Benefits and Risks Associated with Expanding Automated Diverse Actuation System Functions

May 16, 2008

Prepared for:

NEI Digital I&C and Human Factors Working Group

Prepared by:

Applied Reliability Engineering
Erin Engineering

DRAFT

EPRI Project Manager
R. Torok

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

Executive Summary

Standard Review Plan Branch Technical Position 7-19 (BTP-19) establishes current staff positions with respect to the evaluation of defense-in-depth and diversity (D3) in addressing vulnerabilities to potential software common cause failures (CCF). In September 2007, the NRC staff issued additional interim staff guidance (ISG) with respect to the performance of D3 evaluations. Within this guidance were new criteria suggesting that credit for operator action during design basis events following a digital CCF be limited to those actions for which there are more than 30 minutes available. Where less time is available, independent and diverse automation (a diverse actuation system, or DAS) is suggested as a means of assuring adequate protection against CCF within the digital system design.

There is currently only one requirement for an automated DAS; it is in 10 CFR 50.62, and is commonly referred to as the Anticipated Transient Without Scram (ATWS) Rule. It provides for diverse automated actuation of selected mitigating systems in the event of a failure of the reactor trip system (RTS) during an anticipated operational occurrence (AOO). All operating plants have a DAS that complies with the ATWS Rule. Effectively, the D3 ISG recommends expanding automated DAS functions beyond existing guidance by providing an additional automated DAS to address selected CCF events as described in BTP-19.

The D3 ISG does not provide a technical basis for using a 30 minute threshold, and a more rigorous approach, addressing methods for analyzing and validating the ability of the operators to respond to design basis events in the presence of a postulated software CCF is under consideration by the Human Factors Branch of the NRC. An additional ISG may be issued that would provide an alternative approach to the 30 minute criterion. However, this approach would still leave the new staff position in the D3 ISG that recommends adding another automated DAS to address time for operator action may be limited.

It is recognized that ISGs are not regulatory requirements, but are intended to provide guidance for digital system designs that will result in an expedited NRC staff review. However, other than the ATWS Rule, the need for backup independent and diverse automation is not a part of other regulatory guidance. Therefore, to assure that the safety implications of the proposed automated DAS are well understood before implementation of the new ISGs, the industry undertook an evaluation of the potential benefits and risks associated with the proposed independent and diverse automation.

This report documents the results of a risk-informed evaluation of the effects of the proposed automated DAS suggested by the recently issued digital I&C related ISGs. To assure the results

were realistic as well as generically applicable, the analysis was performed using input from 10 currently operating plant designs - 5 PWRs and 5 BWRs, representing each of the existing U. S. vendor NSSS designs.

The results of the analysis show that the potential benefits of the proposed automated DAS are very small and, under some circumstances, competing risks may result in a negative impact on safety. The primary factors that limit the impact of the proposed new DAS functions to a small impact on risk include:

1) The existing defense-in-depth that is provided in the plant design in the form of the independence between the initiating events for which the DAS is being proposed and the mitigating systems that are needed to respond to these events.
2) The relatively low frequency of the events for which the automated DAS is proposed .
3) The high reliability of the 1E actuation systems (analog or digital) which must fail before the automated DAS would be called upon to operate. The conclusions of the study remain unchanged, even using extremely conservative assumptions in regard to digital ESFAS system reliability and CCF potential.

The possible negative effects are a result of the potential for spurious actuations of the proposed DAS that could occur at a frequency significantly greater than the accidents the proposed automated system is intended to address.

A final recommendation coming out of this evaluation is to modify the scope of BTP-19 to assure D3 evaluations are focused on events that are most important with respect to managing the risk associated with software CCF and that resulting changes to the plant design have significant safety benefit. This change in scope would also bring the D3 guidance into alignment with existing precedents and guidance, result in less complexity in the plant I&C design and fewer potential plant transients, while possibly achieving a small improvement in safety over the current scope of BTP-19 and the ISGs.

Acronyms

ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without SCRAM
BTP	Branch Technical Position
BWR	Boiling Water Reactor
CCDP	Conditional core damage probability
CCF	Common cause failure
CCFP	Conditional containment failure probability
CDF	Core damage frequency
CRD	Control Rod Drive
CVCS	Chemical Volume Control System
D3	Defense-in-Depth and Diversity
DAS	Diverse actuation system
ECCS	Emergency Core Cooling System
EF	Error factor
EOP	Emergency Operating Procedure
ESFAS	Engineered Safety Feature Actuation System
FWLB	Feedwater line break
HEP	Human error probability
HPCI	High Pressure Coolant Injection
HPCS	High Pressure Core Spray
HPSI	High Pressure Safety Injection
I&C	Instrumentation and control
IE	Initiating event
IEC	International Electrotechnical Commission
ISG	Interim Staff Guidance
LER	Licensee event report
LERF	Large early release frequency
LOCA	Loss of coolant accident
LPCI	Low Pressure Coolant Injection
LPCS	Low Pressure Core Spray
LPSI	Low Pressure Safety Injection
MSIV	Main steam isolation valve
NRC	Nuclear Regulatory Commission
PORV	Power operated relief valve
PRA	Probabilistic Risk Assessment

PTS	Pressurized Thermal Shock
PWR	Pressurized Water Reactor
RCIC	Reactor Core Isolation Cooling
RTS	Reactor Trip System
SAMA	Severe accident mitigation alternatives
SLB	Steam line break
SRP	Standard Review Plan
SRV	Safety relief valve
V&V	verification and validation

Contents

1 Introduction

Current Nuclear Regulatory Commission (NRC) staff positions regarding defense-in-depth and diversity (D3) evaluations are found in the Standard Review Plan (SRP) Branch Technical Position 19 (BTP-19)[1]. Attachment A summarizes current staff positions regarding D3 evaluations that are found in BTP-19. In September 2007, the NRC staff issued additional interim staff guidance (ISG) with respect to D3 evaluations addressing vulnerabilities to potential software common cause failures (CCF)[2]. New staff positions provided in the ISG includes criteria limiting credit for operator action during design basis events following a digital CCF to those for which there are more than 30 minutes available. Where shorter time frames exist, independent and diverse automation is suggested as a means of demonstrating adequate coping with the plant event and a concurrent software CCF within the digital system design.

This report documents the results of a risk-informed evaluation of the effects of the automated diverse actuation systems (DAS) proposed by the recently issued digital I&C related ISG. To assure the results had generic applicability, the analysis was performed considering the design of 10 currently operating plant designs including 5 PWRs and 5 BWRs representing the spectrum of existing NSSS vendors.

The report discusses:

- the scope of initiating events considered in US power plant PRAs (Section 2),
- the scope of events which could benefit from the proposed automated DAS (Section 3 - deterministic evaluation),
- the effect of the proposed automated DAS on risk (Section 4 - probabilistic evaluation),
- sensitivity studies and uncertainty analyses (Section 5),
- conclusions and possible changes to current regulatory policy that would enhance the effectiveness in D3 evaluations in addressing the risk from potential software CCF (Section 6).

While the analysis is directed at evaluating the effects of new NRC staff positions regarding diversity and defense-in-depth, it has been performed in accordance with the principles of risk informed regulation as defined in Regulatory Guide 1.174[3]. A discussion of each of the principles and how they are addressed in this evaluation are found in Attachment B. Furthermore, the risk insights developed as a part of this analysis have a clear deterministic basis which can be translated to plant design features and operating practices that confirm the assumptions and conclusions of this analysis.

2 Selection of Accident and Transient Initiating Events for Evaluation

The first step in the evaluation of benefits and risks associated with the proposed automated diverse actuation system was to identify the accident sequence initiators for which the DAS could affect plant response.

Typical transient and accident initiating events considered in internal events PRAs are presented in Table 2-1. To identify the events which would benefit from the proposed automated DAS, a series of deterministic analyses were performed for selected BWR and PWR plants. Detailed results of these deterministic evaluations and the impact of the automated DAS are summarized in Section 3 and Attachment C. It should be noted that the scope of this analysis considers accident and transient initiators beyond that for which the automated DAS is proposed as it may have a beneficial effect on more than just those events where the operator cannot be credited as an effective means of actuation. Table 2-1 summarizes where the proposed automated DAS is assumed to have a possible benefit in this analysis, whether or not the DAS is required to meet the ISG for those events. Assumptions regarding the design of the proposed automated DAS and the basis for selection of the events that benefit from its installation are presented in detail in Section 3.

Table 2-1 Typical PRA Initiating Events

PWR

Initiating Event	*Benefit from proposed automated DAS*[*]
Transients	
Manual shutdown	No
Turbine trip	No
Loss of feedwater	No
Loss of offsite power	No
Spurious ESFAS	No
Loss of major support systems	
Loss of instrument air system	No
Loss of service water	No
Loss of CCW	No
Loss of vital buses	
Loss of an AC bus	No
Loss of a 125V DC bus	No
LOCA	
Large LOCA	Yes (low pressure injection)
Medium LOCA	No
Small LOCA	No
Spurious Pressurizer PORV or SRV	No
Steam generator tube rupture	No
Interfacing system LOCA	No
Main steam/main feed line break	
SLB/FWLB in/outside containment	No
Location dependent events	
Internal floods	No
ATWS	
See Transients above	No

BWR

Initiating Event	*Benefit from proposed automated DAS*[*]
Transients	
Manual shutdown	No
Turbine trip	No
Loss of feedwater	No
Loss of condenser vacuum	No
MSIV closure	No
Loss of offsite power	No
Loss of major support systems	
Loss of instrument air system	No
Loss of service water	No
Loss of CCW	No
Loss of vital buses	
Loss of an AC bus	No
Loss of a 125V DC bus	No
LOCA	
Large LOCA	Yes (low pressure injection)
Medium LOCA	Yes (low pressure injection)
Small LOCA	Yes (high pressure injection)
Inadvertently open SRV	No
SLB outside containment	Yes (Large/Med SLB only)
Interfacing system LOCA	No
Reference line leak	No
Location dependent events	
Internal floods	No
ATWS	
See Transients above	No

[*] See Section 3 for identification of initiating events for which the proposed automated DAS would benefit.

3 Effects of the Proposed Automated DAS (Deterministic Analysis)

An understanding of the response of the plants to the accident initiators for which the automated DAS is being proposed and how the DAS would function in these accident sequences is a necessary first step before the benefits and risks can be determined. Using the PRA accident sequence initiators as a basis, a deterministic assessment of three classes of initiating events is performed;

- events initiated by primary or secondary coolant pressure boundary failures,
- transient initiators
- Anticipated Transients without SCRAM (ATWS).

3.1 Plant Response Including Effects of the Proposed Automated DAS

The following three subsections summarize plant response to the spectrum of transients and accidents noted above as well as a conclusion as to which could benefit from the proposed automated DAS. Attachment C contains the results of detailed deterministic analyses performed for a number of accident initiators considered in this evaluation.

In reviewing plant response these events, it is necessary to consider the design, purpose and function of the proposed automated DAS and how it would function. Some characteristics of the proposed DAS system are considered in order to meet the ISG such as the assumption that the DAS provide diverse actuation that must occur within the first 30 minutes of a design basis accident or transient. Other features relate to what the DAS is to actuate. Candidate systems for actuation by the proposed automated DAS are assumed to be safety systems such as high and low pressure injection and any supporting equipment needed to assure their proper functioning. Which safety systems actually need to be automated in order to meet the ISG is accident specific and discussed in Section 3.1.1 to 3.1.3 below. Finally, the manner in which the proposed automated DAS is actuated is considered. When actuating a safety system with the automated DAS, an initial assumption has been made that it is desirable for there to be two different plant conditions present before the proposed DAS will actuate these systems. For injection systems to the primary coolant system, for example, low reactor level plus high drywell pressure should be present in BWRs and low pressurizer pressure plus high containment pressure in PWRs. By requiring two coincident signals before the DAS is actuated, the DAS would actuate on plant conditions clearly representing the design basis events for which it is being proposed while at the same time minimizing the potential for spurious operations due to input conditions.

Following review of plant response to these events and determination of the benefits and risks of the DAS, sensitivity studies are performed modifying the scope of systems actuated by the DAS

and the symptoms on which it is actuated in order to determine the effects of assumptions regarding the design of the DAS on the results.

3.1.1 Plant response to accidents initiated by passive pressure boundary failure

A spectrum of loss of coolant accidents (LOCA) and steam line breaks (SLB) were analyzed in determining the plant response to events which may benefit from the proposed automated DAS. Detailed analysis of these breaks is summarized in Attachment C. Several analyses (Cases 1 and 3 of Attachment C) were performed to establish the range of LOCAs for both PWRs and BWRs that would need an automated DAS in order to meet the ISG. Cases 2 and 5 consider the response of PWRs and BWRs to steam line breaks.

For BWRs, it is found from Case 3 of Attachment C that large to medium LOCAs may result in the need to actuate the ECCS in less than 30 minutes, resulting in the assumption that both high and low pressure injection systems would be provided with the automated DAS. While not required to meet the ISG, the proposed automated DAS may then have a potential beneficial effect on other events such as the small LOCA. For steam line breaks outside containment in BWRs, Case 5 indicates that there is significant time for the operators to initiate injection systems to the reactor and the automated DAS is not required for this purpose. However, the evaluation also assumes that an automated DAS for isolation of the main steam lines during a large steam line break may likely be required to meet the ISG.

For PWRs, Cases 1 of Attachment C suggests that only the large LOCAs would benefit from the proposed DAS as initiation of the ECCS is not needed during the first 30 minutes for smaller break sizes. The accumulators provide sufficient injection to preclude the need for the proposed automated DAS for LOCAs in the medium break range. As a result, only the low pressure injection system needs to be provided with the proposed automated DAS to provide core cooling for the large LOCA. For PWR steam line breaks, Case 2 of Attachment C demonstrates that actuation of the DAS in response to these events could increase the severity of plant conditions and, therefore, the proposed automated DAS would not be needed for these events.

The following discussion provides the bases for these conclusions. Loss of coolant accidents are presented first followed by a discussion of plant response to steam line breaks.

Loss of Coolant Accidents (LOCAs)

LOCA break sizes typically considered in the PRA range from the small LOCAs to the double ended guillotine break of the largest pipe in the primary coolant system. The smaller end of this break spectrum are roughly equivalent to the makeup capacity of low volume, high pressure systems such as charging in PWRs (CVCS) or control rod drive pumps in BWRs (CRD). For the purpose of this analysis, the large LOCA break sizes will be defined as those for which low pressure coolant makeup systems (LPSI or LPCI/LPCS) are capable of providing adequate core cooling without operation of higher pressure injection systems. The ESFAS function provides the actuation of these makeup systems to the reactor. The analyses performed to establish this break range is summarized in Cases 1 and 3 of Attachment C.

To define this large LOCA break range, an analysis of plants from each of the four US reactor vendors was performed. For the PWRs, a rupture of piping in a cold leg was considered assuming only safety injection tanks (accumulators) and low pressure safety injection (LPSI) were available. For the selected BWR, the break was postulated in one of the recirculation loops and only LPCI or LPCS injection was credited following injection of the hotwell contents with condensate pumps. The smallest break size for which low pressure injection was capable of preventing core damage was determined and used to define the lower end of the large break range. The upper end of the large break range remains the double ended guillotine break of the largest pipe.

On establishing the size of large breaks to be considered in this evaluation, a time to core damage was determined under the assumption that no injection to the reactor from LPSI/LPCI. Should a digital CCF result in the failure to initiate these systems, it is within this time frame that the operators must be successful in initiate LPSI/LPCI. For the largest break size, it is assumed only a few minutes would be available before initiation of low pressure systems is necessary. An analysis of the lower end of the break spectrum is performed to determine its timing with respect to the 30 minute limit in the ISG. As shown in Case 1b of Attachment C, the time to core damage for the lower end of the large break range is appreciable for the three PWR designs, well above the 30 minutes suggested by the ISG for crediting operator action. Therefore for PWRs, it is assumed in this evaluation that only low pressure injection systems are candidates for the automated DAS suggested by the ISG. For BWRs, however, the time to onset of core damage is shorter, on the order of 10 to 15 minutes as indicated in Case 3b of Attachment C. The accumulators that are connected to each of the primary coolant loops in a PWR account for the longer timing than that for the BWRs. While 10 to 15 minutes may be sufficient time for the operators to initiate a high pressure makeup system under medium break LOCA conditions, it will be assumed in this analysis that BWRs must provide the proposed automated DAS for HPCI/HPCS in addition to LPCI/LPCS in order to meet the ISG. While not required by the ISG, this assumption results in the proposed automated DAS for BWR LPCI/LPCS and HPCI/HPCS being effective for the full LOCA break spectrum, from small to large break sizes.

Steam Line Breaks (SLBs)

For BWRs, plant response to steam line breaks inside containment are similar to the LOCAs defined above. When located downstream of the main steam isolation valves (MSIV), steam line breaks will be outside the containment. ESFAS functions during steam line breaks are initiation of MSIV closure as well as actuation of the ECCS. Plant response to two break sizes are considered for the BWR SLBs, large and small SLBs outside containment.

BWR large SLB outside containment

Similar to the LOCAs, large SLBs outside containment can result in the need for emergency core cooling systems. A difference, however, is that the break can be isolated by closure of the MSIVs. For the purpose of this analysis, it is assumed that MSIV closure does not occur due to the postulated digital CCF. Unless a means of isolating the steam line is provided, this results in a demand on low pressure makeup systems as the reactor depressurizes. High pressure makeup will also receive a demand, but for many BWRs these systems are turbine driven and, even when successful, will trip on low turbine

pressure ultimately resulting in the need for low pressure makeup. Like the LOCA inside containment, condensate makeup is available until such time as the hotwell is depleted.

An evaluation of the time to core damage for the largest SLB outside containment assuming no ECCS was performed for the selected BWR. Results are provided in Attachment C Case 5b. It can be seen that the time available for the operators to manually initiate a system such as LPCI in the event automatic actuation does not occur for this event is several hours. At the time of core damage, reactor pressure is below the shutoff head of LPCI/LPCS and so it is assumed that the operator has ample opportunity to actuate low pressure makeup for this event making the proposed automated DAS for this purpose unnecessary. However, as the offsite dose consequences associated with an unisolated blowdown of the primary coolant system outside the containment is not available, it is assumed that main steam line isolation remains candidate for the proposed automated DAS in order to meet the ISG.

BWR small SLB outside containment

Plant response to small SLBs outside containment differs from small LOCAs inside containment. As the turbine follows the reactor in a BWR, the expected plant response will be to reduce load and maintain a reactor pressure near normal. While there will be a mismatch between steam and feedwater flow, containment pressure is not rising and no reactor trip setpoints are expected to be exceeded. Eventually temperatures in the pipe tunnel will rise to the point that MSIV closure would be expected (isolation of HPCI and RCIC steam lines as well). However, the assumption is being made that a digital CCF fails ESFAS and steam line isolation does not occur. This event does not lead to a reactor trip unless initiated by the operator. Because the size of the break is small, the appropriate response to this event is an orderly shutdown. Given adequate time for such operator action, the automated DAS for this event not anticipated to be of benefit whether it initiates MSIV closure or initiates ECCS.

For PWRs, steam line breaks occur on the secondary side of the plant. As in the case of the BWR, a large SLB was analyzed for one of the PWRs. ESFAS functions during steam line breaks in PWRs includes actuation of steam generator isolation in the form of MSIV closure, terminating feedwater flow to the steam generators and initiation of safety injection systems. The effect of loss of feedwater isolation and safety injection was considered on plant response to a large SLB. The analyses are summarized in Attachment C Cases 2a through 2d.

PWR large SLB effects on core cooling

Following the large SLB, primary coolant pressure response and fuel temperature were examined with and without feedwater isolation and/or safety injection flow. In each case, primary system pressure response was less severe (lower pressure as a function of time) and fuel temperatures remained well below regulatory limits.

Pressurized Thermal Shock (PTS) considerations

While fuel and reactor coolant pressure may be less severe during SLBs without ESFAS operation, the cooldown of the vessel can be more significant. The NRC recently has redeveloped the technical basis for the PTS Rule, 10CFR50.61, and generated new insights regarding the risks from PTS at PWRs[4]. A conclusion reached in the analysis is that the most significant accidents from a PTS standpoint are large and medium LOCAs in which rapid and continuous ECCS injection occurs and stuck open pressurizer SRVs in which flow stagnation occurs followed by reclosure of the SRV. During large SLBs, significant circulation and mixing occurs of the cold ECCS water due to the rapid heat removal through the affected steam generator. Therefore, even if safety injection makeup is successful, the potential for vessel failure from PTS is low during SLBs. Probabilistic fracture mechanics analyses performed by the NRC confirms the low potential for a through wall vessel crack for these events.

It is concluded that loss of the feedwater isolation and safety injection functions during PWR large SLB conditions does not jeopardize core cooling or vessel integrity during SLBs and these events would not benefit from the proposed automated DAS.

3.1.2 Plant Response to Transients

Two classes of transient initiated events are examined to determine whether they would benefit from the proposed automated DAS; transients in which heat is being removed from the reactor at decay heat rates and transient induced LOCAs.

For BWRs, the proposed automated DAS would not be effective for transient events at decay heat removal rates as the actuating conditions for the DAS would not be present. Because the reactor coolant system would not be at a sufficiently low pressure, an actuating signal would not occur in PWRs either. In addition, reactor pressure is too high for LPSI to inject in some PWRs. Therefore, the proposed automated DAS is not found to be effective for these events. The following provides the basis for these conclusions.

Transients with the need to remove and provide makeup for decay heat

BWRs

At decay heat levels, BWR transients in which the primary coolant system remains intact can result in a demand on high pressure injection systems within 10 to 20 minutes of the reactor trip given the assumption that normally operating makeup systems such as feedwater are lost. However, even on loss of these high pressure systems, there is sufficient inventory in the reactor vessel, that emergency depressurization and actuation of low pressure systems can be delayed to well beyond 30 minutes without jeopardizing core cooling. Furthermore, given the BWR EOPs call for inhibiting the ADS early in a transient, emergency depressurization effectively is a manual action. If the reactor is successfully depressurized by the operators, then it is reasonable to assume they would be effective in initiating an injection system at the same time as called out in the EOPs. Therefore, the proposed automated DAS would not be called upon during BWR transients in which loss of reactor coolant from the primary system is only at decay heat levels.

PWRs
Removal of decay heat through the steam generators in a PWR can lead to a demand on auxiliary feedwater within 10 minutes of the transient initiator. However, dryout of steam generators to the point that initiation of feed and bleed is called for in accordance with EOPs takes longer, on the order of 20 to 30 minutes at decay heat levels depending on the capacity of the steam generators. Bleed and feed is a manual action with initiation of high head injection before the PORVs would be opened. Further, the PORVs are not typically sized to reduce primary coolant pressure to the shutoff head of low pressure injection systems. Therefore, transient initiated events in which the removal of heat at decay heat levels is required do not need the proposed automated DAS in order to meet the ISG.

Transient induced LOCAs

Two types of LOCAs are considered; stuck open pressure relief valves and seal LOCAs.

BWRs
For BWRs, a stuck open SRV can occur as an initiating event or in response to another transient initiator during pressure relief. An analysis of a spurious SRV actuation with the reactor at power was performed to determine the plant response to the event. The analysis is summarized in Attachment C Case 4a. Similar to small SLBs outside the containment, the turbine control valves will begin to close in response to the pressure reduction at the turbine inlet. On restoration of reactor pressure to normal, the plant will continue to operate, although there will be a mismatch between steam flow and feedwater flow. Unlike SLBs inside containment, the steam from the stuck open SRV will be directed through tail pipes to the suppression pool where it will be condensed. As the pool and wetwell air space heat, containment will slowly pressurize. An automatic reactor trip would be expected for this event only on a high drywell pressure, which would take on the order of a half hour to occur and even longer before it was necessary. In the interim, the operators would be expected to initiate a reactor shutdown in a controlled manner, with a manual scram or a normal shutdown. Given the time available for operator intervention for this event, the automated DAS is not expected to receive a demand.

A stuck open SRV also can occur in a BWR in response to other transient initiators in which decay heat removal to the main condenser is not available. This event begins with a reactor trip followed by a gradual reduction in reactor pressure given the stuck open SRV. For core cooling to be jeopardized, feedwater/condensate must be lost as a result of the initiating event, otherwise they will preclude a reduction in reactor inventory. Analysis of this type of event for a typical BWR is summarized in Attachment C Case 4b and suggests that reactor depressurization will occur on the order of a half hour before significant heat up of the fuel begins even with no injection at all. It is noted that this is a design basis event with a single failure and would not need the proposed automated DAS to meet the ISG. Even so, transient events with a stuck open SRV in which a makeup system with as little capacity as normal CRD makeup would likely not require the proposed automated DAS at all.

BWR recirculation pumps are of the Byron Jackson design in BWRs. Tests of the seals of these pumps have been performed and demonstrate that they do not increase significantly in seal leakage on loss of seal cooling[5]. Therefore, seal LOCAs are not generally considered in BWR PRAs.

PWRs
A stuck open PORV or SRV in a PWR is in the small to medium LOCA range (i.e, smaller than the break sizes demonstrated to provide more than 30 minutes for actuation in Attachment C). The capacity of the PORV/SRVs are such that the operator has significant time to initiate a high pressure injection system should they fail to actuate in order to provide adequate core cooling. In addition, PORV block valves can be isolated manually to terminate loss of coolant through this path. Finally, primary coolant system pressure is not expected to fall below the shutoff head of low pressure injection systems prior to uncovering the core, limiting the ability of the proposed automated DAS to be of benefit for this event.

For some primary coolant pump designs, loss of seal cooling can lead to seal failure and LOCAs in the small to medium break size range. Conditions leading to loss of seal cooling would likely require the complete loss of a support system (such as service water, component cooling water or all AC power). These conditions would also result in the loss of support for injection systems in most PWRs. This and the relatively small break size for seal LOCAs suggest that the proposed automated DAS would neither be required to meet the ISG nor would it be of benefit for these events.

3.1.3 Plant Response to ATWS

The principle concern in immediate response to an ATWS is to preclude reactor coolant system overpressure. For this reason, ATWS mitigating systems for BWRs trip the recirc pumps and for PWRs they trip the turbine and initiate AFW. For reactivity control purposes, ATWS mitigating systems also initiate alternate rod insertion (ARI) in BWRs and a diverse reactor trip signal in some PWRs. These automated DAS systems exist in all current plants and are a requirement for new plants. The proposed automated DAS, on the other hand, plays little role in response to an ATWS. The following provides additional information supporting this conclusion.

BWRs
Among the first steps in the failure to SCRAM emergency operating procedures are inhibiting the ADS and terminating flow to the reactor in order to lower level to limit loads on containment and allow time for SLC to be effective. Whether or not the proposed automated DAS were to actuate during an ATWS, the operators would be instructed to defeat it in accordance with the EOPs limiting its usefulness for these events.

PWRs
On a transient initiator with failure to SCRAM, reactor pressure increases to the point that pressurizer PORVs and SRVs lift. No safety injection actuation signal is initiated and, for some plants, reactor pressure remains sufficiently high that it exceeds shutoff of the safety injection systems, rendering the proposed automated DAS ineffective for these events.

3.2 EVENTS FOR WHICH THE PROPOSED AUTOMATED DAS IS BENEFICIAL – SUMMARY

For both BWRs and PWRs, there are specific events for which the proposed automated DAS would be needed to meet the ISG. For the reasons stated above, these events are as follows:

BWRs (automated DAS forLPCI/LPCS and HPCI/HPCS)
Large LOCA (>6" effective diameter)
Medium – Small LOCA (>0.5" effective diameter)
Large/Medium SLB outside containment (MSIV closure)

PWRs (automated DAS for LPSI)
Large LOCA (>4" effective diameter).

It should be noted that the definition of the large LOCA for this evaluation encompasses breaks traditionally considered in the medium break range for most PRAs. In addition, several of these initiating events (including a portion of the Large LOCA ranges) may provide greater than 30 minute limit contained in the ISG for crediting operator action. However, the remainder of this evaluation recognizes that the proposed automated DAS can be useful, for events beyond those suggested by the ISG and considers those benefits.

