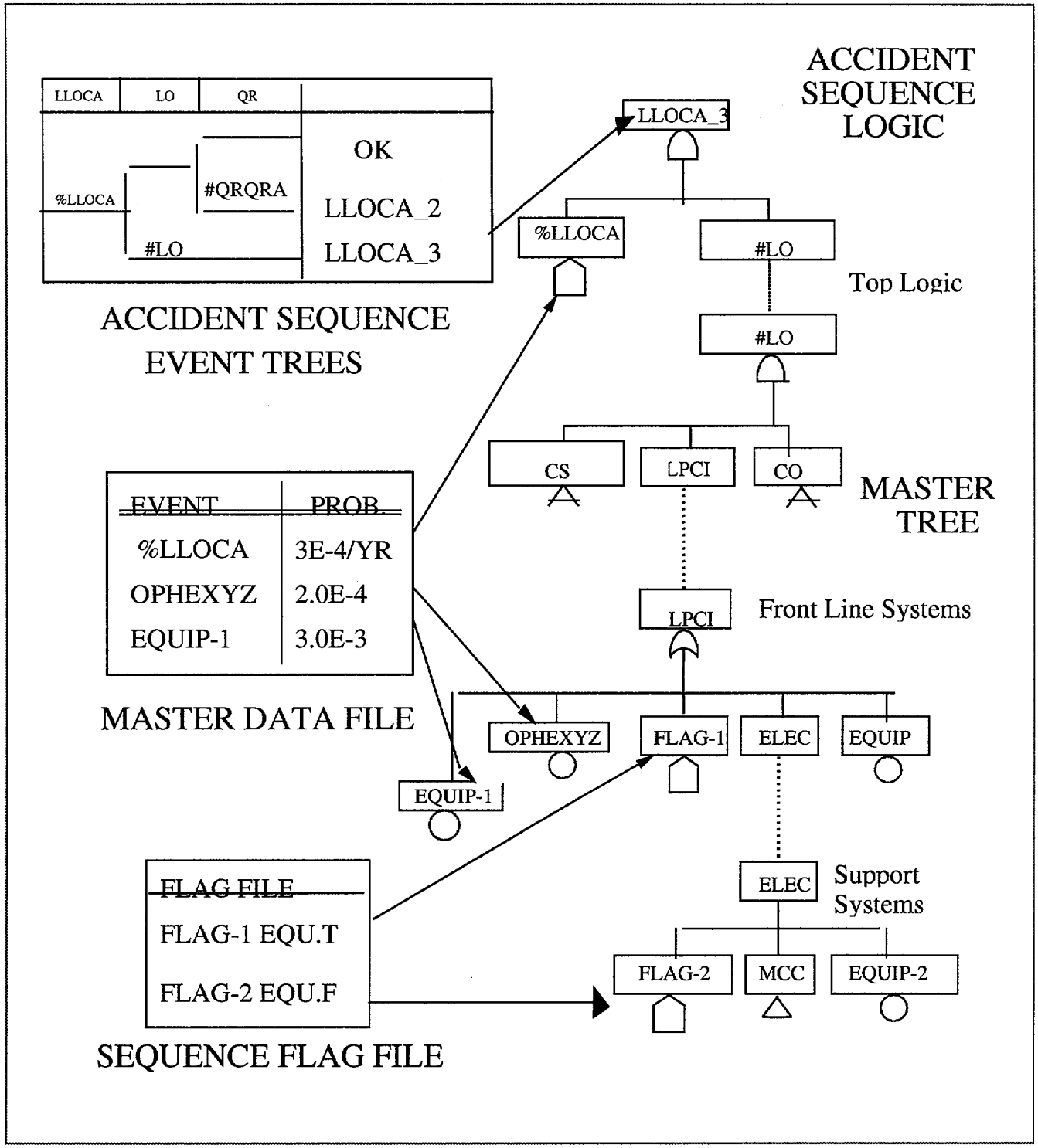
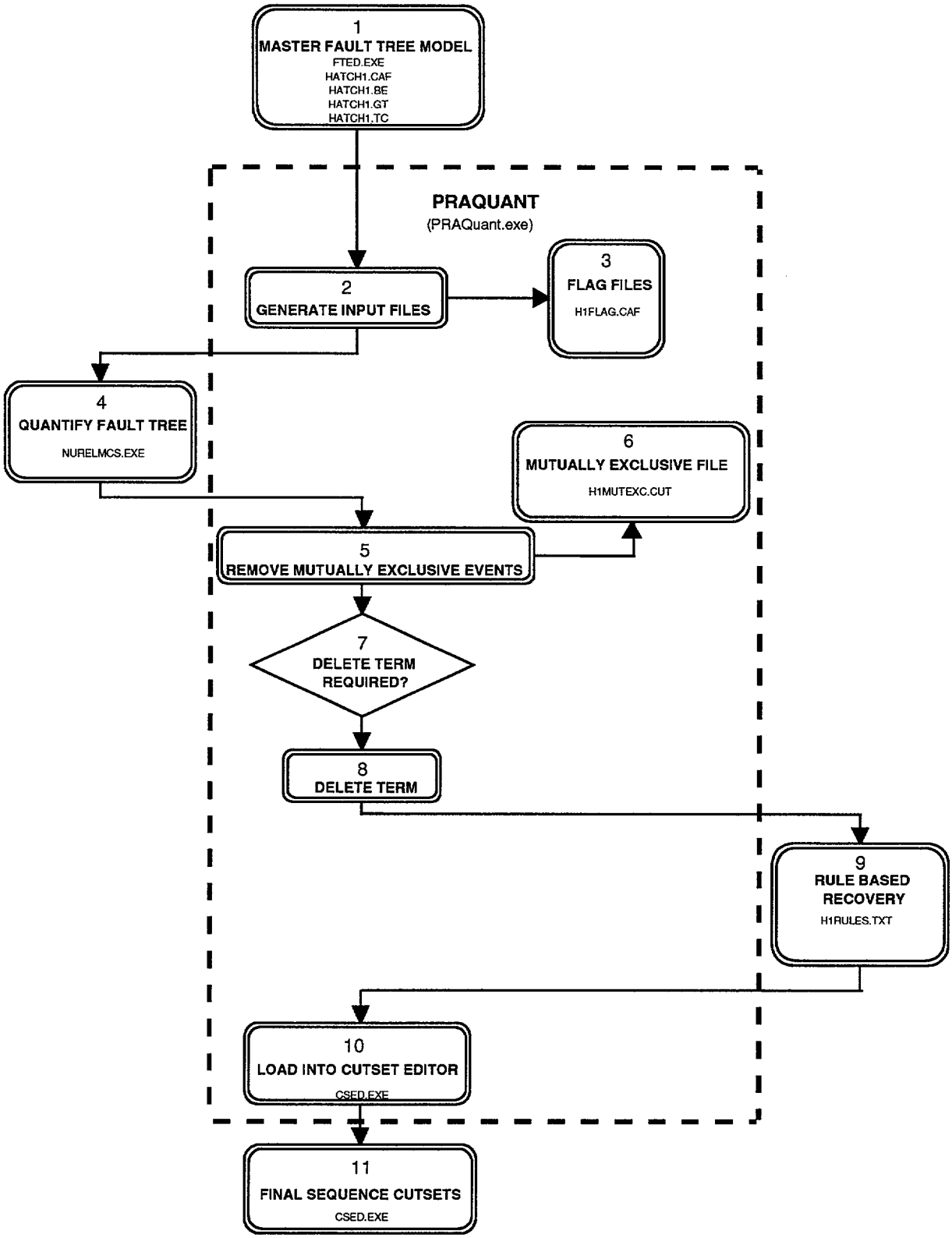


Figure 1.3 Quantification Methodology Overview Using CAFTA Software



2.0 DEVELOPMENT OF ACCIDENT SEQUENCE MODELS

2.1 Fault Tree Model Integration

As discussed in section 1.0, the quantification methodology employed for this project requires that the accident sequence logic, top logic, front-line system logic, and the support system logic fault tree be integrated into a single fault tree model. This process was implemented within the CAFTA software package by way of combining the fault tree models and associated data base into the following computer files:

FILE	PURPOSE
HATCH1.CAF	CAFTA file containing the accident sequence, top logic, front-line system logic and support system logic fault tree models.
HATCH1.GT	CAFTA file containing descriptions of logic gates used in HATCH1.CAF.
HATCH1.BE	CAFTA file containing description and numerical data for basic events used in HATCH1.CAF.
HATCH1.TC	CAFTA file containing component failure rates for basic events used in HATCH1.CAF.

