INL/EXT-13-28528

SPAR Model Structural Efficiencies

John Schroeder
Dan Henry
Zhegang Ma

April 2013

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/EXT-13-28528

SPAR Model Structural Efficiencies

John Schroeder
Dan Henry
Zhegang Ma

April 2013

Idaho National Laboratory
Risk Assessment & Management Services (C210)
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Nuclear Regulatory Commission
Washington, DC 20555

(blank page)

(blank page)

ABSTRACT

The Nuclear Regulatory Commission (NRC) and the Electric Power Research Institute (EPRI) are supporting initiatives aimed at improving the quality of probabilistic risk assessments (PRAs). Included in these initiatives are the resolution of key technical issues that are have been judged to have the most significant influence on the baseline core damage frequency of the NRC's Standardized Plant Analysis Risk (SPAR) models and licensee PRA models. Previous work addressed issues associated with support system initiating event analysis and loss of off-site power/station blackout analysis. The key technical issues were:

- Development of a standard methodology and implementation of support system initiating events
- Treatment of loss of offsite power
- Development of standard approach for emergency core cooling following containment failure

Some of the related issues were not fully resolved. This project continues the effort to resolve outstanding issues. The work scope was intended to include substantial collaboration with EPRI; however, EPRI has had other higher priority initiatives to support. Therefore this project has addressed SPAR modeling issues. The issues addressed are

- SPAR model transparency
- Common cause failure modeling deficiencies and approaches
- Ac and dc modeling deficiencies and approaches
- Instrumentation and control system modeling deficiencies and approaches

CONTENTS

FIGURES

TABLES

ACRONYMS

AC	Alternating Current
ADS	Automatic Depressurization System
AFW	Auxiliary Feedwater
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient without SCRAM
BWR	Boiling Water Reactor
CCF	Common Cause Failure
CCW	Component or Closed Cooling Water system
CDF	Core Damage Frequency
CF	Containment Failure
CV	Containment Venting
CWS	Circulating Water System
DC	Direct Current
DIM	Differential Importance Measure
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EE	Extreme Environmental
EPRI	Electric Power Research Institute
EPS	Emergency Power System
ESF	Emergency Safeguards Features
HCTL	Heat Capacity Temperature Limit
HEP	Human Error Probability
HPCI	High Pressure Coolant Injection
HVAC	Heating Ventilation and Cooling
I&C	Instrumentation and Control
INL	Idaho National Laboratory
LERF	Large Early Release Fraction
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LOSW	Loss of Service Water
LPCI	Low Pressure Coolant Injection
MAAP	Modular Accident Analysis Program

ACRONYMS (cont)

MSPI	Mitigating Systems Performance Indicator
NRC	Nuclear Regulatory Commission
PORV	Power Operated Relief Valve
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
RAW	Risk Achievement Worth
RCIC	Reactor Core isolation Cooling
RCS	Reactor Coolant System
RIR	Risk Increase Ratio
RPS	Reactor Protective System
RPV	Reactor Pressure Vessel
SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations
SBO	Station Blackout
SDP	Significance Determination Process
SG	Steam Generator
SORV	Stuck Open Relief Valve
SP	Suppression Pool
SPAR	Standardized Plant Analysis Risk
SSC	Systems, Structures and Components
SSIE	Support System Initiating Event
SWS	Service Water System

SPAR Model Structural Efficiencies

The Nuclear Regulatory Commission (NRC) and the Electric Power Research Institute (EPRI) are supporting initiatives aimed at improving the quality of probabilistic risk assessments (PRAs). Included in these initiatives are the resolution of key technical issues that are have been judged to have the most significant influence on the baseline core damage frequency of the NRC's Standardized Plant Analysis Risk (SPAR) models and licensee PRA models. Previous work addressed issues associated with support system initiating event analysis and loss of off-site power/station blackout analysis. The key technical issues were:

- Development of a standard methodology and implementation of support system initiating events
- Treatment of loss of offsite power
- Development of standard approach for emergency core cooling following containment failure

Some of the related issues were not fully resolved. This project continues the effort to resolve outstanding issues. The work scope was intended to include substantial collaboration with EPRI; however, EPRI has had other higher priority initiatives to support. Therefore this project has addressed SPAR modeling issues. The issues addressed are

- SPAR model transparency
- Common cause failure modeling deficiencies and approaches
- Ac and dc modeling deficiencies and approaches
- Instrumentation and control system modeling deficiencies and approaches

The following sections address these topics.

Table ES-1 summarizes the SPAR model completion status for the major elements addressed above. Specifically, the table shows the status of support system initiating event modeling, intake structure modeling, and enhanced loss of offsite power/station blackout modeling for each existing SPAR model as of April 26, 2013. An X indicates the element is complete. Table endnotes explain partial completion status.

Table ES-1. SPAR Model Completion Status for SSIE and LOOP/SBO Modeling Elements

SPAR	SSIE Enhancement			Intake Structure	Loss of Offsite Power
MODEL	Service Water	Closed Cooling Water	Instrument Air	& Environment	Station Blackout
ABWR-G					X
ABWR-T-SD				X	X
ANO1	X			X	X
ANO2	X	X		X	X
AP10-EE					d., f.
APWR	c.	c.		X	d., f.
ARND-EE	X		a.	X	X
BRF1	b.		c.		X
BRF2	e.			X	d.
BRF3					X
BRU1-SD	c.	a.	a.		d.
BRU2	c.	c.	c.		d.
BRWD	e.	X		X	d., f.
BVS1	X	X	X	X	X
BVS2	X	X	X	X	d.
BYRN	c.	X		X	g.
CALL-EE	c.	X		X	d., f.
CATA	c.	X	X	X	X
CCF1	X	X	X	X	d., f.
CCF2	X	X	X	X	d., f.
CLNT	X		a.	X	d.
COLM-SD					d., f.
COOK	c.	X		X	
COOP					d.
COPK-SD	c.	c.			X
CRYS	X	X		X	X
DAVB-EE-SD	X	X	X	X	X
DCAN	c.	X		X	X
DRES	e.		a.	X	d., f.
FARL	c., e.	c.	a.	X	d., f.
FCAL	c.	c.	c.	X	X
FERM-II					d.
FITZ				X	d., f.

ES-1. (continued)

SPAR	SSIE Enhancement			Intake Structure	Loss of Offsite Power
MODEL	Service Water	Closed Cooling Water	Instrument Air	& Environment	Station Blackout
GGUL-SD					d., f.
GINA	c.	c.	c.	X	d., f.
HARR-EE	c.	c.	c.	X	d., f.
HATC	c., e.		c.	X	X
HOPE	c., e.	c.	c.	X	X
IPT2	c.	c.		X	X
IPT3-EE	c.	c.		X	X
KEWA-EE					X
LIM1-EE	h.	h.	h.	X	d., f.
LIM2-EE	h.	h.	h.	X	d., f.
LSAL				X	d., i.
MCGU					X
MIL2				X	X
MIL3					d., i.
MONT-EE	c.		a.	X	d., i.
NANN	X	X	X	X	d., f.
NMP1	X	X	X	X	d., i.
NM P2				X	X
OCON	X	X	X	X	X
OYST	c., e.		a.	X	d., f.
PALI	X	X		X	X
PBCH	c.	c.	c.	X	
PBT2-EE-L2	X	X	X	X	X
PBT3-EE				X	d., i.
PERY	X		a.	X	d., f.
PILG	c.	c.	c.	X	d., f.
PRAI					X
PVNG					X
QCTY	c.	c.	c.	X	d., f.
RIVB	c.	c.	a.	X	d.
ROBN					d., f.
SALM-EE	c.	c.	c.	X	d., f.
SBRK-SD	c.	c.		X	d., f.
SEQH-L2	c., e.	c., e.			X
SONG-SD					d., f.
STEX				X	f., j.

ES-1. (continued)

SPAR MODEL	SSIE Enhancement			Intake Structure & Environment	Loss of Offsite Power Station Blackout
	Service Water	Closed Cooling Water	Instrument Air		
STL1	X	X	X	X	X
STL2	X	X		X	X
SUMM-EE	c.	c.	c.	X	X
SUR1-EE					d., f.
SUR2-EE	c., e.	c., e.	c.		d., f.
SUS1		X		X	d., i.
SUS2		c.		X	d., i.
TKPT-EE-SD					d., f.
TMI1	c.	c.	c.	X	X
US-EPR					X
VOGT	c.	c.		X	d., f.
VYAN	c., e.			X	d., f.
WBAR	X	X		X	d., f.
WOLF-EE	c.	c.		X	d., f.
WTRF				X	X

a. Event tree but no SSIE fault tree
b. Uses multiplier method
c. SSIE events do not use current CCF calc types (Q type)
d. Does not include consequential LOOP
e. Does not use templates developed on intake structure event tree.
f. Includes switchyard components in fault tree logic
g. Includes non-standard consequential LOOP and switchyard modeling
h. Non-standard methodology
i. Does not include switchyard logic
j. Includes consequential LOOP in fault tree logic (non-standard)

1. Key Technical Issues

The Nuclear Regulatory Commission (NRC) and the Electric Power Research Institute (EPRI) are supporting initiatives aimed at improving the quality of probabilistic risk assessments (PRAs). Included in these initiatives are the resolution of key technical issues that are have been judged to have the most significant influence on the baseline core damage frequency of the NRC's Standardized Plant Analysis Risk (SPAR) models and licensee PRA models. Previous work addressed issues associated with support system initiating event analysis and loss of off-site power/station blackout analysis. The key technical issues were:

- Development of a standard methodology and implementation of support system initiating events
- Treatment of loss of offsite power
- Development of standard approach for emergency core cooling following containment failure

The importance of these technical issues, and the current status of those efforts with respect to the SPAR models, was documented in INL/EXT-10-20739, Resolution of SPAR Model Technical Issues [1]. A summary of the key technical issues and their current status is presented below.

1.1 Implementation of Support System Initiating Events

Support system initiating events (SSIEs) are those component or system failures that both cause a nuclear power plant trip, and affect the ability of the plant protection systems to safely shut down the plant in response to the trip. Probabilistic risk assessments (PRAs) that model the dual nature of SSIEs report a higher component importance for components composing these systems. This is particularly so when using PRA to evaluate the risk significance of equipment failures and other off-normal conditions. PRA models that do not represent the dual nature of SSIEs are under-reporting component importance and possibly plant core damage risk. A further motivation for improving the way SSIEs are treated in PRAs comes from the fact that there has been no complete loss service water (SWS) system and only one potential loss of component cooling water (CCW) recorded in the Nuclear Regulatory Commission's (NRC's) initiating event report [2]. Both CCW and SWS systems are key support systems in most industry PRAs. Therefore, while it is known that SSIEs are rare events, the available data can only provide an upper bound on the occurrence frequency; other methods are required to provide an actual occurrence frequency estimate. Also, the consequences of a total loss of many support systems might be severe, and because of variations in plant design, both the frequency of loss and the consequences resulting from a loss can vary greatly from plant to plant.

1.1.1 Status

The Electric Power Research Institute (EPRI) issued a technical report [3] that established the framework and basic requirements for using fault tree models to predict SSIE frequencies using methods that integrate well with existing probabilistic safety assessment methods and tools. The EPRI report was developed in cooperation with the NRC and with the Idaho National Laboratory, and represents a consensus approach to SSIE modeling. As such, it is intended to serve as a guide to be applied to the development of SSIE models in both industry PRAs, and in development of the NRC Standardized Plant Analysis Risk (SPAR) models.

PRAs that have SSIE models typically use fault trees to determine the initiating event occurrence rate for cooling water systems and for plant air systems. There are two main classes of cooling water systems for which SPAR initiating event fault trees are to be built. They are closed systems, and open systems. Closed systems circulate cooling water in a cooling loop that is not open to the outside environment. These systems are not subject to plugging and fouling to the same extent as systems that circulate untreated water, closed system are expected to have higher component reliabilities and lower system failure rates than open systems. Component reliabilities for closed systems should be calculated from the failure information in the RADs or EPIX systems with good accuracy because of the relatively large number of recorded failure events, and because of the relative similarity of the operating environments from one contributing plant to the next. Open systems are different in that environmental factors are expected to have a large effect on system reliability. A study of the available system failure event records for these systems suggests that it might be reasonable to separate the effects of the environmental factors from the basic component reliability information. INL has made some initial attempts to understand the impact of environmental factors on the open systems. The direction of that effort is summarized in one of the following sections.

The SSIE methodology from the EPRI report has been applied to a number of SPAR models. The resulting SPAR SSIE frequency predictions are typically higher than the corresponding industry estimates, with the results dominated by common cause failure events. This outcome resulted in separate NRC efforts to address potential common cause failure (CCF) data conservatisms, particularly with respect to how CCF failure rate parameters are calculated for components in closed cooling water systems, and in separate efforts to address the impact of environmental affects in the open cooling water systems.

1.1.2 Issue Resolution

With the release of the EPRI guidelines, the SSIE modeling issue is considered resolved. The resolution with respect to SPAR model development is largely a matter of following the EPRI recommendations describing the consensus method for developing SSIE fault trees. The working group did not reach a consensus with respect to three modeling issues: 1) the correct procedures for estimating common cause failure rates, 2) the best procedure for calculating importance measures for events that both create a reactor trip and mitigate it, and 3) the best procedure for capturing the impact of water quality on open cooling water systems. These items were considered beyond the scope of what the working group could accomplish. This section summarizes selected aspects of the methodology described in the EPRI report and briefly summarizes how the SPAR models will address the aforementioned items for which no consensus was achieved.