4 Effects of the Proposed Automated DAS (Probabilistic Analysis)

Having identified the spectrum of initiating events for which the proposed automated DAS may be of benefit, the next part of the analysis develops initiating event frequencies, failure probabilities and consequences needed to quantify the benefits and risks associated with the affected accident sequences. In addition to generic data, input was obtained from 10 currently operating plants to assess the potential impact of the proposed DAS across a variety of plant designs. The following summarizes the plant types providing input to the analysis:

PWRs	*BWRs*
Westinghouse - 2 loop	BWR 2 Mark I containment
Westinghouse - 4 loop	BWR 3 Mark I containment
Combustion Engineering	BWR 4 Mark I containment
Dual unit site	
Single unit site	
Babcock &Wilcox	BWR 5 Mark II containment
	BWR 6 Mark III containment

Appendix B Section 4 lists the plant specific information obtained for each of these plants including ESFAS functions, conditional core damage probabilities for specific initiating events and containment performance information.

4.1 QUANTIATIVE INPUT

The benefits associated with the proposed automated DAS effectively can be estimated by taking the sum of the product of five parameters for each plant:

$$Benefit_{DAS} = \Sigma\ FIE_i * P_{ESFAS} * P_{OP} * PCONT_i * DOSE_i$$

where

$Benefit_{DAS}$ - The avoided offsite dose consequences that are realized by providing the proposed automated DAS (person-rem/year)

FIE_i - The frequency for initiating event i (1/year)

P_{ESFAS} - The probability of failure of the digital ESFAS for which the proposed automated DAS is being provided as a backup

P_{OP} - The probability of failure of the operator to manually initiate the systems for that the ESFAS failed to actuate

$PCONT_i$ - The conditional containment failure probability for the accident sequence in which the ESFAS failure is postulated

$DOSE_i$ - The conditional offsite dose consequences associated with the accident sequence in which ESFAS failure and containment failure occur (person-rem within a 50 mile radius of the site).

In this section, values for each of these five parameters are developed.

4.1.1 Initiating Event Frequencies

In Section 3.1, two different ranges of LOCAs were identified as potentially benefiting from the proposed automated DAS depending on the plant type; the full spectrum of break sizes for BWRs and the large LOCA only for PWRs. The following derives the frequencies for these ranges of break sizes.

Large LOCA

Recently developed generic frequencies[6] were used to generate the Large LOCA initiating event frequency. The Large LOCA sizes defined for the purpose of this analysis were derived in Attachment C, their associated frequencies in Attachment D Section 1.

BWR (>6" effective break size)

Mean	1.5E-05/year
Upper bound (95%)	5.7E-05/year
Lower bound (5%)	1.9E-07/year

PWR (>4" effective break size)

Mean	2.6E-05/year
Upper bound (95%)	1.0E-04/year
Lower bound (5%)	3.4E-07/year

It should be noted that these frequencies are as much as an order of magnitude larger than that typically used in a PRA for large LOCAs (see Table 5-1 in NUREG/CR-6928[7]). The larger frequency in this analysis is a result of including a portion of the medium break spectrum into the break ranges for which low pressure makeup systems are effective and, hence, the proposed automated DAS may be of benefit. The smaller end of the redefined large break range may allow longer than 30 minutes before initiation of an injection system is needed and, as a result, the proposed automated DAS is recognized as having a potential benefit for sequences beyond that suggested in the ISG.

Medium – Small LOCA

The same generic sources of data (see Reference 6) were used to develop LOCA frequencies in the medium to small range for BWRs as it is being assumed that both high and low pressure injection systems would be actuated by the proposed automated DAS. Again, these events may have longer than 30 minutes to initiate ECCS. Because there is significant time available to

actuate an injection system for breaks in this range, the proposed automated DAS is redundant not only to the ESFAS, but to operator actions to initiate makeup to the reactor as well.

BWR (>0.5" effective break size)

Mean	6.0E-04/year
Upper bound (95%)	2.0E-03/year
Lower bound (5%)	2.6E-05/year

Per Section 3.1.1, PWR small and medium breaks would not benefit from the proposed automated DAS as it is expected that only low pressure injection systems would be actuated. Development of a frequency for these initiators in PWRs is not necessary for this analysis.

Large – Medium Steam Line Breaks Outside Containment

NUREG/CR-6928 does not provide estimates for steam line breaks outside containment. Estimates were provided in NUREG/CR-5750[8], but they were for small break sizes (on the order of 1" effective diameter).

For the purpose of this evaluation, a best estimate to bounding frequency will be developed for large SLB outside containment based on the LOCA frequencies of Table D-1 in Attachment D. It will be assumed that the medium SLB threshold is on the order of the 1 7/8" effective break size for BWRs. The feedwater system is likely capable of making up for this break (1500gpm) and the break size that would lead to a plant trip actually may be larger.

BWR (>1.875" effective break size)

Mean	1.1E-04/year
Upper bound (95%)	4.1E-04/year
Lower bound (5%)	2.2E-06/year

From Section 3.1.1, PWR steam line breaks outside containment are not likely to provide a threat to adequate core cooling even without the proposed automated DAS. An estimate of PWR SLB frequency outside containment is not needed for this analysis as a result.

4.1.2 Digital ESFAS Failure Probability

The analysis does not assume a particular design or architecture for the digital ESFAS. For the purpose of this analysis, a base case probability of failure of the ESFAS and uncertainty distribution is assumed. The probability and distribution represent the potential for there being a fault in the ESFAS software that can disable safety system actuation and the occurrence of a coincident set of plant conditions that will trigger this error such that the safety function is unavailable at a time when it is needed (note that with simple ESFAS algorithms and a well designed digital platform that uses appropriate design features to preclude or limit digital CCFs, (defensive measures), there is little potential for plant conditions to trigger the error). Sensitivity studies varying both the failure probability and uncertainty across broad ranges are performed to establish whether the conclusions are sensitive to these assumptions.

Attachment D Section 2 provides details regarding the bases for the initially assumed failure probability. The failure probability assumes a high quality software development process similar to that found in IEC standards[9] in which it is stated that 10^{-4} is an appropriate limit on the reliability of the system given process alone. The failure probability applies largely to the application software. An assumption is made that there is little potential for operating system failure coincident with the accident because of design features implemented specifically to preclude this type of failure. Initially, an EF of 10 is assumed. As noted above, sensitivity studies are performed varying both the failure probability and the assumed EF by orders of magnitude to determine their impact on the results.

4.1.3 Human Error Probability

Attachment D Section 3 contains a human reliability analysis that assesses the failure probability of the operators initiating an injection system in the presence of failures that affect the normal indication used by the operators to implement the EOPs. Note that in this evaluation credit for operator action as a backup to ESFAS is taken only if 30 minutes or more is available from the beginning of the accident to accomplish this action. The analysis assumes a LOCA with failure of automatic ECCS initiation. In addition, a limiting situation in which the operators' normal indication is conflicting or inconclusive regarding key plant parameters is assumed. (It is not assumed that the operators' screens go dark as that would be clear indication that the normal indication cannot be trusted. Rather, the normal indication is assumed to be reading near normal, not indicative of the actual LOCA related plant conditions). The operators are assumed to have independent backup instrumentation in accordance with Point 4 of BTP-19. Symptom oriented emergency procedures also are assumed to be available, essentially the same as those that exist for the current generation of plants.

Two failure probabilities are derived; one in which the operators must discern for themselves that the normal instrumentation is conflicting and the other in which a prompting alarm is available to suggest that the operator confirm plant conditions with backup instrumentation.

Given 30 minutes to manually initiate a makeup system, Attachment D Section 3 derives the following human error probabilities:

Conflicting normal instrumentation

$P_{OP} = 0.17$ EF = 1

Conflicting normal instrumentation with a prompting alarm

$P_{OP} = 4E\text{-}3$ EF = 10

Longer time frames than assumed in this analysis would improve the likelihood that the operators would be able to complete the actions specified in the EOPs. As noted above, this evaluation depends on the manner in which the failure of the operators' primary indication manifests itself. If the failure modes yield clearly incorrect information or no information, then the response of the reliability of the operators to implement the existing EOPs would be significantly better than assumed in this analysis.

4.1.4 Frequency of Spurious Operation

In estimating possible risks associated with the proposed automated DAS, it is necessary to consider the potential for its spurious operation. This frequency, the type of transient it may cause (e.g., no trip at all, an uncomplicated turbine trip, a loss of feedwater, challenge to primary system SRVs, etc.) and the availability of mitigating systems in response a given transient will dictate the risks associated with the introduction of an automated DAS.

Current plants do not have diverse actuation systems intended to provide functions that backup ESFAS for systems such as safety injection. Therefore, the potential for the proposed automated DAS to initiate a spurious trip must be estimated from operating experience with other existing systems. The potential for ESFAS itself to operate spuriously is examined for its relevance to deriving a spurious DAS frequency. Attachment D Section 2 contains a review of LERs between 1988 and 2005 in which spurious ESFAS actuations lead to plant trips. Roughly four dozen events are identified in which an unintended ESFAS actuation lead to a reactor scram (see Attachment D Section 1.2). A review of the plant conditions which resulted in these inadvertent trips suggests that only a subset would be applicable to the proposed automated DAS.

- The proposed automated DAS should not be subject to Technical Specification test and surveillance requirements and, therefore, may not be as vulnerable to inadvertent trips as a result of these types of activities.

- The industry has successfully reduced the frequency of spurious ESFAS actuation as a result of test and surveillance activities. Where online testing and maintenance did occur, the processes used to prevent such inadvertent trips from ESFAS would also likely apply to the proposed automated DAS.

- Similar to the ATWS mitigation systems, the proposed automated DAS would likely not be fail safe. Inadvertent ESFAS trips to which loss of sources of instrument power would not likely be applicable to the proposed automated DAS.

In addition, the plant conditions on which the proposed automated DAS actuates do not necessarily have to be identical to the ESFAS. Greater margin on trip setpoints and multiple diverse plant conditions on which to actuate the DAS can further reduce the potential for spurious actuation.

Given the above assumptions, Attachment D Section 2 screens out those spurious ESFAS events which would not appear to be applicable to an automated DAS. The following frequency for spurious plant trips resulting from the proposed automated DAS is derived from the remaining events. While on the order of as much as once in the licensed lifetime of each plant, these frequencies are roughly a factor of two to four less than operating experience suggests for spurious ESFAS actuations.

Expected frequency of spurious DAS (sensors and logic)

Mean	0.018/yr

Upper bound (95%)	0.087/yr
Lower bound (5%)	ε

Expected frequency of spurious DAS (logic only) = 0.005/yr

Mean	0.005/yr
Upper bound (95%)	0.026/yr
Lower bound (5%)	ε

Further examination of operating experience related to spurious safety system actuation reveals that they are roughly distributed evenly between those that cause plant trips initiated by ECCS and those involving isolation of the secondary side of the plant.

4.1.5 Plant Specific Data

The quantitative input described in the preceding four sections for the most part is generic in nature. Several additional plant specific inputs are needed to quantify the benefits and risks associated with the proposed automated DAS.

- Containment performance data and offsite dose consequences given the applicable events identified in Section 3 with a coincident failure of the ESFAS
  - Conditional large early release probability
  - Large early release offsite dose consequences.

- Conditional core damage probability for the transients caused by spurious operation of the proposed automated DAS.

Attachment D Section 4 contains data sheets for 10 plants (5 BWRs and 5 PWRs) providing the above plant specific information.

The containment performance information is used in estimating the benefits of the proposed automated DAS and was obtained from the Severe Accident Mitigation Alternative evaluations submitted for each of the plants (or for a similar plant) in the license renewal application.

The conditional core damage probabilities are used in estimating risks associated with the proposed automated DAS that results from its spurious operation. These conditional core damage probabilities are obtained from versions of the plant specific PRAs used during or updated subsequent to the development of the license renewal submittals.

4.2 QUANTITATIVE ANALYSIS

Given the information developed in the preceding section, a quantitative estimate of the effects of the proposed automated DAS on risk can be derived. Tables 4-1 and 4-2 summarize the quantitative results for BWRs and PWRs respectively. The benefits of the proposed automated DAS are first derived followed by an estimate of the risks that it introduces.

4.2.1 Benefits of the Proposed Automated DAS

In the upper half of Tables 4-1 and 4-2 is a summary of the benefits of the proposed automated DAS for the five BWRs and five PWRs. The benefits are provided in terms of the reduction in core damage frequency and offsite dose consequences that can be expected from the proposed automated DAS.

In the upper left of the tables, the initiating events for which the DAS may be of benefit are listed along with their frequencies. Section 3.1.1 provides the basis for selection of these particular events and Section 4.1.1 provides the derivation of their frequencies.

- As noted in Section 4.1.1, the definition of the large LOCA frequency was expanded for this evaluation to include all break sizes for which low pressure injection systems would be effective. Therefore, the large LOCA frequency is about an order of magnitude greater than what typically is used in PRA.
- Whether the event leads to core damage within 30 minutes is noted. Analysis of the timing of events are provided in Attachment C.
- Credit for operator action to initiate ESFAS is taken only if more than 30 minutes is available. As noted in Section 4.1.3 the human error probabilities in Tables 4-1 are derived for 30 minutes total available time even though some of the events may allow for a greater time to take action. The human error probabilities in the tables also assume a unique prompting alarm is available to direct the operators to the appropriate actions in the symptom oriented EOPs. A sensitivity analysis on this assumption is performed in Section 5.
- The base case probability of a software CCF that disables the ESFAS function is assumed to be 10^{-4}/demand. This base case value is discussed in Section 4.1.2. Sensitivity analyses on this value are performed in Section 5.

For the purpose of estimating the benefits, the proposed automated DAS is assumed to eliminated all of the risk stemming from failure of the ESFAS. In this regard, the proposed DAS is redundant to the ESFAS and operator actions to initiate safety systems (where credited). The reduction in CDF that is estimated for the proposed automated DAS is approximately 2E-9/year for BWRs and 3E-9/year for PWRs. The risk is dominated by large LOCAs for both plant types. Even though both high and low pressure systems are assumed to be provided with the proposed automated DAS in BWRs, this distribution in risk is to be expected given that significant time is available for the operators to initiate safety systems for all but the large LOCAs. No accident sequences benefit other than those for the large LOCA in PWRs as only the low pressure injection systems would need to be provided with the proposed automated DAS to meet the ISG.

The analysis is expanded to determine the benefits in terms of offsite consequences. The upper middle section of Tables 4-1 and 4-2 provide the conditional containment failure probabilities for each of the five BWRs and five PWRs for the large LOCA without injection. Also provided is the large early release dose magnitude for each of the plants as provided in the Severe Accident Mitigation Alternatives (SAMA) evaluations as a part of their license

renewal applications. Insights related to the information in the offsite consequences section of the tables are as follows:

- The BWR2 through BWR5 containments are isolated and inerted. This results in a low potential for a number of containment failure modes such as hydrogen combustion and containment isolation failure.
- For the BWRs, several of the plants show relatively high conditional containment failure probabilities (~.2). The containment failure probability for these plants is dominated by liner meltthrough as a containment failure mode. It is noted that given several hours for the core to penetrate the vessel, there may be ample time for the operators to initiate an injection system and recover the event in-vessel that is not being credited in this analysis. The remaining BWR conditional containment failure probabilities are dominated by the short periods of time the plants are operated deinerted and the effects of in-vessel or ex-vessel steam explosions.
- The PWR conditional containments are also normally isolated. Failure probabilities for large early releases are dominated by missile generation from in-vessel steam explosions, ex-vessel steam explosions and hydrogen combustion.
- The difference in offsite dose consequences between each of the plants is due largely to the plant's size and location with respect to population centers.

It is recognized that there are additional consequences that could be considered in the form of smaller or late releases as well as economic consequences (both on-site cleanup and offsite costs). Sensitivity studies are performed in Section 5 for several of the plants to determine whether consideration of these additional costs would have an effect on the conclusions of the analysis.

The estimated offsite dose consequences that could be avoided by the proposed automated DAS are shown for each plant. This is converted to a present value using $2,000/person-rem, a 7% annual discount rate and assuming 20 remaining years in the life of the plant. These assumptions are similar to those used in each of the plants' SAMA evaluations in support of the life extension submittals.

Acceptance criteria for the benefits of the proposed automated DAS are assumed to be similar to that found in NUREG/BR-0058[10]. These criteria are summarized in Attachment E. The total value of the avoided offsite consequences should be compared to 10^6 as an estimated lifetime cost for the proposed automated DAS. This estimated cost includes initial design and installation costs as well as lifetime maintenance, test and operational costs. Based on the information presented in Tables 4-1 and 4-2, it can be seen that the benefits of the proposed automated DAS, in terms of both change in CDF and offsite consequences, are several orders of magnitude below that suggested by the NRC in the performance of cost-benefit analyses. When comparing to commonly accepted value-impact, it appears that the recommendations of the ISG do not provide a substantial improvement in safety nor can the costs be justified in light of this improvement.

4.2.2 Risks Associated with the Proposed Automated DAS

Any plant changes or new regulatory guidance that affect plant design and operation can carry with the risks in addition to benefits. Most changes to the plant design which undergo a realistic

evaluation of their effects will either result in or can be adjusted to provide more benefits than risks. To assure that is the case for the proposed automated DAS, a review of its potential spurious operation has been performed on the 10 plants representative of each of the reactor types in operation in the US.

Spurious actuation of safety systems can have a variety effects ranging from simply starting pumps and opening valves to isolation of balance of plant support systems and/or and shedding of non-critical loads from safety and non-safety related power supplies. Other effects that may occur depending on the actuated systems and equipment include flow diversion, water hammer and reactivity transients. While the plant design basis considers these events, they are not without risk. Plant trips resulting from the spurious operation of the proposed DAS require successful operation of mitigating systems in order to prevent consequences not unlike those the DAS is intended to prevent.

The lower half of Tables 4-1 and 4-2 provide an estimate of the increase in CDF for each of the 10 plants as a result of spurious operation of the DAS. The left columns of the lower rows of the tables provide the expected frequency of the DAS spurious operation. This frequency was derived in Section 4.1.4 and is based on a subset of historical ESFAS actuations that are considered to be applicable to the proposed DAS. In order to minimize this frequency, an assumption also has been made that actuation of diverse sensors is needed to initiate the DAS (low pressurizer pressure and high containment pressure for PWRs, low reactor level and high drywell pressure for BWRs).

The plant response to a spurious DAS operation depends on what is actuated by the DAS. For all but one of the BWRs, either primary system isolation or an uncomplicated general transient is expected. These trips are due to the DAS isolating or shedding loads needed to support plant operation in order to assure the successful operation of the safety systems they actuate. The exception is spurious actuation of the ECCS for the BWR2. High and low pressure injection systems will actuate and inject cold water to the reactor for this plant. However, all balance of plant systems remain available and the operators may well be able to secure these systems before a plant trip occurred. For the PWRs, anything from no plant trip at all through a general transient, a loss of feedwater or isolation of key balance of plant support systems is assumed. Three of the PWRs are not expected to trip on initiation of low pressure injection as successful operation of the ECCS does not require isolation or trip of equipment needed for plant operation[i]. For the remainder of the spurious DAS actuations, the choice of plant transient is dependent on what the ESFAS (and hence the DAS) must initiate in order to support successful safety system operation. Attachment D Section 4 lists the assumed effects of spurious operation of the DAS for each of the 10 plants. The conditional core damage probability for each of the possible transient initiators is provided in the next to last rows of the lower half of Tables 4-1 and 4-2. Insights regarding these conditional core damage probabilities are as follows:

- For BWRs, MSIV closure events have a higher conditional core damage probability than for general transients. This is due to loss of balance of plant equipment following a MSIV closure such as the main condenser as a decay heat removal system and feedwater (for those plants with turbine driven feedwater pumps).

[i] The three plants are the 2 loop and 4 loop Westinghouse plants and the B&W plant. Note that isolation or tripping of balance of plant systems is required for some plants of these designs.

- For PWRs with spurious SI initiators, the conditional core damage probability is higher than general transients or loss of feedwater as a result of the additional isolation of balance of plant support systems or due to the pressurizer going solid and lifting pressurizer safety valves.

The overall core damage frequency associated with the potential for spurious DAS operation is shown in the last row of Tables 4-1 and 4-2. It is noted that the core damage frequencies estimated for spurious DAS operation are a factor of 2 to 10 higher than the expected reduction in core damage frequencies provided by the DAS following a LOCA with a software CCF.

4.3 QUANTITATIVE ANALYSIS – SUMMARY

There are several reasons that the benefits of the proposed automated DAS are so limited.

- The events for which the proposed automated DAS is being considered have very low frequencies, the large and medium LOCAs.
    - By designing the primary coolant pressure boundary in accordance with accepted codes such as Section III of the ASME Boiler and Pressure Vessel Code or ANSI B31.1, the reactor coolant system is designed to limit the potential for ruptures of the size for which the proposed automated DAS may be beneficial.
    - Periodic inspection of the reactor coolant pressure boundary in accordance with Section XI of the ASME Boiler and Pressure Vessel Code precludes growth of flaws that may exist and prevents aging mechanisms from significantly increasing the likelihood of a pressure boundary.
    - Routine monitoring of the performance of the reactor coolant pressure boundary during operation[i]. If a digital monitoring system is used, there would need to be little potential for a CCF of the leakage detection system and the ESFAS.
- The digital ESFAS is expected to be an improvement in reliability over current analog systems. There is a low potential for software CCF of these systems due to defensive measures that are typically taken in the design and operation of digital systems important to safety. Such defensive measures include
    - Cyclic system operation that is always active, with constant bus loading (processors and communications), operating system confined to well-tested trajectories that remain invariant during plant transients, etc. (see Reference 11 for more extensive list)
    - Very simple application software. For example, the functional logic for ECCS actuation may require only a single process input to reach a single fixed setpoint. There are very few interlocks that can potentially block or interfere with the actuation. Such actuation logic is very simple and has been operating

[i] Per Reference 6, leakage detection systems play a role in developing LOCA frequencies (e.g., mass balance calculations, sump level monitoring, airborne particulate and gaseous monitoring). However, the LOCA frequencies are insensitive to the monitoring interval on the order of each shift to weekly.

in nuclear plants for more than 30 years. There is minimal potential for specification error or misinterpretation of the specifications by the software designer.
    - Software that meets industry consensus design standards.
    - Quality software development life cycle processes, including independent verification and validation (IV&V) methodologies that provide assurance that the application software is adequately specified, designed, implemented, tested, and controlled.
    - Features such as fault tolerance, data validation and functional diversity of input sensors.
- The primary coolant pressure boundary and the ESFAS share no common elements. Further, a LOCA is highly unlikely to trigger a software failure in the ESFAS, because it is intentionally designed such that faults in the platform software cannot be triggered by plant transients and the application software algorithm is sufficiently simple and well analyzed and tested that unanticipated conditions are highly unlikely. Therefore, multiple barriers are in place to protect against the occurrence of a software CCF leading to the loss of a safety function:
    - A software error must be introduced into the digital ESFAS.
    - The software error must be capable of disabling the ESFAS from successfully actuating its safety systems.
    - Plant conditions must occur that were not anticipated as a part of the analysis of the accident.
    - The unanticipated plant conditions must be capable triggering the software error.

The low potential for the large and medium LOCAs, the expected high reliability of the ESFAS and the independence of the reactor coolant pressure boundary from the ESFAS combine to provide adequate defense-in-depth against the simultaneous failure of the digital system during the LOCA were it to occur.

That the proposed automated DAS should result in greater risk than it addresses is a result of the differences in the frequencies of spurious operation as opposed to the large LOCA events for which the DAS is intended. In an attempt to address risk for an initiating event (large/medium LOCA) that is not expected to occur in any plant over the life of the entire fleet, the proposed automated DAS may result in an inadvertent trip of a plant somewhere in the fleet once every several years. Unless it can be shown that the proposed automated DAS has essentially no possibility to cause a plant trip were it to spuriously actuate, the proposed automated DAS appears to have a negative impact on safety.

Table 4-1 Benefits and Risks Associated with the Proposed Automated DAS (BWRs)

				BWR 2	BWR 3	BWR 4	BWR 5	BWR 6
IE	IE Frequency NUREG/CR-1829	Time to 2200°F	HEP	CDF resulting from digital CCF (P_{CCF} ~ 1E-4/dem)				
Large LOCA	1.5E-05yr	<30m		1.5E-09/yr				
Sm/Med LOCA	6.0E-04/yr	>30m	4E-3	2.4E-10/yr				
Med/Large SLB outside cont	1.0E-04/yr	>30m	4E-3	4E-11/yr				
Total CDF				**1.7E-09/yr**				

		BWR 2	BWR 3	BWR 4	BWR 5	BWR 6
		Offsite Consequences				
Conditional Large Early Release Probability		0.15	0.02	0.21	0.22	0.01
Person Rem (Large Early)		1.5E+06	3.0E+05	6.5E+05	2.5E+06	8.4E+05[2]
Dose (person-rem/yr)		3.83E-04	1.02E-05	2.32E-04	9.35E-04	1.5E-05
Present Value (@ $2000/person-rem)		**$8**	**$0.2**	**$5**	**$20**	**$.3**

		BWR 2	BWR 3	BWR 4	BWR 5	BWR 6
		CCDP by plant type				
MSIV Closure		2.6E-06	3.9E-06	6.0E-06	1.4E-06	1.8E-06
General Trans		7.0E-07	1.1E-06	1.6E-06	7.0E-07	7.6E-07

	IE Frequency NUREG/CR-6928 LERs		BWR 2	BWR 3	BWR 4	BWR 5	BWR 6
			Spurious DAS CDF (per year) by plant type				
Spurious MSIV	0.0024/year		6.24E-09	9.36E-09	1.44E-08	3.36E-09	4.32E-09
Spurious Rx Trip	0.0024/year		-[1]	2.64E-09	3.84E-09	1.68E-09	1.82E-09
Total CDF			**6.24E-09**	**1.20E-08**	**1.82E-08**	**5.04E-09**	**6.14E-09**

[1] While it may result in a cold water addition transient, DAS initiation of ECCS for this plant is not expected to trip or isolate systems that would result in a plant trip (see Table B.4-1).

[2] Scaled based on BWR 4 site characteristics and core inventory.

Table 4-2 Benefits and Risks Associated with the Proposed Automated DAS (PWRs)

				W 2 loop	W 4 loop	CE #1	CE #2	B&W
IE	IE Frequency NUREG/CR-1829	Time to 2200°F	HEP	CDF resulting from digital CCF (P_{CCF} ~ 1E-4/dem)				
Large LOCA	2.8E-05/yr	-		2.8E-09				
Total				**2.8E-09**				

	Offsite Consequences				
Conditional Large Early Release Probability	0.01	0.014	0.01	0.008	0.01
Person Rem (Large Early Release)	3.4E+06	3.1E+05	2.4E+06	6.2E+06	1.0E+06
Dose (person-rem/yr)	9.86E-05	1.26E-05	6.72E-05	1.44E-04	2.90E-05
Present Value (@ $2000/person-rem)	**$2**	**$0.3**	**$1**	**$3**	**$0.6**

		CCDP by plant type				
General Trans		1.5E-06	3.2E-07	2.8E-06	1.8E-06	1.3E-06
LOFW		1.3E-06	5.8E-06	5.0E-06	1.8E-06	4.0E-06
Spurious SI		-	-	2.1E-05	-	3.1E-05

	IE Frequency NUREG/CR-6928 LERs		Spurious DAS CDF (per year) by plant type				
Spurious SI	0.0024/year		- [1]	- [1]	1.2E-08	4.32E-09	- [1]
Spurious SGI	0.0024/year		3.12E-09	1.39E-08	5.0E-08	4.32E-09	9.6E-09
Total			**3.12E-09**	**1.39E-08**	**6.2E-08**	**8.64E-09**	**9.6E-09**

[1] DAS initiation of only low pressure injection systems for these plants is not expected to result in trip or isolation of systems that would result in a plant trip (see Tables B.4-6, 7 and 10).