The CAFTA software treats these files as a single fault tree model containing all required logic with associated descriptions and data. A description of how the Hatch Unit 1 fault tree model is developed is provided in this section.

Proper integration of the Hatch Unit 1 fault tree model was ensured by verifying that the appropriate gates were accurately defined at the following interfaces:

(1) Accident sequence fault tree to top logic fault tree.
(2) Accident sequence fault tree to front line system fault tree.
(3) Top logic fault tree to front line system fault tree.
(4) Front-line system fault tree to support system fault tree.

2.2 Accident Sequence Fault Tree Models

The methodology for developing accident sequence fault tree models was discussed in section 1.0. This process requires the identification of top logic fault tree models, and/or front-line fault tree models for each failed branch along the event tree path for a given accident sequence. Table 2.1 contains a summary of fault tree models identified for each accident sequence. The information in Table 2.1 was used to derive the accident sequence fault tree models described in sections 2.2.1 through 2.2.6.

Table (2.1) Fault Tree Models for Failed Event Tree Branches		
Initiator	***Accident Sequence Names***	***Fault Tree Models***
Large LOCAs (IEGALLOCA)	LLOCA_2, LLOCA_3	#LO, #QRQRA
Medium LOCAs (%MLOCA)	MLOCA_2, MLOCA_3, MLOCA_7	#HP-1, #DEHICO1, #LO, #QRQRA
Inadvertent Opening of An SRV (%IORV)	IORV_2, IORV_5, IORV_9, IORV_12, IORV_16	BVA, #PCS, #HP-1, #DEHICO1, #LO, #QRQRA
Transients (IEGGT)	GT_3, GT_4, GT_7, GT_9, GT_14, GT_15, GT_16, GT_18, GT_21, GT_25, GT_27, GT_30, GT_34, GT_36, GT_37, GT_39, GT_42, GT_46	#BVPR, #SORV0, #SORV1, #SORV2, #SORV3, #PCS, #HP-1, #ADED, #RP, #DEHICO1, #LO, #QRIN1REC, #QT, #QR, #QRQRA, #HP-3
Anticipated Transients Without Scram (IEGATWS)	ATWS_3, ATWS_6, ATWS_7, ATWS_10B, ATWS_12, ATWS_19, ATWS_20, ATWS_21, ATWS_24, ATWS_25, ATWS_26, ATWS_29, ATWS_32, ATWS_45, ATWS_46, ATWS_47, ATWS_49, ATWS_50, ATWS_54, ATWS_58, ATWS_59, ATWS_63, ATWS_64, ATWS_102, ATWS_103, ATWS_107, ATWS_108, ATWS_110, ATWS_111, ATWS_112, ATWS_113, ATWS_114, ATWS_115, ATWS_116	#RSCRAM, RPT, #BVPR, #SORV0, #SORV1, #SORV2, #SORV3, #PCS, HPCI-1, #BI, #TINJ, #HR, ADW, #ADEDWS, ADWS, #DEWS, #DE, #LOWS, #QR, #QT
Loss of Offsite Power (%LOSP)	LOSP_2, LOSP_4, LOSP_7, LOSP_9B, LOSP_10A, LOSP_10B, LOSP_11A, LOSP_11B, LOSP_13, LOSP_14, LOSP_18, LOSP_20, LOSP_21, LOSP_25, LOSP_27, LOSP_28, LOSP_30, LOSP_31, LOSP_35	#BVPR, #SORV0, #SORV1, #SORV2, #SORV3, #HP-1, #ADED, #DE, #LO, #QR, #QT, #HP-B (Rev 1 change removed FL-HPI-B-S)

Table (2.1) Fault Tree Models for Failed Event Tree Branches		
Initiator	***Accident Sequence Names***	***Fault Tree Models***
Break Outside Containment and Interfacing System LOCA (%ULFWA, %ULFWB, %ULHPCI, %ULRCIC, %RWCU, %MSL, %VSEQ)	N/A	ULFWA, ULFWB, ULHPCI, ULRCIC, ULRWCU, ULMSL, %VSEQ

2.2.1. Large LOCA Sequences

Sequence Name(s)

LLOCA_2, LLOCA_3

Accident Sequence Logic

LLOCA_2:	IEGALLOCA	#QRQRA
LLOCA_3:	IEGALLOCA	#LO

2.2.2. Medium LOCA Sequences

Sequence Name(s)

MLOCA_2, MLOCA_3, MLOCA_7

Accident Sequence Logic

MLOCA_2:	%MLOCA	#QRQRA	
MLOCA_3:	%MLOCA	#LO	
MLOCA_7:	%MLOCA	#HP-1	#DEHICO1

2.2.3. Inadvertent Opening of an SRV Sequences

Sequence Name(s)

IORV_2, IORV_5, IORV_9, IORV_12, IORV_16

Accident Sequence Logic

IORV_2:	%IORV	#QRQRA		
IORV_5:	%IORV	#PCS	#LO	
IORV_9:	%IORV	#PCS	#HP-1	#DEHICO1
IORV_12:	%IORV	BVA	#LO	
IORV_16:	%IORV	BVA	#HP-1	#DEHICO1

2.2.4 Transient Sequences

Sequence Name(s)

GT_3, GT_4, GT_7, GT_9, GT_14, GT_15, GT_16, GT_18, GT_21, GT_25, GT_27, GT_30, GT_34, GT_36, GT_37, GT_39, GT_42, GT_46

Accident Sequence Logic

GT_3:	#SORV0	#ADED	#QRIN1REC		
GT_4:	#SORV0	#ADED	#LO		
GT_7:	#SORV0	#PCS	#RP	#QRIN1REC	
GT_9:	#SORV0	#PCS	#RP	#LO	#QT
GT_14:	#SORV0	#PCS	#HP-1	#QR	
GT_15 :	#SORV0	#PCS	#HP-1	#LO	
GT_16 :	#SORV0	#PCS	#HP-3	#DEHICO1 (Rev 1 added NOT gate GT-G021)	
GT_18 :	#SORV1	#QRQRA			
GT_21 :	#SORV1	#PCS	#LO		
GT_25 :	#SORV1	#PCS	#HP-3	#DEHICO1	
GT_27 :	#SORV2	#QRQRA			
GT_30 :	#SORV2	#PCS	#LO		

GT_34 : #SORV2 #PCS #HP-3 #DEHICO1

GT_36 : #SORV3 #QRQRA

GT_37 : #SORV3 #LO

GT_39 : #BVPR #QRQRA

GT_42 : #BVPR #PCS #LO

GT_46 : #BVPR #PCS #HP-3 #DEHICO1

2.2.5. ATWS Sequences

Sequence Name(s)