1.1.2.1 System Failure Occurrence Rate

The possible ways of obtaining system failure occurrence rates for support systems include direct simulation, Markov models, and fault tree methods. Simulation and Markov methods require software that is not currently part of the existing software packages used for industry PRAs or for SPAR model development. Fault tree methods can be integrated into the existing PRAs and SPAR models using the existing software suites (CAFTA, SAPHIRE, etc.). Of the possible SSIE fault tree approaches there are three that either regularly appear in the literature or are used in existing industry PRAs and in the SPAR models. These methods do not have proper names, but can be described as the unavailability method [4, 5], the multiplier method, and the explicit event method. The unavailability method provides the most rigorous approach to the problem, but the existing quantification codes do not, at present, have the algorithms required to determine the system failure rate from a system unavailability model. The last two methods, multiplier and explicit event, are both in common use and each have their advocates in industry. The two methods are roughly equivalent, each with some advantages over the other. The EPRI guidance states the explicit event method is the preferred method of the two, so future SPAR model development will focus on that approach.

Two ways of applying the explicit event method to the SPAR models were tested while developing prototype SPAR models. The first uses a SSIE fault tree to estimate the subject system failure frequency.

The resulting failure frequency is then used as a point estimate input to an existing initiating event. The second option takes the cut sets from the SSIE fault tree, instead of just the estimated failure occurrence rate, and makes them visible in the core damage sequence cut sets. With the first method a reading of the PRA cut sets will show only one event representative of the frequency of the subject system failure. With the second method a reading of the cut sets will show many events contributing to the frequency of system failure. Since the first option represents the least disruption to the structure of existing PRAs and SPAR models, it is the option described here. Note that the SAPHIRE code used for SPAR model development allows the initiating event fault tree to be fully integrated into the model with either option.

1.1.2.2 Importance Measures

The methods required to rank or categorize structures, systems, and components (SSCs) with respect to their risk significance rely on the application of importance measures. One shortcoming specifically related to the modeling of SSIEs is the difficulty of applying the standard importance measures often used in PRA when some components or structures are both initiating and enabling events. Accident sequences are quantified by combining the frequency of the initiating event (typically a yearly frequency) and the conditional probability of the mitigating events (conditional on the occurrence of the initiating event). If a particular event is both an initiating event and a mitigating event there is no established method for manipulating the risk equation to obtain an importance that captures the combined influence of the event on the risk result. The MSPI program guidance provides methods for adjusting importance measures critical to the MSPI program and obtained by conventional methods to account for this circumstance. Application of the MSPI guidance provides a reasonable resolution to this shortcoming. However, the MSPI guidance is not easily implemented in PRA quantification software. Therefore there is reason to continue to research this issue.

A possible method for capturing the combined influence of SSIEs is the application of partial derivatives to the risk equation with respect to the event occurrence rate. The differential importance measure (DIM) [6], in particular, provides an example of an importance measure that can be used for representing SSC importance as a sum of the importances of the associated events. The shortcoming of this method is that importance measures obtained with respect to event occurrence rates are not comparable to importance measures obtained with respect to event probabilities. This is a significant consideration when attempting to use the resulting values for either ranking or categorization of SSCs. However, the resulting importance measures do address the need to estimate changes in the risk result given changes in component reliability.

The DIM and the Birnbaum are both examples of the application of partial derivatives to the risk equation. The DIM is more complicated to compute than the Birnbaum and not in wide use by the US nuclear industry. It is mentioned here because it solves the issue of combining event importance measures to indicate component importance, it allows prediction of changes in the risk result given changes in component reliability, and it has the potential to address the dual influence of SSIEs. It therefore deserves more attention than it has received. However, it suffers the main short-coming of differential methods: the results are dimensionally different for events representing probabilities versus events representing rate parameters. They are therefore not comparable, and therefore not directly useful for component ranking.

Borgonovo and Apostolakis [6] have shown the DIM provides some advantages over the Birnbaum and other local measures. Therefore additional efforts to resolve the importance measure issue should be directed at exploring the application of the DIM to the parameters of risk models that apply SSIE methodology.

1.1.2.3 Intake Structure Modeling and Water Quality

Typically, the intake structure(s) is the source of water for multiple open-loop cooling systems at a plant. In an open loop system, water is drawn from some external raw water source (such as a river, lake, bay, or ocean) via the intake structure, circulated through various heat exchangers for closed loop cooling water systems (such as component cooling water), removing heat from those systems, and then discharging the heated water back into the external raw water source. A plant will typically have multiple open-loop cooling systems including a circulating water system (CWS), which provides cooling for the main condensers, and service water systems (SWS), both essential and non-essential.

There is wide variability in the designs of intake structures and in geographic locations for nuclear power plants (which of course affects the type of environmental events that might pose a hazard to the intake structure). The impact of these variations in designs and location remains to be fully evaluated; one obvious aspect is the susceptibility of a particular site to the various environmental events (e.g., aquatic flora, aquatic fauna, ice, and storm blown debris).

The loss of intake structure model currently under development addresses the situation whereby some environmental material such as aquatic flora, aquatic fauna, ice, debris, etc., accumulates in the openings to the circulating water intake structure resulting degradation of components in the service water system (SWS), possibly leading to a loss of service water. The loss of service water (LOSW) component event tree presented in Figure 1-1 starts with an occurrence of an extreme environmental (EE) event. The system response is then modeled to determine the frequency of failure of pumps, strainers, and heat exchanges in the service water system.

While the quantification of this event tree is still under development, it is expected that the final intake structure model will be very close to Figure 1-1. The key concepts in the application of this intake structure model to a SPAR model is that there are three end states that represent failures of service water pumps, strainers, and heat exchangers, as a result of an environmental event, that may lead to a loss of service water. The three end states represent a contribution to the total failure probability for a particular component in a particular service water system. When these end states are quantified they will be used as template events that specify the environmental event-caused failure rate of the pumps, strainers, and heat exchangers in the target systems. This rate contribution will be treated as additive to the pump, strainer, and heat exchanger failure rates that are already being used in the SPAR models.

1.1.3 SPAR Model Application

Reference 1 discusses several other issues related to SSIE modeling which have not been discussed here. Guidance developed in that effort and within the EPRI working group was applied to a series of SPAR demonstration models. Reference 1 discusses some of the preliminary results of these models. Generally, the calculated system failure rates are plausible. However, the rates are high enough to result in unacceptable core damage frequency predictions at a few plants that have very high conditional core damage probabilities for loss of component cooling water initiating events. The magnitudes of the SSIE rates are largely a result of the calculated common cause failure frequencies for pumps and heat exchangers in these systems. Review of the failure rates and alpha factors in a forthcoming data update to the SPAR models shows that calculated CCF rates are likely to be halved. Therefore the potential for unacceptably high SSIE predictions does not appear to be a problem, particularly if recovery is applied to the dominant CCF rate terms.

Also note that the SSIE frequencies for the modeled open cooling water systems lack intake structure (i.e., environmental impact) development. When the intake structure model is included it is expected that some plants with a history of environmental issues affecting the cooling water intake will see somewhat higher SSIE frequencies. How much higher has not yet been determined.

A final lesson learned from this modeling effort is that highly redundant systems such as the Browns Ferry raw cooling water system are too complicated to model using the preferred explicit event method. In such cases the number of initiating event and enabling event combinations that must be enumerated in the fault tree logic becomes unmanageable and the only workable alternative is to assume that common cause failure will be dominated the more global terms of the basic parameter expansion. It should also be noted that SAPHIRE is limited to six trains when using the internal common cause failure calculator and the SPAR standard template set only includes common cause failure alpha factors for up to 8 trains in a common cause group. These issues point to the need for some additional thinking about how the highly redundant systems should be modeled.

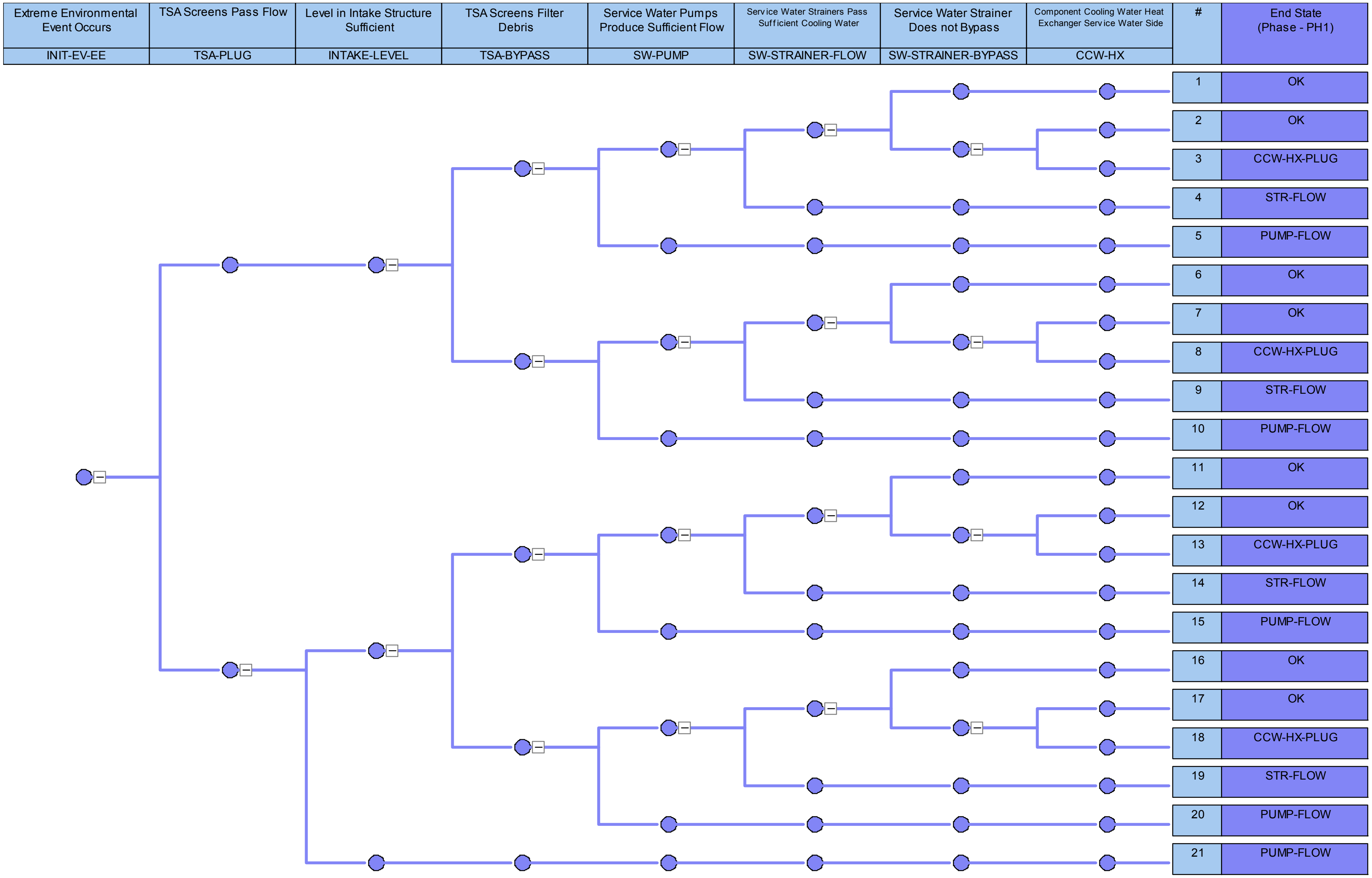


Figure 1-1. Service water system component failure process event tree.

1.2 Development of Loss of Offsite Power

The core damage risk from loss of offsite power (LOOP) and station blackout (SBO) is evaluated in commercial reactor probabilistic risk assessments and in the NRC SPAR models. Often LOOP/SBO is the dominant contributor to the overall core damage frequency (CDF) from internal events occurring while a plant is at power. Specific portions of the LOOP/SBO model that most impact the risk result include the following: initiating event frequency for LOOP, curves for recovery of offsite power (probability versus time), emergency diesel generator (EDG) mission time, convolution of EDG failure and offsite power recovery, and the consequences of battery (dc power) depletion.

The frequency and duration of LOOP used in the SPAR models is provided by NUREG/CR-6890 [7]. Industry appears to hold the view that this data, as it is used in the SPAR models, does not sufficiently capture plant-to-plant variability in LOOP frequency and duration. Conversely, plant-specific data is too sparse to give a reasonably accurate picture of LOOP frequency and duration.

Knowledge of the time to core uncovery during various SBO scenarios is essential to correctly modeling restoration of offsite power. Without detailed thermal hydraulic calculations the SPAR modelers must use conservative assumptions, engineering judgment, or estimates from the licensee PRAs. Licensee models also struggle with these issues. There is considerable variability in the quality and depth of analysis performed in industry PRAs to determine the time available for restoration of offsite power.

In the SPAR models there are three key scenarios for PWRs and two for BWRs. The PWR scenarios are as follows:

- Sequences with failure of secondary side makeup and with the power-operated relief valves (PORVs) lifting only intermittently to relieve pressure and then reseating
- Sequences with secondary side cooling success but with a stuck open PORV
- Sequences with secondary side cooling success but with reactor coolant pump seal leakage

The BWR scenarios are as follows:

- Sequences involving loss of coolant injection with the reactor coolant system bottled up with the exception of the relief valves opening intermittently to relieve pressure
- Sequences involving a stuck open relief valve with only HPCI or RCIC as an injection source

The SPAR models need a consistent basis for assessing the time available for restoration of offsite power under these scenarios, including both consistency from one SPAR model to the next and consistency with best industry practices.

Emergency diesel generator mission time is a modeling issue because there are several approaches used in industry. A simplistic approach to quantifying multiple EDG fail-to-run events in conjunction with failure to recover offsite power may overestimate risk by more than an order of magnitude. What is needed is a standard approach to quantifying these events that is both manageable, reflects a standard PRA mission, and is accurate.

The current SPAR modeling philosophy concerning battery operation during SBO events is to terminate credit for recovery of offsite power upon battery depletion. It is assumed that the plant is unable to recover offsite power in a timely and accurate manner without the use of dc power for breaker alignment and indication. However, many industry PRAs typically allow some credit for such recovery. This difference in assumptions can lead to large differences in core damage frequency predictions, especially for plants with short battery lives (less than three hours).