5 Sensitivity Studies and Uncertainty Analyses

The risks and benefits of the proposed automated DAS are now examined to determine the sensitivity of the results of the evaluation to a number of the assumptions made in the analysis. Included in this section is a discussion of parametric, modeling and completeness uncertainties and their effects on the results presented in Section 4. Also included is an evaluation of a proposal to eliminate inconsistencies between BTP-19 and other regulatory requirements directed at addressing the risks of CCF (e.g., the ATWS Rule).

The outcome of these sensitivity studies is that the conclusions of the analysis remain unchanged over wide ranges of probabilities and assumptions. That is, the defense-in-depth provided between the initiating events for which the automated DAS is being proposed and the ESFAS is sufficient to manage risk at an acceptably low level even without the proposed automated DAS.

5.1 PARAMETRIC UNCERTAINTIES

Three variables define the benefits of the proposed automated DAS from a core damage perspective, the frequency of the large LOCA, the failure probability of the ESFAS and operator action to initiate the ECCS (where credited in the analysis). Two remaining variables, conditional containment failure probability and offsite dose, define the benefits of the automated DAS given core damage. The sensitivity of the results presented in Section 4 to each variable was assessed.

5.1.1 Effect of assumptions regarding LOCA frequency

The mean and distribution assumed for these variables as described in Sections 4.1 are as follows

BWR (>6" effective break size)

Mean	1.5E-05/year
Upper bound (95%)	5.7E-05/year
Lower bound (5%)	1.9E-07/year

PWR (>4" effective break size)

Mean	2.6E-05/year
Upper bound (95%)	1.0E-04/year
Lower bound (5%)	3.4E-07/year

P_{ESFAS}

Mean	1E-4
EF	10

Setting the LOCA frequencies to their upper bounds yields the following benefits associated with the proposed automated DAS:

BWR (upper bound DAS benefits – CDF) = 5.7E-09/year
PWR (upper bound DAS benefits – CDF) = 1.0E-08/year.

Both upper bounds are several orders of magnitude below the threshold suggested in NUREG/BR-0058 for screening changes to generic licensing guidance and requirements. When combined with the offsite consequences, the margin to NUREG/CR-0058 criteria is even greater.

5.1.2 Effect of assumed ESFAS failure probability

With respect to P_{ESFAS}, the mean and error factor are not based on a particular digital system design. Rather, a probability of failure based on meeting consensus process standards is assumed (10^{-4}/demand). To assess the sensitivity of the CDF to this variable, an estimate of how much the assumed failure probability would need to increase to reach the screening value of NUREG/BR-0058.

P_{ESFAS} (BWR CDF value-impact screening value, 1E-6/year) = 0.06
P_{ESFAS} (PWR CDF value-impact screening value, 1E-5/year) = 0.4

The above values suggest that the digital ESFAS must be orders of magnitude less reliable than comparable analog systems before the value-impact screening criteria would be met. When considering offsite consequences, an even greater failure probability is required to reach the screening value in NUREG/CR-0058. It is expected that the ESFAS for actuation of the ECCS during LOCAs is significantly more reliable than that needed to justify the proposed automated DAS.

5.1.3 Effect of assumptions regarding operator action to initiate ESFAS

Credit for operator action as a backup means to initiate safety systems in addition to the ESFAS and the proposed DAS was limited to the BWRs, and then only if 30 minutes or more was available for this action. (While it may be possible for the operators to initiate the ECCS within 10 to 15 minutes for some events, such action in less than 30 minutes was not credited in this analysis). A prompting alarm was assumed that provides additional assurance of directing the operator to appropriate actions within the symptom oriented EOPs. A sensitivity of the results to this prompting alarm was performed with the results shown below.

The distribution of risk changes if no credit is given for the prompting alarm. The accident sequences that now benefit most from the proposed automated DAS are the small LOCAs (or those LOCA initiators having more than 30 minutes available for the operator to take action and for which the ISG does not suggest that the proposed automated DAS is needed). The reason the benefit is greatest for the more slowly evolving events is due simply to their frequency of occurrence as compared to the larger LOCAs. Even considering this redistribution in benefits, the proposed automated DAS remains well below any acceptance criteria with respect to the value-impact of the DAS. In addition, when comparing the benefits to the risks introduced by the DAS, the proposed automated DAS remains break even to slightly negative in terms of its net effect on safety.

5.1.4 Uncertainty analysis of benefits

Tables 4-1 and 4-2 indicated that the benefits associated with the proposed automated DAS were relatively small. To assess the likelihood that the benefits meet the NRC's cost-benefit criteria, an uncertainty analysis was performed for one of the PWRs (CE#2). As credit for operator action was not taken for the PWRs, the benefits are defined by the following expression:

$$Benefit_{DAS} = \Sigma F_{LOCAi} * P_{ESFAS.}$$

The results of this uncertainty analysis are shown in Figure 5-1. It is noted that virtually the entire distribution associated with the benefits of the DAS falls well below a CDF of 1E-7/year. This suggests that only a small fraction of a percent would meet the NRC's threshold for cost benefit as presented in NUREG/BR-0058 (see Attachment E).

That the benefits of the proposed automated DAS are substantially below suggested acceptance criteria is due to the rarity of the events for which the DAS would be of benefit, the reliability of mitigating systems in response to those events and the independence of the mitigating systems with respect to the initiating events. An uncertainty analysis in terms of offsite dose consequences has even greater margin on published acceptance criteria.

An additional sensitivity study is performed on the distribution assumed for the ESFAS (EF =

				BWR 2	BWR 3	BWR 4	BWR 5	BWR 6
IE	IE Frequency NUREG/CR-1829	Time to 2200°F	HEP	CDF resulting from digital CCF (P_{CCF} ~ 1E-4/dem)				
Large LOCA	1.5E-05yr	<30m		1.5E-09/yr				
Sm/Med LOCA	6.0E-04/yr	>30m	0.17	1.0E-08/yr				
Med/Large SLB outside cont	1.0E-04/yr	>30m	0.17	1.7E-09/yr				
Total CDF				**1.3E-08/yr**				

10). The error factor is raised to factor of 100 as an estimate of significant uncertainty in knowledge of the probability of a digital CCF and is reduced to 1.0 to estimate the impact of pursuing precision in the knowledge of the probability of a digital CCF. Varying the uncertainty

of P_{ESFAS} over a wide range in this manner has little effect on the results suggesting that the assumed distribution and its uncertainty play little role in determining the outcome of this application. The reason that the benefits of the proposed automated DAS is so insensitive to the uncertainty in the failure probability of the ESFAS is because of the defense-in-depth that already exists between the initiating events for which the DAS is being proposed and the ESFAS and its mitigating systems, resulting in the need for multiple independent failures to exist before a software CCF would result in the loss of the safety function initiated by the ESFAS.

5.1.5 Uncertainty analysis of net benefits

Tables 4-1 and 4-2 indicated that the risks introduced by the proposed automated DAS were a factor of 2 to 10 greater than the expected benefits. To assess the likelihood that the automated DAS could achieve a net benefit with respect to safety, an uncertainty analysis was performed. The difference between the benefits and risks associated with the DAS was examined using the following expression. It is desirable that this difference be positive. When it is not, it is worthwhile knowing how much of the benefit and risk profiles overlap or, in other words, what is the likelihood that the proposed automated DAS has a positive or negative impact on safety.

$$Diff_{Benefit\text{-}Risk} = (\Sigma F_{LOCAi} * P_{ESFAS} * P_{OPi}) - (F_{SpurDAS} * CCDP_{SpurDAS})$$

where

$Diff_{Benefit\text{-}Risk}$ – Net benefits for the proposed automated DAS (person-rem/year)_
F_{LOCAi} – LOCA frequency for break range i (Section 4.1.1 – 1/year)
P_{ESFAS} – the probability of failure of the digital ESFAS for which the proposed automated DAS is being provided as a backup (Section 4.1.2)
P_{OPi} – operator action to initiate ESFAS probability of failure, if applicable (Section 4.1.3)
$F_{SpurDAS}$ – frequency of plant trips resulting from spurious operation of the DAS (Section 4.1.4 – 1/year)
$CCDP_{SpurDAS}$ – conditional core damage probability for accident sequences resulting from spurious operation of the DAS (Attachment B.4).

Figure 5-2 presents the results of this uncertainty analysis performed for one of the PWRs (CE#2). The mean of the difference between benefits and risks is similar to the point estimate shown in Table 4-2, but still negative. Break even, in terms of benefits vs. risks, is shown at zero in the figure. The top plot in Figure 5-2 assumes that the spurious operation of the proposed automated DAS is not likely to be caused by sensors, as multiple diverse signals would be used in its actuation. The lower plot in the figure is a sensitivity analysis assuming that the proposed automated DAS is actuated on the same plant conditions as ESFAS (see Section 5.2.1 for additional information on this sensitivity analysis).

The probability that the proposed automated DAS has a positive impact on safety is roughly 40% and is shown on the right side of the top plot in Figure 5-2. Should the DAS be actuated in a manner similar to ESFAS, the lower plot suggests that there is only a 10% chance that it will have a positive impact on safety.

Efforts made by the industry to eliminate test and calibration activities from causing plant trips and the combinations of sensor inputs assumed in this analysis needed to initiate the DAS are effective in keeping the potential for spurious plants low. However, they are insufficient to assure that the proposed automated DAS has a positive impact on safety.

5.2 MODELING UNCERTAINTIES

In this section, two types of modeling uncertainties are evaluated; the manner in which the proposed automated DAS is actuated and the manner in which digital ESFAS failure modes are modeled.

5.2.1 Assumptions regarding DAS actuation

Section 4 evaluated the benefits and risks associated with an automated DAS for which a relatively significant effort had been made to preclude spurious operation and its effects. This effort involved limiting the actuation of equipment to only that which was needed in response to a large LOCA. Also, multiple and diverse signals were assumed to be required to initiate the proposed automated DAS (e.g., low reactor level and high containment pressure for BWRs) so as to assure that the system operated only in an actual event requiring its operation.

It is recognized that these efforts to reduce the impact of spurious operation may also reduce its benefits. The sensitivity studies in this section examine two possible changes to the manner in which the proposed automated DAS operates; expanding the systems actuated by the DAS to address the full spectrum of LOCAs (i.e, actuate both high and low pressure safety injection in PWRs) and initiate the DAS on the same signals as ESFAS (i.e., low reactor level or high containment pressure in BWRs and low pressurizer pressure or high containment pressure in PWRs).

DAS actuation of high and low pressure injection systems

In Section 3.1.1, it was noted that both high and low pressure systems were assumed to require the proposed automated DAS in order to meet the ISG for BWRs. PWRs, on the other hand, needed only to automate the actuation of low pressure safety injection for large LOCAs due to the availability of accumulators in extending the time available to initiate safety injection for smaller breaks. As a result, this sensitivity study focuses on the benefits of automating both high and low pressure systems in PWRs.

Table 5-1 shows the results of this sensitivity study. All changes from the base case in Table 4-2 are noted in italics.

Added to the events that benefit from the proposed automated DAS are small/medium LOCA, SGTR and stuck open pressurizer SRVs. Given the time available for these events, the need for the proposed automated DAS requires failure of the ESFAS as well as the operators not being

able to initiate an injection system. The overall benefits roughly double, with SGTR and the stuck open SRV collectively being similar to the large LOCA in terms of risk avoided with the automated DAS. However, this is insufficient improvement in safety to justify the costs of the proposed automated DAS.

In the lower half of Table 5-1, the risks associated with the proposed automated DAS remain unchanged with the exception of one plant (B&W). Because the high head safety injection pumps have a shutoff head higher than the pressurizer SRVs, spurious operation of the DAS has the potential to challenge the SRVs, possibly leading to a stuck open SRV and small LOCA conditions. For plants with this characteristic, the net effect of providing the DAS for high pressure injection systems increases risk over limiting the DAS to actuation of only low pressure systems.

DAS actuation of high and low pressure injection systems

An assessment of the effects of actuating the proposed automated DAS on similar plant conditions that actuate the ESFAS is shown in Tables 5-2 (BWR) and 5-3 (PWR).

For BWRs, the change in the manner in which the DAS is actuated has two effects; an increase in the events for which the DAS can provide backup actuation and an increase in the frequency of spurious actuation. Because the DAS would automatically actuate on reactor low level by itself, actuation could occur for many transient events as well as for the LOCAs. The upper half of Table 5-2 shows the additional events in italics for one plant (BWR4). The total benefits from such a DAS increase by a factor of 50, virtually all of the increase being a result of transients such as loss of the main condenser and loss of offsite power. It should be noted that these events have significantly longer for the operator to initiate a makeup system than the 30 minutes being credited in this analysis (with 45 minutes to an hour available on a transient with loss of all injection, HEPs an order of magnitude lower than being assumed in this analysis are common). This increase, however, remains insufficient to conclude that the benefits of the proposed automated DAS can be justified in light of their costs. Further offsetting these benefits, the risks associated with spurious operation of the DAS also rise for BWRs. The lower half of Table 5-2 shows an increase in risk that is within a factor of two of the increase in benefits. With this additional risk, the net benefits of the proposed automated DAS are slightly positive, but essentially break even.

For PWRs, there appear to be no additional benefits associated with making the proposed automated DAS actuate on signals similar to the ESFAS. Because the shutoff head of low pressure injection is below that which would exist for all but the large LOCA (as defined in this analysis), only the large LOCA benefits from the system. However, the potential for spurious operation of the DAS rises if the method of actuation is made similar to the ESFAS. This increase in risk is shown in the lower half of Table 5-3. For PWRs, modifying the actuation signals for the proposed automated DAS to be similar to that for the ESFAS would appear to result in even a larger negative effect on safety than suggested in Table 4-2.

5.2.2 Modeling uncertainties related to failure modes

A potential additional source of uncertainty regarding the conclusions of this analysis is the nature of the failure modes associated with the ESFAS.

It should be understood that the ESFAS, by itself, does little to mitigate an accident. What mitigates the accident are the mechanical and electrical equipment actuated by the ESFAS that are a part of the mitigating systems credited in response to the accident (e.g., pumps, valves, buses, breakers, etc.). The failure modes associated with these mechanical and electrical components are known and well understood. The combinations of these components and the failure modes that we wish to avoid are modeled in detail in the PRA.

For the purpose of this analysis, it has been assumed that the most limiting failure modes of the equipment credited in the PRA are the principal effects of the failure of the ESFAS. For example, either the low pressure injection pumps fail to start or the injection valves to the reactor fail to open. This essentially results in a complete loss of the reactor makeup function following the postulated LOCA. Partial, intermittent or delayed operation of these systems reduce the consequences of the accident as assessed in this analysis.

A further assumption is made in this analysis that the injection function is permanently disabled and cannot be recovered, thus resulting in long term penetration of the lower vessel head and the challenges to the containment associated with an ex-vessel core melt scenario. In fact, the cause of the loss of injection, the ESFAS, is one of the more easily recoverable failures. Although manual actuation of injection may be delayed, more likely scenarios associated with failure of the ESFAS are those in which recovery within the vessel is possible.

By examining the failure modes of the equipment actuated by the ESFAS, modeling uncertainties associated with the failure of the ESFAS have been bounded.

5.3 COMPLETENESS UNCERTAINTY

Completeness uncertainty is a reflection of scope limitations. The scope of this evaluation is examined to assess its completeness with respect to 1) events in the plant design basis, 2) events that could benefit from the proposed automated DAS beyond those suggested in the ISG, 3) events in the PRA beyond those considered in the internal events analysis and 4) additional economic consequences associated with the DAS.

Design Basis Events vs. PRA

The scope of BTP-19 and the ISGs are limited to design basis events. Table 5-4 provides a listing of design basis events typically evaluated in PWR and BWR safety analyses[12]. To assure completeness of this evaluation, the table identifies the PRA internal event initiators that are representative of plant response for each event in the safety analysis. Each of the design basis events can be categorized under one of the initiating events in the internal events PRA. In addition, the PRA considers the potential for multiple failures beyond just the initiating event

and the coincident CCF. It is concluded that the PRA not only encompasses the events considered in BTP-19 and related ISGs, but is broader in scope.

Benefits beyond those in the ISG

It was recognized that the proposed automated DAS could have effects beyond just those events suggested in the ISG. For the purpose of addressing this uncertainty, the following were considered in determining the benefits and risks of the proposed automated DAS, making the analysis as complete or even more so than the ISG.

- The range of break sizes defined as part of the large LOCA was expanded well beyond that typically considered in plant specific PRAs,
- The benefits of the proposed automated DAS were considered for non-LOCA events such as steam line breaks outside containment, stuck open SRVs, transient induced events and ATWS. Where the automated DAS was expected to have no effect, a deterministic basis was provided. Any beneficial effects were taken into account, even if not required to meet the ISG.
- Possible negative effects were considered in the form of additional plant trips that may be introduced with the installation of the proposed automated DAS.

External events and shutdown operation

Additional completeness questions could arise as a result of external events. It should be noted, however, that the proposed automated DAS is intended only for those events for which there is limited time for operator action, such as the large LOCA. Seismic events are part of the design basis for the primary coolant pressure boundary and seismic PRAs generally show a low potential for small pipe breaks as a result of a seismic event, much less a large LOCA. Other initiators, such as winds, tornadoes, missiles and internal fires are not expected to lead to large/medium LOCA type conditions under which the proposed automated DAS would be of benefit.

Finally, shutdown conditions are such that ESFAS (and likely the proposed automated DAS) is generally disabled during such operations. In addition, these conditions are not generally included as a part of the design basis and the proposed automated DAS would not be required to meet the ISG. The relatively low decay heat loads and slowly evolving nature of events associated with shutdown operation likely would also provide ample time for operator action during risk significant events.

Offsite and onsite economic benefits

In examining the consequences of accident sequences which may benefit from the proposed automated DAS, core damage frequency, large early release frequency and offsite dose consequences were used as figures of merit. In fact there are other consequences which could be addressed by the proposed DAS including intermediate to late releases, smaller releases, offsite economic consequences and on-site decontamination and cleanup costs. Table 5-5 modifies the consequence related information for several of the plants from Tables 4-1 and 4-2 to include consideration of these additional benefits. The conditional containment failure probabilities now

include scenarios in which containment over pressure, basemat penetration and other long term failure modes occur. Offsite economic consequences and accident cleanup costs are also included. Estimates for these were obtained from the information provided in the SAMA evaluations for each plant. The dose consequences, however, have been left at the large early release values, making them bounding. It can be seen from Table 5-5 that benefits are now dominated by offsite economics and cleanup costs. Even though bounding values were used, the offsite dose consequences do not dominate the results. Even so, the additional benefits provided by the proposed automated DAS in the form of avoided economic costs remain several orders of magnitude less than needed to justify the costs.

5.4 REGULATORY INCONSISTENCIES

It was noted earlier that the only current staff position directed at addressing CCF that results in the need for an automated DAS is 10CFR50.62 (the ATWS Rule)[13]. BTP-19 and the digital I&C ISGs have a similar objective in that they are intended to address the effects of CCFs, in this case from potential software errors. However, the staff positions contained in the ISGs expand the scope of automated diverse actuation systems to well beyond the collection of transients considered in the ATWS Rule. The obvious question is why is the ATWS Rule limited to anticipated transients whereas BTP-19 and the ISGs consider a much broader scope of events that include accident initiators (e.g., LOCAs)?

A review of the Statements of Consideration for the ATWS Rule[14] reveals that the Commission based the rule on the NRC's evaluation of ATWS risk[15] and the Utility Group on ATWS's evaluation[16] of proposed modifications to address ATWS. In the NRC's evaluation, an overall objective of achieving a core damage frequency due to ATWS of 10^{-6}.year was proposed. In its evaluation, the Utility Group on ATWS states that their proposed modifications were "straightforward and well understood by the industry and the staff…Most important of all, the proposed modifications clearly decrease the risk of ATWS without simultaneously increasing other, competing risks."

It cannot be concluded that the proposed automated DAS suggested by the digital I&C ISGs clearly decreases risk. Further, there are aspects of the proposed automated DAS that are not at all straightforward or well understood (e.g., load sequencing), particularly for current plant upgrades. Given the apparent benefits of the ATWS Rule, it is worthwhile examining the effect on risk were BTP-19 and the digital I&C ISGs assigned a similar scope.

To evaluate this proposal, the PRAs for one of the BWRs and one of the PWRs in this study were modified as though a digital upgrade of the ESFAS was to be performed, directed at ECCS actuation. The existing ESFAS analog logic was removed while retaining the sensors that initiate the ECCS. An event representing software CCF of the ESFAS logic was incorporated into the models in a way that all ECCS systems would be disabled were it to occur (i.e., all high and low pressure injection systems). Key assumptions and results of the analysis are as follows.

- The digital CCF (P_{ESFAS}) is assumed to be 10^{-4}/demand assuming the system meets existing process standards (see Section 4.1.2).

- The digital CCF is applied to the automatic actuation of high and low pressure injection systems.
- Credit for operator action to initiate the ECCS is taken only if 30 minutes or more is available to accomplish this action (no credit is taken for operator action to initiate the ECCS for the large or medium LOCA).
- BWR loss of main condenser and general transient frequencies are raised 0.0024/yr assuming an automated DAS is provided for large LOCA. PWR loss of feedwater frequency is raised 0.0048/yr assuming the automated DAS. (see Section 4.1.4).

Plant	Baseline CDF	CDF (current BTP-19 and ISG scope)	CDF (BTP-19 scope similar to ATWS Rule)
BWR 4	1.438E-5/yr	1.444E-5/yr	1.438E-5/yr
CE #2	2.68E-5/yr	2.60E-5/yr	2.55E-5/yr

The results suggest that replacement of the current relatively detailed ESFAS logic with the software CCF and the proposed automated DAS for large LOCA reduces CDF slightly for the PWR. Even with the introduction of an ECCS wide software CCF, there is a slight improvement in risk. For the BWR, however, the reduction in LOCA CDF does not completely offset the effects of spurious operation of the DAS. Both plants show a reduction in CDF when the LOCAs are eliminated from the scope of the BTP-19 D3 evaluation. The replacement of the analog logic with the digital CCF (this time without the proposed automated DAS) eliminates the increase in transient frequency due to spurious operation of the DAS, keeping the CDF it near its original value (BWR) or showing a slight improvement (PWR).

For the BWR, changing the scope of BTP-19 to make it consistent with the ATWS rule appears to be roughly break even. That is, the increase in risk for the large, medium and small LOCAs without the proposed automated DAS is offset by the reduction in risk that would be realized by avoiding plant trips from spurious operation of the DAS.

For the PWR, making the scope of BTP-19 consistent with the ATWS Rule appears to reduce risk slightly. That is, the expected risk resulting from spurious plant trips exceeds the benefits that would be realized were the rarest design basis events required to be provided with an automated DAS. That the PWR shows a larger benefit from making the scope of BTP-19 consistent with the ATWS Rule is due to the fact that only low pressure injection systems would require the proposed automated DAS to meet the ISGs. In the BWR, it is being assumed that both high and low pressure injection systems would require the DAS.

Table 5-1 Effects of Automated DAS for Both High and Low Pressure Injection (PWRs)

				W 2 loop	W 4 loop	CE #1	CE #2	B&W
IE	IE Frequency NUREG/CR-1829	Time to 2200°F	HEP	CDF resulting from digital CCF (P_{CCF} ~ 1E-4/dem)				
Large LOCA	2.8E-05/yr	-		2.8E-09				
Small/med LOCA	*5.8E-04/yr*	*>30m*	*4E-3*	*2.3E-10*				
SGTR	*3.5E-03/yr*	*>30m*	*4E-3*	*1.4E-09*				
SORV	*2.9E-03/yr*	*>30m*	*4E-3*	*1.2E-09*				
Total				***5.6E-09***				

	Offsite Consequences				
Conditional Large Early Release Probability	0.01	0.014	0.01	0.008	0.01
Person Rem (Large Early Release)	3.4E+06	3.1E+05	2.4E+06	6.2E+06	1.0E+06
Dose (person-rem/yr)	*1.9E-04*	*2.4E-05*	*1.3E-04*	*2.8E-4*	*5.6E-05*
Present Value (@ $2000/person-rem)	***$4***	***$0.5***	***$3***	***$6***	***$1***

		CCDP by plant type				
General Trans		1.5E-06	3.2E-07	2.8E-06	1.8E-06	1.3E-06
LOFW		1.3E-06	5.8E-06	5.0E-06	1.8E-06	4.0E-06
Spurious SI		-	-	2.1E-05	-	3.1E-05

	IE Frequency NUREG/CR-6928 LERs						
			Spurious DAS CDF (per year) by plant type				
Spurious SI	0.0024/year		-	-	1.2E-08	4.32E-09	*7.4E-8*
Spurious SGI	0.0024/year		3.12E-09	1.39E-08	5.0E-08	4.32E-09	9.6E-09
Total			**3.12E-09**	**1.39E-08**	**6.2E-08**	**8.64E-09**	***8.4E-08***

Table 5-2 Automated DAS Actuation Similar to ESFAS (BWR)

IE	IE Frequency NUREG/CR-1829, NUREG/CR-6928	Time to 2200°F	HEP	BWR 4 CDF resulting from digital CCF (P_{CCF} ~ 1E-4/dem)
Large LOCA	1.5E-05yr	<30m		1.50E-09
Sm/Med LOCA	6.0E-04/yr	>30m	4E-3	2.40E-10
Med/Large SLB outside cont	1.0E-04/yr	>30m	4E-3	4.00E-11
Tran w/ PCS	*0.83 * 1.2E-2*	*>30m*	*4E-3*	*3.98E-09*
Tran w/o PCS	*0.20*	*>30m*	*4E-3*	*8.00E-08*
Loss of OSP	*0.036*	*>30m*	*4E-3*	*1.44E-08*
Loss of IA	*0.010*	*>30m*	*4E-3*	*4.00E-09*
SORV	*0.022 * 3.3E-2*	*>30m*	*4E-3*	*2.90E-10*
Loss of AC bus	*8.8E-3 * 0.11*	*>30m*	*4E-3*	*3.87E-10*
Loss of DC bus	*1.2E-3 * 0.13*	*>30m*	*4E-3*	*6.24E-11*
Loss of SW	*3.9E-4*	*>30m*	*4E-3*	*1.56E-10*
Loss of TBCCW	*3.9E-4*	*>30m*	*4E-3*	*1.56E-10*
Loss of RBCCW	*3.9E-4 * 1.0E-2*	*>30m*	*4E-3*	*1.56E-12*
Total CDF				***1.05E-07***

		Offsite Consequences
Conditional LERP		0.21
Person Rem		6.5E+05
Total Dose (person-rem/yr)		1.4E-02
Present Value (@ $2000/person-rem)		**$308**

		CCDP by plant type
MSIV Closure		6.0E-06
General Trans		1.6E-06

	IE Frequency NUREG/CR-6928 LERs		Spurious DAS CDF (per year) by plant type
Spurious MSIV	*0.009/year*		*5.4E-08*
Spurious Rx Trip	*0.009/year*		*1.4E-08*
Total CDF			***6.8E-08***

Table 5-3 Automated DAS Actuation Similar to ESFAS (PWR)

				W 2 loop	W 4 loop	CE #1	CE #2	B&W
IE	IE Frequency NUREG/CR-1829	Time to 2200°F	HEP	CDF resulting from digital CCF (P_{CCF} ~ 1E-4/dem)				
Large LOCA	2.8E-05/yr	-		2.8E-09				
Total				**2.8E-09**				

	Offsite Consequences				
Conditional Large Early Release Probability	0.01	0.014	0.01	0.008	0.01
Person Rem (Large Early Release)	3.4E+06	3.1E+05	2.4E+06	6.2E+06	1.0E+06
Dose (person-rem/yr)	9.86E-05	1.26E-05	6.72E-05	1.44E-04	2.90E-05
Present Value (@ $2000/person-rem)	**$2**	**$0.3**	**$1**	**$3**	**$0.6**

		CCDP by plant type				
General Trans		1.5E-06	3.2E-07	2.8E-06	1.8E-06	1.3E-06
LOFW		1.3E-06	5.8E-06	5.0E-06	1.8E-06	4.0E-06
Spurious SI		-	-	2.1E-05	-	3.1E-05