ATWS_3, ATWS_6, ATWS_7, ATWS_10B, ATWS_12, ATWS_19, ATWS_20, ATWS_21, ATWS_24, ATWS_25, ATWS_26, ATWS_29, ATWS_32, ATWS_45, ATWS_46, ATWS_47, ATWS_49, ATWS_50, ATWS_54, ATWS_58, ATWS_59, ATWS_63, ATWS_64, ATWS_102, ATWS_103, ATWS_107, ATWS_108, ATWS_110, ATWS_111, ATWS_112, ATWS_113, ATWS_114, ATWS_115, ATWS_116

Accident Sequence Logic

ATWS_3: #RSCRAM #SORV0 #QR

ATWS_6: #RSCRAM #SORV0 #ADEDWS #LOWS

ATWS_7: #RSCRAM #SORV0 #ADEDWS #DEWS

ATWS_10B: #RSCRAM #SORV0 #PCS #LOWS #QT

ATWS_12: #RSCRAM #SORV0 #PCS #DE #QT

ATWS_19: #RSCRAM #SORV0 #PCS #HR #LOWS

ATWS_20: #RSCRAM #SORV0 #PCS #HR #DE

ATWS_21: #RSCRAM #SORV0 #PCS #HR ADWS

ATWS_24: #RSCRAM #SORV0 #PCS #TINJ #LOWS

ATWS_25: #RSCRAM #SORV0 #PCS #TINJ #DE

ATWS_26: #RSCRAM #SORV0 #PCS #TINJ ADWS

ATWS_29: #RSCRAM #SORV0 #PCS #BI #LOWS

ATWS_32: #RSCRAM #SORV0 #PCS #BI ADWS

ATWS_45: #RSCRAM #SORV0 #PCS HPCI-1 #LOWS

ATWS_46:	#RSCRAM	#SORV0	#PCS	HPCI-1 #DE	
ATWS_47:	#RSCRAM	#SORV0	#PCS	HPCI-1 ADWS	
ATWS_49:	#RSCRAM	#SORV1	#QR		
ATWS_50:	#RSCRAM	#SORV1	#LOWS		
ATWS_54:	#RSCRAM	#SORV1	#ADEDWS	#DEWS	
ATWS_58:	#RSCRAM	#SORV1	#HR	#DE	
ATWS_59:	#RSCRAM	#SORV1	#HR	ADWS	
ATWS_63:	#RSCRAM	#SORV1	#TINJ	#DE	
ATWS_64:	#RSCRAM	#SORV1	#TINJ	ADWS	
ATWS_102:	#RSCRAM	#SORV1	#PCS	#BI	#DE
ATWS_103:	#RSCRAM	#SORV1	#PCS	#BI	ADWS
ATWS_107:	#RSCRAM	#SORV1	#PCS	HPCI-1 #DE	
ATWS_108:	#RSCRAM	#SORV1	#PCS	HPCI-1 ADWS	
ATWS_110:	#RSCRAM	#SORV2	#QR		
ATWS_111:	#RSCRAM	#SORV2	#LOWS		
ATWS_112:	#RSCRAM	#SORV2	#DE		
ATWS_113:	#RSCRAM	#SORV2	ADWS		
ATWS_114:	#RSCRAM	#SORV3			
ATWS_115:	#RSCRAM	#BVPR			
ATWS_116:	#RSCRAM	RPT			

2.2.6. Loss of Offsite Power Sequences

Sequence Name(s)

LOSP_2, LOSP_4, LOSP_7, LOSP_9B, LOSP_10A, LOSP_10B, LOSP_11A, LOSP_11B, LOSP_13, LOSP_14, LOSP_18, LOSP_20, LOSP_21, LOSP_25, LOSP_27, LOSP_28, LOSP_30, LOSP_31, LOSP_35

Accident Sequence Logic

LOSP_2:	%LOSP	#SORV0	#QR	FL_HPI-B-S		
LOSP_4: FL_HPI-S)	%LOSP	#SORV0	#LO	#QT	(Rev1	removed
LOSP_7: FL_HPI-S)	%LOSP	#SORV0	#ADED	#LO	(Rev1	removed
LOSP_9B:	%LOSP	#SORV0	#HP-1	#QR		#HP-B
LOSP_10A: FL_HPI-S)	%LOSP	#SORV0	#HP-1	#LO	(Rev1	removed
LOSP_10B:	%LOSP	#SORV0	#HP-1	#LO		#HP-B
LOSP_11A: FL_HPI-S)	%LOSP	#SORV0	#HP-1	#DE	(Rev1	removed
LOSP_11B:	%LOSP	#SORV0	#HP-1	#DE		#HP-B
LOSP_13:	%LOSP	#SORV1	#QR			
LOSP_14:	%LOSP	#SORV1	#LO			
LOSP_18:	%LOSP	#SORV1	#HP-1	#DE		
LOSP_20:	%LOSP	#SORV2	#QR			
LOSP_21:	%LOSP	#SORV2	#LO			
LOSP_25:	%LOSP	#SORV2	#HP-1	#DE		
LOSP_27:	%LOSP	#SORV3	#QR			
LOSP_28:	%LOSP	#SORV3	#LO			
LOSP_30:	%LOSP	#BVPR#QR				
LOSP_31:	%LOSP	#BVPR#LO				
LOSP_35:	%LOSP	#BVPR#HP-1	#DE			

2.2.7. Break Outside Containment and Interfacing System LOCA Sequences

Sequence Name(s)

ULFWA, ULFWB, ULHPCI, ULRCIC, ULRWCU, ULMSL, %VSEQ

Accident Sequence Logic

ULFWA:	%ULFWA	FWAISO
ULFWB:	%ULFWB	FWBISO
ULHPCI:	%ULHPCI	HPISO
ULRCIC:	%ULRCIC	RCISO
ULRWCU:	%RWCU	RWISO
ULMSL:	%MSL	MSISO
%VSEQ:	%VSEQ	

2.2.8 Development of Core Damage Frequency (CDF) Model

The top gates of the fault tree logic models representing the failed (core damage) branches of the event trees for each of the initiating events considered, as outlined in Table 2.1, were connected under an OR gate named @H1CDFTOP. The gate inputs to @H1CDFTOP, shown below, are comprised of gates representing core damage sequence names defined previously in sections 2.2.1 through 2.2.7 . Quantification of gate @H1CDFTOP yields the total (average) core damage frequency, since the data used for the initiating events in all the fault tree logic models under this gate are expressed in terms of events per year.

Gates Under @CDFTOP	Defined by Sequence Name(s)
@ALLOCA	LLOCA_2, LLOCA_3
@MLOCA	MLOCA_2, MLOCA_3, MLOCA_7
@IORV	IORV_2, IORV_5, IORV_9, IORV_12, IORV_16
@TRANS	GT_3, GT_4, GT_7, GT_9, GT_14, GT_15, GT_16, GT_18, GT_21, GT_25, GT_27, GT_30, GT_34, GT_36, GT_37, GT_39, GT_42, GT_46

@ATWS	ATWS_3, ATWS_6, ATWS_7, ATWS_10B, ATWS_12, ATWS_19, ATWS_20, ATWS_21, ATWS_24, ATWS_25, ATWS_26, ATWS_29, ATWS_32, ATWS_45, ATWS_46, ATWS_47, ATWS_49, ATWS_50, ATWS_54, ATWS_58, ATWS_59, ATWS_63, ATWS_64, ATWS_102, ATWS_103, ATWS_107, ATWS_108, ATWS_110, ATWS_111, ATWS_112, ATWS_113, ATWS_114, ATWS_115, ATWS_116
@LOSP	LOSP_2, LOSP_4, LOSP_7, LOSP_9B, LOSP_10A, LOSP_10B, LOSP_11A, LOSP_11B, LOSP_13, LOSP_14, LOSP_18, LOSP_20, LOSP_21, LOSP_25, LOSP_27, LOSP_28, LOSP_30, LOSP_31, LOSP_35
@ULOCAVSEQ	ULFWA, ULFWB, ULHPCI, ULRCIC, ULRWCU, ULMSL, %VSEQ

2.2.9. Development of Large Early Release Frequency (LERF) Model

In the development of the CAFTA fault tree model, the Large Early Release Frequency model has been completely restructured based on the analysis performed by Fauske and Associates Incorporated (FAI). The following core damage sequences are identified as leading to large early release:

1. Containment Bypass (LER_CB). This involves all break outside containment and interfacing system LOCA sequences.

2. Containment Overpressure Failure (LER_OPD). This involves sequences with vessel injection available, but no containment heat removal. Containment fails due to overpressure prior to or soon after the vessel failure. The containment failure location is either in the drywell or in the wetwell water space.