The optimum strategy for modeling these elements of the risk calculation must remove unnecessary conservatisms and at the same time capture plant-to-plant variability in a consistent way. The need for a uniform approach to these issues has been recognized by industry and resulted in the creation of best-practices document that summarizes the state of the art with respect to these issues. The following summarizes the SPAR model changes that should be made to comply with the industry best practices document.

1.2.1 Issue Resolution

Reference 1 summarizes in more detail the SPAR model changes that are being made to comply with the industry best practices for the following subject areas:

- LOOP Frequency and Duration
- Consequential LOOP
- Multi-Unit Site Considerations
- EDG Recovery Curve
- Convolution and Surrogate EDG Mission Time
- Long-Term SBO Sequences

1.2.2 Summary of SPAR Model Changes

The following SPAR model modifications are recommended and are currently being made to the models. Plants with completed SSIE logic will also have the following modifications

1. The current SPAR composite LOOP event trees are split into separate event trees for each LOOP source:

    - Plant Centered
    - Switchyard Centered
    - Grid Related
    - Weather Related
    - Extreme Weather

    Splitting the event trees allows better initiator-specific modeling of the mitigating actions. In particular, the extreme weather case may have logic more representative of a manual shutdown than of a plant trip. For extreme weather (hurricane) cases the event tree logic should reflect the fact that a manual shutdown is performed as the hurricane approaches the plant. As a result, sequences with SORVs may not be applicable. Offsite power recovery during the 24-hour mission is not considered likely, and the availability of cross-ties on dual unit sites may be affected. These details can best be represented with initiator-specific logic, instead of with flag-sets and averaged values as was done before the initiators were split out.

2. Conditional LOOP logic should be added. For LOOP scenarios that follow LOCA initiators, the LOOP is modeled in the ac power support logic, and as a result, offsite power recovery is not included in the logic. For conditional LOOP scenarios that follow transient initiators, the conditional LOOP is developed in the event tree structure using transfers from each initiating event tree into the average LOOP event tree. As a result, the higher-frequency conditional LOOP contributors include recovery of offsite power logic like any other LOOP initiator. The resulting recovery values are the class-averaged values. Additional research may prove the plant-centered recovery curves a better choice.

3. The best practices document calls for consideration of BWR recirculation pump seal failures (especially for isolation condenser plants) during station blackout events. This consideration also includes potential impacts of containment heatup with respect to forced depressurization. This logic should be added to station blackout logic. Other than SBO scenarios, recirculation pump seal failures are considered as just another contributor to the existing LOCA class frequencies.

4. The LOOP/SBO logic has been expanded to include system failures following recovery of ac power, such that the complete 24-hour mission is represented in the SBO logic, even following recovery of ac power. The SBO logic has also been modified to accommodate long-term considerations, although the default operator HEPs for these actions have been set to TRUE.

5. DC power support system fault tree logic should be split into long-term and short-term failures. The short-term logic may credit both batteries and chargers, or just batteries depending on charger capacity. The long-term logic reflects the requirements of a 24-hour mission and credits only the chargers.

6. A generic SPAR convolution credit has been added to the model. Correction factors are available for up to four fail-to-run events in a single cut set, or one common cause fail-to-run of all trains. Combinations of independent fail-to-run events and common cause failure events in a single cut set have not been addressed.

7. Detailed modeling of switchyard response to plant trips should be added. This is thought especially important for plants that operate with emergency buses normally supplied from the main generator (i.e., require fast bus transfer following trip). At a minimum the modeling includes the SATs/RATs.

1.3 ECCS Injection Following Containment Failure

Many licensee BWR PRAs credit coolant injection following containment venting (CV) and containment failure (CF) caused by the slow over-pressurization of containment resulting from a loss of containment heat removal. The key characteristic of these sequences is the failure of containment (or the venting of containment) before core damage occurs. These sequences often involve a loss of ac power and are sometimes called “core vulnerable” sequences, but are generally known as TW sequences. Although historically the SPAR models have not given credit for injection following containment failure; recently some of the new revisions to the SPAR models include some credit for late (post-CF) injection. Whether or not credit for coolant injection is given post containment failure (or venting) will significantly affect core damage frequency.

There are a number of concerns regarding emergency coolant injection performance during the time leading up to and immediately after containment failure (or venting). These issues are primarily associated with accident sequences that include failure of long term heat removal (TW) or anticipated transients without scram (ATWS) where heat removal is simply inadequate for the heat being generated. The progression of these sequences includes the effects of high pressure inside containment and then the consequences of subsequent containment failure or venting. Specifically, as the containment atmosphere pressurizes, there is the potential that some injection systems might cease working because of increased back pressure on the turbine steam exhaust and/or the automatic depressurization system (ADS) valves being forced closed by the high ambient pressure. Additional concerns arise when the containment fails, or is vented. In this case, there is the potential that the severely adverse environment produced in the reactor building as a result of containment failure (or venting) could fail needed safety equipment. Also, at the time of containment failure (or venting) the rapid depressurization of the suppression pool (SP) water could generate boiling in the SP, and ECCS pumps not designed for two-phase flow could fail.

Each of these mechanisms has the potential to result in failure of some or all coolant injection and hence lead to core damage. These phenomena are identified here as follows:

- High Pressure inside Containment
- Containment Failure or Venting Results in Harsh Reactor Building Environment
- Saturation of Suppression Pool Water
- Rupture of Containment Fails Injection Lines

Each of these issues is discussed in the sections that follow.

An additional issue has received attention in recent years concerns the reliance on containment overpressure when assessing the operability of emergency coolant injection during a postulated design basis accident. Specifically, to support a power uprate application some licensees count on the increased containment pressure to maintain the suppression pool water in a subcooled condition in order to allow emergency coolant injection pumps (i.e., HPCI and RCIC) to continue to operate during a design basis accident. This is a licensing issue that some decision-makers have questioned, as the licensee is counting on one aspect of the severe environment (i.e., increased containment pressure) to overcome the detrimental effects of another aspect of the severe environment (i.e., increased temperature of the suppression pool water). However, this concern is not relevant to assessing the operability of injection after containment failure in the context of PRA, for two reasons. First, most computer codes used in examining potential core damage accidents for PRA applications (i.e., MELCOR, MAAP) attempt to reflect the actual operability requirements and context of the severe accident when assessing the nominal availability of plant systems and components. If the water is subcooled, then it is subcooled, regardless of conditions that produce the subcooling (i.e., any existing containment overpressure condition). Second, the focus of this current discussion is this: what happens once containment fails and the overpressure condition no longer exists.

1.3.1 High Pressure inside Containment

High pressure inside containment can result in closure of the ADS valves. By the time containment pressure has risen to the point when the operability of the ADS is threatened, the primary reactor coolant system (RCS) has already been depressurized by the control room operators. Emergency operating procedures direct the control room operators to depressurize the RCS whenever the suppression pool (SP) has reached the heat capacity temperature limit (HCTL). Operators are also inclined to manually depressurize the RCS when the relief valves are repeatedly cycling open/closed and susceptible to failing and sticking open. Forcing closed the ADS valves would result (assuming the RCS pressure boundary is otherwise intact) in pressurization of the RCS, which would then prevent injection by low pressure injection systems. The ADS valves require pressurized nitrogen to open. If the differential pressure between the ambient environment and the pressurized nitrogen approaches zero the ADS valves will be unable to open, or if already open, will drift closed. The pressurized nitrogen is typically maintained at about 100 psia. Therefore, if the ambient pressure rises to 100 psia, then there is no differential pressure available to operate the valves. A similar issue concerns the operability of steam turbine exhaust discharging to the suppression pool. This affects the operability of HPCI and RCIC pumps. If the pressure raises high enough, the turbines will trip on high exhaust pressure. For RCIC turbines this pressure is relatively low (about 50 psig). For HPCI turbines the trip pressure is relatively high (about 150 psig).

For this issue the key point is: at what pressure will the containment be vented? If the emergency operating procedures specify a pressure that is significantly lower than the pressure at which the ADS valves will close, then the only scenarios for which the re-pressurization of the RCS is a concern, are those in which venting has not occurred. In these cases, where venting does not occur and the containment is threatened by over-pressurization, it is likely that the ADS valves will close and if there is no other breach of the RCS pressure boundary, the RCS will pressurize just before the containment fails.

For the SPAR models, the assumption will be that venting (if it occurs) will be at a pressure low enough that the relief valves remain open (if they were open), and the RCS pressure will remain low (if the RCS had previously been depressurized). If venting does not take place, then containment failure occurs at a pressure high enough such that any open relief valves are forced closed (and all that implies) before containment fails (by whatever failure mechanism).

1.3.2 Reactor Building Environment

The venting of containment via a soft vent path (i.e., not a hard pipe) or containment failure, would likely result in a harsh environment (high temperature steam) in the reactor building. This harsh environment could then result in the failure of equipment (e.g., ECCS pumps) located in the reactor building.

This issue is much less straightforward compared to the other issues, and there are two considerations that must be addressed. The first question is about containment venting. Most BWR containments incorporate a variety of possible venting paths. Some of these are hard-pipe vents and some are basically ventilation system duct-work that would likely rupture if they were used in a containment venting capacity. In addition, these various vent paths span a range of sizes. Obviously, the preferred vent path would be a hard-pipe vent from the suppression pool airspace. However, emergency operating procedures basically direct the control room operators to continue opening additional vent paths until the desired effect (i.e., reduce pressure in containment) has been achieved. This might or might not include soft vent paths, and would definitely be dependent on the details of the severe accident. The second question is on the consequence of containment venting (or containment failure). Given venting by a soft-vent path, or containment failure, what would be the resulting environmental conditions in the reactor building, and more importantly, how would vital safety equipment located in the reactor building be affected.

There are two considerations for evaluating the operability of injection equipment located in a reactor building subject to the severe environment that might result from containment failure or venting. First is the obvious issue of equipment qualification. Potential concerns are typically electrical connections and junction boxes. However, for the steam-turbine driven pumps (i.e., HPCI and RCIC) the other factor to consider is the increased temperature in the reactor building that can result from containment failure or venting can activate a steam line break signal causing an isolation of the steam line to the pump turbine. This isolation typically occurs when the ambient temperature reaches 200oF.

Determining likely containment failure locations (and potential vent paths) relative to the locations of the relevant coolant injection equipment, as well as the configuration of the reactor building (e.g., open stairwells and closed doors) is a very plant-specific process. Therefore, to maintain this issue as tractable the simple assumption is, containment failure from overpressure can result in one of two failure mechanisms. Either the drywell head leaks or the containment wall ruptures. If the drywell head leaks, the harsh environment is produced in the refueling bay and reactor building equipment is nominally available. If the containment wall ruptures, all equipment in the reactor building is assumed to be failed. For containment venting, if a hard-pipe flow path is used, all reactor building equipment is assumed to be nominally available. If a soft path (e.g., HVAC duct work) is used, all reactor building equipment is assumed to be failed.

1.3.3 Saturated Water in Suppression Pool

Overpressure conditions in containment would likely imply (in accident sequences where the core and RPV are still intact) saturated conditions in the suppression pool. Once containment is vented (or failed) the drop in pressure inside containment would produce boiling of the SP water. This could result in the cavitation of any pump taking suction from the SP. Any pump not designed for two-phase flow would probably fail. Some PRAs credit the possibility of the control room operators being able to vent containment in a controlled fashion such that bulk boiling of the SP water is prevented.

For this issue, if the containment is vented or fails, the reduction in pressure (combined with the high temperatures expected at the time) will result in the suppression pool water becoming saturated. Assuming the pumps that are taking suction from the suppression pool are not capable of pumping two-phase water, then they will fail. There are two qualifiers to this scenario: first, it appears that most HPCS pumps are capable of pumping two-phase water (this should be verified). Second, some licensee PRAs postulate that the containment can be vented in a controlled manner such that saturated conditions in the suppression pool can be avoided. However, given that venting the containment in a controlled manner is not something that can be practiced, and is likely to be highly variable and dependent on the specifics of the severe accident, the likelihood of successfully avoiding saturated conditions in the suppression pool would seem to be very low.

For the SPAR models the assumption will be, if the containment fails as a result of overpressure, then the suppression pool is unavailable as a source of water for late injection. If the containment is vented, there is a small chance (10%) that it could be vented in a manner to prevent bulk boiling and maintain sufficient net positive suction head for the pumps taking suction from the suppression pool.