	IE Frequency NUREG/CR-6928 LERs		Spurious DAS CDF (per year) by plant type				
Spurious SI	*0.009/year*		*-*	*-*	*1.89E-07*	*1.62E-08*	*-*
Spurious SGI	*0.009/year*		*1.35E-08*	*5.22E-08*	*4.50E-08*	*1.62E-08*	*3.60E-08*
Total			***1.35E-08***	***5.22E-08***	***2.34E-07***	***3.24E-08***	***3.60E-08***

Table 5-4 Safety Analysis Transients and Accidents

PWR

Event	*Category*	*PRA Initiating Event*
Decrease in feedwater temperature Increase in feedwater flow Increase in steam flow	AOO	Turbine trip
Inadvertent opening of a SG relief or SRV	AOO	SLB outside containment
Steam system piping failure inside and outside containment	Accident	SLB inside cont SLB outside cont
Loss of external load Turbine trip Loss of condenser vacuum Steam pressure regulator failure	AOO	Turbine trip
Loss of normal feedwater flow	AOO	Loss of feedwater
Feedwater system pipe breaks inside and outside containment	Accident	FWLB inside cont FWLB outside cont
Loss of forced reactor coolant flow RCP rotor seizure or shaft break	AOO	Turbine trip
Uncontrolled rod withdrawal Control rod misoperation	AOO	Turbine trip
Decrease in boron concentration	AOO	Turbine trip
Inadvertent loading of fuel assembly	AOO	NA
Rod ejection	Accident	Small LOCA
Inadvertent ECCS	AOO	Turbine trip Loss of feedwater or Spurious ESFAS
Inadvertent opening of pressurizer relief	AOO	Spurious pressurizer SRV

BWR

Event	*Category*	*PRA Initiating Event*
Decrease in feedwater temperature Increase in feedwater flow Increase in steam flow	AOO	Turbine trip
Loss of external load Turbine trip Steam pressure regulator failure	AOO	Turbine trip
Loss of condenser vacuum	AOO	Loss of condenser vacuum
MSIV closure	AOO	MSIV closure
Loss of normal feedwater flow	AOO	Loss of feedwater
Loss of forced reactor coolant flow RCP rotor seizure or shaft break	AOO	Turbine trip
Uncontrolled rod withdrawal Control rod misoperation	AOO	Turbine trip
Startup of an inactive recirc loop Flow controller malfunction	AOO	Turbine trip
Inadvertent loading of fuel assembly	AOO	NA
Rod drop	Accident	Turbine trip?
Inadvertent ECCS	AOO	Turbine trip or Spurious ESFAS
Inadvertent opening of SRV	AOO	Spurious SRV

Event	*Category*	*PRA Initiating Event*
Steam generator tube rupture	Accident	Steam generator tube rupture
Loss of coolant accidents	Accident	Large LOCA Medium LOCA Small LOCA
Anticipated Transient Without SCRAM	Accident	Anticipated transients and LOCAs

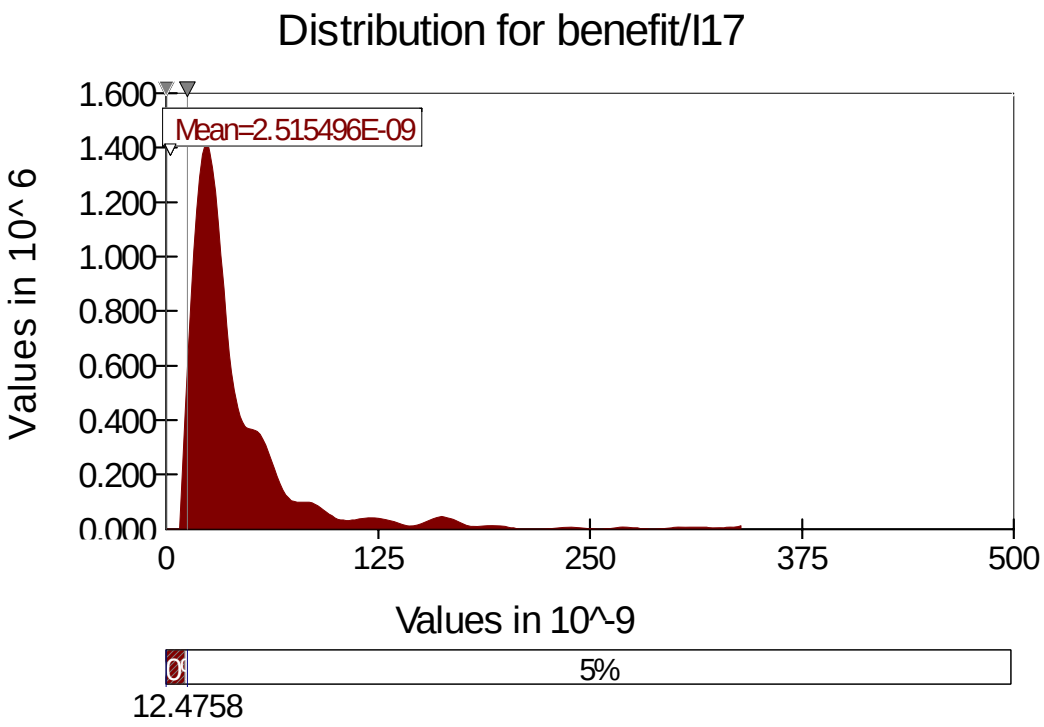
Event	*Category*	*PRA Initiating Event*
Main steam line failure outside containment	Accident	MSLB outside containment
Loss of coolant accidents	Accident	Large LOCA Medium LOCA Small LOCA
Anticipated Transient Without SCRAM	Accident	Anticipated transients and LOCAs

Table 5-5 Proposed Automated DAS - Consideration of Additional Offsite and Onsite Economic Consequences

	W 2loop	W 4loop	BWR3	BWR5
CDF (total[1] – 1/yr)	3.97E-05	3.16E-05	5.24E-05	6.17E-05
CDF (DAS seq – 1/yr)[2]	2.60E-09		1.70E-09	
CCFP[3] (total, all but small)	5.54E-02	1.16E-01	2.40E-01	3.00E-01
CCFP (DAS sequences)	4.81E-03	5.00E-02		
Avg Offsite Exp (total all seq – person rem)	1.03E+05	9.05E+04	7.25E+05	8.25E+05
LER Offsite Exp (person rem)[4]	3.40E+06	3.10E+05	4.10E+06	2.43E+06
$/person-rem[5]	$2,000			
annual discount rate	3%			
Offsite Exp (total)[6]	$88k	$86k	$817k	$1,100k
Offsite Econ (total)	$259k	$30k	$2,729k	$1,350k
Onsite Exp (total)	$15k	$18k	$17k	
Onsite Cleanup (total)	$461k	$581k	$529k	
Offsite Exp (DAS)[7,8]	$1	$1	$50	$37
Offsite Econ (DAS)	$68	$5	$700	$150
Onsite Exp (DAS)	$1	$2	$1	
Onsite Econ (DAS)	$42	$48	$10	
Total DAS value-impact	**$110**	**$75**	**$760**	**$190**

[1] Values labeled 'total' are developed from each plant's respective SAMA evaluation.
[2] CDF – core damage frequency avoided by the DAS from Tables 4-1 and 4-2.
[3] CCFP – conditional containment failure probability, all releases except small, includes intermediate and late releases – PWR DAS related CCFP from SAMA eliminating ISLOCA & SGTR, BWR DAS related CCFP assumed to be the same as for all sequences given the magnitude.
[4] LER – large early release offsite exposure magnitude (person-rem) from Attachment D.4.
[5] $/person-rem applies only to offsite exposure economic consequences.
[6] Offsite and onsite economic consequences as reported in each plant's respective SAMA evaluation (which used a 7% annual discount rate in each case).
[7] DAS sequence related offsite exposure scales the SAMA offsite exposure by the ratios of the CDF, CCFP and offsite exposures (DAS/total).
[8] Offsite and onsite economic consequences scale the SAMA economic consequences by the ratio of the CDF (DAS/total).

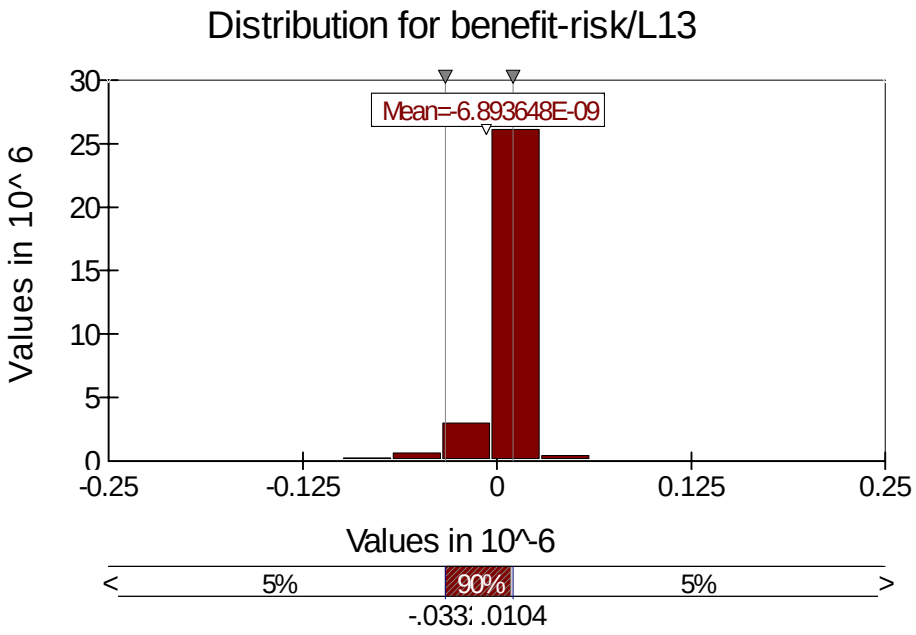
Figure 5-1 Automated DAS Benefits Uncertainty Analysis (CDF)



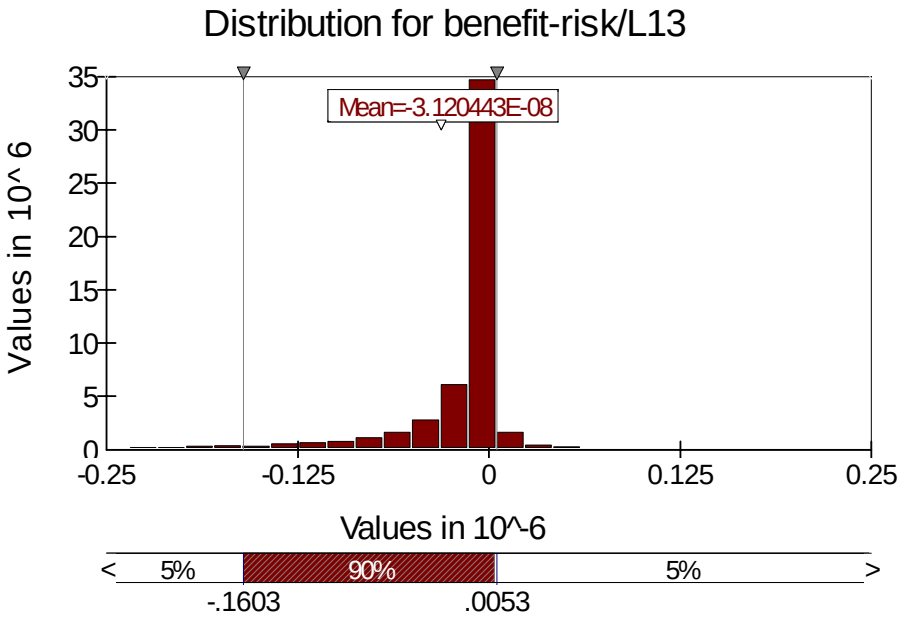
Uncertainty analysis is for PWR CE#2.

Acceptance criteria is 1E-5/year (NUREG/BR-0058).

Figure 5-2 Automated DAS Net Benefits Uncertainty Analysis (Benefits – Risk)



Spurious Operation due to Logic Only (PWR CE#2)



Spurious Operation due to Sensors and Logic (PWR CE#2)

6 Summary of Risk Insights

The NRC staff has proposed the need for an additional (in addition to ATWS) automated DAS for design basis events in which a software CCF occurs disabling the ESFAS. The proposed automated DAS is suggested for design basis events where there is less than 30 minutes available for the operators to initiate the safety systems normally actuated by the ESFAS. The preceding evaluation of the risks and benefits associated with the proposed automated DAS suggest that it accomplishes little from a safety perspective and, for some plants, may even have a negative impact on safety.

At the heart of the NRC staff's proposal for the automated DAS is the need to provide adequate defense-in-depth during design basis events in the presence of credible software CCFs. There are no formal staff positions requiring such an automated DAS in existing regulatory guidance (e.g., 10CFR50, BTP-19). Yet, in public meetings with the industry, the staff has expressed the desire to expand existing guidance to require an automated DAS for events such as a large LOCA.

To demonstrate that adequate defense-in-depth and diversity is being provided even in the absence of the proposed automated DAS, the technical reasons behind the results of the deterministic and probabilistic analyses of the preceding five sections are reviewed.

1. There are few transients or accidents for which an automated DAS is needed or for which there is not sufficient time for the operators to take appropriate action.

   For LOCA sizes where there may be insufficient time, the events are rare, e.g., the Large to Medium LOCA range. The reasons for the low frequency of these events are:
   - The reactor coolant pressure boundary is designed to prevent failures of this size through conformance with design requirements such as Section III of the ASME Boiler and Pressure Vessel Code and ANSI B31.1.
   - Periodic inspection of the reactor coolant pressure boundary is performed under Section XI of the ASME Boiler and Pressure Vessel Code.
   - Monitoring of the reactor coolant pressure boundary is performed routinely during reactor operation.

2. Digital RTS/ESFAS being designed and installed are highly reliable and are expected to be an improvement over existing analog systems. The reasons for the low potential for software CCF of these systems are the defensive measures that are typically taken in the design and operation of safety related digital systems. Examples include:
   - Cyclic system operation that is always active, with constant bus loading (processors and communications), operating system confined to well-tested trajectories that remain invariant during plant transients, etc. (see Reference 11 for more extensive list)

- Very simple application software.
- Quality software development life cycle processes, including independent verification and validation (IV&V) methodologies.
- Features such as fault tolerance, data validation and functional diversity of input sensors.
- Software that meets industry consensus design standards.

3. There are no common elements between the piping that is postulated to lead to the LOCA/SLB and the RTS/ESFAS. Therefore, the LOCA or SLB for which the proposed automated DAS may be beneficial and the postulated CCF of the mitigating systems necessarily would be a result of independent faults or errors.

Because of these design features, adequate defense-in-depth is provided by the reliability and independence of the plant equipment that may cause the initiating events for which the proposed automated DAS might be effective and the mitigating systems required to respond to these events. This existing defense-in-depth and reliability both limits the potential for the initiating events in question and ensures that the required mitigating systems are capable of performing their intended functions.

The defense-in-depth and diversity provided between the cause of the accidents (large and medium LOCA) and the mitigating systems (ECCS) meet the intent of existing SRP guidance. The basis for BTP-19 is provided in NUREG/CR-6303[17]. It is in this NUREG that the concept of echelons of defense is introduced as well as different types of CCF for which defense-in-depth is considered desirable. Considering the plant design in an integrated manner, the 'echelons' would be a part of defense-in-depth barriers that include all causes of initiating events, both hardware and I&C related events, and would consider the mitigating system hardware in addition to the I&C.

Defense-in-depth barriers (includes echelons of defense)	Purpose (from NUREG/CR-6303)
Initiating event systems and equipment (includes control systems and mechanical equipment that can cause plant trips)	Limit the potential for plant transients and accidents. Minimize challenges to mitigating systems. Function as a backup to mitigating systems.
Mitigating systems and equipment (includes RTS/ESFAS[i] and the mechanical and electrical systems that perform required safety functions, e.g., • Reactivity control • Heat removal	Respond to plant transients and accidents should they occur by accomplishing mitigating functions

[i] RTS and ESFAS are not considered to be 'concentric' echelons of defense in this analysis as might be implied in NUREG/CR-6303.

Defense-in-depth barriers (includes echelons of defense)	Purpose (from NUREG/CR-6303)
• Reactor inventory control • Containment control)	
Backup mitigating systems and equipment (includes diverse monitoring and indication as well as systems and equipment useful under beyond design basis conditions).	Provide independent and diverse indicators and controls for use by the operators for control of systems credited in the EOPs.

NUREG/CR-6303 expands on the intent of D3 evaluations in Guideline 12, "Diversity Among the Echelons of Defense", in which it states that diversity between the echelons is necessary and is a concern of the analysis. It further emphasizes that plant systems should be examined for potential interactions between the echelons of defense "with the intent of determining that the functions of at least two of the echelons are unimpaired by interactions".

For the large and medium LOCA range of breaks, this analysis demonstrates that two of the defense-in-depth barriers, which encompass the 'echelons of defense', have been shown to be protected from common failures, e.g., by limiting the potential for reactor coolant system failure and through mitigation of the accident with the ESFAS and the core cooling and containment systems it controls. Therefore, adequate defense-in-depth is being provided that meets the intent of D3 evaluations as stated in NUREG/CR-6303 even without the proposed automated DAS. For the staff to require still an additional automated diverse actuation system would expand the required level diversity to three independent systems (e.g., the reactor coolant system, ESFAS and the DAS), a degree of protection that is not found in any other existing regulatory guidance.

The conclusions of this evaluation were found to be insensitive to wide variations in the frequency of the LOCA that might benefit from the proposed automated DAS, the probability of the postulated CCF and modeling assumptions associated with the software failure modes. Finally, inconsistencies between the scope of BTP-19 and other regulatory requirements directed at addressing CCF (e.g., the ATWS Rule) were noted. An outcome of the analysis is a recommendation to modify the scope of BTP-19 to make it more consistent with the ATWS Rule. This change in scope would result in less complexity in the digital system design, fewer potential plant transients while possibly being accompanied by a small improvement in safety.

7 Conclusions

In digital I&C related ISGs, the US Nuclear Regulatory Commission has recently proposed to expand the use of diverse automated actuation systems to address software CCF to beyond that in existing regulatory guidance.

The analysis described in this report indicates that the proposed automated DAS has very little benefit and, for some plants, may have a negative impact on safety. The reasons are as follows:

- Defense-in-depth already exists in the plant design in the form of the independence between the initiating events for which the DAS is being proposed and the mitigating systems that are needed to respond to these events.
- The events for which the automated DAS is proposed (e.g., LOCA) are rare.
- The 1E actuation systems which must fail before the automated DAS would be called upon to operate are high in reliability.
- Transient initiators may be introduced by the proposed automated DAS at a frequency significantly greater than the events for which the DAS is intended to respond.

The conclusions of the study remain unchanged, over a broad range of assumptions with respect to the frequency of events for which the automated DAS is proposed, digital 1E actuation system reliability and CCF potential.

Because adequate defense-in-depth exists even without the proposed automated DAS, a final recommendation of the study is to consider modifying the scope of existing guidance to bring it into alignment with existing precedents and guidance that address the ability of the plants to cope with CCF (such as the ATWS Rule). Such a change in scope would result in less complexity in the plant I&C design and fewer potential plant transients, while possibly achieving a small improvement in safety.

8 References

1 Branch Technical Position HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems".

2 DI&C-ISG-02, Task Working Group #2, Defense-in-Depth and Diversity Issues, Interim Staff Guidance, Revision 1, September 26, 2008.

3 Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-informed Decisions on Plant-Specific Changes to the Licensing Basis", July 1998

4 NUREG-1806, Technical Basis for Revision of the Pressurized Thermal Shock (PTS) Screening Limit in the PTS Rule (10CFR50.61): Summary Report", May 24, 2006.

5 "Full Scale Station Blackout Test Conducted on an Advanced RCP Mechanical Seal", Nuclear Plant Journal, September-October 1988, Volume 6 No. 5

6 NUREG-1829, "Estimating Loss of Coolant (LOCA) Frequencies Through the Elicitation Process" (Draft), March 2005.

7 NUREG/CR-6928, "Industry Average Performance for Components and Initiating Events at U. S. Commercial Nuclear Power Plants", January 2007.

8 NUREG/CR-5750, "Rates of Initiating Events at U.S. Nuclear Power Plants 1987-1995", December 1998.

9 IEC 61226, "Nuclear Power Plants - Instrumentation and Control Systems Important for Safety - Classification", 1993.

10 NUREG/BR-0058, Revision 4, "Regulatory Analysis Guidelines of the U.S. Nuclear Regulatory Commission", August 2004.

11 EPRI, "Common Cause Failure Applicability", January 2008.

12 NUREG-0800, Standard Review Plan, Chapter 15.

13 10CFR50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants."

14 49FR20644, Statements of Consideration for the ATWS Rule, June 19, 1984.

15 NUREG-0460, "Anticipated Transient Without Scram for Light Water Reactors", April 1978.

16 SAI-011-82-Sj, Utility Group on ATWS, "Quantitative Evaluation of Industry Proposed Modifications Relative to Existing Plant ATWS Requirements", December 1981.

17 NUREG/CR-6303, "Method for Performing Defense-in-Depth and Diversity Analyses of Reactor Protection Systems."

A
DIVERSE ACTUATION STAFF POSITIONS AND ACCEPTANCE CRITERIA (BTP-19)

Point 1 The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed.

Point 2 In performing the assessment, the vendor or applicant/licensee should analyze each postulated common-cause failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate or SAR Chapter 15 analysis methods. The vendor or applicant/licensee should demonstrate adequate diversity within the design for each of these events.

Point 3 If a postulated common-cause failure could disable a safety function, a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-cause failure, should be required to perform either the same function as the safety system function that is vulnerable to common-cause failure or a different function that provides adequate protection. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

Point 4 A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3.

The D-in-D&D assessment submitted by the applicant/licensee should demonstrate compliance with the four-point position described above. To reach a conclusion of acceptability, the following four conclusions should be reached and supported by summation of the results of the analyses:

1. For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-mode failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary. The applicant/licensee should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.
2. For each postulated accident in the design basis occurring in conjunction with each single postulated common-mode failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits). The applicant/licensee should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.
3. When a failure of a common element or signal source shared between the control system and the RTS is postulated, and (1) this common-mode failure results in a plant response that requires reactor trip, and (2) the common-mode failure also impairs the trip function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the RTS function. The diverse means should ensure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary.

   When a failure of a common element or signal source shared between the control system and the ESFAS is postulated, and (1) this common-mode failure results in a plant response that requires ESF, and (2) the common-mode failure also impairs the ESF function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the ESF function. The diverse means should ensure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10% of the 10 CFR 100 guideline value, or violation of the integrity of the primary coolant pressure boundary.

   Interconnections between reactor trip and ESFAS (for interlocks providing for (1) reactor trip if certain ESFs are initiated, (2) ESF initiation when a reactor trip occurs, or (3) operating bypass functions) are permitted provided that it can be demonstrated that functions required by the ATWS rule (10 CFR 50.62) are not impaired.

4. No failure of monitoring or display systems should influence the functioning of the reactor trip system or the ESFAS. If plant monitoring system failure induces operators to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation, the analysis should demonstrate that such operator-induced transients will be compensated by protection system function.

B
THE PROPOSED AUTOMATED DAS AND THE PRINCIPLES OF RISK-INFORMED REGULATION

This evaluation examines the benefits and risks associated with the automated DAS proposed by the NRC staff in its digital I&C defense in depth and diversity ISG. The ISG proposes a new staff position that expands the scope of automated diverse actuation systems to accidents and transients analyzed in the design basis. Never the less, the principles of risk-informed regulation as defined in Regulatory Guide 1.174 are appropriate and have been implemented throughout the performance of the analysis.

Two of the five principles of risk-informed regulation are met by definition:

1) The proposed change meets the current regulations
3) The proposed change maintains sufficient safety margin

The risk-informed D3 evaluation addresses a beyond design basis issue in the form of digital CCF. The capability of the plant to cope with conditions associated with design basis events is not affected, and current regulations will therefore continue to be met. The plant continues to meet regulatory criteria with respect to the single failure criterion and diversity in response to ATWS. The plant still has features that address General Design Criteria with respect to protection system reliability, independence, and separation. The initiating events analyzed in the SAR continue to be addressed. The ability of the plant to mitigate the events analyzed in the SAR is preserved, and as the analysis of such events will still comply with acceptance criteria in the licensing basis, the margin of safety that exists for these events is maintained. These conclusions remain the case for digital CCFs leading to accident sequences that may benefit from addition of a DAS to address operator actions that would need to occur in less than 30 m whether or not diverse actuation systems are provided to address these potential CCFs.

The remaining three principles are addressed explicitly in the evaluations performed in assessing the benefits of the proposed automated DAS:

2) The proposed change is consistent with the defense-in-depth philosophy.

Defense-in-depth is addressed from two perspectives: 1) maintenance of fission product barriers, and 2) redundancy and diversity in maintaining adequate core cooling or preventing a significant release given the frequency of various challenges. The potential effects of digital CCFs are directly evaluated. For those events occurring in less than 30 min for which diverse actuation systems would not be provided, diversity is achieved by

limiting the frequency of the initiating events (e.g., designing primary coolant system components and steam lines to preclude loss of pressure boundary integrity, managing the aging of primary system components through a rigorous ISI program and monitoring the performance of primary system integrity through relatively frequent leakage monitoring) as well as providing design processes and features which assure high dependability of safety system actuation. Defense-in-depth and diversity therefore play an integral role in the demonstration of the ability to cope with the effects of digital CCF.

4) When proposed changes result in an increase in core damage frequency or risk, the increases should be small and consistent with the intent of the Commission's Safety Goal Policy Statement.

In fact, it is the NRC staff that is proposing the change and it is addressing risks that appear to be significantly less than the guidance of Regulatory Guide 1.174. In addition, there are competing risks associated with providing diverse actuation systems. The quantitative assessments performed in this evaluation suggest that not providing diverse actuation systems for accident initiators such as LOCAs and steam line breaks is essentially risk neutral and may actually reduce risk as a result of eliminating the potential for more frequent spurious operations of these systems.

5) The impact of the proposed change should be monitored using performance measurement strategies.

Existing plant corrective action, maintenance rule and reporting programs govern documentation and response to any non-conformances that occur associated with digital systems. Whether risk-informed or deterministic D3 evaluations are performed, monitoring of satisfactory operation of the upgrade is performed subsequent to its installation. This conclusion applies to the plant I&C systems with or without the DAS that would be required in place of operator actions needed within 30 m.

C
DETERMINISTIC ANALYSIS

C.1 BACKGROUND

Selected deterministic analyses were performed using the Modular Accident Analysis Program (MAAP) in order to assess the benefits of the proposed automated DAS. Representative plant parameter files for a BWR with a Mark I containment and a Combustion Engineering PWR were selected in order to estimate accident progression timing for a variety of postulated scenarios. These plant models were selected since the plants have undergone recent updates of the MAAP parameter files and were exercised as part of their recent License Renewal applications. BWR analyses were performed with MAAP BWR Version 4.0.6 and the PWR calculations using MAAP PWR Version 4.0.5. Selected confirmatory evaluations also were performed for a 2 loop Westinghouse PWR and a Babcock and Wilcox PWR.

C.2 ACCIDENT SEQUENCE DEFINITIONS

The following provides the sequence definition for each of the MAAP4 calculations performed.

Case 1a: PWR LOCA.

A series of LOCA calculations were performed in order to determine the smallest break size that could be mitigated prior to core damage assuming that only low pressure safety injection (LPSI) and the safety injection tanks (SITs) were available. The accident sequence was assumed to be initiated with a break in the cold leg followed by a reactor trip, loss of main feedwater, closure of main steam isolation valves and trip of the main coolant pumps.

Case 1b: PWR LOCA w/o Injection.