3. Drywell Venting (LER_VD). This involves sequences with vessel injection, containment heat removal, and wetwell venting unavailable.

4. Containment Overtemperature Failure (LER_OT). This involves sequences with vessel injection, containment heat removal, containment venting, vessel depressurization, and drywell spray unavailable.

The top gates of the fault tree logic models representing the above four types of large early release sequences were connected under an OR gate named @H1LERFTOP. The gate inputs to @H1LERFTOP, shown below, are comprised of gates representing core damage sequences characterized by the function failures defined in the preceding. To make the tree logic evaluation as efficient as possible, failures of functions listed above that are already accounted for in the core damage sequences defined previously are not repeated in the top logic for @H1LERFTOP. Quantification of gate @H1LERFTOP yields the total (average) large early release frequency, since the data used for the initiating events in all the fault tree logic models under this gate are expressed in terms of events per year.

There are four gates under @H1LERFTOP: LER_CB, LER_OPD, LER_VD, and LER_OT.

Gate LER_CB is identical to gate @ULOCAVSEQ defined in Section 2.2.7.

Gate LER_OPD represents containment drywell failure due to overpressure resulting from core damage sequences with vessel injection and no containment heat removal. Basic event CNMT2&3 models drywell failure given containment overpressure failure. In addition to basic event CNMT2&3 two NOT gates are included under LER_OPD. Each describes a SUCCESS path for vessel injection. These items take the place of Mutually Exclusive Events which were made obsolete with Revision 1 to the CAFTA model. The NOT gates are LER-G007 and LER-G008. (Rev 1) Four groups of core damage sequences are included in this end state. The first group includes LLOCA_2, MLOCA_2, IORV_2, GT_3, GT_7, GT_14, GT_18, GT_27, GT_36, GT_39, ATWS_49, ATWS_110, LOSP_2, LOSP_9B, LOSP_13, LOSP_20, LOSP_27, and LOSP_30. In this group of core damage sequences, vessel injection is available and containment heat removal is lost. No additional logic is needed to account for these functional characteristics.

The second group of core damage sequences include ATWS_29, ATWS_32, ATWS_102, ATWS_103, and ATWS_116. For this group of sequences, vessel injection is available. Containment heat removal would be completely lost if the hardened vent fails. As such, gate QV that models failure of the hardened vent is ANDed with these sequences to account for the complete loss of containment heat removal.

The third group of core damage sequences include ATWS_21, ATWS_25, ATWS_26, ATWS_54, ATWS_59, ATWS_63, ATWS_64, ATWS_112, ATWS_113, ATWS_114, and ATWS_115. To account for the total loss of the containment heat removal, this group of sequences is ANDed with both gates QV and CHR. Gate CHR models the containment heat removal including suppression pool cooling and drywell spray.

The fourth group of core damage sequences include ATWS_45, ATWS_46, ATWS_47, ATWS_107, ATWS_108, ATWS_111, ATWS_112, ATWS_113, ATWS_114, and ATWS_115. For this group of sequences, there would be insufficient containment heat removal if boron injection by the standby liquid control system is unavailable. As such, this group of sequences is ANDed with gate #BI.

Gate LER_VD represents drywell venting with both vessel injection and containment heat removal unavailable. However, drywell venting would only be used if the wetwell vent is unavailable. To account for this condition, gate QV-G00MIE (VENT LINE FROM TORUS FAILS) modeling failure of the wetwell venting is ANDed with all of the sequences in this end state. In addition NOT gate VD_G010 is ANDED with the group sequences to account for SUCCESS of drywell venting. This NOT gate accounts for failures which would preclude drywell venting. This NOT gate takes the place of Mutually Exclusive Events that were made obsolete by removal of flag, FL_LER_VD. (Rev 1). There are four groups of sequences in this end state. The first group

includes GT_9 and LOSP_4. Vessel injection and containment heat removal failure are already included as part of the sequence logic for these core damage sequences. As such, no additional logic is needed for these two sequences.

The second group includes LLOCA_3, MLOCA_3, MLOCA_7, IORV_5, IORV_9, IORV_12, IORV_16, GT_4, GT_15, GT_16, GT_21, GT_25, GT_30, GT_34, GT_37, GT_42, GT_46, ATWS_10B, ATWS_12, ATWS_19, ATWS_20, ATWS_24, ATWS_25, ATWS_45, ATWS_46, ATWS_50, ATWS_58, ATWS_107, ATWS_111, LOSP_7, LOSP_10A, LOSP_10B, LOSP_11A, LOSP_11B, LOSP_14, LOSP_18, LOSP_21, LOSP_25, LOSP_28, LOSP_31, and LOSP_35. These sequences are ANDed with gate CHR to account for containment heat removal failure.

The third group of sequences includes ATWS_21, ATWS_26, ATWS_47, ATWS_54, ATWS_59, ATWS_63, ATWS_64, ATWS_108, ATWS_113, and ATWS_114. These sequences are ANDed with gate #LOWS to account for failure of low pressure injection.

The fourth group of sequences includes ATWS_112 and ATWS_115. For these sequences, both gate LER_VD-G064 modeling failure of high pressure injection and gate #LOWS modeling failure of low pressure injection are included in the top logic to account for the unavailability of vessel injection.

High pressure injection (i.e., feedwater or HPCI) is needed for vessel depressurization to allow injection by the low pressure injection systems.

Gate LER_OT represents overtemperature failure of the containment drywell with vessel injection, containment heat removal, containment venting, vessel depressurization, and drywell spray unavailable. To account for the unavailability of the drywell spray, sequences in this end state are ANDed with gate OW. In addition, they are also ANDed with gate QV to account for failure of containment venting. There are four groups of sequences in this end state. The first group includes GT_9 and LOSP_4. These two sequences are ANDed with gate #DE to account for failure of vessel depressurization.

The second group of core damage sequences includes MLOCA_7, IORV_9, IORV_16, GT_15, GT_16, GT_25, GT_34, GT_46, ATWS_12, ATWS_20, ATWS_25, ATWS_46, ATWS_58, ATWS_107, LOSP_11A, LOSP_11B, LOSP_18, LOSP_25, and LOSP_35. These sequences are ANDed with gate CHR to account for loss of containment heat removal.

The third group of sequence includes ATWS_112. This sequence is ANDed with gates #PCS and HPCI-1 to account for the unavailability of vessel depressurization. The fourth group includes ATWS_115. This sequence is also ANDed with gate #DE, in addition to #PCS and HPCI-1, to account for vessel depressurization failure.