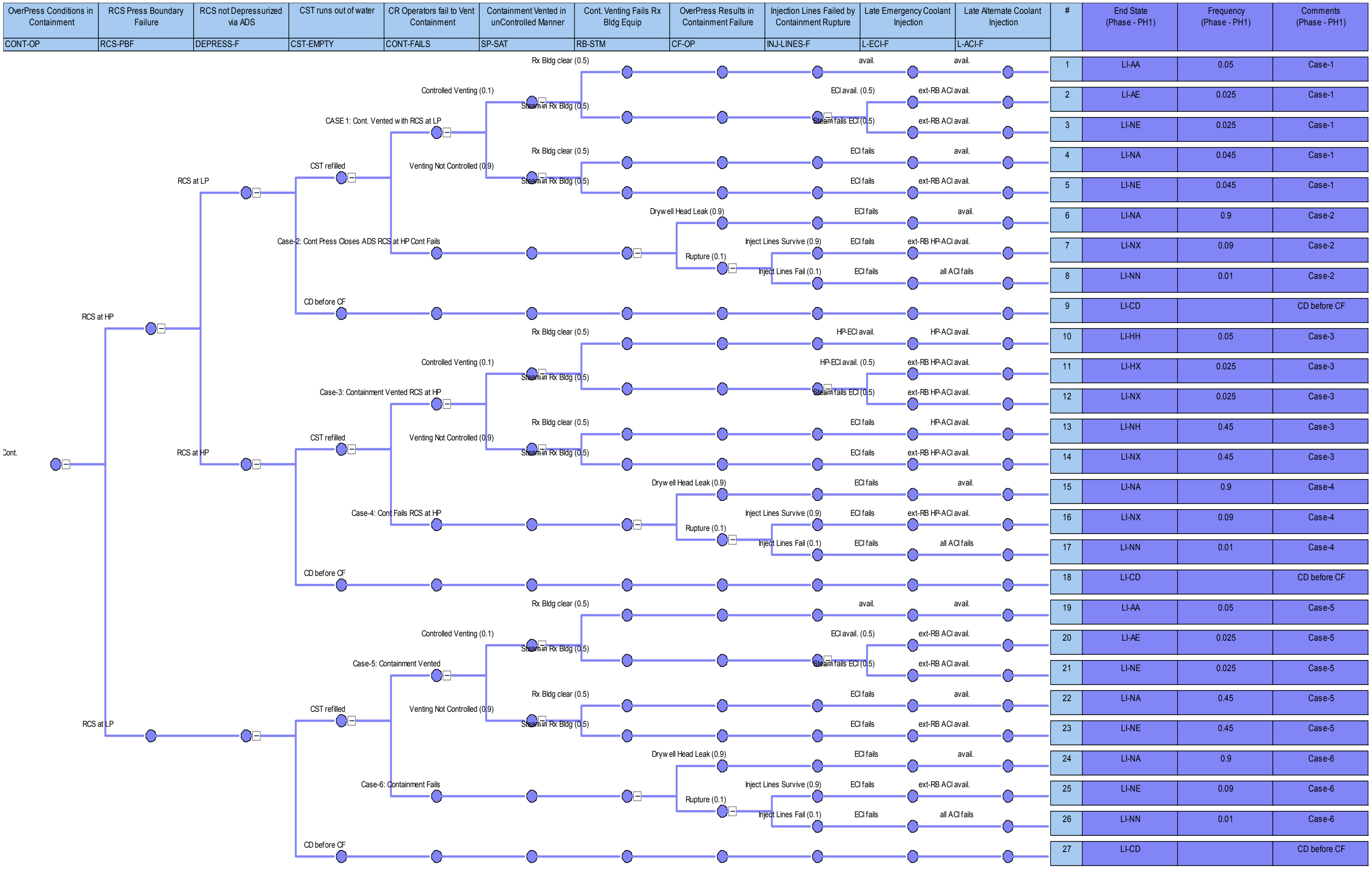
1.3.4 Injection Line Integrity

Catastrophic failure of containment from overpressure can result the failure of injection lines. The concern is that the physical forces on the containment structure caused by the catastrophic overpressure failure can result in the failure of the injection lines that pass through the containment wall. For the SPAR models, two containment failure mechanisms are considered. The drywell head might leak or the containment wall could rupture. If the DW head leaks, no adverse impact is assumed on the injection lines penetrating the containment wall. If the containment ruptures, there is assumed a 50%-50% chance that the physical forces that result will fail the injection lines.

1.3.5 Issue Resolution

Reference 1 presents a modeling framework that accounts for these issues, based upon the event tree depicted in Figure 1- (for BWRs). The first four top events on the CONT-OP event tree delineate the various cases that can occur and basically summarize the relevant characteristics and actions that are currently modeled in the existing level-1 SPAR models. The remaining top events represent modeling that would be new to the SPAR models, and identify the various outcomes for late coolant injection.

This extension of ECCS capability following containment failure should be considered for implementation in the rest of the SPAR models.


OverPress Conditions in Containment
CONT-OP
RCS Press Boundary Failure
RCS-PBF
RCS not Depressurized via ADS
DEPRESS-F
CST runs out of water
CST-EMPTY
CR Operators fail to Vent Containment
CONT-FAILS
Containment Vented in unControlled Manner
SP-SAT
Cont. Venting Fails Rx Bldg Equip
RB-STM
OverPress Results in Containment Failure
CF-OP
Injection Lines Failed by Containment Rupture
INJ-LINES-F
Late Emergency Coolant Injection
L-ECI-F
Late Alternate Coolant Injection
L-ACI-F
Cont.
RCS at HP
RCS at LP
RCS at LP
RCS at HP
CST refilled
CD before CF
CASE 1: Cont. Vented with RCS at LP
Case-2: Cont Press Closes ADS RCS at HP Cont Fails
Case-3: Containment Vented RCS at HP
Case-4: Cont Fails RCS at HP
Case-5: Containment Vented
Case-6: Containment Fails
Controlled Venting (0.1)
Venting Not Controlled (0.9)
Rx Bldg clear (0.5)
Steam in Rx Bldg (0.5)
Drywell Head Leak (0.9)
Rupture (0.1)
Inject Lines Survive (0.9)
Inject Lines Fail (0.1)
avail.
ECI avail. (0.5)
Steam fails ECI (0.5)
ECI fails
HP-ECI avail.
HP-ECI avail. (0.5)
ext-RB ACI avail.
ext-RB HP-ACI avail.
HP-ACI avail.
all ACI fails

#	End State (Phase - PH1)	Frequency (Phase - PH1)	Comments (Phase - PH1)
1	LI-AA	0.05	Case-1
2	LI-AE	0.025	Case-1
3	LI-NE	0.025	Case-1
4	LI-NA	0.045	Case-1
5	LI-NE	0.045	Case-1
6	LI-NA	0.9	Case-2
7	LI-NX	0.09	Case-2
8	LI-NN	0.01	Case-2
9	LI-CD		CD before CF
10	LI-HH	0.05	Case-3
11	LI-HX	0.025	Case-3
12	LI-NX	0.025	Case-3
13	LI-NH	0.45	Case-3
14	LI-NX	0.45	Case-3
15	LI-NA	0.9	Case-4
16	LI-NX	0.09	Case-4
17	LI-NN	0.01	Case-4
18	LI-CD		CD before CF
19	LI-AA	0.05	Case-5
20	LI-AE	0.025	Case-5
21	LI-NE	0.025	Case-5
22	LI-NA	0.45	Case-5
23	LI-NE	0.45	Case-5
24	LI-NA	0.9	Case-6
25	LI-NE	0.09	Case-6
26	LI-NN	0.01	Case-6
27	LI-CD		CD before CF

Figure 1-2. Status of late coolant injection after containment failure or venting.

2. SPAR Modeling Issues

This section discusses additional issues not covered by the major technical issues described in Section 0.

2.1 SPAR MODEL TRANSPARENCY

The goal of this task was to identify and document SPAR model structures that will streamline a typical SPAR model and improve model transparency, and to identify solutions to any asymmetrical modeling issues that might be found. The SPAR models have a diverse community of users within the NRC. While most of these users have been trained in the use of the SAPHIRE code that is the SPAR model database and quantification tool, not all have job responsibilities that allow them to spend substantial time maintaining a familiarity with the models. These infrequent users of the models often have a hard time understanding all the details involved in modification, manipulation, and general use of the models. Therefore it is desirable to make the models as transparent as possible. The transparency issue also involves the SAPHIRE code user interface design, since many SPAR modeling paradigms are a direct consequence of the code capabilities and design. The goal is to make the user community as confident in the results of SPAR model manipulations as possible. The areas with the most influence on this are the verification and validation of the models, documentation of the models, and the use of obscure SAPHIRE capabilities to achieve model quantification.

2.1.1 Verification and Validation

2.1.1.1 Validate the System Models and Success Criteria

The SPAR model documentation is required to reference sources for system success criteria. This is generally done by referencing licensee calculations when they can be obtained. This points to a more general SPAR model development issue: lack of current or complete licensee PRA information. The quality of licensee information varies widely, and in some cases it is completely unavailable. Even when the quality of the licensee information is high, referencing it in the SPAR models leaves the model user often unable to obtain the information needed for a more complete understanding of a system that might be needed during event assessment. Also, relying on plant PRA information alone could lead to the situation where nearly identical plants may have differing success criteria.

Solution: Producing a full suite of support calculations is no doubt beyond the resources available to the SPAR program. However, more confidence could be achieved by performing confirmatory calculations to validate current SPAR model assumptions. The types of calculations could easily be prioritized to identify the areas with significant added value and reduced uncertainty. An example of this type of calculation is the recently completed suite of thermal-hydraulic calculations to confirm the success criteria for plants of the 3-LOOP Westinghouse design. A follow-on task is now performing a similar review of 4-LOOP Westinghouse designs. Confirmatory analyses for additional plant design groups should also be considered.

2.1.1.2 Boundary Conditions

This idea is related to plant alignment issues. Currently alignment issues are modeled either by assuming a preferred alignment or using an average alignment. Neither method is easy to detect, understand, or manipulate in workspaces such as the SAPHIRE SDP workspace. Even the licensees' PRAs often use one of these approaches. The problem for the user community is that event assessments typically require evaluation of an event that occurred in a particular plant alignment that might be significantly different from the assumed alignment. These issues are most likely to occur in support systems such as service water systems, closed cooling water systems, and ac and dc electrical power systems. There is a certain amount of inconsistency across the SPAR models in this regard, largely related to the amount of plant-specific information available at the time the model was built.

Solution: The possible solutions include building in alignment events in a consistent way that represent the probability a system is in a particular alignment, and possibly modifying the analysis workspaces to make identification and manipulation of the alignment events more obvious. Both of these solution options would require significant expenditure of resources.

2.1.1.3 Extended Mission Times

The idea identified here is that the traditional twenty-four hour mission may be insufficient. The ASME requirement for a safe and stable end point is rarely interpreted to mean anything other than a twenty-four hour mission. The Fukushima accidents illustrate that this may not be realistic. For example, it has been estimated that Unit 1core damage occurred within 24 hours, Unit 3 core damage in 48 hours, and Unit 2 beyond 48 hours. This suggests mission times may need to be sequence dependent, which is very hard to achieve in the current SAPHIRE context. To achieve sequence dependent mission times using current SAPHIRE capabilities requires using different basic events in different sequences to represent a particular component and failure model. This is a severe modeling burden because it implies many versions of the same fault tree (e.g., AFW during general transient versus AFW during station blackout). Essentially the same logic would be repeated in many places in the model, making it hard to update and maintain the models. Furthermore, this would make importance measure calculations suspect, since the true component importance for a particular failure mode would then be an aggregate of events occurring in different sequences. SAPHIRE has no mechanism to aggregate the importance measures. Finally, the mission time refinements should be based on thermal hydraulic calculations and there is no reasonable prospect for creating independent models for verification calculations.

Solution: For the reasons given above it is clear that significant challenges exist before this issue can be resolved. This issue deserves further discussion and deliberation.

2.1.1.4 Recovery Event Identification

This idea is with respect to the SDP workspace. It is not easy for a user to tell if a component has an associated recovery event or events. However, this is a general issue that could be improved for the entire SPAR user community.

Solution: Recovery events applied through recovery rules are discussed in Section 2.1.3.3. The suggestion is to provide some color-coding to indicate the application of a rule for transparency purposes. Additionally, it might be beneficial to provide a mechanism within SAPHIRE to tie recovery actions in the model to the basic events or event tree top events to which they are applicable. Providing that graphic connection in appropriate places could improve transparency for the users.

2.1.2 Documentation

Easier, better integrated access to P&IDs, plant information, and SPAR documentation would improve transparency for the user community.

Solution: This would require changes to the SAPHIRE code to provided context-dependent links to available documentation. Such links could be added to both the event tree and fault tree editing modes. An additional facet of this issue could be resolved by automating SPAR model documentation. Much of the SPAR model documentation is common from model to model. Examples of the documentation sections that are common (i.e., boilerplate) include Initiating Event Analysis, Data Analysis, and large portions of other sections. This common information could be located in a single location and accessed by the SAPHIRE code. Model specific portions could be added as appropriate and the entire documentation package could then be generated by SAPHIRE.

2.1.3 Less Visible SAPHIRE capabilities

Some critical capabilities required to implement a state-of-the-practice PRA are not obvious by inspection of the primary model elements; event trees, fault trees, and basic events. These necessary but obscure capabilities are discussed in the following sections.

2.1.3.1 Event Tree Linking Rules

The development of correct event tree sequences has been highly dependent on using a system of rules that operate behind the graphical representation of the event tree sequences, and is mostly independent of the graphical representation. The rules are encoded using a SAPHIRE-specific programming language and the result of rule application is not visible in the event trees used to describe or enumerate the event tree sequences. This has been a frequent source of error in the past. Infrequent SPAR model users sometimes forget about the separation of rules and graphic representation and are sometimes unaware of how to verify the result of an event tree modification or if it is actually being applied as intended.

Solution: SAPHIRE has a relatively new capability that allows the modeler to implement sequence-specific top event substitution directly on the event tree graphic. Most all event tree models were in place before this capability became available. As a result the capability is not used to the extent that it could be. Model transparency would be improved if event tree linkage rules were replaced by graphic representation wherever possible. This feature would also reduce model errors due to conflicting and overlapping rules application. This would require editing nearly all the SPAR model event trees.

2.1.3.2 Flag Set Application

The application of sequence flag sets shares some of the same issues as event tree linking rules. Currently there is no way to make the application of flag sets more obvious. There are two kinds of flag sets: sequence flag sets and fault tree flag sets. The use of flag sets is critical to the use of fault-tree-linked methods that are used in the SPAR models. The alternative is the use of the large event tree/small fault tree models that have largely fallen out of favor in the nuclear industry. The primary function of fault tree and event tree flag sets is to customize system fault trees to the particular circumstance of a particular initiator or place in an event sequence. The most frequent and troublesome application of this is in LOOP/SBO sequence with recovery of ac power. Typically sequence flag sets are used to force the dependency of front line system on emergency diesels. The problem with this is that sequence flag sets apply to the entire sequence and affect all systems in the sequence the same way. That is, if they set a house event to TRUE, they do so for all systems in a particular event sequence. To implement recovery of ac power at some point in the sequence requires the house event is either reset to FALSE, or fault trees are used that don’t have a diesel dependency. The latter is the older large event tree methodology. The former is the SPAR practice. It is implemented using fault tree flags sets as opposed to event tree flag sets. This results in multiple flag sets being in-play at the same time, with sometimes unexpected results. The current methodology of applying flag sets is very hard for an infrequent user of the SPAR models to grasp, and is the source of frequent errors made by model developers.