Once the appropriate LOCA size was obtained in Case 1a, the same break size was run assuming that LPSI was not available. This allowed for an estimate of the time to core damage assuming no operator action in response to failure of the safety injection actuation signal.

Case 2a: PWR Steam Line Break

This calculation assumed a large steam line break with a diameter of 2.79 ft. The accident initiator was assumed to include a reactor scram, closure of the main steam isolation valves, loss of main feedwater and trip of the main coolant pumps. Both high pressure safety injection

(HPSI) and low pressure safety injection (LPSI) were assumed to be available along with the safety injection tanks (SITs). Auxiliary feedwater (AFW) was assumed to be isolated in the broken steam generator (SG) and available to the other SG. This represents a base case main steam line break analysis in which all actuation systems perform as designed.

Case 2b: PWR Steam Line Break w/o Injection

This calculation is identical to Case 2a above but without either HPSI or LPSI. This case represents plant response to a main steam line break under the assumption that safety injection actuation does not occur.

Case 2c: PWR Steam Line Break w/o AFW isolation

This calculation is identical to Case 2a above but without isolation of AFW in the broken steam generator. This case represents plant response to a main steam line break under the assumption that actuation of feedwater isolation does not occur.

Case 2d: PWR Steam Line Break w/o AFW isolation and w/o Injection

This calculation is identical to Case 2a above but without isolation of AFW in the broken steam generator and without either HPSI or LPSI. This represents plant response to a main steam line break under which essentially no ESFAS actuation occurs.

Case 3a: BWR LOCA

A series of LOCA calculations were performed in order to determine the smallest break size that could be mitigated prior to core damage assuming that only low pressure coolant injection (LPCI) was available. The accident sequence was assumed to be initiated with a break in the recirculation loop followed by closure of the main steam isolation valves and trip of main feedwater.

Case 3b: BWR LOCA w/o Injection.

Once the appropriate LOCA size was obtained in Case 3a, the same break size was run assuming that LPCI was not available. This allowed for an estimate of the time to core damage assuming no operator action. As there is no automatic isolation of feedwater on initiation of the ECCS in a BWR, the condensate pumps are assumed to be available to provide makeup to the reactor until the hotwell inventory was depleted. Flow characteristics were obtained for the BWR condensate pumps along with an estimated hotwell volume of 43,000 gallons.

Case 4a: BWR Inadvertent Opening of One SRV

This BWR sequence was initiated with the inadvertent opening of a single safety relief valve (SRV). Pool heatup will commence as a result of the energy addition to the pool resulting in an increase in the containment steam partial pressure. The objective of this run was to estimate the time to reach the 2 psig containment pressure scram point.

Case 4b: BWR Inadvertent Opening of One SRV

Scenario Case 4a was executed assuming that the automatic scram occurred, however, all injection was assumed to be lost. This allowed for an estimate of the time to core damage assuming no operator action given a stuck open SRV

Case 5a: BWR Large Main Steam Line Break Outside Containment

This BWR sequence was initiated with a break in the main steam line outside of containment. A break diameter of 1.5 ft. was assumed followed by trip of main feedwater and loss of all injection.

Case 5b: BWR Large Main Steam Line Break Outside Containment with Condensate

Case 5a above was executed assuming that the condensate pumps were available to provide makeup until the hotwell volume was depleted. Condensate flow characteristics were obtained for the BWR along with an estimated hotwell volume of 43,000 gallons.

C.3 RESULTS

The following provides a brief summary of the key results for each of the sequences described in Section C.2. Key results for all cases are summarized in Table C-1.

Case 1a: PWR LOCA.

The results for this case indicated that, for a 4” break in the cold leg, LPSI and the SITs would be sufficient to prevent core damage. Figure C-1 shows the primary system pressure for this scenario. Figure C-2 provides a plot of the maximum core temperature, showing that the core temperature increase was mitigated after reaching a peak of about 2000 °F. It was determined that since the time above 1800 °F was short, this case would be considered to be successfully recoveed.

Case 1b: PWR LOCA w/o Injection

Case 1a was executed assuming that all injection was lost. The core was estimated to uncover at 19 minutes into the event with the onset of core damage at 4.1 hr. The SITs were successful in providing core makeup as the primary system pressure decreased. Figure C-3 provides a plot of the primary system pressure response for this event. As can be seen on this plot, the SITs are discharging from .5 to 3 hours into the event.

Case 2a: PWR Steam Line Break

Figures C-4 and C-5 provide the pressurizer pressure and level response to this event. It can be observed that once safety injection begins to provide makeup, the pressure increases with water flow from the pressurizer relief valves (PORVs) estimated to occur at about 23 minutes into the event. Figure C-6 provides a plot of the maximum core temperature.

Case 2b: PWR Steam Line Break w/o Injection

This calculation is identical to Case 2a above but without either HPSI or LPSI. Due to the rapid secondary side depressurization, the primary system cools with a drop in the pressurizer level. As the primary system begins to heat back up, pressurizer level is restored. Water level increases to the point of discharge through the PORVs at about 1.4 hours into the event. Figures C-7 and C-8 provide plots of the pressurizer pressure and level response to this event. Figure C-9 provides a plot of the maximum core temperature.

Case 2c: PWR Steam Line Break w/o AFW isolation

This calculation is identical to Case 2a but without isolation of AFW in the broken steam generator. By not isolating the AFW in the broken steam generator, the pressure decrease is not as rapid as in the case without AFW. Figures C-10 and C-11 provide plots of the pressurizer pressure and level response to this event. Figure C-12 provides a plot of the maximum core temperature.

Case 2d: PWR Steam Line Break w/o AFW isolation and w/o Injection

This calculation is identical to Case 2a but without isolation of AFW in the broken steam generator and without either HPSI or LPSI. This combination results in the pressurizer level never increasing to the level of the PORVs. Figures C-13 and C-14 provide plots of the pressurizer pressure and level response to this event. Figure C-15 provides a plot of the maximum core temperature.

Case 3a: BWR LOCA

The results for this case indicated that, for a 4.8” break in the recirculation loop, LPCI would be sufficient to prevent core damage. Figure C-16 shows the reactor pressure vessel pressure for this

scenario. Figure C-17 provides a plot of the maximum core temperature, showing that the core temperature increase was mitigated after reaching a peak of just under 1800 °F.

Case 3b: BWR LOCA w/o Injection.

Case 3a was executed assuming that all injection was lost. The core was estimated to uncover at 1 minute into the event with the onset of core damage at 13 min.

Case 4a: BWR Inadvertent Opening of One SRV

This BWR sequence was initiated with the inadvertent opening of a single safety relief valve (SRV). Pool heatup and subsequent containment pressurization resulted in exceeding 2 psig at 27 minutes into the event.

Case 4b: BWR Inadvertent Opening of One SRV

Scenario Case 4a was executed assuming that the automatic scram occurred, however, all injection was assumed to be lost. The core was uncovered at 5 minutes with the onset of core damage occurring at 27 min. Figures C-18 and C-19 provide the RPV pressure and maximum core temperature for this case.

Case 5a: BWR Large Main Steam Line Break Outside Containment

This BWR sequence was initiated with a break in the main steam line outside of containment. A break diameter of 1.5 ft. was assumed followed by trip of the main feedwater and loss of all injection. Due to the rapid loss of RPV inventory, the core uncovered at 30 seconds with the onset of core damage estimated to occur at about 11 minutes. Figure C-20 provides the maximum core temperature response for this event.

Case 5b: BWR Large Main Steam Line Break Outside Containment with Condensate

Case 5a above was executed assuming that the condensate pumps were available to provide makeup until the hotwell volume was depleted. Condensate flow characteristics were obtained along with an estimated hotwell volume of 43,000 gallons. The condensate pumps are able to maintain core cooling until the hotwell is depleted at 47 minutes. The onset of core damage occurred at 3.2 hours into the event. Figures C-21 and C-22 provide the RPV downcomer level and the maximum core temperature response for this event.

Table C-1
Summary of Key Results

Case Name	PWR/BWR	Description[1]	TAF[2]	Core Damage	Vessel Breach	Comments
Case 1a	CE PWR	Large LOCA Calculate smallest size that allows LPSI + SIT to prevent core damage	19 min	NA[3]	NA	4" break in cold leg
	2 loop PWR Westinghouse		10 min	NA	NA	4" break in cold leg
	B&W PWR		10 min	NA	NA	4.5" break in cold leg
Case 1b	CE PWR	Same as case 1a w/o LPSI	19 min	4.1 hr	7.5 hr	
	2 loop PWR Westinghouse		10 min	2.2 hr		
	B&W PWR		10 min	45 min	4.9 hr	
Case 2a[4]	PWR	Main Steam Line Break Successful SI Isolation of AFW to Broken SG	NA	NA	NA	Pressurizer repressurizes with reflood and water flow from the PORV at 23 min
Case 2b[4]	PWR	Same as 2a w/o SI	NA	NA	NA	Pressurizer repressurizes with reflood and water flow from the PORV at 1.4 hr
Case 2c[4]	PWR	Same as 2a except FW not isolated	NA	NA	NA	Pressurizer repressurizes with reflood and water flow from the PORV at 45 min
Case 2d[4]	PWR	Same as 2a w/o SI and w/o isolation of FW	NA	NA	NA	Pressurizer does not repressurize and does not reflood
Case 3a	BWR	Large liq line LOCA (recirc loop) Calculate smallest size that allows LPCI to prevent core damage	1 min	NA	NA	4.8" ID break in recirc line 4 LPCI pumps operating

Table C-1
Summary of Key Results

Case Name	PWR/BWR	Description[1]	TAF[2]	Core Damage	Vessel Breach	Comments
Case 3b	BWR	Same as 3b w/o LPCI	1 min	13 min	3.1 hr	Condensate providing injection until hotwell depleted at 17 min. (43,000 gal)., however, does not prevent early core damage.
Case 4a	BWR	IORV Determine time available prior to auto trip of reactor	NA	NA	NA	Hi Drywell pressure resulted in reactor scram at 27 min.
Case4b	BWR	IORV with Rx Trip w/o ECCS	5 min	27 min	3.1 hrs	
Case 5a	BWR	Large Steam Line Break w/o FW w/o ECCS	30 sec	11 min	3.3 hrs	
Case 5b	BWR	Large Steam Line Break w/o FW w/o ECCS w condensate	34 sec	3.2 hr	8.6 hrs	Hotwell depleted in 47 min.

1. All cases assume AFW available unless noted
2. Time to reach TAF based on collapsed downcomer level (BWR), two-phase level (PWR)
3. Maximum core temperature exceeded 1800 °F for only 1 min. Not considered core damage
4. MSLB cases run for 6 hrs. accident time

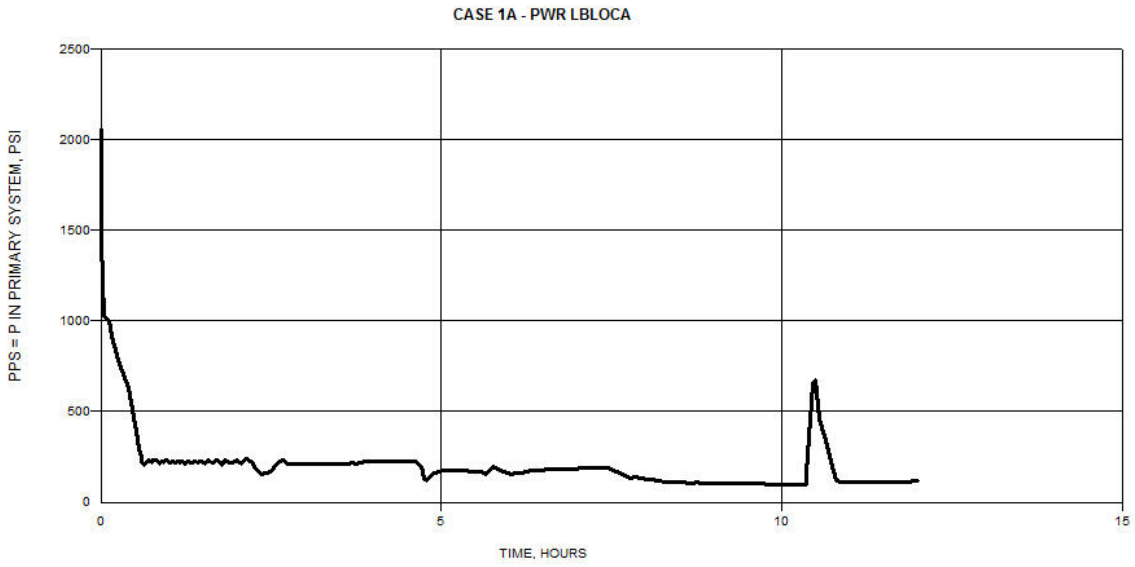


Figure C-1
Case 1a: Primary System Pressure (psia)

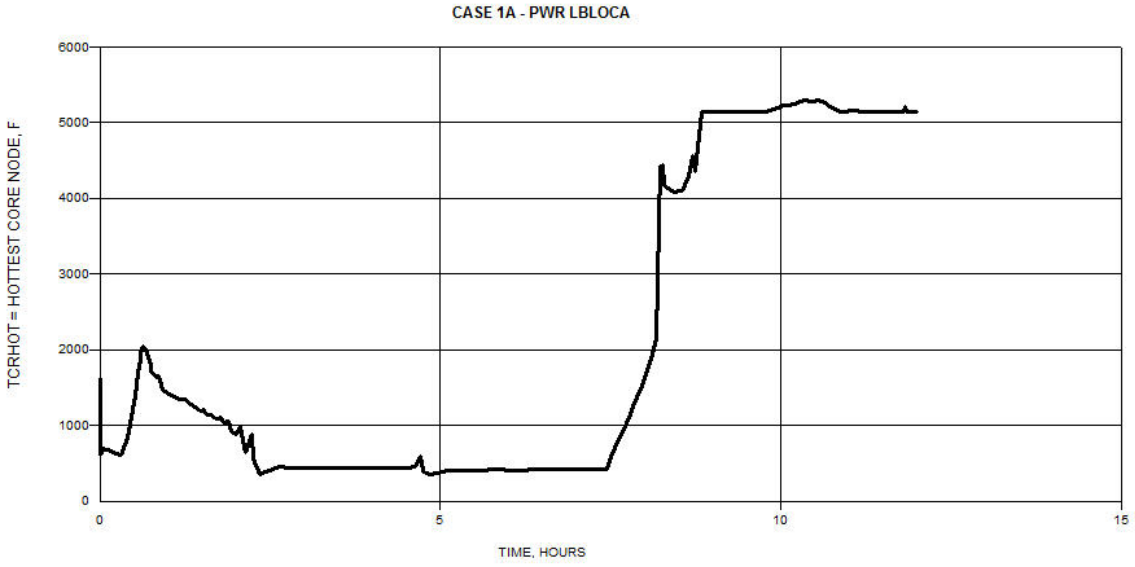


Figure C-2
Case 1a: Maximum Core Temperature (°F)

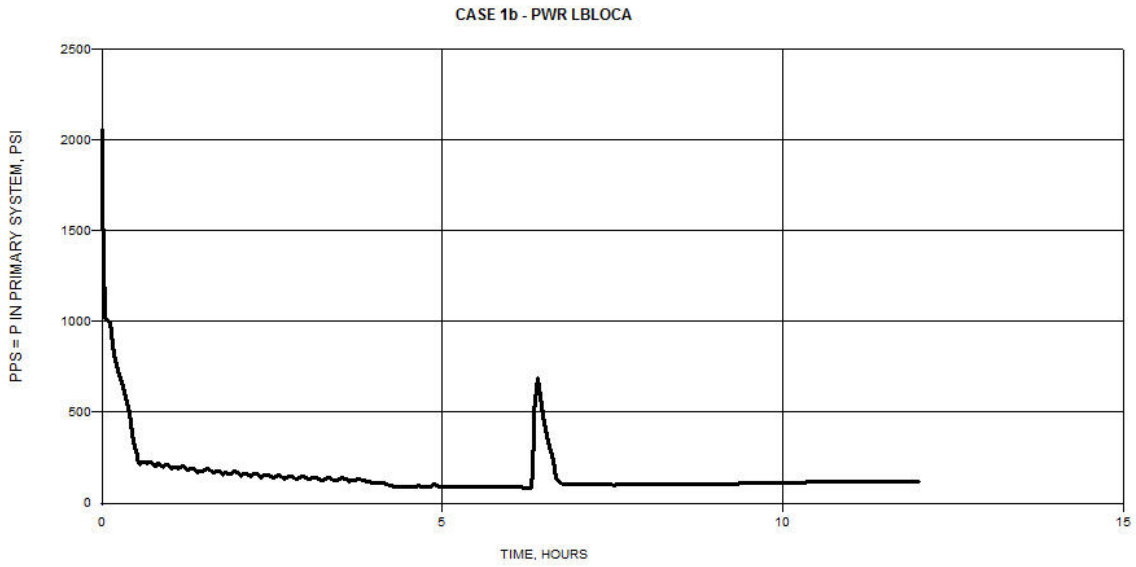


Figure C-3
Case 1b: Primary System Pressure (psia)

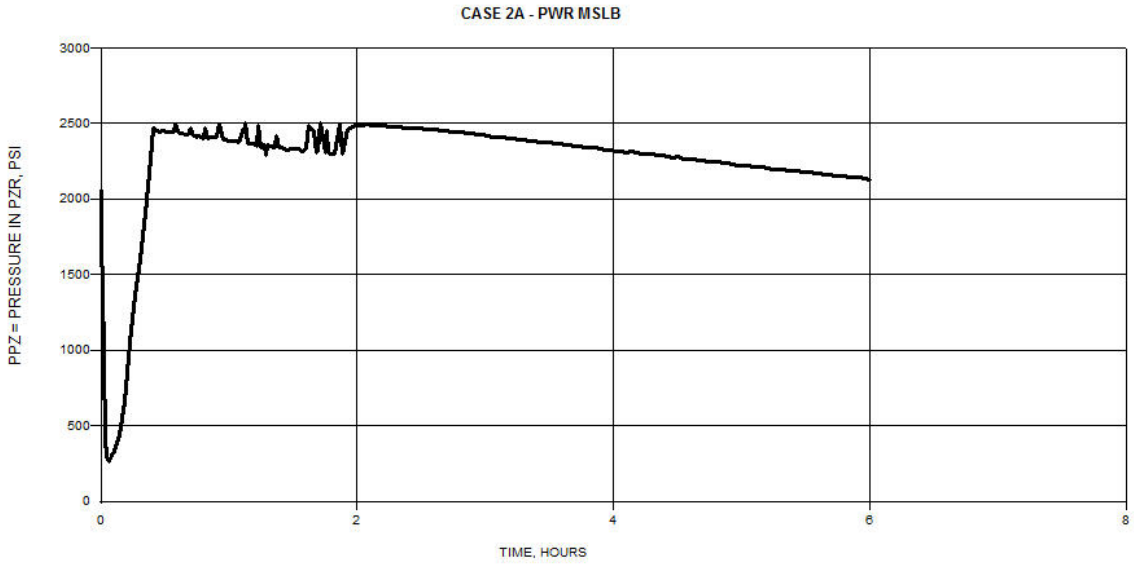


Figure C-4
Case 2a: Pressurizer Pressure (psia)

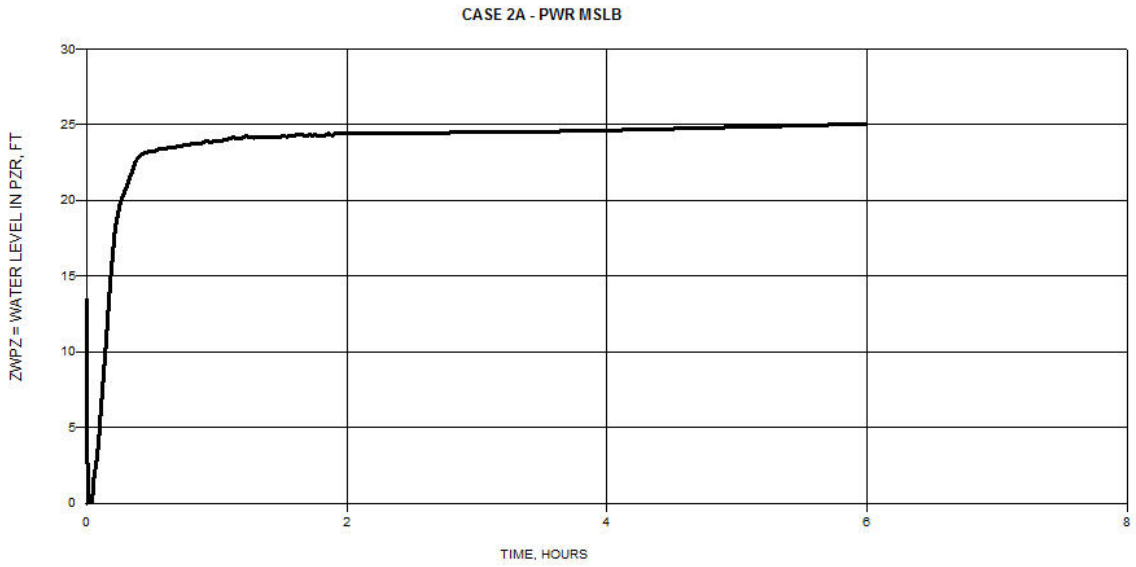


Figure C-5
Case 2a: Pressurizer Level (ft)

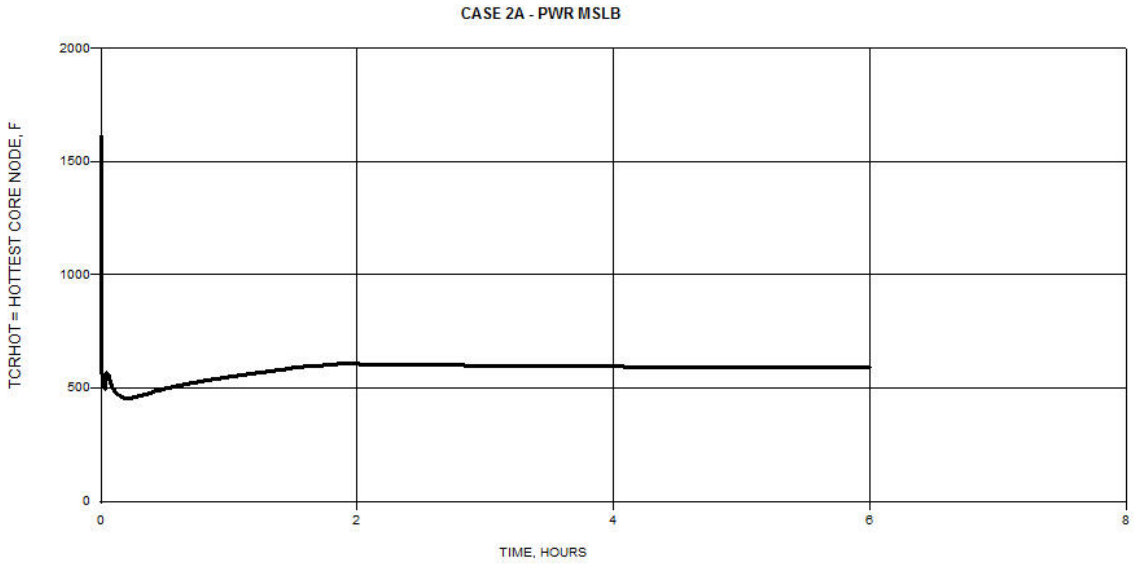


Figure C-6
Case 2a: Maximum Core Temperature (°F)

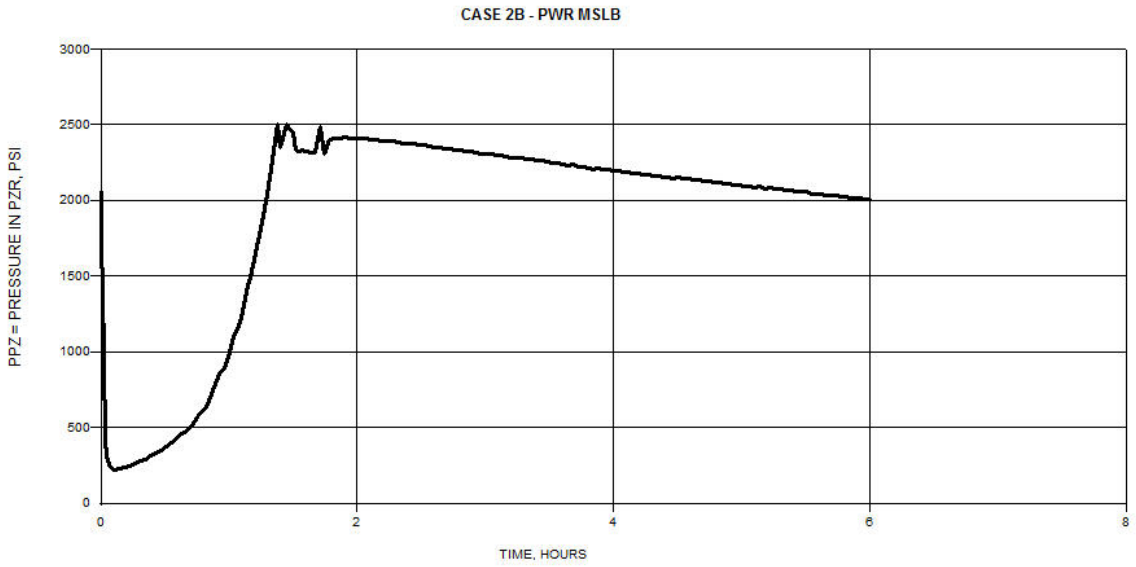


Figure C-7
Case 2b: Pressurizer Pressure (psia)

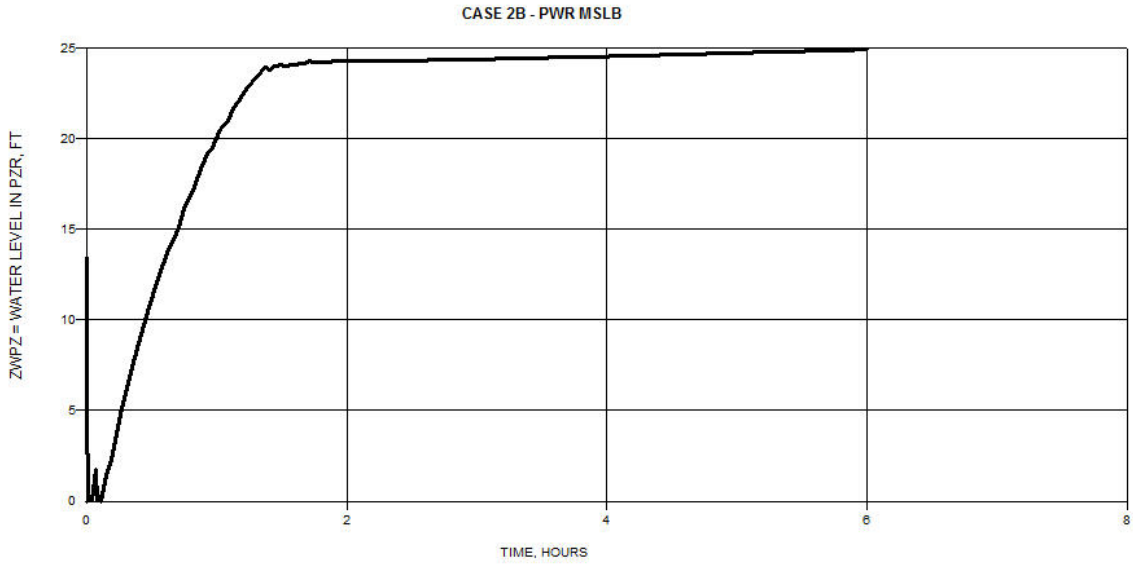


Figure C-8
Case 2b: Pressurizer Level (ft)