2.3 Development of Flag Files

Flag files are CAFTA files that are merged with HATCH1.CAF during the quantification process, to control the configuration of fault tree models. The flag files contain logic flag events which are used to enable or disable portions of the fault tree logic models. They may also include initiating events that are excluded from the accident fault tree models during the quantification process.

The flag files define the status (i.e., True or False) of these events for different groups of sequences during the quantification process. Each line in a flag file contains the event name, a logic gate type (i.e., EQU), and a status identifier (i.e., .T. = TRUE and .F. = FALSE), separated by at least one blank space. The quantification analyst may assign any name to a flag file as long as an extension

".CAF" is included.

Typical entries in a flag file are represented as follows:

Flag Name	Gate	Setting	Description
FL-1T47B007A-R	EQU	.T.	Sets drywell cooler 1T47B007A as RUNNING (In Service) at the start of the event.
FL-1T47B007B-NR	EQU	.F.	Sets drywell cooler 1T47B007B as NOT RUNNING (Standby) at the start of the event.

The flag files may also be in the form of CAFTA logic structure files (i.e., ".CAF" files). Representation identical to the settings in the table above is used in these logic structure files.

For the Hatch Unit 1 model, all of the flag event settings are contained in H1FLAG.CAF

It is important to note that events defined as ***"true"*** or ***"false"*** no longer belong in the fault tree logic, and are deleted by CAFTA. When redefining events *true* and *false*, CAFTA automatically restructures the fault tree logic. If it is desirable to keep the logic intact (i.e., when performing sensitivity on a conditional probability event), the event probability should be set to 1 or 0, corresponding to true and false, respectively. By assigning an event probability as opposed to logical redefinition, the events are retained, and the logic remains intact.

2.4 Development Of Mutually Exclusive Events Files

The mutually exclusive events file, H1MUTEXC.CUT, is a CAFTA cutset file that contains the mutually exclusive events defined by the Accident Sequence and Systems Analysis Task Leaders. These may include all dual-initiator events and combinations of component maintenance events that violate the plant technical specifications. Each cutset in the file contains a set of mutually exclusive events identified by their CAFTA fault tree basic event names.

2.5 Initiating Event Impacts

An essential step in the quantification process is to accurately account for the impact of initiating events in the Hatch Unit 1 fault tree model. For example, a loss of DC power initiating event may cause a reactor scram, fail RCIC, and fail power to DC related equipment. The impact of this initiator is accounted for by inserting this initiating event under fault tree gates that fail DC power and other affected equipment. Table 2.3 contains a summary of logic gates in the Hatch Unit 1 fault tree model that are affected by each initiator.

Table (2.3) SUMMARY OF INITIATING EVENT IMPACT			
Initiator	**Description**	**Quantification**	**Affected Gates in HATCH1.CAF**
%ALOCA	LOCA INITIATING EVENT - SPURIOUS ELECTRICAL SRV ACTUATION AND BLOWDOWN	Data Analysis	CO, CO-1, HP-G012, IEGALLOCA, IEGLOCA, IEGMLOCA, LBL, NOLOPLOPSW
%ATWSFW	ATWS FOLLOWING LOSS OF FEEDWATER EVENT	Data Analysis	(Rev 1 removes FW-G007), IEGATWS-A, IEGLOFW, MC-G008, MC-G022, RPSSIG-G007, (Rev 1 adds FW-G002 and FW-G023)
%ATWSMS	ATWS FOLLOWING MSIV CLOSURE/LOSS OF CONDENSER VACUUM EVENT	Data Analysis	BVPR-G019, FW-MSCVML, IEGATWS-A, MC-G003, RPSSIG-G009
%ATWSTT	ATWS FOLLOWING TURBINE TRIP EVENT	Data Analysis	(Rev 1 removes FW-G007), FWNOLOFW, IEGATWS-A, MC-G008, MC-G022, RPSSIG-G008, (Rev 1 adds FW-G002 and FW-G023)
%IORV	INADVERTENTLY OPENED SRV INITIATING EVENT	Data Analysis	CONOLOFW, CO-SORV, (Rev 1 removes FR-G009 and FW-G004), FWNOLOFW, IEGLOCA, LOCASIG-NOMLBL, MC-G022, NOLOPLOPSW, #SORV1, (Rev 1 adds FW-G083)
%LLOCA	LARGE BREAK LOCA INSIDE DRYWELL INITIATING EVENT	Data Analysis	CO, CO-1, HP-G012, IEGALLOCA, IEGLOCA, IEGMLOCA, JS-G004, JS-G013, JS-G00MDE, JS-G00MMG, LBL, NOLOPLOPSW
%LOCV	LOSS OF CONDENSER VACUUM INITIATING EVENT	Data Analysis	BVPR-G004, BVPR-G022, BVPR-G034, CONOLOFW, FR-G004, FW-MSCVML, IEGGT, MC-G007, MC-G022, NBA-G024, NOLOCLOPLOPSW, NOLOPLOPSW, SORV0-G007, SORV1-G007, SORV2-G007, SORV3-G007, V18
Rev 1 splits %LOFW into two events. %LOFW-FW %LOFW-CO	LOSS OF FEEDWATER INITIATING EVENT (Rev 1 allows for LOFW due to loss of condensate system alone and LOFW due to other faults)	Data Analysis	BVPR-G022, BVPR-G043, (Rev 1 removes FR-G007), IEGGT, IEGLOFW, MC-G022, NBA-G024, NOLOCLOPLOPSW, NOLOPLOPSW, SORV0-G004, SORV1-G004, SORV2-G004, SORV3-G004, V18, (Rev 1 adds %LOFW-FW and %LOFW-CO under SORV0-G042)
%LOSP	LOSS OF OFFSITE POWER INITIATING EVENT	Data Analysis	CONOLOFW, HP-A_START_COND, HP-B_START_COND, NBA-G024, OGA, U2LOSP

Table (2.3) SUMMARY OF INITIATING EVENT IMPACT			
Initiator	**Description**	**Quantification**	**Affected Gates in HATCH1.CAF**
%MLOCA	MEDIUM BREAK LOCA INSIDE DRYWELL INITIATING EVENT	Data Analysis	CO-MLOCA, CONOLOFW, IEGLOCA, IEGMLOCA, MBL, NOLOPLOPSW
%MSIVC	MSIV CLOSURE INITIATING EVENT	Data Analysis	IEGMSIVC, NBA-G024
%SCRAM	REACTOR SCRAM INITIATING EVENT	Data Analysis	IEGSCRAM, NOLOCLOPLOPSW, V18
%SLOCA	SMALL BREAK LOCA INSIDE DRYWELL INITIATING EVENT	Data Analysis	DE-G037, IEGLOCA, IEGSCRAM, LOCASIG-NOMLBL, SMALLLEAK
%TTRIP	TURBINE TRIP INITIATING EVENT	Data Analysis	IEGTTRIP
%ULFWA	FEEDWATER LINE A BREAK INITIATING EVENT	Data Analysis	ULFWA
%ULFWB	FEEDWATER LINE B BREAK INITIATING EVENT	Data Analysis	ULFWB
%ULHPCI	HPCI STEAM LINE BREAK INITIATING EVENT	Data Analysis	ULHPCI
%ULMSL	MAIN STEAM LINE BREAK INITIATING EVENT	Data Analysis	ULMSL
%ULRCIC	RCIC STEAM LINE BREAK INITIATING EVENT	Data Analysis	ULRCIC
%ULRWCU	RWCU LINE BREAK INITIATING EVENT	Data Analysis	ULRWCU
%VSEQ	INTERFACING SYSTEMS LOCA INITIATING EVENT	Data and Special Analysis	LER_CB, @ULOCAVSEQ
&BUSC	TRIP CAUSED BY LOSS OF 600-V BUS C	Fault Tree	AC-1R23S003, FR-G008, FW-MSCVML, IEGSCRAM, L-BC, NOLOCLOPLOPSW, V18
&BUSD	TRIP CAUSED BY LOSS OF 600-V BUS D	Fault Tree	AC-1R23S004, IEGSCRAM, L-BD, NOLOCLOPLOPSW, V18
&DCPAN	LOSS OF DC PANEL R25-S001 INITIATING EVENT	Fault Tree	IEGMSIVC, L-1R25S001, R25S001-G005
&DISCH	PSW DISCH VALVE TRANSFERS CLOSED INITIATING EVENT	Fault Tree	IEGLOPSW, NOLOCLOPLOPSW, PSWDISCHARGE