Solution: There is no simple solution to this problem. PRAs are complex because the nuclear power plants they model are complex in their system relationships and in their response to potential core damage challenges. Experience over the years has shown that capturing the essential nuances with flag sets simplifies model maintenance and modification to such an extent that the difficulty modelers have understanding the flag sets is of secondary importance. However this situation can be improved with a more flexible method of applying both sequence and fault tree flag sets. The details of how such a method might be designed are not clear and could require some research to work out. However, the critical elements of the improved method would be: 1) hierarchical application of both sequence and fault tree flag sets, with a clear way of adjusting the order of application, 2) a clear way of displaying the result of flag set application. There is the potential that the benefit of increasing modeling accuracy may be outweighed by the increase in modeling complexity, though it is not clear that that is the case. To achieve clarity, a completely new and as yet undetermined user interface may be required.

2.1.3.3 Recovery Rules

Recovery rules also operate invisibly, behind the scenes. They are also critical to capturing the complexity of nuclear plant operation. Furthermore, all state of the practice PRA tools have a similar capability that operates in a similar way. Still, there are subtle flaws in the current system. Model users cannot easily determine what has been done by the application of recovery rules. The rules operate, a result is obtained, and there is no report or visible representation of what has been done by rule operations.

Solution: One solution (currently used by CAFTA) is revise the user interface to allow the model user to see the cut sets before rule application, then apply the rules and have SAPHIRE color code the result of rule application prior to making the result permanent. For example, all cut sets or events removed by rule application would be highlighted red, while all events added would be highlighted green. Accepting the result would save the cut sets and clear the highlighting.

Part of the complexity in the recovery rules involves the application of convolution. That subject is addressed in Section 2.1.3.4.

2.1.3.4 Convolution

SPAR models currently have about 1000 rules that operate only to apply convolution corrections to basic events. This method is generally opaque to the casual SPAR model user, and is difficult for any user to follow and validate.

Solution: A new SAPHIRE capability has been developed to calculate convolution integrals internally (calculation type O). The SPAR models should be modified to use this new capability. This will improve model performance and decrease the complexity and obfuscation of the models.

However, to improve the transparency of the model, color-coding techniques as described in Section 2.1.3.3 could also be employed so that it is obvious to the user when cut sets have been modified via convolution.

2.1.3.5 Automated Application of LERF Factors

LERF factors were incorporated into the SPAR models a number of years ago. These factors were manually entered into the SPAR models on an initiator and sequence level. However, conversion of the models from SAPHIRE version 7 to SAPHIRE version 8 resulted in corruption of these factors. These factors can again be manually entered into the models. The problem with this approach is that it is time consuming and that a single modification to the event tree structure necessitates reapplication of the factors to the entire set of sequences. Additionally, if the philosophy behind these LERF factors changes, the entire set of factors would have to be reset manually.

Solution: A relatively simple change can be incorporated into SAPHIRE such that the LERF factors can be automatically applied using a straight forward methodology based on a set of rules. The rules would be readily visible thus facilitating transparency. Consistency in application as well as error checking would also be enhanced with this feature.

2.1.4 Other Prospects for Increasing SPAR Model Transparency, Efficiency, Consistency, Completeness and Ease of Use

- Combining multiple plant models into a single integrated site model. - Due to significant differences between units, several of the multi-unit sites have a SPAR model for each unit. This is problematic in that the impact on the other/opposite unit is not clear and shared dependencies and cross-ties are not evaluated correctly when the models are evaluated independently. Multi-unit sites should be merged into a single model with unit specific event trees so that the shared dependencies can be correctly evaluated.
- Upgrading/updating SPAR model data - A complete SPAR data set is typically generated and incorporated into the SPAR models every couple of years. In addition to updating the existing data, the most recent set of data included many additional data templates and alpha factors for new or reconfigured CCF groups. These new data events have not yet been incorporated into the SPAR models. Additionally, due to the large number of models and the number of analysts working the project, consistency in the data linkage and naming conventions tends to diminish over time. A focused effort to upgrade and standardize the data in the entire set of models is warranted.
- Eliminate/reduce asymmetric modeling (e.g., preferential alignment of swing diesels)
- Implement Global variables
- Improve SAPHIRE capabilities for filtering basic events, event trees, end states, etc.
- Modularize fault trees to minimize the number of times a particular set of logic is replicated in the models.
- More standardized and consistent use of –L, -SBO, etc, top logic.

2.2 COMMON CAUSE FAILURE MODELING

2.2.1 Introduction

Common cause failure modeling has been a part of nuclear plant risk analysis almost since its inception. As the levels of sophistication and detail in PRA models have evolved, so to have CCF methods and applications. A new CCF application has recently been incorporated into the SAPHIRE quantification code.

2.2.2 'R' and 'Q'-Type Common Cause Calculation Types

SAPHIRE was recently enhanced to allow use of additional common cause failure (CCF) modeling options. These options ('R' and 'Q' types) provide automatic generation/application of CCF subgroups as well as expand the maximum group size from six to eight components. Because of the generation of CCF subgroups, the 'R' and 'Q' type CCF calculation are also the cornerstone of future logic that will account for CCF subgroup cross products. Conversion of the existing SPAR model CCF events to 'R' and 'Q' type events is necessary to facilitate the construction of logic to fully account for risk associated with CCF subgroup sets.

2.3 AC AND DC POWER MODELING

2.3.1 Short- and Long-Term DC Power

Power dependencies are a source of opaqueness and confusion in the SPAR models. In particular, the way that short- and long-term DC power dependencies are handled. Generally, the SPAR models include a short-term battery model that does not include backup from the chargers, and a longer-term model that includes charger backup following AC power recovery. The models are identical except for the inclusion of the chargers and AC power dependency.

In addition, there may be inconsistencies in the way that short- and long-term modeling of DC power is handled across the various SPAR models as this modeling has evolved over a number of years.

Solution: A solution would involve a review of DC modeling practices, which could take place as other changes and modifications are implemented. Any inconsistencies can be addressed once the scope of the issue is understood. A change in how best to model the AC dependency would be closely related to the issue discussed in Section 2.1.3.2.

2.3.2 4160V Breaker Control Power

Control power for 4160V breakers is not generally modeled. Control power may be included for diesel generator breakers in some SPAR models, but is not typically included for fast bus transfer, for example. It is not clear how important such control power modeling will be with respect to core damage frequency (CDF) or component importance.

Solution: Incorporate control power for the remaining 4160V breakers.

2.3.3 480V AC Buses

The SPAR models typically do not model power distribution down to the 480V bus level, although most utilities do capture this level of detail.

Although capturing the 480V buses may not have much direct impact on CDF for internal events, it could be much more significant for external event modeling (internal flooding and fires, specifically). It can also be significant during assessment of specific failures.

Solution: Significant effort would be required to perform this level of modeling. The INL currently does not have access to sufficient plant documentation to accomplish this task for all plants, so data gathering would also be required.

2.4 SECONDARY-SIDE COOLING MODELS

2.4.1 Introduction

SPAR models currently include only rudimentary feed/condenser models, focusing primarily on the dump and bypass valves. This lack of detail in these and other balance of plant (BOP) systems limits the range of events where the SPAR models can be used to support risk assessments.

2.4.2 Vogtle Example

For example, the Vogtle SPAR model is typical of the balance of plant/secondary side modeling and includes the following:

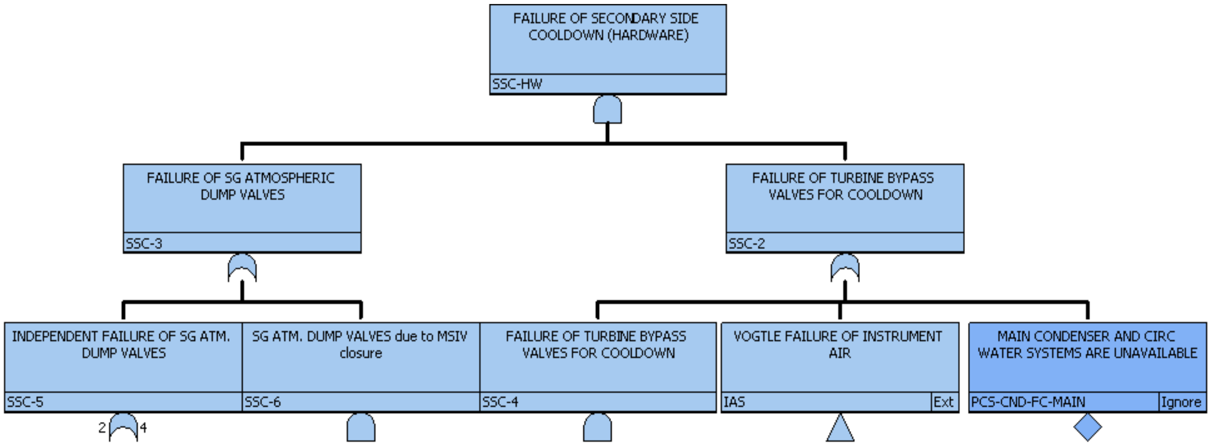

FAILURE OF SECONDARY SIDE COOLDOWN (HARDWARE)
SSC-HW
FAILURE OF SG ATMOSPHERIC DUMP VALVES
SSC-3
FAILURE OF TURBINE BYPASS VALVES FOR COOLDOWN
SSC-2
INDEPENDENT FAILURE OF SG ATM. DUMP VALVES
SSC-5
2
4
SG ATM. DUMP VALVES due to MSIV closure
SSC-6
FAILURE OF TURBINE BYPASS VALVES FOR COOLDOWN
SSC-4
VOGTLE FAILURE OF INSTRUMENT AIR
IAS
Ext
MAIN CONDENSER AND CIRC WATER SYSTEMS ARE UNAVAILABLE
PCS-CND-FC-MAIN
Ignore

Figure 2-1. Vogtle SPAR model for secondary side cooldown.

All cooling water systems are included in the PCSCNDFCMAIN basic event, which is not quantified. In other SPAR models, key equipment and functions such as Main Steam Isolation Valves (MSIVs), circulating water to cool the condensers and turbine control valves may not have more than rudimentary logic or may be missing entirely. Addition of SG isolation valve logic and dependencies is of particular importance to PWR models.

Solution: Expansion of secondary side cooling/balance of plant logic, especially systems associated with heat removal for BWRs and SG isolation logic for PWRs, would yield models that would be useable for a larger set of events requiring risk assessment.

2.5 INSTRUMENTATION AND CONTROL

2.5.1 Introduction

The Standardized Plant Analysis Risk (SPAR) models for the U.S. commercial nuclear power plants currently have very limited instrumentation and control (I&C) modeling. Most of the I&C components in the operating plant SPAR models are related to the reactor protection system. While the recent developed advanced SPAR models for AP1000 and ABWR contain more I&C details and the Integrated Capability Model Project incorporates the Emergency Safeguard Features (ESF) actuation and control system into the Peach Bottom Unit 2 SPAR model [8], an issue was raised on whether it is worth to expend resources for detailed I&C modeling in other numerous SPAR models [9].

I&C system plays a very important role in the operation of a nuclear power plant. Being the nervous system of the plant, I&C system affects every aspects of plant operation with its monitoring, control, and protection functions. It measures plant variables such as neutron flux, temperature, pressure, and level from sensors; processes the acquired data; provides indications and alarms to the operators; and sends signals to controllers, logic circuitries, or actuation systems for actions to keep the plant in a safe condition. I&C system can initiate a reactor scram, actuate systems necessary for emergency core cooling, RCS coolant inventory control, containment isolation and cooling, radioactive release monitoring and control, emergency power, and component cooling. Some examples of important I&C systems in a typical nuclear power plant are as follows:

- reactor protection system
- emergency safeguard features (ESF) actuation and control system
- emergency diesel generator (EDG) control system
- containment isolation control system
- containment atmosphere control system
- neutron monitoring system
- seismic monitoring system
- feedwater control system
- pressure regulator and turbine-generator control
- process computer system

From the Level 1, internal events PRA modeling aspect, there are two I&C systems that are often included in the models as stand-alone systems: Reactor Protection System (RPS) and ESF Actuation and Control System (ESFAS). The function of the RPS is to initiate an automatic reactor shutdown signal when the monitored parameter(s) exceed the associated setpoint(s). The ESFAS automatically actuates various safety systems, based on the detection of abnormal conditions in the nuclear plant, to mitigate accidents and prevent the core from damage. The other I&C functions that are of interest in a Level 1, internal events PRA model are usually included in the associated system logic. For example, the failure of the load sequencer for the emergency diesel generators is included in the EDG fault trees. Since the RPS is currently modeled in each SPAR model and the ESFAS is only modeled in a few SPAR models, the I&C modeling issue is primarily that of adding the ESFAS logic into the remaining SPAR models.

Section 2.5.2 reviews the ASME/ANS PRA Standard requirements for I&C modeling. Section 2.4.3 looks at the importance measures for the I&C basic events in the related SPAR models. Section 2.5.4 reviews licensee PSA information. Section 2.5.5 presents three different approaches to address the I&C modeling issue in SPAR models. Section 2.4.6 provides a summary.