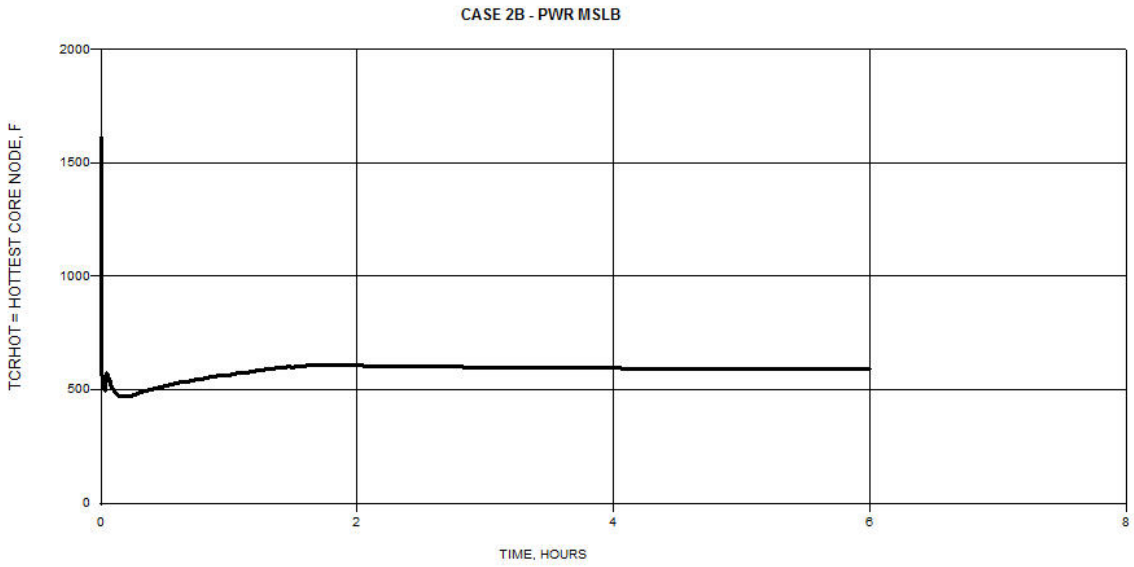


Figure C-9
Case 2b: Maximum Core Temperature (°F)

Figure C-10
Case 2c: Pressurizer Pressure (psia)

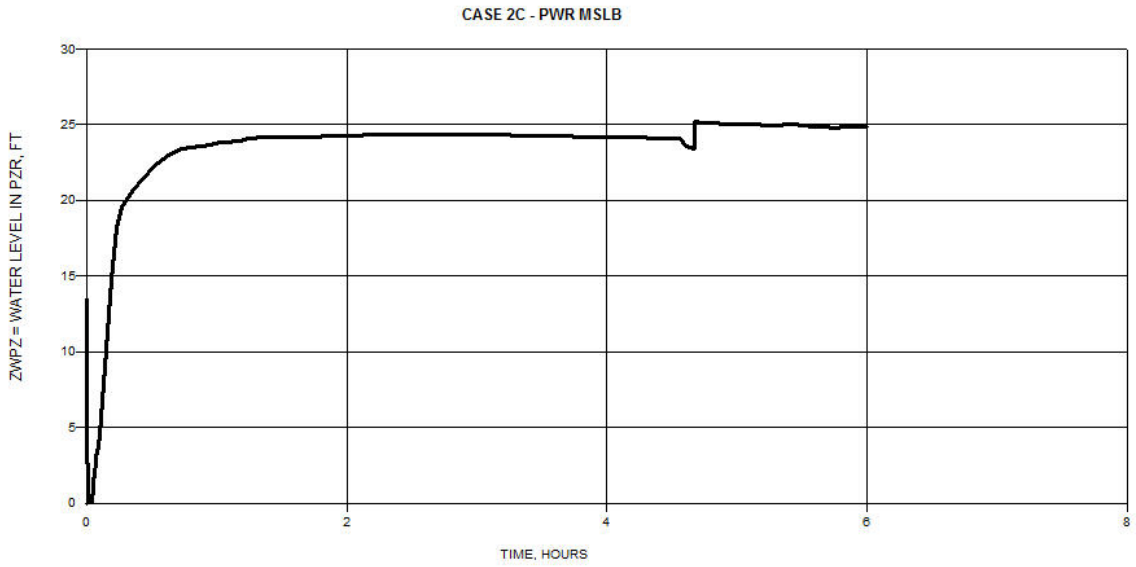


Figure C-11
Case 2c: Pressurizer Level (ft)

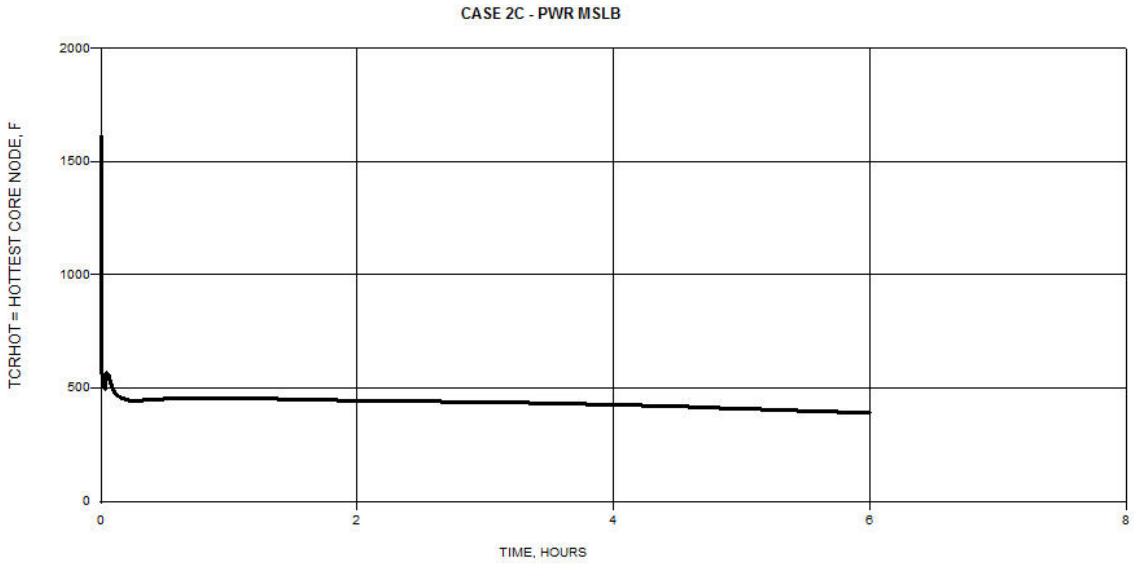


Figure C-12
Case 2c: Maximum Core Temperature (°F)

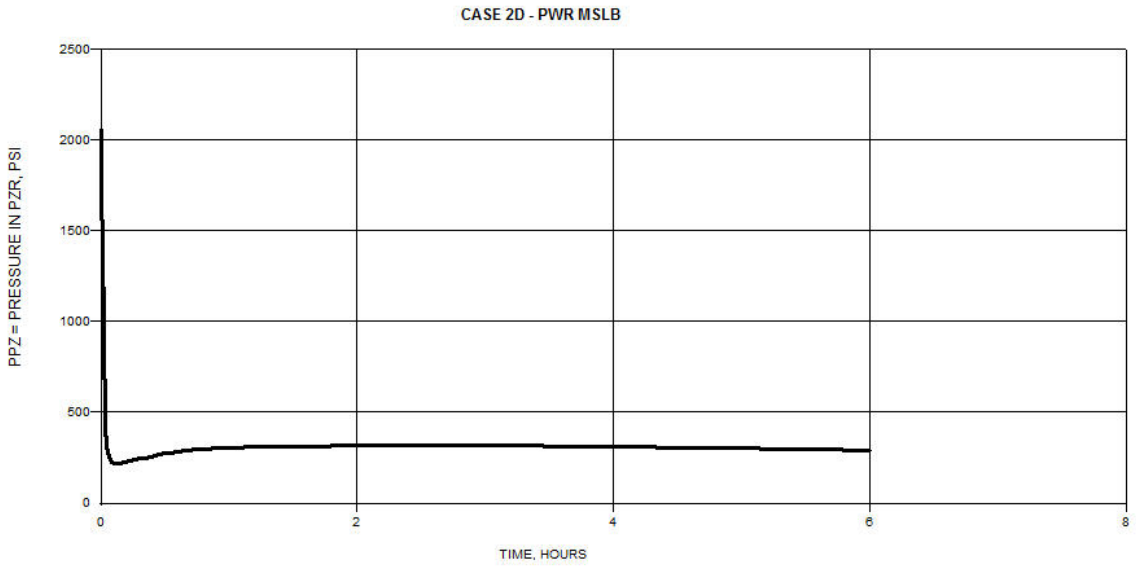


Figure C-13
Case 2d: Pressurizer Pressure (psia)

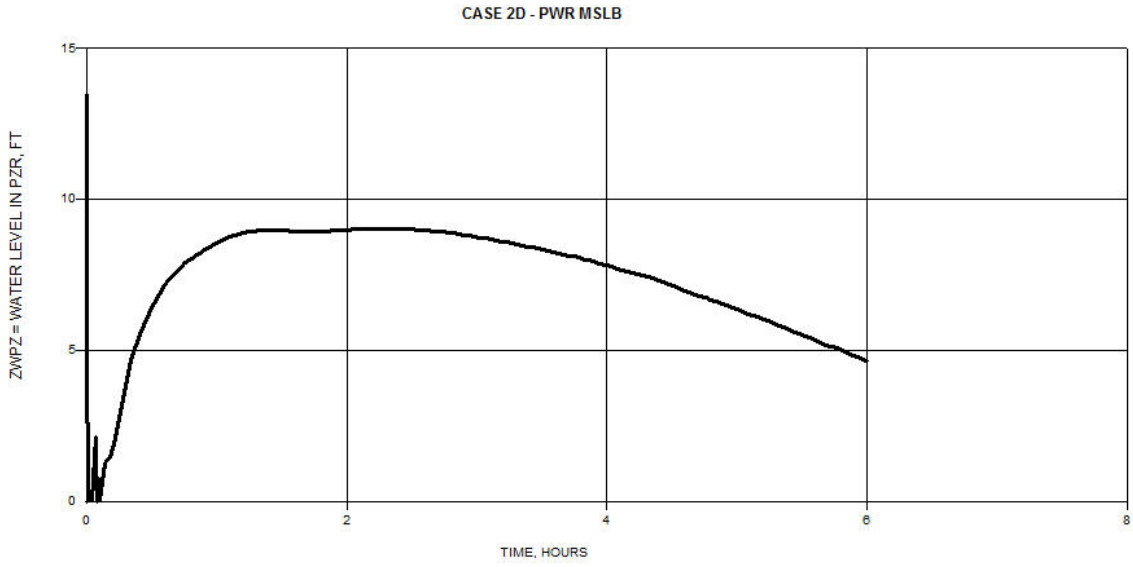


Figure C-14
Case 2d: Pressurizer Level (ft)

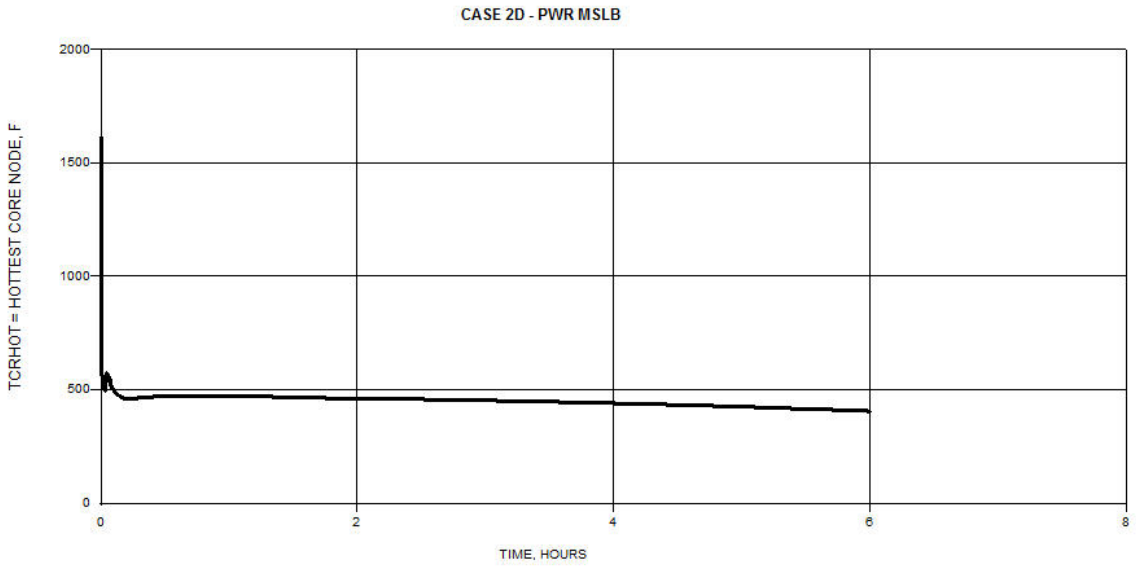


Figure C-15
Case 2d: Maximum Core Temperature (°F)

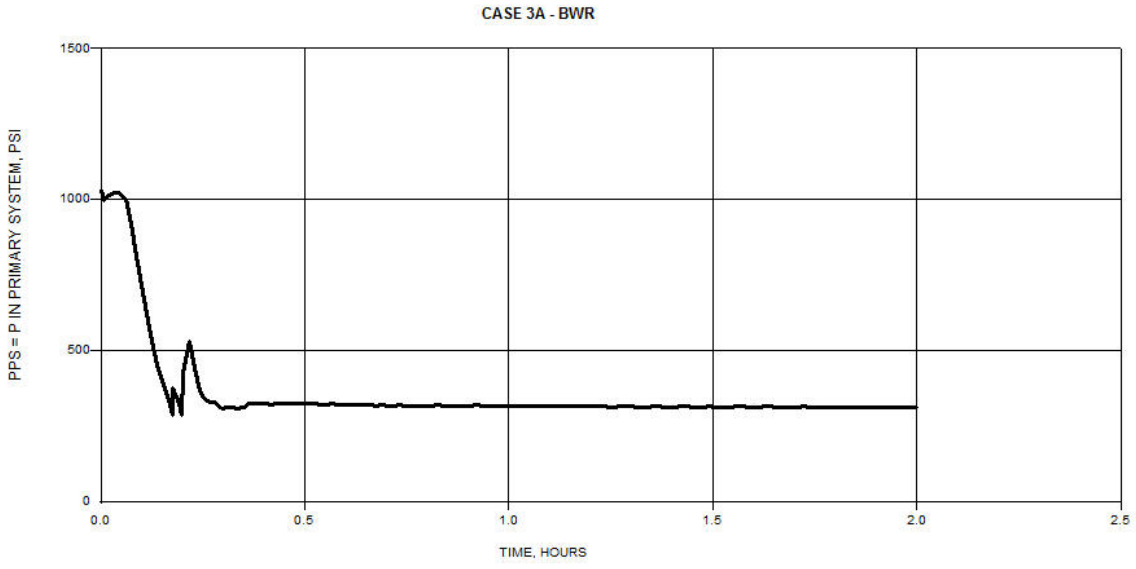


Figure C-16
Case 3a: RPV Pressure (psia)

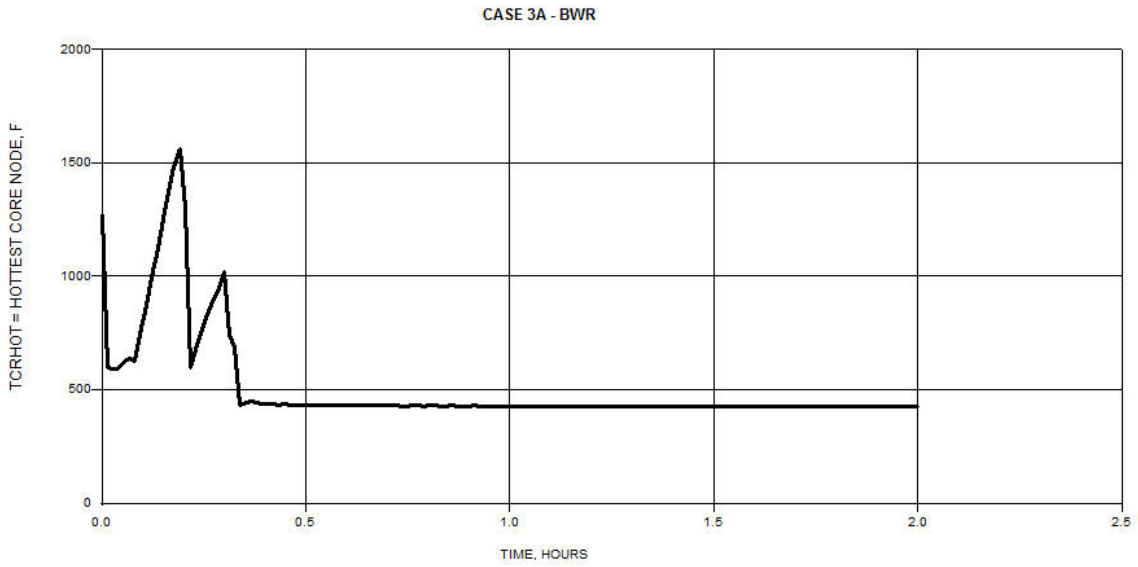


Figure C-17
Case 3a: Maximum Core Temperature (°F)

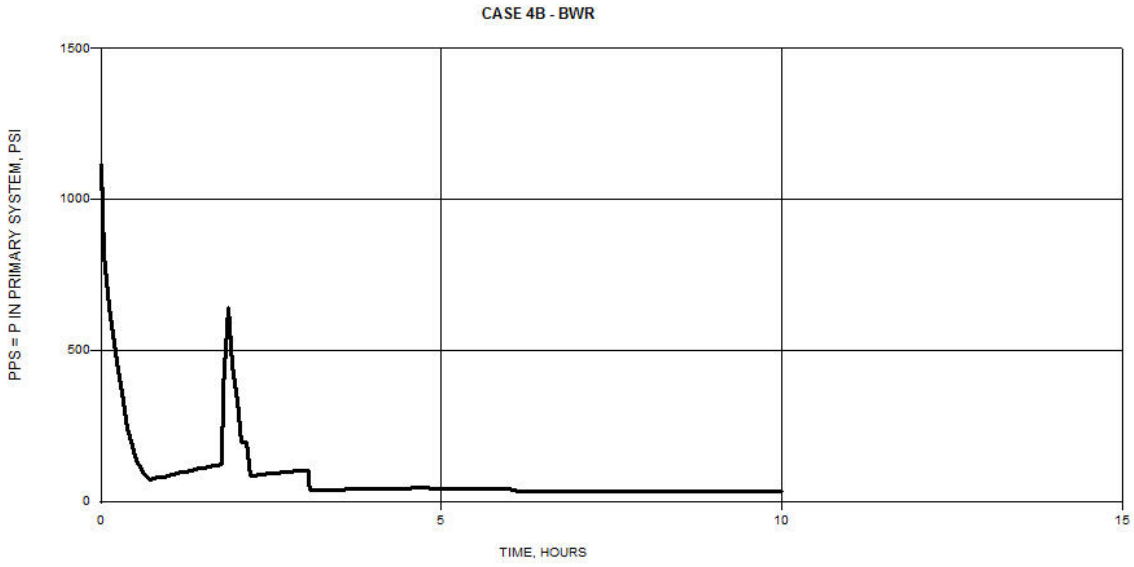


Figure C-18
Case 4b: RPV Pressure (psia)

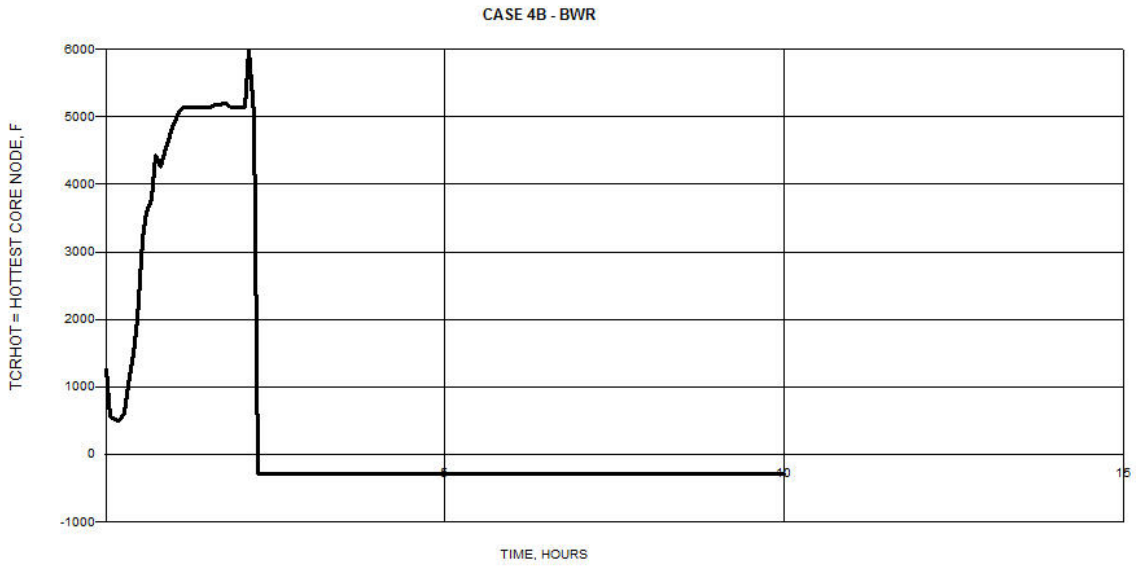


Figure C-19
Case 4b: Maximum Core Temperature (°F)

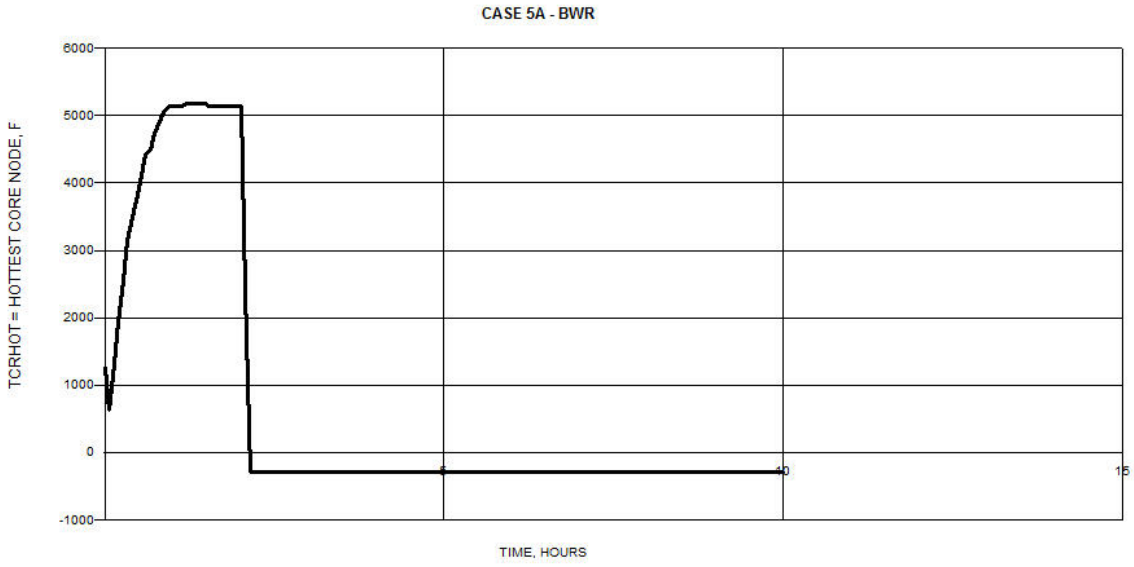


Figure C-20
Case 5a: Maximum Core Temperature (°F)

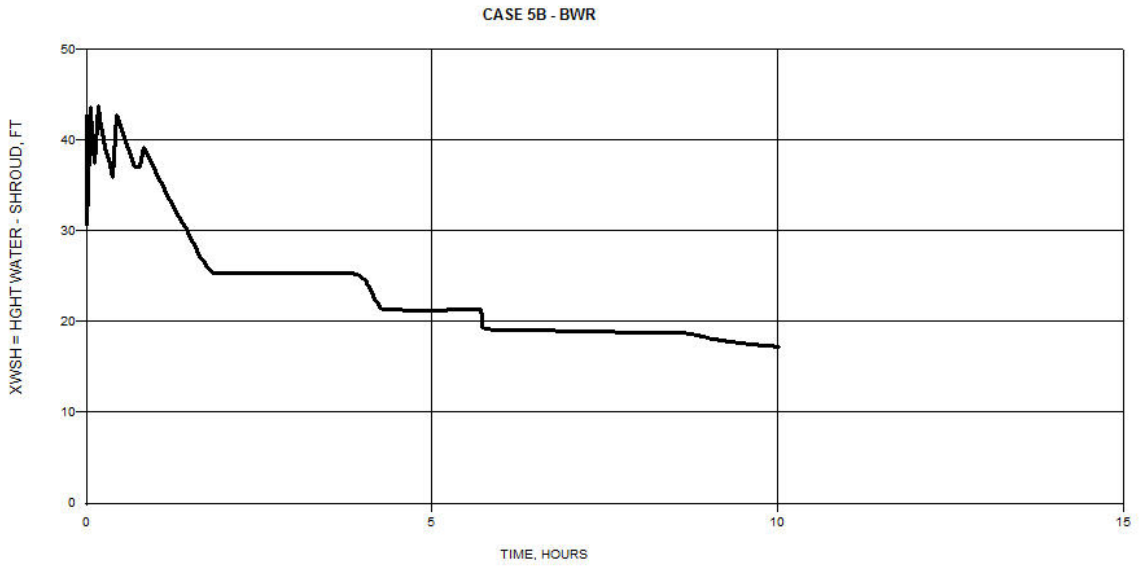


Figure C-21
Case 5b: RPV Downcomer Water Level (ft)

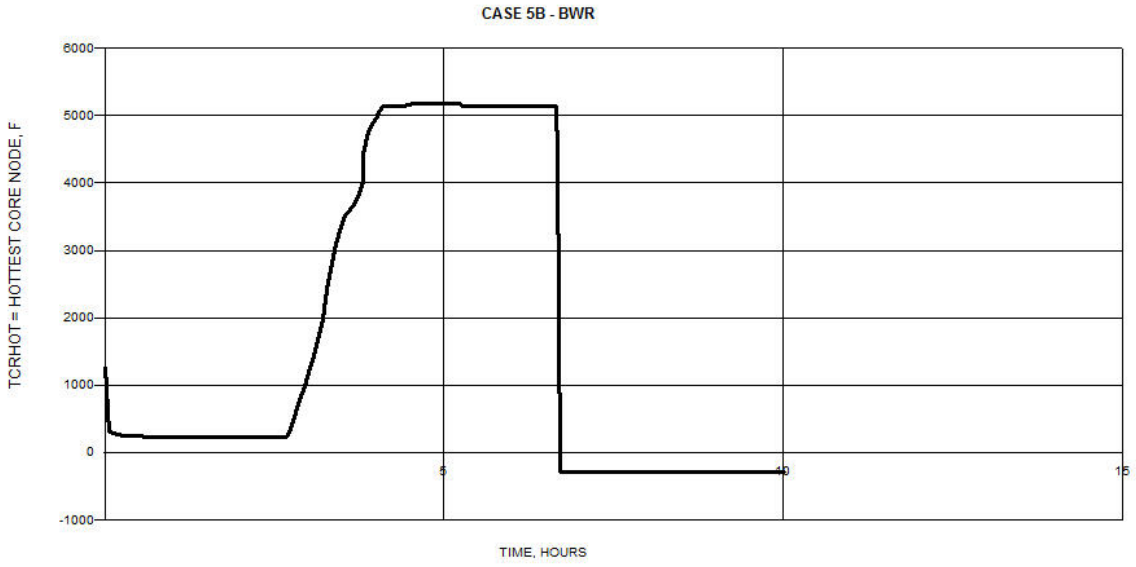


Figure C-22
Case 5b: Maximum Core Temperature (°F)

D
DATA DEVELOPMENT

This section provides the basis for failure rates and other parameters used in the assessment of the benefits and risks associated with an automated DAS. Included in this appendix are:

- Initiating event frequencies
- Assumptions regarding software failure probability
- Human Error Probabilities for actuation of engineered safeguards systems in the presence of a software CCF
- Containment failure probability given core damage
- Large early release consequences

1. INITIATING EVENT FREQUENCIES

Frequencies for three principal classes of initiating events were developed for which the proposed automated DAS either may be useful or may initiate:

- LOCA frequencies (NUREG/CR-1829)
- Transient induced LOCA frequencies (NUREG/CR-6928)
- Spurious actuation frequencies (NUREG/CR-6928 LERs).