Table (2.3) SUMMARY OF INITIATING EVENT IMPACT			
Initiator	**Description**	**Quantification**	**Affected Gates in HATCH1.CAF**
&INTAKE	INTAKE STRUCTURE PLUGGING INITIATING EVENT	Fault Tree	COSUP, CO-1SUP, DE-G102-A, HP-G04MCC-1, HP-G04MKC-1, IEGLOPSW, &INTAKE, INTAKESWREC2, L-PS-G125, NOLOCLOPLOPSW, VMDVINTKLOPSW
&LOBUSE	LOSS OF 4KV BUS E INITIATING EVENT	Fault Tree	BE, FR-G008, FW-MSCVML, IEGSCRAM, L-BE, NOLOCLOPLOPSW, V18
&LOBUSF	LOSS OF 4KV BUS F INITIATING EVENT	Fault Tree	BF, IEGSCRAM, L-BF, NOLOCLOPLOPSW, V18
&LOBUSG	LOSS OF 4KV BUS G INITIATING EVENT	Fault Tree	BG, IEGSCRAM, L-BG, NOLOCLOPLOPSW, V18
&LODC	LOSS OF STATION BATTERY A DC POWER INITIATING EVENT	Fault Tree	IEGMSIVC, L-SA, NBA-G024, SA, SA-1, SA-2
&LODWC	LOSS OF DRYWELL COOLING INITIATING EVENT	Fault Tree	IEGSCRAM, NOLOCLOPLOPSW, VC, VCWS, V18-G001
&LOMCHV	LOSS OF MCR COOLING INITIATING EVENT	Fault Tree	IEGMSIVC, NBA-G024, VM-G025, VM-G025-1
&LOPSW	LOSS OF PLANT SERVICE WATER INITIATING EVENT	Fault Tree	G018, IEGLOPSW, U1PSWA, U1PSWA-1, U1PSWB, U1PSWB-1, VMDVINTKLOPSW (Rev 1 removes &LOPSW under DVNOPSWRESTORE, PSW1MISC and PSW2MISC and adds it under G018)
&LOSUTD	LOSS OF STARTUP TRANSFORMER 1D INITIATING EVENT	Fault Tree	IEGTTRIP

2.6 Recovery Actions

The initial accident sequence modeling is *conservative* in that all possible mitigative actions are not credited. Following an initial quantification of the accident sequences, the highest frequency sequences and their associated cutsets are reviewed to determine possible recovery actions. For example, if Loss of Offsite Power sequences are major contributors to the core damage frequency, then the possibility of recovery of offsite power or other mitigative action is considered.

Following identification of the recovery action, its *failure* probability is determined and the accident sequences/cutsets to which the recovery action can be applied identified. This code examines the "raw" cutsets determined by the initial quantification and applies the recovery rules with the result termed the *analysis* cutsets.

3.0 QUANTIFICATION OF ACCIDENT SEQUENCES

As discussed in section 2.0, before the accident sequences were quantified the following files were linked together into the Hatch Unit 1 fault tree model:

- Accident Sequence Logic Files
- Front-Line System Fault Trees.
- Support System Logic Files.

The sequences defined in the Hatch Unit 1 fault tree model were entered into the PRAQUANT file, HATCH1.QNT. The PRAQUANT records contain the failure and success gate names, truncation limit, and flag file associated with the event sequence. These fields link the sequence quantification to the Hatch Unit 1 fault tree model. The input data to HATCH1.QNT are summarized in Table 3.1.

Once the PRAQUANT sequence database is prepared, it is used to quantify the event sequences by performing the following steps:

1. An accident sequence is read from the HATCH1.QNT file.

2. PRAQUANT takes the name given in F-EVENT and/or S-EVENT field and re-defines a new top in the master fault tree with that event name.

3. If a flag file is present, the logic in the flag file is loaded into the master tree and this tree is saved temporarily as a *.FTP file. This is done by loading in flag files, setting flags to true and false, selecting a top event to run, and writing out the file.

4. The cutsets for the accident sequence are then determined.

5. The accident sequence cutsets have the success sequence cutsets deleted.

6. The mutually exclusive events are removed from the remaining accident sequence cutsets. This produces a set of "raw" cutsets. This raw cutset file indicates that cutsets do not reflect any recovery actions.

7. The QRECOVER code is run at this point to apply recovery actions to selected cutsets and convert the raw cutsets to analysis cutsets. This final step writes out the recovered cutset files for the accident sequence.

8. The above steps are repeated for each selected sequence.

9. PRAQUANT returns values for each sequence in the sequence grid as well as the time required for quantification and number of cutsets generated. At this point the user may view the cutset using the *view cutset* option.

Table (3.1) Summary of Accident Sequence Logic Models Used for Quantification		
Failure Logic	**Flag File**	**Success Logic**
LLOCA_2	H1FLAG.CAF	#LO
LLOCA_3	H1FLAG.CAF	
MLOCA_2	H1FLAG.CAF	#HP-1, #LO
MLOCA_3	H1FLAG.CAF	#HP-1
MLOCA_7	H1FLAG.CAF	
IORV_2	H1FLAG.CAF	BVA, #PCS
IORV_5	H1FLAG.CAF	BVA, #HP-1
IORV_9	H1FLAG.CAF	BVA
IORV_12	H1FLAG.CAF	#HP-1
IORV_16	H1FLAG.CAF	
GT_3	H1FLAG.CAF	#BVPR, #PCS, #LO
GT_4	H1FLAG.CAF	#BVPR, #PCS
GT_7	H1FLAG.CAF	#BVPR, #HP-1, #ADED, #LO
GT_9	H1FLAG.CAF	#BVPR, #HP-1, #ADED
GT_14	H1FLAG.CAF	#BVPR, #DEHICO1, #LO
GT_15	H1FLAG.CAF	#BVPR, #DEHICO1
GT_16	H1FLAG.CAF	#BVPR
GT_18	H1FLAG.CAF	#BVPR, #PCS
GT_21	H1FLAG.CAF	#BVPR, #HP-1
GT_25	H1FLAG.CAF	#BVPR
GT_27	H1FLAG.CAF	#BVPR, #PCS
GT_30	H1FLAG.CAF	#BVPR, #HP-1
GT_34	H1FLAG.CAF	#BVPR
GT_36	H1FLAG.CAF	#BVPR, #LO
GT_37	H1FLAG.CAF	#BVPR
GT_39	H1FLAG.CAF	#PCS
GT_42	H1FLAG.CAF	#HP-1
GT_46	H1FLAG.CAF	
ATWS_3	H1FLAG.CAF	RPT, #BVPR, #PCS, #ADEDWS
ATWS_6	H1FLAG.CAF	RPT, #BVPR, #PCS, #DEWS
ATWS_7	H1FLAG.CAF	RPT, #BVPR, #PCS
ATWS_10B	H1FLAG.CAF	RPT, #BVPR, HPCI-1, #BI, #TINJ, #HR, #ADEDWS, #DE
ATWS_12	H1FLAG.CAF	RPT, #BVPR, HPCI-1, #BI, #TINJ, #HR, #ADEDWS
ATWS_19	H1FLAG.CAF	RPT, #BVPR, HPCI-1, #BI, #TINJ, ADWS, #DE
ATWS_20	H1FLAG.CAF	RPT, #BVPR, HPCI-1, #BI, #TINJ, ADWS
ATWS_21	H1FLAG.CAF	RPT, #BVPR, HPCI-1, #BI, #TINJ
ATWS_24	H1FLAG.CAF	RPT, #BVPR, HPCI-1, #BI, ADWS, #DE
ATWS_25	H1FLAG.CAF	RPT, #BVPR, HPCI-1, #BI, ADWS