2.5.2 PRA Standard Requirements

I&C system is an important support system in nuclear power plant. The system provides various indications and alarms to the operators for plant conditions, trips the reactor and/or actuates standby cooling systems when abnormal event occurs, and provides permissive and lockout function to prevent important equipment from damage. It may adversely impact multiple mitigating systems due to the common instrument and control equipment or operator action failure. ASME/ANS PRA Standard [10] has specific requirements in System Analysis (SY) Element to collect and review plant instrumentation and control information [SY-A2, SY-A3], consider the failure modes from the I&C [SY-A14], identify and model the systems that are required for initiation and actuation of a system including actuation logic, permissive and lockout signals [SY-A18, SY-B9, SY-B10]. Supporting Requirement (SR) SY-A2, Capability Category I/II/III,

> *COLLECT pertinent information to ensure that the systems analysis appropriately reflects the as-built and as-operated systems. Examples of such information include ... instrumentation and control drawings ...*

SR SY-A3, Capability Category I/II/III,

> *REVIEW plant information sources to define or establish*
>
> ...
>
> *(c) instrumentation and control requirements...*

SR SY-A14, Capability Category I/II/III,

> *When identifying the failures in SY-A11 INCLUDE consideration of all failure modes, consistent with available data and model level of detail except where excluded using the criteria in SY-A15.*
>
> *For example,*
>
> ...
>
> *(m) failure to provide signal/operate (e.g., instrumentation)*
>
> *(n) spurious signal/operation*
>
> *(o) pre-initiator human failure events...*

SR SY-A18, Capability Category I/II/III,

> *INCLUDE in either the system model or accident sequence modeling those conditions that cause the system to isolate or trip, or those conditions that once exceeded cause the system to fail, or SHOW that their exclusion does not impact the results.*
> *For example, conditions that isolate or trip a system include*
> *(a) system-related parameters such as a high temperature within the system*
> *(b) external parameters used to protect the system from other failures [e.g., the high reactor pressure vessel (RPV) water level isolation signal used to prevent water intrusion into the turbines of the RCIC and HPCI pumps of a BWR] ...*
>
> SR SY-B9, Capability Category I/II/III, *When modeling a system, INCLUDE appropriate interfaces with the support systems required for successful operation of the system for a required mission time (see also SY-A6). Examples of support systems include*
> *(a) actuation logic*
> *(b) support systems required for control of components...*

SR SY-B10, Capability Category II/III,

> *MODEL those systems that are required for initiation and actuation of a system. In the model quantification, INCLUDE the presence of the conditions needed for automatic actuation (e.g., low vessel water level). INCLUDE permissive and lockout signals that are required to complete actuation logic.*

From the above PRA Standard requirements, I&C modeling is desirable for a PRA model to reflect the as-built and as-operated plant. The failure modes that may be considered in the modeling include automatic actuation signals, permissive and lockout signals, spurious signals, pre-initiator human failure events such as miscalibrations. On the other hand, an exclusion of the modeling may be justified by showing that it does not impact the results as stated in SR SY-A14 and SY-A18. SR SY-A14 refers SY-A15 for two criteria that may exclude some system unavailability and unreliability contributors (i.e., components and specific failure modes) from the model:

- A component may be excluded from the system model if the total failure probability of the component failure modes resulting in the same effect on system operation is at least two orders of magnitude lower than the highest failure probability of the other components in the same system train that results in the same effect on system operation.
- One or more failure modes for a component may be excluded from the systems model if the contribution of them to the total failure rate or probability is less than 1% of the total failure rate or probability for that component, when their effects on system operation are the same.

2.5.3 I&C Basic Event Importance Measures

2.5.3.1 Previous Study

Reference 9 presents a previous study on the need for more instrumentation events in the SPAR models. The study looked at the risk significance of I&C events in the SPAR models for the AP1000, ABWR, and three commercial operating plants that contain I&C modeling. It uses the US NRC definition of risk significance with a risk increase ratio (RIR), or risk achievement ration (RAW), greater than 2.0. After the risk significant I&C basic events are found out, the “slice” function in SAPHIRE 8 is used to determine the risk contribution of these I&C basic events, which selects the cut sets containing the interested basic events.

- The study finds that for AP1000 and ABWR that use the digital logic models, the risk contribution of the I&C events is about 30% of the total CDF. About 60% of the risk significant I&C events are common cause related such as common cause failure (CCF) of digital input models and CCF of transmitters. The highest RIR is more than 1E5 for ABWR and 1E4 for AP1000.

  For the three commercial operating plants, the study has a much wide range differences on the results.

- Brunswick Unit 1, a BWR, has a risk contribution of approximately 30% from eight risk significant I&C events (2 RPS events, 1 EPS event, and 5 ESFAS events), with two of them are CCFs. The highest RIR is 1E3.
- Arkansas Nuclear One Unit 1 (ANO-1), a PWR from B&W, has a risk contribution of approximately 15% from fifteen risk significant I&C events (5 RPS events, 6 ACP events, and 4 MFW events), with one third of them are CCFs. The highest RIR is 2E2.
- ANO-2, a PWR from CE, has a risk contribution of 2% from four risk significant I&C events, with all of them are CCFs and RPS events. The highest RIR is 2E4.

The wide range differences for the commercial operating plants I&C events importance measures are probably due to the plant specific design, different modeling approaches and data estimations.

2.5.3.2 Peach Bottom Unit 2 SPAR Model I&C Events

One of the tasks in the NRC sponsored SPAR Integrated Capabilities Baseline Model (ICBM) Project was to review the selected SPAR model, i.e., Peach Bottom Unit 2 model (version PBT2-EE-L2-819), and enhance the model as necessary to ensure that it meets the current state-of-the-practice in Level 1 systems modeling. After the reviewing and evaluation, the ESF actuation and control system model was developed and incorporated into the Peach Bottom 2 SPAR model. The task performed the ESF actuation system analysis, developed the ESF fault trees, and revised the supported systems fault trees by including the actuation and control failure modes in the logics [8].The ESF actuation system provides actuation or permissive signals to the following cooling systems: High Pressure Coolant Injection System (HPCI), Reactor Core Isolation Cooling System (RCIC), Automatic Depressurization System (ADS), Low Pressure Coolant Injection System (LPCI), Core Spray System (LPCS), Containment Spray System (CSS), Shutdown Cooling System (SDC), Suppression Pool Cooling System (SPC). The modeled actuation and permissive signals include:

- High Drywell Pressure Signal (HDP)
- Low Reactor Pressure Signal (LRP)
- Low Reactor Water Level Signal (LWL)
- Low-Low Reactor Water Level Signal (LLWL)
- High Reactor Water Level Signal (HWL)
- 2/3 Core Height (Low Shroud) Water Level Signal (SWL)

There are about 120 basic events in the new ESF fault tree and the revised supported systems fault trees (version PBT2-EE-L2-820). 38 of them reside in the core damage cut sets with a cutoff value of 1E-13. Eight ESF events are risk significant, i.e., either with RIR greater than 2.0 or with FV greater than 5E-3, with one of them is CCF. The highest RIR of them is 27 while the highest FV is 1.3E-3. Besides the above new added ESF events, there are five existing RPS events and one EPS/EDG I&C event are risk significant. The RPS event, RPS-SYS-FC-PSOVS, has the highest RIR of 1.7E4 and the highest FV of 3E-2. Table 2-1 lists both the new ESF significant events and the existing RPS and EPS significant events.

Table 2-2 presents the risk contributions from the new ESF events and existing RPS and EPS I&C events, significant or non-significant. The risk contributed from the new ESF events is below 0.5%. The risk contribution from the RPS events is about 4%.

Table 2-1. ESF, RPS, and EPS Significant Events in Peach Bottom Unit 2 (PBT2) SPAR Model

I&C Event	Name	Count	Prob	FV	RIR	RRR	Birnbaum	RII	RRI	Uncertainty	Description
8 New ESF Significant Events	ESF-ASP-FC-PT404B	53	9.60E-05	1.63E-04	2.69E+00	1.00E+00	4.19E-06	4.19E-06	4.02E-10	9.93E-10	PRESSURE TRANSMITTER PT-404B FAILS TO OPERATE
	ESF-ASP-FC-PT404D	46	9.60E-05	1.61E-04	2.68E+00	1.00E+00	4.15E-06	4.15E-06	3.99E-10	9.84E-10	PRESSURE TRANSMITTER PT-404D FAILS TO OPERATE
	ESF-PLL-FC-LCS2	173	6.00E-04	1.01E-03	2.68E+00	1.00E+00	4.17E-06	4.17E-06	2.50E-09	3.54E-09	RELAY LOGIC FOR LPCS DIV II FAILS TO OPERATE
	ESF-PLP-FC-PT404B	86	1.50E-04	2.56E-04	2.70E+00	1.00E+00	4.22E-06	4.22E-06	6.33E-10	8.95E-10	PROCESS LOGIC FOR PT-404B FAILS TO OPERATE
	ESF-PLP-FC-PT404D	73	1.50E-04	2.53E-04	2.69E+00	1.00E+00	4.17E-06	4.17E-06	6.26E-10	8.86E-10	PROCESS LOGIC FOR PT-404D FAILS TO OPERATE
	ESF-XHE-MC-LRPALL	305	5.00E-05	1.31E-03	2.71E+01	1.00E+00	6.47E-05	6.47E-05	3.24E-09	4.58E-09	OPERATOR MISCALIBRATION OF ALL LOW RX PRESSURE SENSORS
	ESF-XHE-MC-LRPB	31	1.00E-04	1.66E-04	2.66E+00	1.00E+00	4.10E-06	4.10E-06	4.10E-10	5.80E-10	OPERATOR MISCALIBRATION OF LOW RX PRESSURE SENSOR CHANNEL B
	ESF-XHE-MC-LRPD	31	1.00E-04	1.66E-04	2.66E+00	1.00E+00	4.10E-06	4.10E-06	4.10E-10	5.80E-10	OPERATOR MISCALIBRATION OF LOW RX PRESSURE SENSOR CHANNEL D
1 Existing EPS Significant Event	EPS-SEQ-CF-DGNS	148	1.67E-05	1.59E-04	1.06E+01	1.00E+00	2.37E-05	2.37E-05	3.95E-10	5.93E-10	DG LOAD SEQUENCERS FAIL FROM COMMON CAUSE
5 Existing RPS Significant Events	RPS-SYS-FC-ELECT	30	3.80E-06	9.27E-05	2.54E+01	1.00E+00	6.04E-05	6.04E-05	2.30E-10	3.25E-10	TRIP SYSTEM ELECTRICAL FAILURES
	RPS-SYS-FC-HCU	178	1.10E-07	1.91E-03	1.70E+04	1.00E+00	4.22E-02	4.22E-02	4.72E-09	2.39E-08	HCU COMPONENTS FAIL
	RPS-SYS-FC-MECH	245	2.50E-07	4.34E-03	1.70E+04	1.00E+00	4.22E-02	4.22E-02	1.07E-08	1.04E-07	CONTROL ROD DRIVE MECHANICAL FAILURE
	RPS-SYS-FC-PSOVS	382	1.70E-06	2.95E-02	1.71E+04	1.03E+00	4.22E-02	4.22E-02	7.31E-08	4.25E-06	HCU SCRAM PILOT SOVS FAIL
	RPS-SYS-FC-RELAY	258	3.80E-07	6.60E-03	1.70E+04	1.01E+00	4.22E-02	4.22E-02	1.63E-08	4.91E-07	TRIP SYSTEM RELAYS FAIL

Table 2-2. Risk Contributions from ESF, RPS, and EPS I&C Events in PBT2 SPAR Model

I&C Event		Total	Reside in CDF Cut sets	Risk Significant
ESF Events	Basic Events	120	38	8
	"Sliced" CDF		8.98E-09	8.62E-09
	% of Total CDF		0.36%	0.35%
RPS Events	Basic Events	6	6	5
	"Sliced" CDF		1.05E-07	1.05E-07
	% of Total CDF		4.23%	4.23%
EPS Load Sequencer Events	Basic Events	5	5	1
	"Sliced" CDF		2.70E-09	3.95E-10
	% of Total CDF		0.11%	0.02%

On the other hand, in the old SPAR model without the ESFAS, the failure of operator actions to start and control cooling systems, such as High Pressure Coolant Injection (HPCI), will fail the system/function directly. In reality, these operator actions are actually backups to the automated signals. With the incorporation of ESFAS into the SPAR model, the operator actions are ANDed with the ESF automatic actuation signals correspondingly, and the importance of the associated human failure events will be reduced significantly. This can be verified from the RIR reductions results as shown in the following table. The importance for the action to start low pressure injection (LPI-XHE-XM-ERROR) is reduced from a high RIR of 591 to a non-significance of 1.6. The importance for operator action to start high pressure injection (HPI-XHE-XO-ERROR) has also reduced from a high RIR of 176 to 3.0. Table 2-3 displays the risk reduction in operator action events after the ESFAS system was incorporated into the Peach Bottom Unit 2 SPAR model.

Table 2-3. Risk Reductions in Operator Action Events after ESF Incorporation in PBT2 SPAR Model

Name	RIR			Description
	Without ESF Modeling(PBT 2-EE-L2-819)	With ESF Incorporated (PBT2-EE-L2-820)	RIR Change	
HCI-XHE-XO-ERROR	10.4	3.0	-71%	OPERATOR FAILS TO START/CONTROL HPCI INJECTION
HPI-XHE-XO-ERROR	176	3.0	-98%	OPERATOR FAILS TO START/CONTROL HIGH PRESSURE INJECTION
LPI-XHE-XM-ERROR	591	1.6	-100%	OPERATOR FAILS TO START/CONTROL LOW PRESSURE INJECTION
RCI-XHE-XO-ERROR	32.5	1.0	-97%	OPERATOR FAILS TO START/CONTROL RCIC INJECTION
RHR-XHE-XM-ERROR	90.4	78.7	-13%	OPERATOR FAILS TO START/CONTROL RHR

2.5.4 Licensee PSA Information

During the course of performing model updates on the SPAR models, INL has collected basic event importance measures for all the plants for which SPAR models exist. These importance measures were combined in a spreadsheet, PSASummary.xlsb, and reviewed for I&C events that are modeled in the PSA risk models. The spreadsheet includes the basic events database (BED) for 72 PSA models that represents 95 out of the 104 operating reactors. The review used keywords such as “transmitter,” “sensor,” “logic,” “miscalibration,” and “switch” to search for I&C basic events. The search found that all the 72 PSA models have included I&C events in them, but with big differences on the level of details. While all 72 models contain independent failures for single I&C component such as transmitter / sensor, logic circuit /logic relay / logic card, pressure / temperature / level / flow switch, only 25 of them contain the common cause failures of the I&C components. 59 of them include the miscalibration of I&C components. There are 11 PSA models that have more than 100 I&C basic events in the BED database, and 9 models that have fewer than 20 I&C basic events. Four PSA models (Davis-Besse, Limerick 1, Limerick 2, and Palisades) have the highest level of details on I&C modeling with about 400 I&C basic events in each of them. Table 2-4 shows the summary of the I&C events that are modeled in licensee PSA models.