1.1. LOCA frequencies

LOCA frequency estimates have been developed by the NRC using an expert elicitation process for use in PRA and risk-informed applications. The process consolidates service history data and insights from probabilistic fracture mechanics studies with knowledge of plant design, operation, and material performance. Separate BWR and PWR piping and non-piping passive system LOCA frequency estimates have been developed as a function of effective break size and operating time through the end of license extension. Development of the estimates includes typical reactor coolant system design processes, periodic inspection and monitoring programs implemented for the operation of the current generation of power plants.

Table B-1 provides the estimated frequency of the spectrum of LOCAs for both BWRs and PWRs. Figures B-1 and B-2 provide plots of these frequencies applicable to the end of the operating license for currently operating BWRs and PWRs respectively.

Table B- 1 LOCA Frequencies from NUREG/CR-1829

			Current Estimate				End of Life Estimate			
	GPM	Inch	5th Per.	Median	Mean	95th Per.	5th Per.	Median	Mean	95th Per.
	>100	0.5	3.10E-05	3.00E-04	6.40E-04	2.10E-03	2.60E-05	2.60E-04	6.00E-04	2.00E-03
	>1,500	1.875	2.70E-06	4.80E-05	1.20E-04	4.10E-04	2.20E-06	4.40E-05	1.10E-04	4.10E-04
BWR	>5,000	3.25	5.60E-07	9.70E-06	2.80E-05	1.00E-04	4.90E-07	9.80E-06	3.20E-05	1.20E-04
	>25K	7	9.60E-08	2.20E-06	7.30E-06	2.70E-05	8.70E-08	2.30E-06	9.30E-06	3.40E-05
	>100K	18	7.20E-09	2.90E-07	1.50E-06	5.40E-06	6.20E-09	3.10E-07	2.10E-06	7.30E-06
	>500K	41	5.60E-12	3.00E-10	6.40E-09	1.60E-08	6.70E-12	4.00E-10	1.00E-08	2.50E-08
	>100	0.5	6.00E-04	3.70E-03	6.40E-03	1.80E-02	3.50E-04	2.50E-03	4.70E-03	1.40E-02
	>1,500	1.625	7.00E-06	1.40E-04	6.20E-04	2.20E-03	7.60E-06	1.60E-04	7.60E-04	2.70E-03
PWR	>5,000	3	2.00E-07	3.40E-06	1.60E-05	5.80E-05	4.50E-07	7.60E-06	3.60E-05	1.30E-04
	>25K	7	1.30E-08	3.10E-07	1.60E-06	5.70E-06	2.60E-08	6.50E-07	3.60E-06	1.30E-05
	>100K	14	3.80E-10	1.10E-08	1.90E-07	5.20E-07	9.20E-10	2.70E-08	4.60E-07	1.30E-06
	>500K	31	3.30E-11	1.20E-09	3.10E-08	7.80E-08	8.20E-11	2.90E-09	8.10E-08	2.00E-07

For the purpose of determining the benefits of the proposed DAS, the large LOCA break range was defined as all breaks between the largest double ended guillotine rupture of primary coolant piping to the smallest break range for which low pressure injection is capable of providing adequate core cooling. Attachment C Cases 1 (a and b) and 3 (a and b) provide analyses of a PWR and a BWR that define the smaller end of this break range. From Attachment C, the above

tables are used to establish the large LOCA frequency. The mean, upper and lower bounds are interpolated for the appropriate break sizes from Table B-1.

BWR (>6" effective break size, end of life estimate)

Mean	1.5E-05/year
Upper bound (95%)	5.7E-05/year
Lower bound (5%)	1.9E-07/year

PWR (>4" effective break size, end of life estimate)

Mean	2.6E-05/year
Upper bound (95%)	1.0E-04/year
Lower bound (5%)	3.4E-07/year

The small to medium break range is defined as any break above normal makeup system flow rates such as that for CRD (BWR) and CVCS (PWR). This is assumed to be the break sizes associated with the >100gpm breaks in Table B-1.

BWR (>0.5" effective break size, end of life estimate)

Mean	6.0E-04/year
Upper bound (95%)	2.0E-03/year
Lower bound (5%)	2.6E-05/year

PWR (>0.5" End of life estimate)

Mean	4.7E-03/year
Upper bound (95%)	1.4E-02/year
Lower bound (5%)	3.5E-04/year

Figure B-1

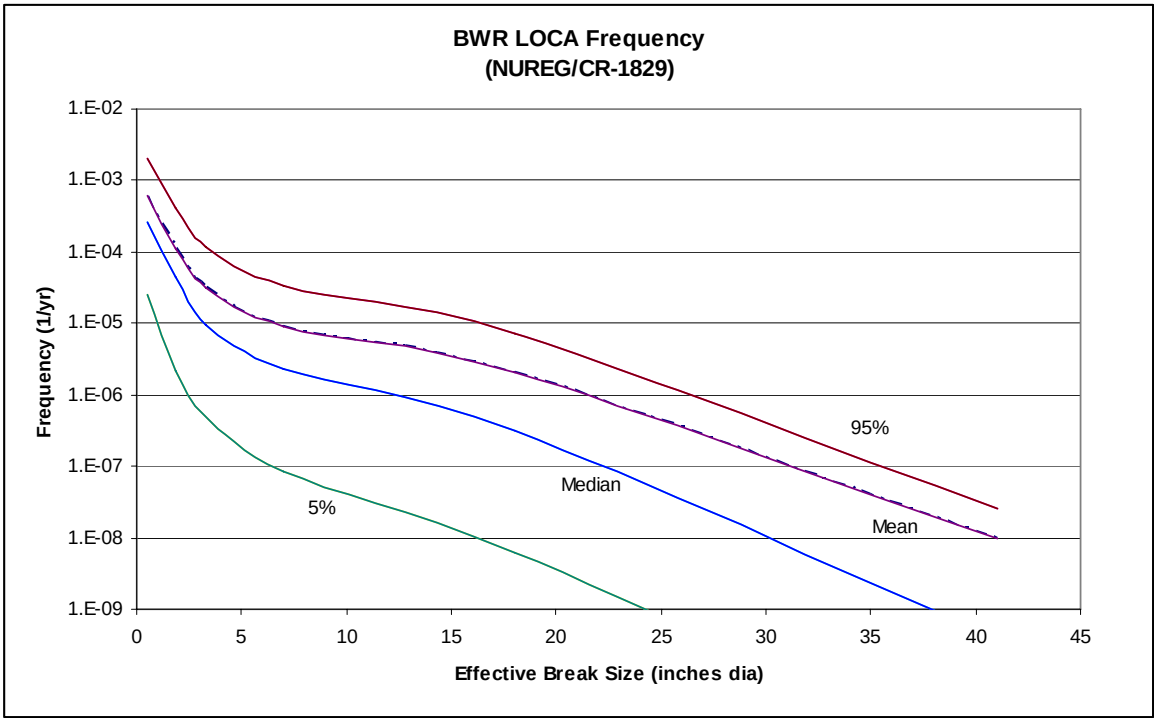
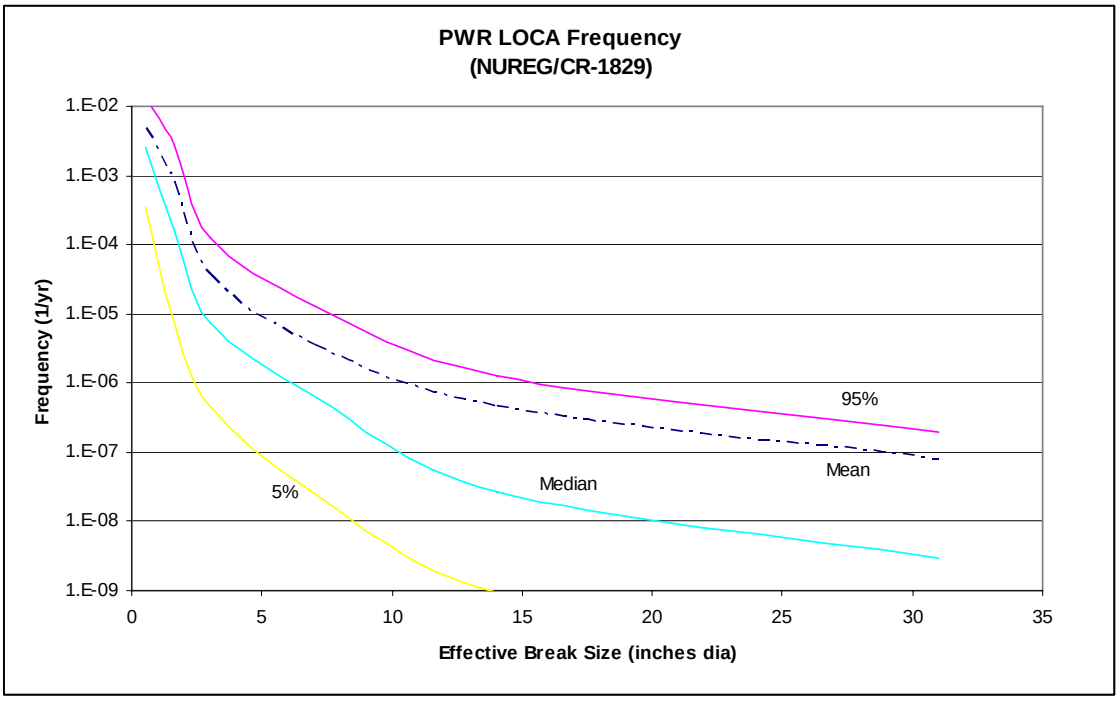


Figure B- 2



1.2. Spurious Actuation Initiating Event Frequencies

To determine the potential for the proposed automated DAS causing plant trips, a review of reactor trip related LERs between 1987 and 2005 was performed. As the proposed automated DAS is not implemented in any plants at this time, spurious ESFAS events were identified as a surrogate, as described in the following paragraphs, and a determination made as to whether the circumstances leading to each of these spurious ESFAS initiated plant trips would also be possible for the proposed DAS.

Examination of plant trip related LERs was performed to determine the frequency of spurious ESFAS initiated trips. LERs listed in Appendix D of NUREG/CR-5750 (Category QR9 – Spurious ESFAS) were reviewed for the period 1987 through 1995. For 1996 through 2005, LERs in the general transient, loss of heat sink and loss of feedwater categories were screened to determine which were spurious ESFAS related. The NRC has made all initiating event related LERs available through their website under the Operational Experience Results and Databases link[1]. While a number of spurious RTS events were identified in this review, they were not retained as a part of this exercise. Only ESFAS related spurious plant trips were considered as candidates possibly representing inadvertent plant trip resulting from the proposed DAS. Of the more than one thousand LERs reviewed, 49 were determined to be spurious ESFAS or ATWS mitigating system initiated.

Table B-3 is a listing of these 49 LERs. A brief description of each is provided as well as an indication of whether the spurious trip was a result of sensor or logic malfunctions. Those that occurred as a result of calibration or surveillance testing activities are also noted. Finally, the type of ESFAS actuation that might occur given the failure are identified (i.e., whether ECCS actuation or secondary system/SLB related).

Figure B-3 provides plots of the annual number of spurious ESFAS related events. It can be seen that a significant reduction in the number of these events during calibration/surveillance activities has occurred with time. This reduction reflects ongoing industry efforts to reduce both the spurious demands on safety systems as well as plant trips. For this reason, the calibration/surveillance related events were removed from consideration in representing the potential for spurious trips associated with an automated DAS. While fewer in number than the calibration/surveillance related events, the strictly sensor and logic events do not necessarily show a similar downward trend with time. Therefore, when considering only the sensor and logic initiated ESFAS events, all 18 years of data was used.

In further screening the spurious ESFAS LERs, assumption had to be made with respect to support system dependencies. Much like the ATWS mitigating systems, it is anticipated that the proposed automated DAS will not be fail safe and likely will require power to actuate. Therefore, events in which the lost of a power source resulted in the actuation of a safety system would not be applicable to the proposed DAS.

[1] http://nrcoe.inel.gov/results/

These calibration/surveillance and power dependency assumptions leave only the sensor initiated and logic initiated spurious ESFAS actuations as potentially being representative of the spurious actuation of the proposed automated DAS.

A spurious ESFAS frequency was derived for the combined sensor and logic trips as well as for the logic trips by themselves. The number of events per unit time, or Maximum Likelihood Estimates (MLE), was generated for each plant in units of events/rcyr (reactor critical year). The MLEs were then ordered from smallest to largest and an empirical fit derived (see Figures B-3 and B-4).

Frequency of spurious ESFAS trips (sensor and logic trips combined)

F_{SpurOp}	=	gamma(0.252, 0.0721)
Mean	=	0.018/year
Upper bound (95%)	=	0.087/year
Lower bound (5%)	=	3.4E-07/year

Frequency of spurious ESFAS trips (logic trips only)

F_{SpurOp}	=	gamma(0.0570,0.0839)
Mean	=	0.0048/year
Upper bound (95%)	=	0.0264/year
Lower bound (5%)	=	ε

As noted earlier, there were two types of spurious ESFAS related trips observed in the operating experience; those associated with actuating the ECCS and those associated with disturbances on the secondary side of the plant or SLB related actuations. For the purpose of this analysis, both types of trips are considered candidates for the proposed automated DAS. The frequencies generated above are therefore split based on the distribution of spurious ESFAS trips found in the operating experience:

Total number of sensor and logic related spurious ESFAS trips

BWR = 10
PWR = 15

Total number of trips related to the actuation of the ECCS

BWR = 5 (50%)
PWR = 8 (53%)

These ratios will be used to distribute the trip frequency for the proposed automated DAS between ECCS and SLB related spurious trips.

Table B- 2 Spurious ESFAS LERs

BWR/PWR	*LER*	*Sensor*	*Logic*	*Cal/Surv/ Power*	*SLB/ECCS*	*Description*
BWR	2371987032	X		X	SLB	Half channel trip (MSL Radiation) during surveillance test. Turbine vibration of steam line pressure sensors on redundant channel.
BWR	2371989019	X		X	SLB	Half channel trip (MSL Radiation) could not be reset during surveillance. Setpoint drift of steam tunnel temperature on redundant channel.
BWR	2371990001	X		X	SLB	Half chanel trip (MSL flow) during surveillance. Trip of redundant steam line flow sensor resulting from shared sensing line.
BWR	2491998003		X	X	SLB	Spurious trip on PCIS channel while opposite channel was in trip for surveillance test
BWR	2541992004	X			SLB	Spurious MSL high flow instrumentation trip
BWR	2651987011	X		X	ECCS	Half channel trip (Reactor level) during surveillance. Trip of redundant reactor level channel due to failure to prepressurize sensing line on return to service.
BWR	2651994006	X			SLB	Maintenance personnel bumped flow sensors during maintenance of RCP seal pressure transmitter on adjacent rack.
PWR	2722000005		X		SLB	False SG isolation signal due to failure of circuit card in SSPS
PWR	2751989009	X			ECCS	Calibration of ADV control pressure transmitter resulted in trip of steam line dp pressure sensors on a common sensing line
BWR	2771989015	X			SLB	EHC RPV Pressure Regulator maintenance causes turbine control valve and TBPV operation with resulting steam line low pressure and MSIV closure.
BWR	2772003003	X			ECCS	Depressurization of variable leg causes false low level signal
BWR	2781992008	X			SLB	Maintenance personnel bumped pressure sensors during maintenance of steam turbine instrumentation on adjacent rack.
BWR	2782000001	X			ECCS	Depressurization of variable leg causes false low level signal
PWR	2801993001		X	X	ECCS	Spurious safety injection actuation while investigating inability to reset SI channel following surveillance (loose connection or high resistance across relay)
PWR	2811991007	X			ECCS	Erratic steam generator pressure channel coincident with an electrical fault in a vital bus
PWR	2851994001	X			ECCS	Coil shorting failure of a supervisory relay

BWR/PWR	*LER*	*Sensor*	*Logic*	*Cal/Surv/ Power*	*SLB/ECCS*	*Description*
PWR	2861999010			P	SLB	Loss of instrument bus
BWR	2962000005	X			ECCS	Returning feedwater level sensor to service caused pressure perturbation in common sensing lines that generated a false low level signal
BWR	2981988021	X			SLB	Electrical noise causes spike in steam line radiation monitors
PWR	~~3151988011~~					~~RTS~~
PWR	3172000005	X			SLB	Spurious isolation of SG
PWR	3181995002	X		X	SLB	Check of trip setpoint for one channel of SGIS while checking cable for future tagout of redundant channel
BWR	3251987017	X				RCPB leakage test results in low pressure in common reference line with reactor level instruments causing spurious low level signal
BWR	3312000001	X		X	ECCS	Return to service after calibration of reactor level transmitter causes pressure oscillation in common sensing line to redundant transmitters
BWR	3531990015	X		X	SLB	Repositioning a temperature switch on one channel of steam line leak detection with calibration of another channel in progress
PWR	3621988002		?	X	ECCS	Premature actuation of ESFAS relays during surveillance test
BWR	3661987003	X		X	SLB	During test of a steam line radiation channel, a failure of a temperature sensor in a redundant channel resulted in steam line isolation
BWR	3661999006			P	SLB	Loss of RPS MG set inititiates ESFAS
PWR	3681988020	?		X	ECCS	Surveillance of one channel of SIAS with a spurious trip of a second channel
PWR	~~3691987017~~					~~Failure of operator's turbine controls during startup results control valves opening leading to low steam line pressure and SIAS~~
PWR	3821991019		?	X	ECCS	Test circuit malfunction leads to inadvertent SI
PWR	3821991022	?		X	ECCS	Surveillance of one channel of SIAS with a spurious trip of a second channel due to failures in test circuitry
PWR	3902001004	X			AMSAC	Implementation of design change to AFW controls results in AMSAC low SG level trip
PWR	4001995011	X		X	SLB	Test of low steam line pressure ESFAS on one steam generator concurrent with failure of relay blocking MSIV closure on that SG leads to MSIV closure

BWR/PWR	*LER*	*Sensor*	*Logic*	*Cal/Surv/ Power*	*SLB/ECCS*	*Description*
PWR	4001995011		X	X	SLB	ESFAS logic test with concurrent loss of contact in redundant channel of steam line pressure
PWR	4121993002			P	ECCS	Transmitter replacement in one channel with random failure of a power supply in a redundant channel
PWR	~~4141989003~~					~~Jumper installation to investigate valve position indication light trips MSIV~~
BWR	4161988019	X			ECCS	Radio keyed in vicinity of low level transmitters causes HPCS initiation, high level trip and loss of reactor level to low level trip setpoint
PWR	4232005002		X		ECCS	SSPS causes spurious actuation of a division of SI
PWR	4241994001	X			ECCS	Replacement of pressurizer pressure transmitter results in inadvertent low pressure in sensing line for a redundant sensor
PWR	4462001001		X		AMSAC	Short circuit on a burned out light bulb replacement in the AMSAC panel
PWR	4551993008	X		X	SLB	SG level channel in test with concurrent failure of circuit card for redundant SSPS
PWR	4561990018		X		ECCS	SSPS processing circuitry
PWR	4561994012		X		SLB	Failed circuit board in SSPS train
PWR	4571988026	X			SLB	Grounded test circuit during investigation of level transmitter anomalies
BWR	4581994030	?		X	SLB	Failure to clear trip on one channel prior to proceeding to test redundant channel
BWR	4612000007		X	X	SLB	MSI test on one channel with coinciden failure of circuit card in redundant channel
PWR	4821987002	X		X	ECCS	Test of one channel with concurrent isolation of the wrong pressure transmitter?
PWR	4821989004		X		SLB	Bumping SSPS equipment during local maintenance
PWR	4822003003	X			SLB	Spurious FWIV closure
PWR	5292001002		X		SLB	Logic board failure in MSFIS
PWR	5301991003	?		X	ECCS	Release of test pushbutton for one channel causes actuation of a redundant channel

Note 1: Shaded rows were screened from the derivation of the spurious trip frequency (see the last two paragraphs on page D-5).
Note 2: Strikethrough rows are NUREG/CR-5750 category QR-9 events that appear to be legitimate plant trips or spurious RTS events not applicable to ESFAS or the proposed automated DAS.

Figure B- 3 Spurious ESFAS Events by Year

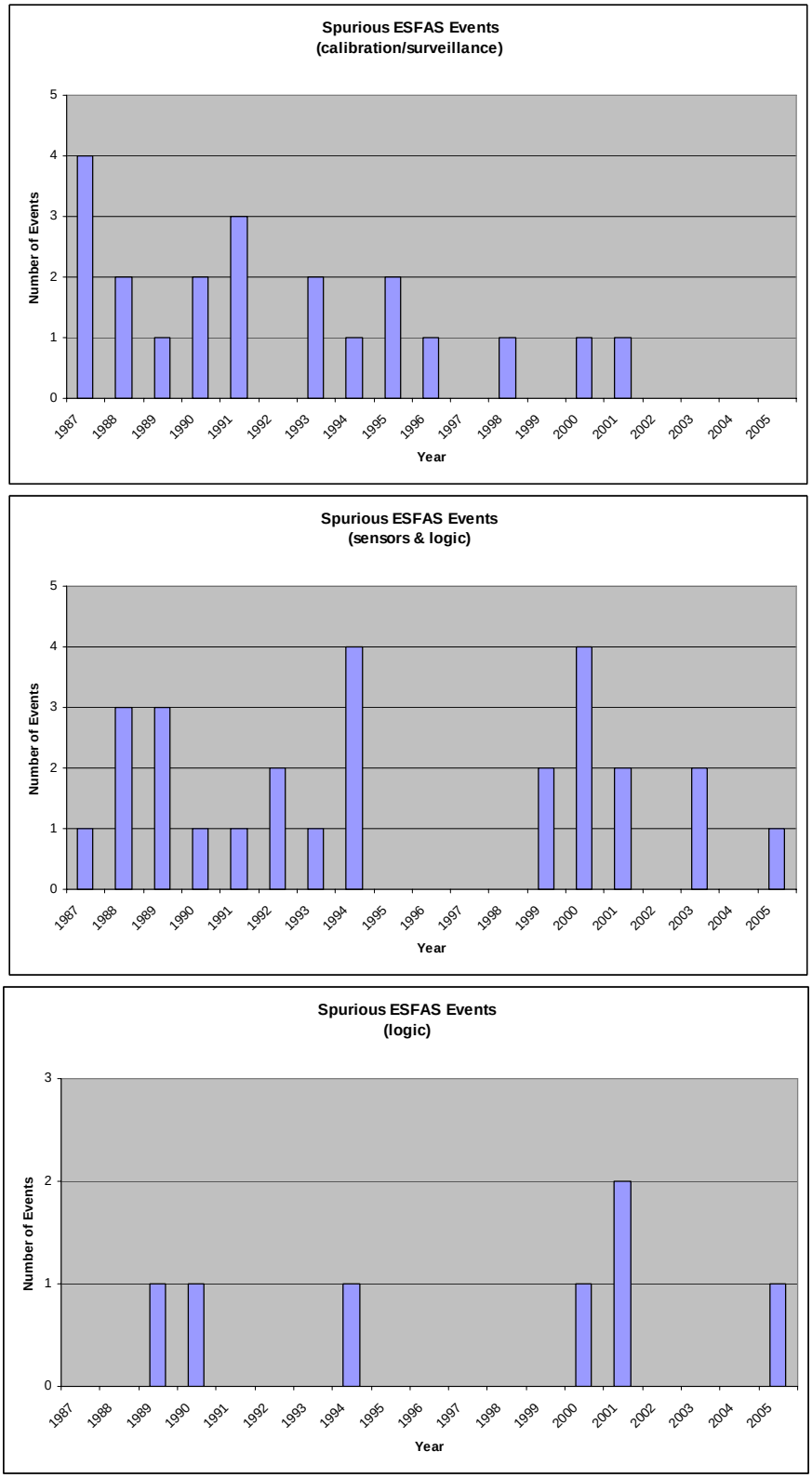


Figure B- 4 Spurious ESFAS Distribution (Sensors & Logic)

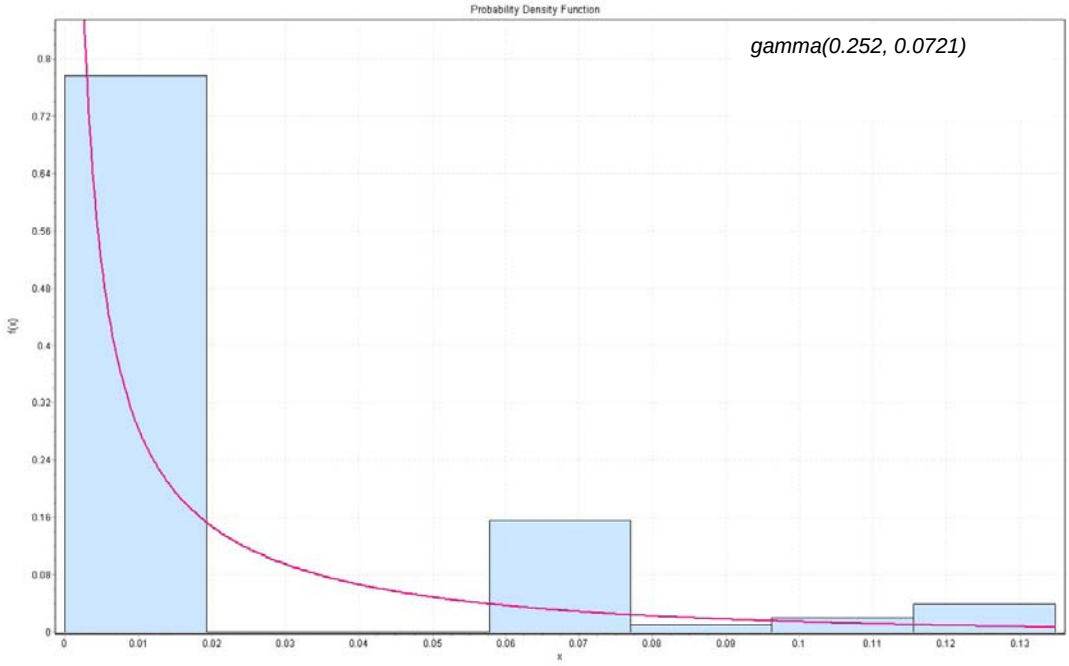
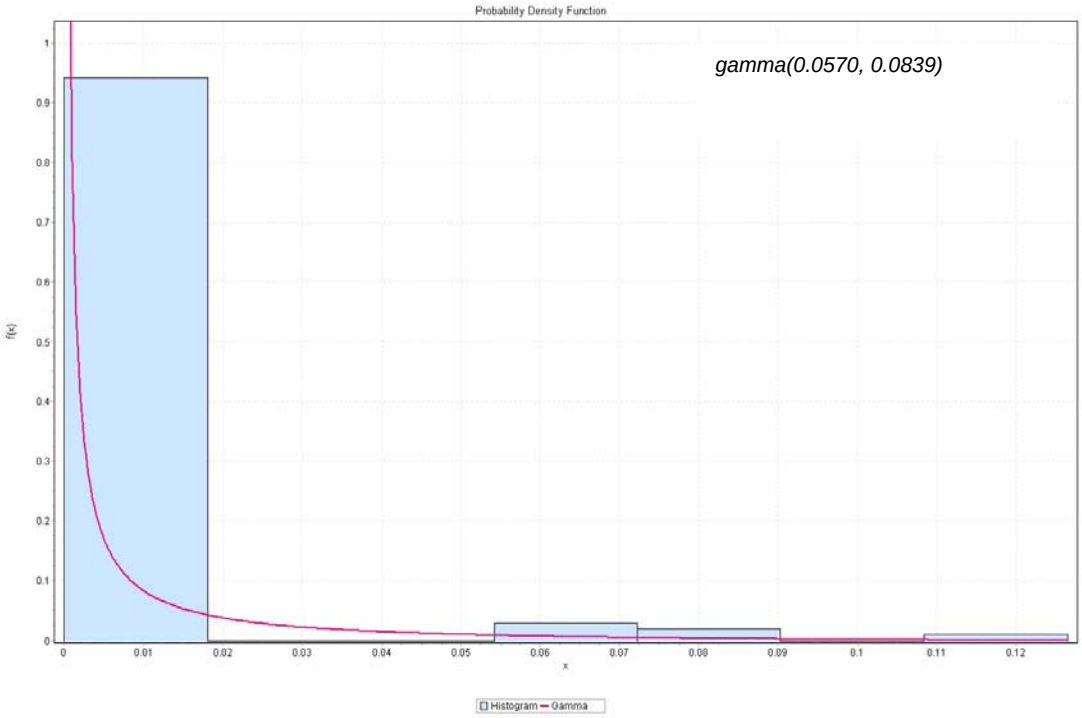


Figure B- 5 Spurious ESFAS Distribution (Logic only)



2. SOFTWARE FAILURE PROBABILITIES

For estimation of software failure probability, this analysis distinguishes between the OS and the application software.