Table (3.1) Summary of Accident Sequence Logic Models Used for Quantification		
Failure Logic	**Flag File**	**Success Logic**
ATWS_26	H1FLAG.CAF	RPT, #BVPR, HPCI-1, #BI
ATWS_29	H1FLAG.CAF	RPT, #BVPR, HPCI-1, #TINJ, #HR, ADWS, #DE
ATWS_32	H1FLAG.CAF	RPT, #BVPR, HPCI-1, #TINJ, #HR
ATWS_45	H1FLAG.CAF	RPT, #BVPR, ADWS, #DE
ATWS_46	H1FLAG.CAF	RPT, #BVPR, ADWS
ATWS_47	H1FLAG.CAF	RPT, #BVPR
ATWS_49	H1FLAG.CAF	RPT, #BVPR, #PCS, #BI, #TINJ, #HR, #ADEDWS, #LOWS
ATWS_50	H1FLAG.CAF	RPT, #BVPR, #PCS, #BI, #TINJ, #HR, #ADEDWS
ATWS_54	H1FLAG.CAF	RPT, #BVPR, #PCS, #BI, #TINJ, #HR
ATWS_58	H1FLAG.CAF	RPT, #BVPR, #PCS, #BI, #TINJ, ADWS
ATWS_59	H1FLAG.CAF	RPT, #BVPR, #PCS, #BI, #TINJ
ATWS_63	H1FLAG.CAF	RPT, #BVPR, #PCS, #BI, ADWS
ATWS_64	H1FLAG.CAF	RPT, #BVPR, #PCS, #BI
ATWS_102	H1FLAG.CAF	RPT, #BVPR, HPCI-1, ADWS
ATWS_103	H1FLAG.CAF	RPT, #BVPR, HPCI-1
ATWS_107	H1FLAG.CAF	RPT, #BVPR, ADWS
ATWS_108	H1FLAG.CAF	RPT, #BVPR
ATWS_110	H1FLAG.CAF	RPT, #BVPR, ADWS, #DE, #LOWS
ATWS_111	H1FLAG.CAF	RPT, #BVPR, ADWS, #DE
ATWS_112	H1FLAG.CAF	RPT, #BVPR, ADWS
ATWS_113	H1FLAG.CAF	RPT, #BVPR
ATWS_114	H1FLAG.CAF	RPT, #BVPR
ATWS_115	H1FLAG.CAF	RPT
ATWS_116	H1FLAG.CAF	
LOSP_2	H1FLAG.CAF	#BVPR, #HP-1, #ADED, #LO
LOSP_4	H1FLAG.CAF	#BVPR, #HP-1, #ADED
LOSP_7	H1FLAG.CAF	#BVPR, #HP-1
LOSP_9B	H1FLAG.CAF	#BVPR, #DE, #LO
LOSP_10A	H1FLAG.CAF	#BVPR, #DE, #HP-B
LOSP_10B	H1FLAG.CAF	#BVPR, #DE
LOSP_11A	H1FLAG.CAF	#BVPR, #HP-B
LOSP_11B	H1FLAG.CAF	#BVPR
LOSP_13	H1FLAG.CAF	#BVPR, #HP-1, #LO
LOSP_14	H1FLAG.CAF	#BVPR, #HP-1
LOSP_18	H1FLAG.CAF	#BVPR
LOSP_20	H1FLAG.CAF	#BVPR, #HP-1, #LO
LOSP_21	H1FLAG.CAF	#BVPR, #HP-1
LOSP_25	H1FLAG.CAF	#BVPR

Table (3.1) Summary of Accident Sequence Logic Models Used for Quantification		
Failure Logic	**Flag File**	**Success Logic**
LOSP_27	H1FLAG.CAF	#BVPR, #LO
LOSP_28	H1FLAG.CAF	#BVPR
LOSP_30	H1FLAG.CAF	#HP-1, #LO
LOSP_31	H1FLAG.CAF	#HP-1
LOSP_35	H1FLAG.CAF	

For the two categories of quantification results, the contribution of the initiating events to core damage and large early release were ranked according to the Fussel-Vesely Method of determining Basic Event importance.

Table 3.2 displays the Core Damage Contribution by Initiating Event for CDF. The quantification results show that %FL-LODC, %LOSP, and %LOFW-CO are the most important contributors to core damage frequency (i.e., category CDF). The initiating events, %FL-BUSC, %FL-LOPSWand %TTRIP are the next most important contributors to core damage. (Rev 1 changes)

Table 3.3 displays the Large Early Release Contribution by Initiating Event for LERF. The quantification results show that %FL-BUSC, loss of bus C initiating event, %LOSP, loss of offsite power, and %FL-LOPSW, loss of plant service water, are the most important contributors to large early release frequency (i.e., category LERF). The initiating events %SCRAM, Reactor Scram, VSEQ, interfacing systems LOCA, and %FL-LODC, loss of station battery A, are the next most important contributors to large early release. (Rev 1)

Both LERF and CDF were quantified to a cutoff level of 1E-10.

CDF Contribution
Table 3.2

EVENT	%CONTRIBUTION	FREQUENCY	EVENT DESCRIPTION
%FL-LODC	26.3	3.03-06	Loss of Station Battery A
%LOSP	21.2	2.44E-06	Loss of Site Power
%LOFW-CO	9.7	1.12E-06	Loss of Feedwater Due to Loss of Condensate
%FL-BUSC	7.2	8.25E-07	Loss of 600V Bus C
%FL-LOPSW	6.3	7.28E-07	Loss of Plant Service Water
%TTRIP	4.1	4.76E-07	Turbine Trip
%FL-DISCH	2.6	3.01E-07	PSW Discharge Flow Path Failed
%FL-BUSD	2.5	2.87E-07	Loss of 600V Bus D
%SCRAM	2.2	2.55E-07	Reactor Scram
%FL-LOMCHV	2.2	2.5E-07	Loss of Main Control Room Air Conditioning
%IORV	2.0	2.26E-07	Inadvertently Opened SRV
Other Events	13.7	1.58E-06	Other Events
TOTAL	100	1.15E-05	

Large Early Release Fraction (LERF) Contribution
Table 3.3

EVENT	%CONTRIBUTION	FREQUENCY	EVENT DESCRIPTION
%LOSP	64.0	1.28E-06	Loss of Site Power
%FL-BUSC	8.6	1.71E-07	Loss of 600V Bus C
%FL-LOPSW	5.3	1.06E-07	Loss of Plant Service Water
%SCRAM	4.7	9.36E-08	Reactor Scram
%VSEQ	4.2	8.5E-08	Interfacing Systems LOCA
%FL-LODC	3.8	7.69E-08	Loss of Station Battery A
Other Events	9.4	1.87E-07	Other Events
TOTAL	100	2.00E-06	

APPENDIX A - ACCIDENT QUANTIFICATION DEFINITIONS

Accident Sequence Logic - The accident sequence logic is a *fault tree* representation of the accident sequence *event tree* logic.