Table 2-4. I&C Events Modeled in Licensee PSA Models

Total PSA Models	Contain Single I&C Component Failure	Contain Common Cause I&C Component Failure	Contain I&C Miscalibration Failure	I&C Events > 100	I&C Events < 20
72	72	25	59	11	9

It should be noted that the PSA Summary spreadsheet does not represent the latest information from the licensee PSA models as the licensees update their models from time to time and the SPAR model data library is only infrequently updated. Especially with the issuances of RG 1.200, the ASME/ANS PRA Standard, and the PRA peer review, the licensee PSA models have been, or are, upgraded as a whole in order to meet the PRA Standard Category Capability II requirements (refer to Section 2.5.2 for the modeling requirements on I&C).

2.5.5 Different Approaches on I&C Modeling

Three different approaches for addressing the I&C modeling issue in the current SPAR models are described in the following sections.

2.5.5.1 Detailed I&C Modeling

This approach is to develop plant-specific ESF Actuation System models and integrate them into the corresponding SPAR models for those SPAR models that have no detailed I&C modeling, as did for Peach Bottom Unit 2 SPAR Model in the SPAR ICBM Project [8]. Figure 2-2 displays an example of ESF fault tree for failure of LPCI actuation in the new Peach Bottom Unit 2 SPAR model. The fault tree includes the failure of various actuation signals to LPCI, the operator backup manual actuation, and the dependency on the DC power. Figure 2-3 shows the incorporation of the I&C modeling into the supported system, LPCI, fault tree. Gate LCI-A-6, Failure of LPCI Actuation or Low Reactor Pressure Permissive, is added to the LPCI Loop A failure logic under Gate LCI-A-2. The new Gate will transfer to the ESF fault trees ESF-LCI for failure of LPCI actuation as in Figure 2-2, and ESF-LCI-LRP for failure to generate a low reactor pressure signals to LPCI.

This approach would completely resolve the I&C issue in the SPAR models. The new SPAR models would represent the as-designed, as-operated plants with high level of detail in each model. The approach allows for representation of all dependencies between the I&C system and other systems to be explicitly modeled and accounted for. However, this approach also has extensive resources requirements and a longer timeline to accomplish. Also, the level of detail may not be possible to support using available documentation, and may be inconsistent with the SPAR modeling philosophy in other areas of the model.

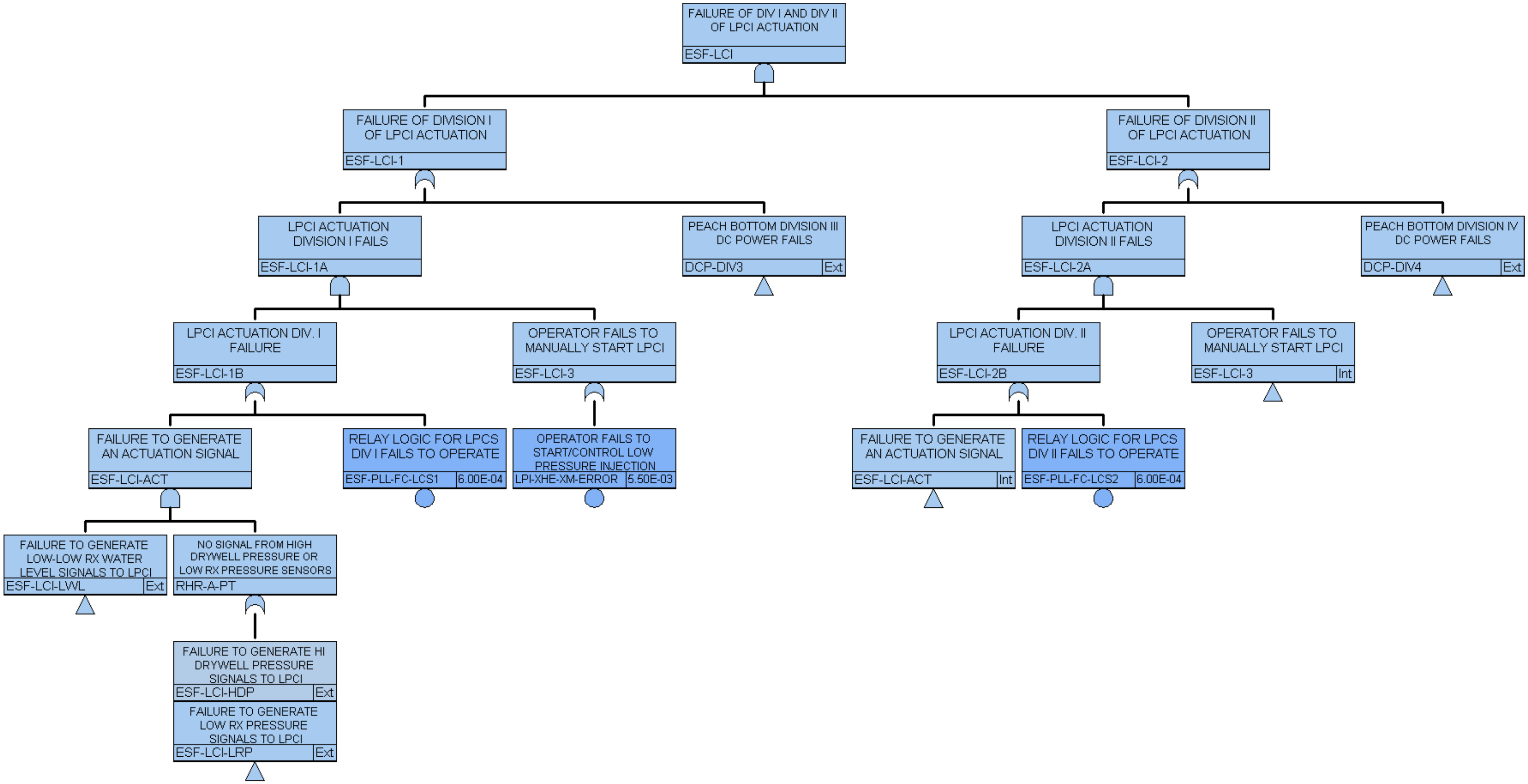

FAILURE OF DIV I AND DIV II OF LPCI ACTUATION
ESF-LCI
FAILURE OF DIVISION I OF LPCI ACTUATION
ESF-LCI-1
FAILURE OF DIVISION II OF LPCI ACTUATION
ESF-LCI-2
LPCI ACTUATION DIVISION I FAILS
ESF-LCI-1A
PEACH BOTTOM DIVISION III DC POWER FAILS
DCP-DIV3
Ext
LPCI ACTUATION DIVISION II FAILS
ESF-LCI-2A
PEACH BOTTOM DIVISION IV DC POWER FAILS
DCP-DIV4
Ext
LPCI ACTUATION DIV. I FAILURE
ESF-LCI-1B
OPERATOR FAILS TO MANUALLY START LPCI
ESF-LCI-3
LPCI ACTUATION DIV. II FAILURE
ESF-LCI-2B
OPERATOR FAILS TO MANUALLY START LPCI
ESF-LCI-3
Int
FAILURE TO GENERATE AN ACTUATION SIGNAL
ESF-LCI-ACT
RELAY LOGIC FOR LPCS DIV I FAILS TO OPERATE
ESF-PLL-FC-LCS1
6.00E-04
OPERATOR FAILS TO START/CONTROL LOW PRESSURE INJECTION
LPI-XHE-XM-ERROR
5.50E-03
FAILURE TO GENERATE AN ACTUATION SIGNAL
ESF-LCI-ACT
Int
RELAY LOGIC FOR LPCS DIV II FAILS TO OPERATE
ESF-PLL-FC-LCS2
6.00E-04
FAILURE TO GENERATE LOW-LOW RX WATER LEVEL SIGNALS TO LPCI
ESF-LCI-LWL
Ext
NO SIGNAL FROM HIGH DRYWELL PRESSURE OR LOW RX PRESSURE SENSORS
RHR-A-PT
FAILURE TO GENERATE HI DRYWELL PRESSURE SIGNALS TO LPCI
ESF-LCI-HDP
Ext
FAILURE TO GENERATE LOW RX PRESSURE SIGNALS TO LPCI
ESF-LCI-LRP
Ext

Figure 2-2. Failure of LPCI Actuation Fault Tree

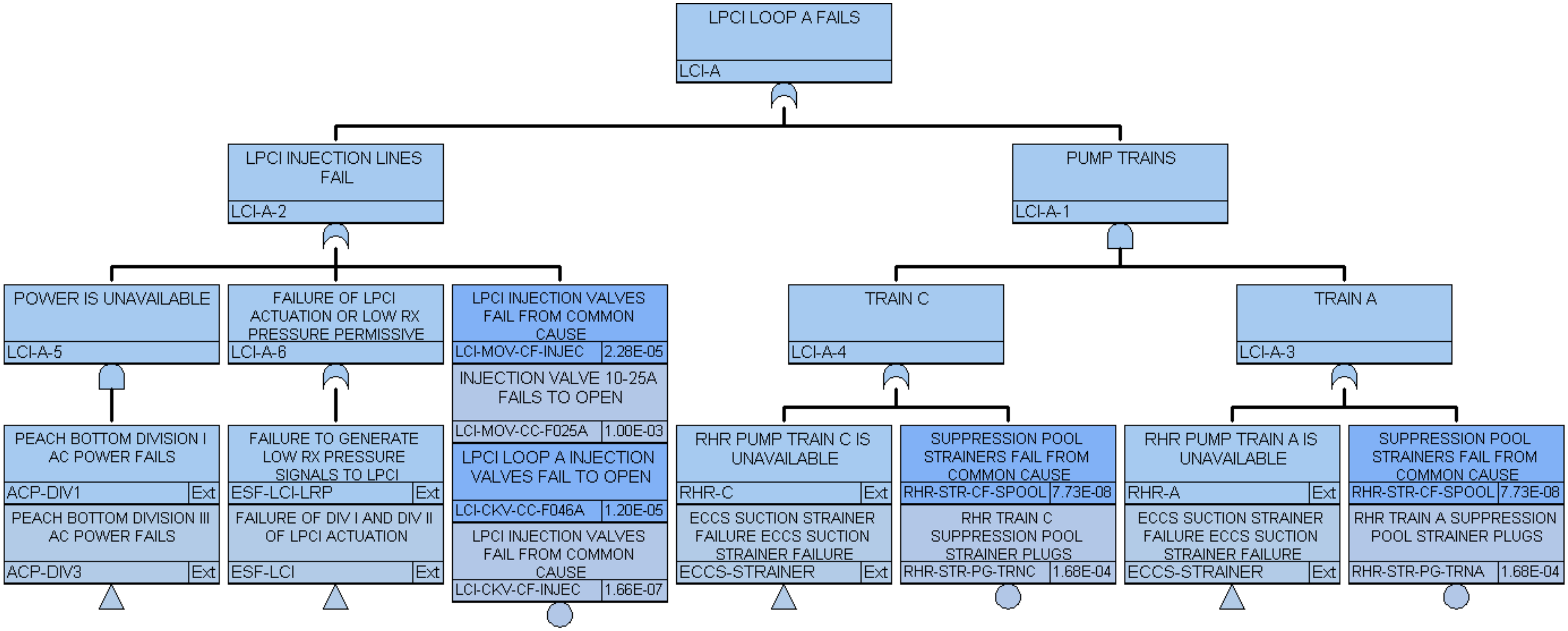

LPCI LOOP A FAILS
LCI-A
LPCI INJECTION LINES FAIL
LCI-A-2
PUMP TRAINS
LCI-A-1
POWER IS UNAVAILABLE
LCI-A-5
FAILURE OF LPCI ACTUATION OR LOW RX PRESSURE PERMISSIVE
LCI-A-6
LPCI INJECTION VALVES FAIL FROM COMMON CAUSE
LCI-MOV-CF-INJEC
2.28E-05
INJECTION VALVE 10-25A FAILS TO OPEN
LCI-MOV-CC-F025A
1.00E-03
LPCI LOOP A INJECTION VALVES FAIL TO OPEN
LCI-CKV-CC-F046A
1.20E-05
LPCI INJECTION VALVES FAIL FROM COMMON CAUSE
LCI-CKV-CF-INJEC
1.66E-07
TRAIN C
LCI-A-4
TRAIN A
LCI-A-3
PEACH BOTTOM DIVISION I AC POWER FAILS
ACP-DIV1
Ext
PEACH BOTTOM DIVISION III AC POWER FAILS
ACP-DIV3
Ext
FAILURE TO GENERATE LOW RX PRESSURE SIGNALS TO LPCI
ESF-LCI-LRP
Ext
FAILURE OF DIV I AND DIV II OF LPCI ACTUATION
ESF-LCI
Ext
RHR PUMP TRAIN C IS UNAVAILABLE
RHR-C
Ext
ECCS SUCTION STRAINER FAILURE ECCS SUCTION STRAINER FAILURE
ECCS-STRAINER
Ext
SUPPRESSION POOL STRAINERS FAIL FROM COMMON CAUSE
RHR-STR-CF-SPOOL
7.73E-08
RHR TRAIN C SUPPRESSION POOL STRAINER PLUGS
RHR-STR-PG-TRNC
1.68E-04
RHR PUMP TRAIN A IS UNAVAILABLE
RHR-A
Ext
ECCS SUCTION STRAINER FAILURE ECCS SUCTION STRAINER FAILURE
ECCS-STRAINER
Ext
SUPPRESSION POOL STRAINERS FAIL FROM COMMON CAUSE
RHR-STR-CF-SPOOL
7.73E-08
RHR TRAIN A SUPPRESSION POOL STRAINER PLUGS
RHR-STR-PG-TRNA
1.68E-04

Figure 2-3. LPCI Loop A Failure Logic with I&C Modeling Incorporated

2.5.5.2 *Minimum I&C Modeling*

Keep the current minimal I&C modeling approach in SPAR models. Note that RPS usually represents the most risk significant I&C system and it is already modeled in all the SPAR models. ESF actuation system may only represent a small risk contributor as shown in Section 2.5.3.2 with smaller than 1% contributions from the new ESF events. Note that the high risk contribution from I&C in AP1000 and ABWR in Section 2.5.3.1 is more an example of importance of digital I&C and how it is modeled. The risk contributions from the three other operating plants vary significantly and include the contributions from other than ESF actuation system. One potential enhancement in keeping with the current minimal I&C modeling approach is to add the verification/justification and documentation in the associated system analyses that the actuation and control signal failure mode may represent an insignificant contributor to the component or system reliability, and thus be excluded from the system model (refer to ASME/ANS PRA Standard SR SY-A15 [3]).