2.1. Operating System

For the purpose of this analysis, the OS is assumed to undergo strictly cyclic operation and constant loading of communication and processing buses. Such a cyclic digital I&C system is always active and always processing the same amount of data regardless of plant conditions. This is an important difference from a hardwired analog system that is in standby until an actual demand occurs or tests are run. Therefore, the actual system demand resulting from the large LOCA or SLB event will place no more stress upon the OS than any other cycle (note that this is not necessarily true of the application software). Other important features are static memory allocation and asynchronous operation, because they prevent OS failures being caused by interference from postulated application software failure. Given that the OS is blind to plant conditions and is available prior to the accident, the OS is considered not to be as significant a source of ESFAS failure as perhaps the application software, sensors or actuation devices.

2.2. Application Software

According to the IEC (International Electrotechnical Commission), the dominant causes of application software failure are latent defects related to faults in the requirements specification, and latent faults introduced during maintenance (software modifications, setpoint changes, version revisions in spare parts). Therefore, they conclude that CCF "can only occur at the combined probability of the existence of the latent systematic fault and the activation of a corresponding triggering mechanism by a signal trajectory." The IEC recommends a defense against CCF that addresses both avoidance of the potential triggering mechanisms and avoidance of the latent faults.

With respect to the application software in this analysis, it is assumed that actuation is initiated by a very simple functions. For example, the functional logic for ECCS actuation may require only a single process input to reach a single fixed setpoint. There are very few interlocks that can potentially block or interfere with the actuation. Such actuation logic is very simple and has been operating in nuclear plants for more than 30 years. There is minimal potential for specification error or misinterpretation of the specifications by the software designer. Further, there is a quality software development life cycle process, including an independent verification and validation (IV&V) methodology to provide assurance that the application software is adequately specified, designed, implemented, tested, and controlled. In addition, the software meets industry consensus design standards such as IEEE Std 379 and IEEE Std. 7-4.3.2. Finally, features such as fault tolerance, data validation and functional diversity of input sensors are assumed to be provided.

Use of appropriate software development standards is a factor in assuring software reliability. IEC 61226 states that "For an individual system which incorporates software developed in

accordance with the highest quality criteria (IEC 60880 and IEC 60987), a figure of the order of 10^{-4} failure / demand may be an appropriate limit to place on the reliability that may be claimed." (Note: IEC 60880 addresses software, while IEC 60987 addresses hardware.) This risk figure applies to the whole of the system from sensors to actuation devices and is intended to encompass all sources of failure due to specification, design, manufacturing, installation operating consideration and maintenance practices. The standard consists largely of software development process requirements and the suggested failure probability should be considered to be the best that can be expected on the basis of process alone. Indeed, a number of regulatory agencies have accepted the use of a failure probability of 10^{-4} for digital equipment qualified for use in safety applications. To justify a lower failure probability estimate, defensive measures beyond just process would need to be present. Application software development processes used in SR nuclear power plant I&C systems are generally comparable to or better than SIL-4, which suggests that a limit to the application software failure probability of 10^{-4} to 10^{-5} is a reasonable value.

For the purpose of this analysis, a base case probability of failure of the ESFAS of 10^{-4} will be assumed. Initially an EF of 10 will be assumed. Sensitivity studies will be performed varying this failure probability by orders of magnitude as well as its EF to determine their impact on the results.

3. OPERATOR ACTIONS

In response to the large LOCA events, no credit is given to the operators initiating low pressure safety injection. The smaller end of the break spectrum has been expanded in the definition of a large LOCA for this analysis and there may be time for the operator to take action for the most likely breaks in this redefined large LOCA break range. The analysis overestimates the benefits of the proposed automated DAS in this regard.

Where operator action is credited is for those transients and accidents for which low pressure injection would be effective in providing adequate core cooling but ample time is available for the operator to take action. From Section 3.2 it is shown that the proposed automated DAS may be redundant to the operators in some scenarios, but only for BWRs. A human error probability is derived for actuating injection systems in the BWRs, as a result.

- PWRs
  No accidents or transients are shown to benefit from the proposed automated DAS as the pressure in the primary system exceeds the shutoff head of the low pressure injection pumps.

- BWRs
  Two accidents potentially benefit from the proposed automated DAS
  Transients without feedwater/condensate plus a coincident SORV
  Medium/large SLB outside containment

The BWR accident with the least amount of time is the transient without feedwater/condensate and a coincident SORV. The medium/large SLB provides more time for the operators as feedwater/condensate is available to provide makeup from the hotwell automatically.

Given the time frame for this operator action (~30m), the Human Cognitive Reliability model is used. It is assumed that the existing BWR EOPs for current plants govern operator response. There are two possible procedures in the BWR EOPs that the operator may take in providing a makeup system; RPV Level Control or RPV Flooding, the former being the preferred path through the EOPs and the latter used when reactor level is unknown. When the normal HSI shows conflicting information, the operator is assumed to leave Reactor Level Control and enter the RPV Flooding Contingency.

A human error probability is derived for the transient with the SORV under two conditions. For the first condition, it is assumed that the operator is using the normal HSI to respond to the event. The second condition assumes a unique prompting alarm exists telling the operator to confirm normal HSI and consider use of the backup diverse HSI. This additional override in the EOPs will leave the operator in the Reactor Level Control procedure as opposed to having to enter the RPV Flooding Contingency.

Operators initiate low pressure injection – RPV Flooding Contingency
Mean = 0.17
EF = 1

Operators initiate low pressure injection – Reactor Level Control
Mean = 3.8E-3
EF = 10

INIT-LPI, Initiate low pressure injection (RPV Flooding Contingency)

Basic Event Summary

Analyst:	
Rev. Date:	03/17/08
Cognitive Method:	HCR/ORE/THERP

Table Error! No text of specified style in document.**-1: INIT-LPI SUMMARY**

Analysis Results:	**without Recovery**	**with Recovery**
P_{cog}	N/A	1.6e-01
P_{exe}	1.0e-02	1.0e-02
Total HEP		1.7e-01
Error Factor		1

HFE Scenario Description:
1. Loss of feedwater
2. Reactor trip on low level (either ESFAS or ARI)
3. SRV operation with SORV
4. Reactor level on normal HSI is conflicting
5. Operator enters RPV flooding

Related Human Interactions:
Initiate high pressure injection
Initiate emergency depressurization

Performance Shaping Factors:
Operators trained on loss of level instrumentation

EOPs contain contingency when vessel level is unknown

Procedure and step governing HI:
RPV Control - Level
RPV Flooding Contingency

Training:

- **None**
X - **Classroom** Frequency: 2
X - **Simulator** Frequency: 1

Degree of Clarity of Cues & Indications:

- **Very Good**
- **Average**
X - **Poor**

Human-Machine Interface:

X - **Control Room Panels**
- **Local Control Panels**
- **Local Equipment**

Special Requirements:

Tools	Parts	Clothing
Required	Required	Required
Adequate	Adequate	Adequate
Available	Available	Available

Type of Response:

- **Skills**
- **X - Rule**
- **Knowledge**

Complexity of Response

Cognitive	Execution
- Complex	- Complex
X - Simple	X - Simple

Environment:

Lighting	Heat/Humidity
X - Normal	X - Normal
- Emergency	- Hot / Humid
- Portable	- Cold
Radiation	**Atmosphere**
X - Background	X - Normal
- Green	- Steam
- Yellow	- Smoke
- Red	- Respirator required

Equipment Accessibility:

	Location	Accessibility
X	**Control Room Front Panels**	Accessible
	Control Room Back Panels	
	Hot Shutdown Panels	
	Auxiliary Building	
	Electrical Building	
	Containment	
	Pump house	
	Switchyard	

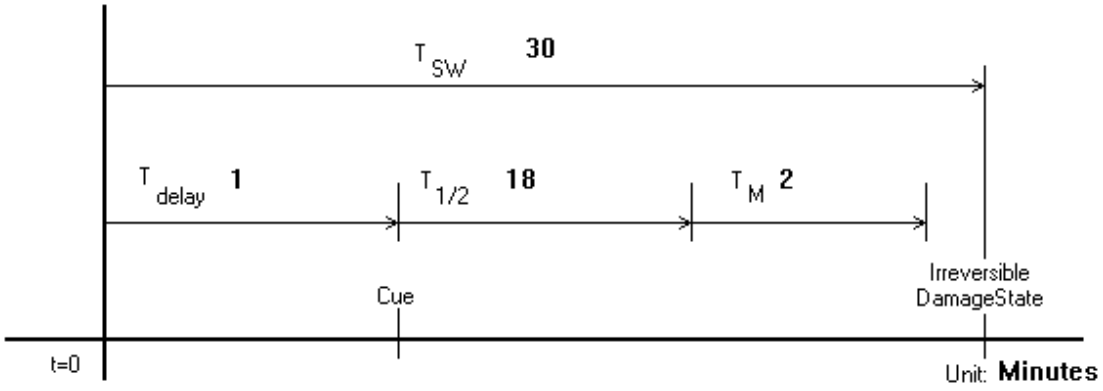
Stress:

- **Optimum (Low)**
- **X - Moderate**
- **Extreme (High)**

Cognitive

INIT-LPI

Cue:
Reactor Trip
Stuck open SRV
Conflicting level indication from normal HSI



Referen

ce for System Time: MAAP SORV no injection

Reference for Manipulation Time: 2 min per step

Duration of time window available for action (TW): 9.00 Minutes

Sigma Decision Tree

	Skill vs. Rule		Procedures		Training		Stress
	Skill	**X**	Yes	**X**	Yes		Yes
X	Rule		No		No	**X**	No

Sigma: 4.0e-01

HEP: 1.6e-01

Execution Unrecovered

INIT-LPI

Table Error! No text of specified style in document.**-2: INIT-LPI EXECUTION UNRECOVERED**

Step		Omission					Commission					Total	
Step No.	HEP	Table Ref.	Item Ref.	Stress E/M/O	Stress Value	HEP	Table Ref.	Item Ref.	Stress E/M/O	Stress Value	Over Ride	Per Step
1	3.8E-3	20-7	3	M	2							7.6e-03
Actions: Open 3 ADS valves						Comments:						
2	1.3E-3	20-7	1	M	2							2.6e-03
Actions: Initiate low pressure injection						Comments:						

Execution Recovery

INIT-LPI

Table Error! No text of specified style in document.**-3: INIT-LPI EXECUTION RECOVERY**

Critical Step No.	Recovery Step No.	Action	HEP (Crit)	HEP (Rec)	Dep.	Cond. HEP (Rec)	Total for Step
1		Open 3 ADS valves	7.6e-03				
2		Initiate low pressure injection	2.6e-03				
		Total Unrecovered:	1.0e-02			Total Recovered:	1.0e-02

INIT-LPI-UPA, Initiate low pressure injection (RPV Level Control)

Basic Event Summary

Analyst:	
Rev. Date:	03/17/08
Cognitive Method:	HCR/ORE/THERP

Table Error! No text of specified style in document.**-4: INIT-LPI-UPA SUMMARY**

Analysis Results:	**without Recovery**	**with Recovery**
P_{cog}	N/A	1.2e-03
P_{exe}	2.6e-03	2.6e-03
Total HEP		3.8e-03
Error Factor		5

HFE Scenario Description:
1. Loss of feedwater
2. Reactor trip on low level (either ESFAS or ARI)
3. SRV operation with SORV
4. Reactor level on normal HSI is conflicting
5. RPT/ARI alarm
6. Operator enters RPV flooding

Related Human Interactions:
Initiate high pressure injection
Initiate emergency depressurization

Performance Shaping Factors:
Operators trained on loss of level instrumentation

EOPs contain override should unique prompting alarm occur

Procedure and step governing HI:
RPV Control - Level

Training:

- **None**
X - **Classroom** Frequency: 2
X - **Simulator** Frequency: 1

Degree of Clarity of Cues & Indications:

- **Very Good**
- **Average**
X - **Poor**

Human-Machine Interface:

X - **Control Room Panels**

- **Local Control Panels**
- **Local Equipment**

Special Requirements:

Tools	**Parts**	**Clothing**
Required	Required	Required
Adequate	Adequate	Adequate
Available	Available	Available

Type of Response:

- **Skills**

X - **Rule**

- **Knowledge**

Complexity of Response

Cognitive		**Execution**	
-	Complex	-	Complex
X	- Simple	**X**	- Simple

Environment:

Lighting		**Heat/Humidity**	
X	- Normal	**X**	- Normal
	- Emergency		- Hot / Humid
	- Portable		- Cold
Radiation		**Atmosphere**	
X	- Background	**X**	- Normal
	- Green		- Steam
	- Yellow		- Smoke
	- Red		- Respirator required

Equipment Accessibility:

	Location	**Accessibility**
X	- **Control Room Front Panels**	Accessible
	- **Control Room Back Panels**	
	- **Hot Shutdown Panels**	
	- **Auxiliary Building**	
	- **Electrical Building**	
	- **Containment**	
	- **Pump house**	
	- **Switchyard**	

Stress:

- **Optimum (Low)**

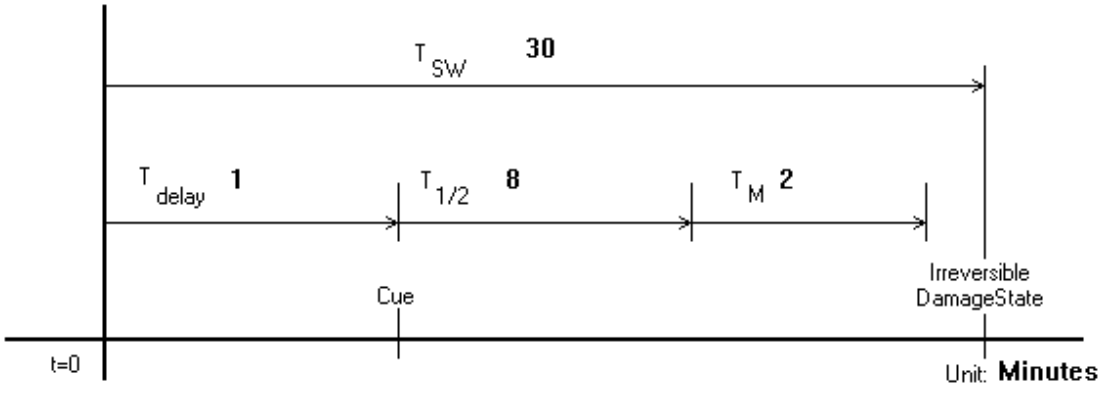
X - **Moderate**

- **Extreme (High)**

Cognitive

INIT-LPI-UPA

Cue:
Reactor Trip
Stuck open SRV
Conflicting level indication from normal HSI



Referen

ce for System Time: MAAP SORV no injection

Reference for Manipulation Time: 2 min per step

Duration of time window available for action (TW): 19.00 Minutes

Sigma Decision Tree

	Skill vs. Rule		Procedures		Training		Stress
	Skill	X	Yes	X	Yes		Yes
X	Rule		No		No	X	No

Sigma: 4.0e-01

HEP: 1.2e-03

Execution Unrecovered

INIT-LPI-UPA

Table Error! No text of specified style in document.**-5: INIT-LPI-UPA EXECUTION UNRECOVERED**

Step	Omission					Commission					Total	
Step No.	HEP	Table Ref.	Item Ref.	Stress E/M/O	Stress Value	HEP	Table Ref.	Item Ref.	Stress E/M/O	Stress Value	Over Ride	Per Step
2	1.3E-3	20-7	1	M	2							2.6e-03
Actions: Initiate low pressure injection						Comments:						

Execution Recovery

INIT-LPI-UPA

Table Error! No text of specified style in document.**-6: INIT-LPI-UPA EXECUTION RECOVERY**

Critical Step No.	Recovery Step No.	Action	HEP (Crit)	HEP (Rec)	Dep.	Cond. HEP (Rec)	Total for Step
2		Initiate low pressure injection	2.6e-03				
		Total Unrecovered:	2.6e-03			Total Recovered:	2.6e-03

4. PLANT RELATED DATA

Information from 10 plants is provided in this attachment as input to the evaluation of benefits and risks associated with the automated DAS proposed by the NRC in its D3 ISG. In this section is found for each of the 10 plants:

- Identification of what is actuated when a safety injection signal or ECCS actuation occurs
- Conditional core damage probabilities for selected initiating events.
- Conditional containment failure probability and offsite dose consequences given a LOCA with failure of injection.

4.1. BWR 2 Plant

ECCS Actuation Functions – low reactor level **(bold indicates assumed automated DAS functions)**

1. Containment Isolation
2. Containment Spray Pump Start
3. **Core Spray Pump Start**
4. **Core Spray Injection Initiation**
5. Emergency Condenser Initiation
6. Reactor Vessel Isolation
7. ADS permissive and timer start

Conditional Core Damage Probabilities

No Trip*	-
General Transient	7.1E-7
MSIV Closure**	7.5E-7

* Assumed effect of spurious ECCS DAS given no load shedding of non-essential loads
** Assumed effect of spurious steam line isolation

Containment Response (LOCA)

Conditional Large Early Release Probability	0.15
Large Early Release Dose	1.5E+6 person-rem

4.2. BWR 3 Plant

ECCS Actuation Functions – low reactor level **(bold indicates assumed automated DAS functions)**

1. ADS permissive and timer start
2. **HPCI initiation**
3. RCIC initiation
4. **Core Spray initiation**
5. **LPCI initiation**
6. Reactor Vessel Isolation
7. Containment Spray Pump Start
8. Containment Isolation
9. **Load shed non-essential systems (RHRSW and DW Coolers)**

Conditional Core Damage Probabilities

General Transient*	5.7E-7
MSIV Closure**	5.9E-7

* Assumed effect of spurious ECCS DAS given load shedding of non-essential systems
** Assumed effect of spurious steam line isolation

Containment Response (LOCA)

Conditional Large Early Release Probability	0.02
Large Early Release Dose	3E+5 person-rem

4.3. BWR 4 Plant

ECCS Actuation Functions – low reactor level **(bold indicates assumed automated DAS functions)**

1. ADS permissive and timer start
2. **HPCI initiation**
3. RCIC initiation
4. **Core Spray initiation**
5. **LPCI initiation**
6. Reactor Vessel Isolation
7. Containment Spray Pump Start
8. Containment Isolation
9. **Load shed non-essential systems (DW Coolers)**

Conditional Core Damage Probabilities

General Transient*	7.6E-7
MSIV Closure**	2.8E-5

* Assumed effect of spurious ECCS DAS given load shedding of non-essential systems
** Assumed effect of spurious steam line isolation

Containment Response (LOCA)

Conditional Large Early Release Probability	0.21
Large Early Release Dose	6.5E+5 person-rem

4.4. BWR 5 Plant

ECCS Actuation Functions – low reactor level **(bold indicates assumed automated DAS functions)**

1. ADS permissive and timer start
2. RCIC initiation
3. **HPCS initiation**
4. **LPCS initiation**
5. **LPCI initiation**
6. **Isolate RBCCW flow to containment (drywell coolers)**

Conditional Core Damage Probabilities

General Transient	6.6E-7
MSIV Closure**	2.0E-6

* Assumed effect of spurious ECCS DAS given isolation of non-essential systems
** Assumed effect of spurious steam line isolation

Containment Response (LOCA)

Conditional Containment Failure Probability	0.22
Large Early Release Dose	2.5E+6 person-rem

4.5. BWR 6 Plant

ECCS Actuation Functions – low reactor level **(bold indicates assumed automated DAS functions)**

1. ADS permissive and timer start
2. RCIC initiation plus turbine trip
3. **HPCS initiation**
4. **LPCS initiation**
5. **LPCI initiation**
6. **Shutdown Service Water initiation**
7. Containment Isolation
8. Control Room Ventilation
9. Standby Gas Treatment System
10. Emergency Diesel and HPCS Diesel start
11. **Trip of non-essential trains of equipment (e.g., drywell coolers)**

Conditional Core Damage Probabilities

General Transient	7.6E-7
MSIV Closure**	1.8E-6

* Assumed effect of spurious ECCS DAS given load shedding of non-essential systems
** Assumed effect of spurious steam line isolation

Containment Response (LOCA)

Conditional Containment Failure Probability	0.01
Large Early Release Dose	8.4E+6 *

* Scaled from BWR 4 large early release dose based on core inventory and similar site characteristics

4.6. Westinghouse 2 Loop Plant

Effects of Safety Injection Actuation

1. SI Pumps Start
2. **RHR Pumps Start**
3. **Align valves as necessary for ECCS flow**
4. Containment Spray Starts
5. Charging Pumps stop
6. MFW Isolations close

Conditional Core Damage Probabilities

General Transient	1.47E-6
Loss of Feedwater	1.30E-6
Spurious ESFAS	NA

Containment Response (LOCA)

Conditional Containment Failure Probability	1.0E-2
Large Early Release Dose	3.4E+6 person-rem

4.7. Westinghouse 4-Loop Plant

Effects of Safety Injection Actuation

1. Start Centrifugal Charging Pumps and stop Normal Charging Pump.
2. **Start SI and RHR pumps**.
3. **Align valves as necessary for ECCS flow.**
4. **Open UHS Return valves and Essential Service Water pumps.**
5. **Start CCW pumps and open CCW Service Loop Supply and Return valves.**
6. **Open CCW to RHR to RHR HX valves.**
7. Close Spent Fuel Pool HX CCW Outlet valves.
8. Stop Spent Fuel Pool Cooling Pumps.
9. Start Containment Cooler Fans and Containment Hydrogen Mixing Fans.
10. Actuate Containment Isolation Phase A and close Phase A valves.
11. Close SG blowdown isolation valves.
12. Actuate Control Room Ventilation Isolation and align CRVIS components.
13. Actuate Containment Purge Isolation and close CPIS dampers.
14. Open Generator output breakers.
15. Trip Main Feedwater pumps and close MFW valves.
16. Start Auxiliary Feedwater pumps and align AFW valves.
17. Close Pressurizer PORVs and Spray Valves.

Conditional Core Damage Probabilities

General Transient	3.2E-7
Loss of Feedwater	5.8E-6
Spurious ESFAS	NA

Containment Response (LOCA)

Conditional Containment Failure Probability	1.4E-2
Large Early Release Dose	3.1E+5 person-rem

4.8. Combustion Engineering Plant #1

Effects of Safety Injection Actuation – low pressurizer pressure **(bold indicates assumed automated DAS functions)**

1. Starts HPSI and opens LOOP MOVs
2. **Starts LPSI and opens LOOP MOVs**
3. **Starts Safety Related Compressed Air**
4. **Starts Service Water and Component Cooling Water pumps (All SR cooling)**
5. Aligns Component Cooling Water to Containment Spray cooling
6. Starts Charging Pumps and aligns Boric Acid suction for charging and isolates Letdown
7. Isolates RCP Seal Bleedoff
8. **Isolates Service Water to the Turbine Bldg – loss of cooling to Secondary and to NSR Air Compressors**
9. CR HVAC to Recirculation
10. Starts Diesel Generators

Various other functions – such as some small Containment Isolations which are normally closed and sends signal to return to normal position for various other valves

Conditional Core Damage Probabilities

General Transient	2.81E-06
Loss of Feedwater	5.02E-06
Spurious ESFAS*	2.06E-5

* Assumed effect of spurious DAS given item 8 under Effects of Safety Injection Actuation

Containment Response (LOCA)

Conditional Containment Failure Probability	0.01
Large Early Release Dose	2.45E+6 person-rem

4.9. Combustion Engineering Plant #2

Effects of Safety Injection Actuation – low pressurizer pressure **(bold indicates assumed automated DAS functions)**

1. Starts HPSI and opens LOOP MOVs
2. **Starts LPSI and opens LOOP MOVs**
3. **Starts Service Water and Component Cooling Water pumps (All SR cooling)**
4. Starts Charging Pumps and aligns Boric Acid suction for charging and isolates letdown
5. Isolates RCP Seal Bleedoff
6. **Isolates Service Water to the Turbine Bldg – loss of cooling to NSR loads**
7. CR HVAC to Recirculation
8. Starts Diesel Generators

Conditional Core Damage Probabilities

General Transient	1.8E-06
Loss of Feedwater*	1.8E-06
Spurious ESFAS	NA

* Assumed effect of spurious DAS given item 6 under Effects of Safety Injection Actuation

Containment Response (LOCA)

Conditional Containment Failure Probability	8E-3
Large Early Release Dose	6.2E+6 person-rem

4.10. Babcock & Wilcox Plant

Effects of Safety Injection Actuation – low pressurizer pressure **(bold indicates assumed automated DAS functions)**

1. Initiates HPI
2. **Initiates LPI**
3. **Initiates Emergency Service Water**
4. Initiates emergency power
5. Isolates non essential reactor building cooling
6. Arms non-essential load shed (but does not load shed unless there is undervoltage)

Conditional Core Damage Probabilities

No Trip*	–
General Transient	1.3E-6
Loss of Feedwater	4.0E-6
Spurious ESFAS**	3.1E-5

* Assumed effect of spurious DAS given lack of undervoltage and low impact of non-essential cooling

** Only if HPI is initiated by the spurious DAS

Containment Response (LOCA)

Conditional Containment Failure Probability	<1E-2
Large Early Release Dose	1E+6 person-rem

E
REGULATORY ACCEPTANCE CRITERIA

Table E-1 is the regulatory acceptance criteria used by the NRC to determine the value-impact of new generic and plant specific regulatory requirements. (Ref: NUREG/BR-0058 “Regulatory Analysis Guidelines of the US Nuclear Regulatory Commission”).

Table E-1 NUREG/BR-0058, Table 3-2 (Safety Goal Screening Criteria)

ΔCDF	**Conditional Containment Failure probability**	
	0.01	0.1
1E-3 – 1E-4	Proceed to Value/Impact portion of Regulatory Analysis	Proceed to Value/Impact portion of Regulatory Analysis
1E-4 – 1E-5	Management decision as to whether to proceed with Value/Impact portion of Regulatory Analysis	Proceed to Value/Impact portion of Regulatory Analysis
1E-5 – 1E-6	No action taken	Management decision as to whether to proceed with Value/Impact portion of Regulatory Analysis

NUREG/BR-0058, Section 4.3.5 Evaluation of Values and Impacts

"In order to place all values and impacts on a common basis, a conversion factor is needed that reflects the monetary worth of a unit of radiation exposure. The currently recommended value for this dollar conversion factor is $2000 per person-rem. This dollar value only captures the health effects attributable to radiological exposure. In select regulatory applications, such as certain severe power reactor accident scenarios, a radiological release could also result in offsite property consequences with monetary consequences that would need to be addressed separately and treated as an additive factor in the overall value-impact assessment."