Failure Logic - The set of failure events (i.e., low pressure injection #LO fails) required for each Accident Sequence (i.e., GT_4). These events are ANDed together in the development of the accident sequence logic for the sequence.

Linked Accident Sequence Model - The linked accident sequence model is a fault tree which contains the accident sequence logic, top logic, the system fault trees, and the modeling automatic merging of multiple fault trees into one integrated fault tree. Further information regarding these links may be found in Reference [2], Section 3.

Modeling Logic Flags - Flags are basic events developed by the quantification analyst and added to the master file. Flag events are used to configure the master file to quantify a specific sequence.

Integrated Fault Tree File - This file represents a single CAFTA tree file which has all of the Accident Sequence Logic, Top Logic, and System Fault Trees loaded into it (usually referred to as the HATCH Unit 1 file for our purposes).

Raw Sequence Cutsets - Raw sequence cutsets represent *all* cutsets output for a given accident sequence from CAFTA. To obtain true cutsets for the sequence, these cutsets require editing to remove mutually exclusive events and/or invalid cutsets.

Reliability Database - This term represents the failure database used by CAFTA to store failure data for components, human failures, and external events/flags. Each database has three associated files; a basic event database (with a .BE extension), which contains hardware failure events, human failure events and modeling/flag events, a failure rate database (with a .TC extension), which contains the failure rates for each hardware failure, and a gate database (with a .GT extension), which contains gate descriptions.

Success Logic - The set of success events required for each accident sequence (i.e., to analyze sequence GT_4, power conversion system #PCS must first be successful).

Top Logic - Top logic represents the intermediate logic required to link the events in the accident sequence event trees with the system fault tree top events.

Attachment 2

Edwin I. Hatch Nuclear Plant
Request to Revise Technical Specifications:
Extension of Completion Times for Inoperable Emergency Diesel Generators

Probabilistic Safety Assessment Peer Certification Comments

Probabilistic Safety Assessment Peer Certification Comments

Attachment 2

Edwin I. Hatch Nuclear Plant
Request to Revise Technical Specifications:
Extension of Completion Times for Inoperable Emergency Diesel Generators

Probabilistic Safety Assessment (PSA) Peer Certification Comments

The E. I. Hatch PSA model has undergone the Probabilistic Risk Assessment (PRA) Peer Review Process used by the Boiling Water Reactor (BWR) Owner's Group. The review team used Revision A-3 Nuclear Energy Institute (NEI) "Probabilistic Risk Assessment (PRA) Peer Review Process Guidance" dated June 2, 2000 as the basis for review. In addition to hosting the industry team performing the review, Southern Nuclear also hosted a 3-member NRC team who observed the entire process during the review week.

Eleven elements were reviewed as per the guidance. Three of these elements received overall grades of 2 with the stipulation that consideration of the facts and observations would make these items fully supportive of grade 3 applications. The remaining eight elements received overall grades of 3. A grade of 3 is considered fully supportive of risk significant determinations including regulatory applications when combined with deterministic insights. The overall assessment for the Hatch Certification is that the PSA can be effectively used to support applications involving absolute risk determination.

One of the elements evaluated as 2 is affiliated with administrative control of the PSA. This is a common issue with the industry because the constant expansion of PSA applications makes administrative procedure update an ongoing issue. This is not considered to have an effect on the proposed Hatch diesel generator (DG) completion time extension.

The second element with a grade of 2 is affiliated with accident sequence descriptions. These comments are being evaluated at present and for the most part have nothing to do with the proposed DG completion time extension. Their overall contribution to the core damage frequency (CDF) and large early release frequency (LERF) values are negligible. There is a comment with regard to binning Level 1 sequences into the Level 2 (LERF) evaluation. This comment seems to be based on an old individual plant examination (IPE) method that included late and intermediate release sequences and such items as explicit high and low pressure sequence categorization. The Hatch model has undergone a revision from Event Tree to Fault Tree modeling since the IPE. The present LERF model which is complete, not a surrogate or temporary device used for one time analysis, is based on a revised Containment Event Tree. It is a conservative model and designed for the LERF case only. Actually, many of the intermediate and some late release states are included in the present LERF categories. The overall arrangement is quite complete and is explained in Attachment 1 to this submittal. It has a degree of conservatism that is based on present engineering calculations, and as a result, is developed with a sound basis.

The final element that received a grade of 2 is related to the Hatch PSA Containment Performance. Hatch has an extensive set of background documentation justifying the modeling used for LERF and the design of the Containment Event Tree. Incorporation of this information into brief summaries for system notebooks has not been done. It is therefore possible that some portions of this documentation may have missed review, although it was introduced as additional volumes of information to the reviewers.

One general comment on the containment model was the lack of interface with the Severe Accident Guidelines (SAGs). This relationship has been evaluated. In brief, the total lack of water to put over the core leads one to the SAGs. The systems addressed for core coverage have already been evaluated by the operator and the PSA prior to SAG implementation. The Hatch PSA does not remodel the systems or apply unique explicit recoveries to these systems once in the containment model. The reason is that there is little information with which to calculate recovery numbers. It is conservative and defendable in these cases to do this because it is in keeping with the continuous flow of the scenario at hand. In other words the scenario does not stop when core damage has occurred and start from time zero once the containment model is entered. There is one system mentioned specifically that is not modeled in the Hatch PSA: injection to the vessel by RHR Service Water. Due to the redundancy of low-pressure injection sources, although proceduralized, the worth of this system in preventing core damage is very small. Consideration of this source for debris coverage provides very little reduction in LERF when considering drywell spray. With the predominate LERF sequences being station blackout (SBO) and loss of offsite power (LOSP), Residual Heat Removal (RHR) Service water will be lost or its use will have to be closely scrutinized to prevent overloading the diesel generators. There is also a very low probability that all other low pressure injection sources will be lost and RHR Service Water will be the only one left. In addition, use of this system is allowed prior to SAG implementation therefore it is not necessarily a SAG issue.

A comment was made that the LERF model does not consider "radionuclide holdup" in the reactor building. A model for this is really a Level III application and Hatch does not have a specific Level III model. SAMA analysis for Hatch License Renewal did model this, but it is not used for Level II work. A single number for "holdup" may be available but its use is certainly left to much scrutiny.

There were comments with regard to where drywell failure occurs within the LERF tree. It is clearly stated in the documentation, both calculational and the IPE work which is still valid for this issue, where drywell failure is modeled to occur, i.e., the drywell head. Other areas are evaluated, along with this area in a fragility analysis, which shows the head closure area to ultimately be the most likely failure area resulting in a Large Early Release.

There were some comments regarding anticipated transient without scram (ATWS) failures and their impact on containment. ATWS is a small fraction of the Hatch CDF and LERF models. It is not significant in comparison to the LOSP and SBO contribution to the LERF overall value. In addition, General Electric has provided new values regarding common cause mechanical and electrical failures of control rods which will tend to drive ATWS to an even lower worth. This general information is presented in NUREG/CR-5500 Volume 3.

Overall each of the three sections discussed are supportive of grade 3 applications when the comments are addressed. The containment performance section is actually the only element that can be considered pertinent out of the three to the proposed application. The general comments have been preliminarily addressed within. The Hatch LERF model and containment model are somewhat conservative, but they are based on detailed calculations and are adequate for use in the proposed DG completion time submittal.