For example, Figure 2-4 represents the logic of Low Pressure Core Injection (LPCI) Loop A injection line failure in Peach Bottom Unit 2 SPAR Model after incorporating the ESF actuation system model. The highest failure probability that would fail LCI-A-2 (LPCI Injection Lines Fail) is 1.00E-3, due to the injection valve 10-25A failing to open (LCI-MOV-CC-F025A). The probability for failure to generate a LPCI actuation signal can be obtained by solving the external transfer fault tree ESF-LCI, which is 7.66E-8. It is four orders of magnitude lower than the highest failure probability of the other components in the same system train that results in the same effect on system operation, and thus can be excluded from the system model without impact on the system model.

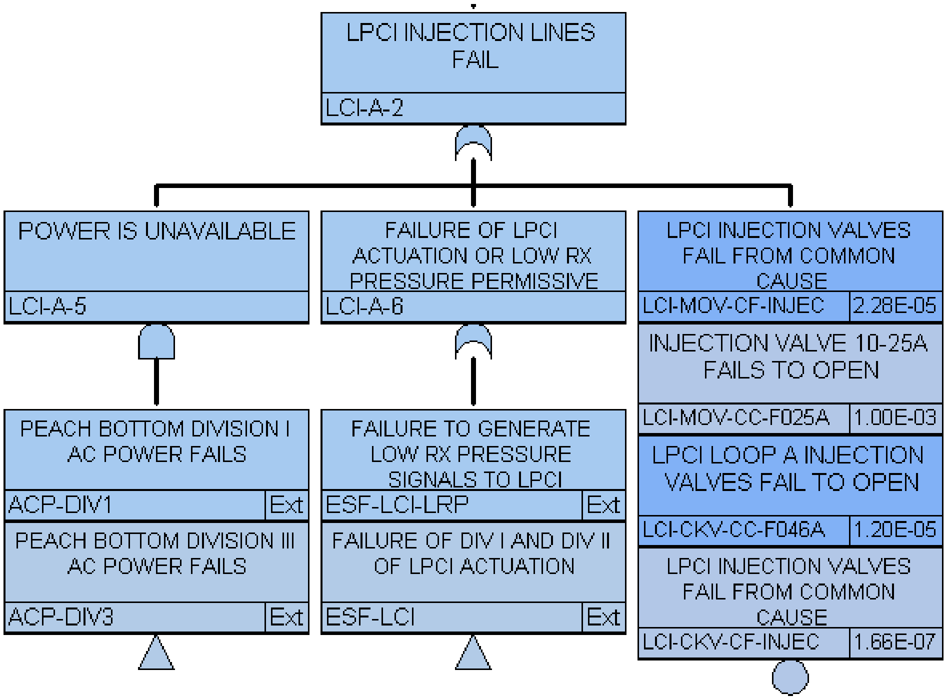

LPCI INJECTION LINES FAIL
LCI-A-2
POWER IS UNAVAILABLE
LCI-A-5
FAILURE OF LPCI ACTUATION OR LOW RX PRESSURE PERMISSIVE
LCI-A-6
LPCI INJECTION VALVES FAIL FROM COMMON CAUSE
LCI-MOV-CF-INJEC
2.28E-05
INJECTION VALVE 10-25A FAILS TO OPEN
LCI-MOV-CC-F025A
1.00E-03
PEACH BOTTOM DIVISION I AC POWER FAILS
ACP-DIV1
Ext
FAILURE TO GENERATE LOW RX PRESSURE SIGNALS TO LPCI
ESF-LCI-LRP
Ext
LPCI LOOP A INJECTION VALVES FAIL TO OPEN
LCI-CKV-CC-F046A
1.20E-05
PEACH BOTTOM DIVISION III AC POWER FAILS
ACP-DIV3
Ext
FAILURE OF DIV I AND DIV II OF LPCI ACTUATION
ESF-LCI
Ext
LPCI INJECTION VALVES FAIL FROM COMMON CAUSE
LCI-CKV-CF-INJEC
1.66E-07

Figure 2-4. LPCI Loop A Injection Lines Failure Logic with I&C Modeling Incorporated

One problem related with this approach is that the exclusion criteria in SR SY-A15 are not always met for I&C models. While the actuation signal failure probability is often very low due to the redundant instrumentation channels and logic, the trip signal or permissive signal failure probability might be too high to be excluded. Still using Figure 2-4 as the example, the failure to generate low reactor pressure permissive signals to LPCI has a probability of 5.18E-5 by solving the external transfer fault tree ESF-LCI-LRP. It does not meet the “two orders of magnitude lower” criterion and thus cannot be excluded from the system model.

2.5.5.3 Expanded I&C Modeling

This approach expands I&C modeling by incorporating the automatic actuation and control signals into the current SPAR models as undeveloped basic events. This approach involves developing a few detailed ESF actuation system models that will represent different types of nuclear plants, for example, PWR and BWR, Westinghouse, CE, and B&W. The representative model is then evaluated. The relevant measures of the ESF actuation system, such as failure to generate a signal to actuate low pressure coolant injection, can be obtained and modeled as basic events in corresponding fault trees. The unreliability from the representing ESF system model is used as the probability of failure of the I&C event in the SPAR model. With the example of Figure 2-4, the External Transfers of ESF-LCI-LRP and ESF-LCI are now replaced with basic events ESF-LCI-CC-LRPPERMIS and ESF-LCI-CC-ACTUATION, respectively. The failure probabilities for the new events use the rounded values from the representative system models, i.e., 5.5E-5 from ESF-LCI-LRP for ESF-LCI-CC-LRPPERMIS, and 1E-7 from ESF-LCI for ESF-LCI-CC-ACTUATION. Figure 2-5displays the new LPCI Loop A injection lines failure logic with the expanded I&C modeling approach. Note that the previous external transfers ESF-LCI-LRP and ESF-LCI are now replaced with ESF-LCI-CC-LRPPERMIS and ESF-LCI-CC-ACTUATION basic events.

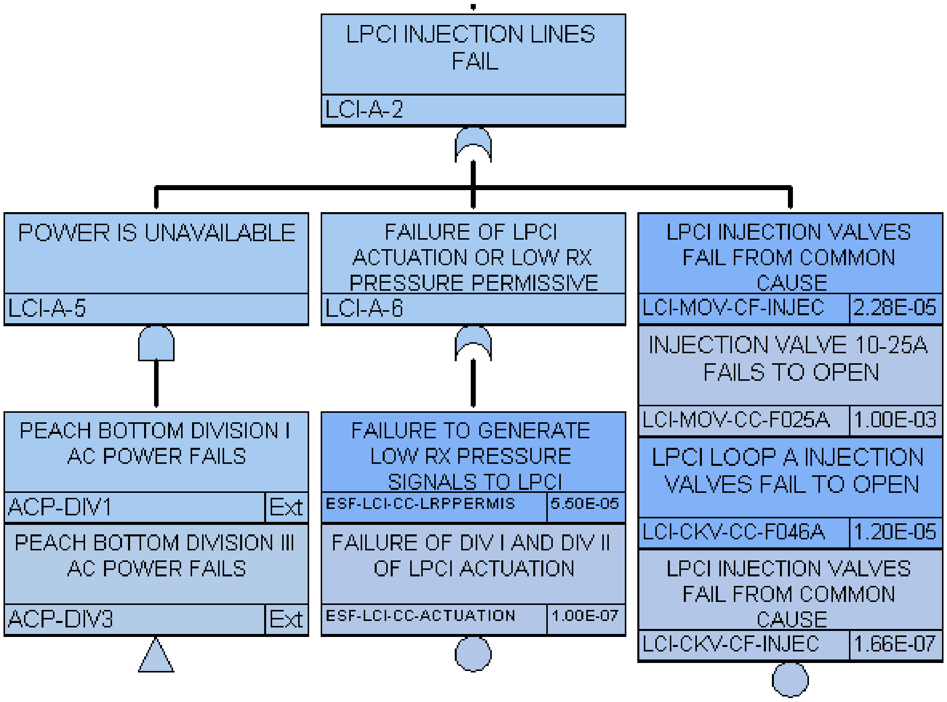

LPCI INJECTION LINES FAIL
LCI-A-2
POWER IS UNAVAILABLE
LCI-A-5
FAILURE OF LPCI ACTUATION OR LOW RX PRESSURE PERMISSIVE
LCI-A-6
LPCI INJECTION VALVES FAIL FROM COMMON CAUSE
LCI-MOV-CF-INJEC
2.28E-05
INJECTION VALVE 10-25A FAILS TO OPEN
LCI-MOV-CC-F025A
1.00E-03
LPCI LOOP A INJECTION VALVES FAIL TO OPEN
LCI-CKV-CC-F046A
1.20E-05
LPCI INJECTION VALVES FAIL FROM COMMON CAUSE
LCI-CKV-CF-INJEC
1.66E-07
PEACH BOTTOM DIVISION I AC POWER FAILS
ACP-DIV1
Ext
PEACH BOTTOM DIVISION III AC POWER FAILS
ACP-DIV3
Ext
FAILURE TO GENERATE LOW RX PRESSURE SIGNALS TO LPCI
ESF-LCI-CC-LRPPERMIS
5.50E-05
FAILURE OF DIV I AND DIV II OF LPCI ACTUATION
ESF-LCI-CC-ACTUATION
1.00E-07

Figure 2-5. LPCI Loop A Injection Lines Failure Logic with I&C Basic Events

Note that the inter-system dependencies associated with the ESF actuation system need to be properly accounted for in this approach.

This approach is recommended to address the I&C modeling issue in SPAR model. It would enable the SPAR models to meet the ASME/ANS PRA Standard specific requirements and represent the as-designed, as-operated plants better with minimum resources allocation. Since the recently developed ESF actuation system for Peach Bottom Unit 2 can be used as the representative I&C system model for the BWR plants, the next step is to find and develop a representative ESF actuation system model for the PWR plants (or a few representing ESF actuation system model for Westinghouse, CE, and B&W each if the different designs warrant). Then the representing ESF models are applied to other SPAR models.

2.5.6 Summary

The Standardized Plant Analysis Risk (SPAR) models for the U.S. commercial nuclear power plants currently have very limited instrumentation and control (I&C) modeling. Most of the I&C components in the operating plant SPAR models are related to the reactor protection system. This report reviews the ASME/ANS PRA Standard requirements on I&C modeling, the importance measures for the I&C basic events in the related SPAR models, and the licensee PSA information. The effort to develop and incorporate the ESF actuation and control system model into the Peach Bottom 2 SPAR model was reviewed. Three different approaches, Detailed I&C Modeling, Minimum I&C Modeling, and Expanded I&C Modeling, are then presented. Expanded I&C Modeling is recommended to address the I&C modeling issue in SPAR model. This approach would enable the SPAR models to meet the ASME/ANS PRA Standard specific requirements and better represent the as-designed, as-operated plants with minimum resources allocation.

3. REFERENCES

1. John A. Schroeder and William Galyean, *Resolution of SPAR Model Technical Issues*, December 2010, INL/EXT-10-20739

2. S.A. Eide, et al, *Industry-Averaged Performance of Components and Initiating Events at U.S Commercial Nuclear Power Plants*, February 2007, NUREG/CR-6928.

3. D. Hance, K. Canavan, *Support System Initiating Event, Identification and Quantification Guideline*, Electric Power Research Institute Technical Report 1016741, Technical Update, December 2008.

4. Ernest J. Henley, Hiromitsu Kumamoto, *Reliability Engineering and Risk Assessment*, Prentice-Hall, Inc., 1981, ISBN-0-13-772251-6.

5. J. D. Andrews and T. R. Moss, *Reliability and Risk Assessment*, American Society of Mechanical Engineers, 2002, ISBN-0-7918-0183-7.

6. E.Borgonovo and G.E. Apostolakis, *A New Importance Measure for Risk-Informed Decision Making*, Reliability Engineering and System Safety, 72 (2001), 192-212.

7. S.A. Eide, et al, *Reevaluation of Station Blackout Risk at Nuclear Power Plants, Analysis of Loss of Offsite Power Events: 1986-2004*, NUREG/CR-6890, December 2005.

8. Z. Ma, J. Schroeder, *Modeling ESF Actuation and Control System for Peach Bottom 2 SPAR Model*, INL internal report, November 2011

9. J. Phillips, *An Evaluation of the Need for More Instrumentation Events in the SPAR Models*, INL internal report

10. ASME/ANS RA-Sa-2009, Addenda to ASME/ANS RA-S-2008, *Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications*, February 2009

4. EPRI MOU SUPPORT

A substantial portion of this project was intended for EPRI MOU support. However, EPRI had more urgent projects to fund and did not participate in any MOU projects during the lifetime of this project. The funds that could have been used to support the MOU were, at the direction of the NRC project manager, used to complete improvements to the ac power and LOOP/SBO modeling in SPAR models that had not previously been upgraded to the current standard. A summary of the current status of LOOP/SBO modeling for each SPAR model is provided in Table ES-1.