Appendix A

Significance Determination of Reactor Inspection Findings for At-Power Situations

1. Entry Conditions

This SDP provides a simplified risk-informed framework to estimate the increase in core damage frequency during at-power operations due to conditions which contribute unintended risk increases caused by deficient licensee performance. Conditions which do NOT represent deficient licensee performance, as determined by the staff, are considered part of the acceptable plant normal operating risk, and are NOT candidates for SDP evaluation. The entry conditions for the plant-specific reactor safety SDP described in this Appendix are degraded plant equipment, functions, or processes affecting initiating event frequency, mitigation system availability/reliability, or RCS barrier integrity that result from deficient licensee performance. Concurrent performance deficiencies should be assessed collectively, as applicable, to determine total contribution to change in the CDF, however, each performance deficiency should be assigned a color individually. Screening questions are also provided for inspection findings in the Barrier cornerstone, and the inspector is referred to Appendix H of this Chapter if appropriate.

Each issue should first be screened by using manual chapter 0610* Appendix B group 1, 2 and 3 questions to determine whether or not the issue is a minor issue. If the issue sreens as minor this SDP should not be entered.

2. Applicability

The process in this Chapter is designed to provide NRC inspectors and management with a simple probabilistic risk framework for use in identifying potentially risk-significant issues within the initiating events, mitigation systems, and barriers cornerstones. This SDP also helps facilitate communication of the basis for significance between the NRC and licensees. In addition, it identifies findings that do not warrant further NRC engagement, due to very low risk significance, when these findings are entered into the licensee's corrective action program. The user of this SDP should have a basic understanding of the specific reactor technology associated with the inspection finding being evaluated and generally of the probabilistic risk analysis framework, to a depth provided by NRC training courses required for reactor inspector qualification.

3. Non-Applicability of SDP for NRC Determination of Risk Significance of Events

The risk significance of actual reactor events caused or complicated by equipment malfunction or operator error should always be assessed by NRC risk analysts in accordance with applicable NRC event response guidance. Although this SDP may provide useful risk insights to inspectors for event response or followup, it was not designed or intended to be used for this purpose. The risk significance of an event is characterized by the probability that the core could have been damaged at the moment of

the event given all the known conditions. Conversely, the SDP estimates the increase in core damage frequency for the spectrum of all postulated initiating events over a period of time during which known equipment or functional degradation existed. Therefore, the SDP is not used for event significance evaluations.

4. Relationship to the Risk-Informed Performance Indicators

The NRC Reactor Oversight Process (as defined in IMC 2515) evaluates licensee performance using a combination of Performance Indicators (PIs) and inspections. Thresholds have been established for the PIs, which, if exceeded, may prompt additional NRC actions to focus both licensee and NRC attention toward areas in which there is a potential decline in licensee performance. The SDP described in this Appendix and illustrated in Figure 1 estimates the risk- significance of inspection findings using the same "scale" as is used for the risk-informed performance indicators (i.e., initiating events and safety system unavailability) so that licensee performance can be assessed by comparing and "adding" the contributions of both performance indicators and inspection findings. Licensee-identified issues, when reviewed by NRC inspectors, are also candidates for this process because the NRC reactor oversight process uses risk significance estimation as a more objective means to evaluate licensee performance.

5. Organization of Appendix A

Attachment 1 - User Guidance for Significance Determination of Reactor Inspection Findings for At-Power Situations

Basic Guidance

SDP Phase 1 Worksheet For Degraded Plant Condition
Reactor Safety SDP Table 1 - Estimated Likelihood for Initiating Event Occurrence During Degraded Period
Reactor Safety SDP Table 2 - Risk Significance Estimation Matrix
Reactor Safety SDP Table 3 - Remaining Capability Rating Values

Detailed Guidance

Use of SDP for Event Response

Attachment 2 - Basis Information

Attachment 3 - Site Specific Phase 2 Worksheets, Notebooks. Placeholder.

END

ATTACHMENT 1

User Guidance
for Significance Determination of Reactor Inspection Findings
for At-Power Situations

1. Phase 1, 2, and 3

The plant-specific reactor safety SDP described in this Appendix uses a graduated three-phase process to differentiate inspection findings on the basis of their potential risk significance.

Phase 1 - Characterization and Initial Screening of Findings: Precise characterization of the finding and an initial screening of very low-significance findings for disposition by the licensee's corrective action program

Phase 2 - Initial Risk Significance Approximation and Basis: Initial approximation of the risk significance of the finding and development of the basis for this determination for those findings that pass through the Phase 1 screening

Phase 3 - Risk Significance Finalization and Justification: Review and as-needed refinement of the risk significance estimation results from Phase 2, or development of any risk analysis outside of this guidance, by an NRC risk analyst (any departure from the guidance provided in this Appendix for Phase 1 or Phase 2 constitutes a Phase 3 analysis and must be performed by an NRC risk analyst)

Phases 1 and 2 are intended to be accomplished primarily by field inspectors and their supervisors/managers. Until a user becomes practiced in its use, it is expected that an NRC risk analyst may be needed to assist with some of the assumptions used for the Phase 2 assessment. However, as inspection personnel become more familiar with the process, involvement of a risk analyst is expected to become more limited. The Phase 3 review/analysis is intended to confirm or modify Phase 2 results that may have greater than very low significance ("white" or above), potentially significant ("green" next to "white"), or controversial. Phase 3 analysis methods will utilize current PRA techniques and rely on the expertise of NRC risk analysts.

Inspectors are encouraged to obtain licensee risk perspectives as early in the SDP process as a licensee is prepared to offer them, and to use the SDP framework to the extent possible to evaluate the adequacy of the licensee's assumptions.

2. Use of SDP Phase 1 and Phase 2 Worksheets

Inspectors may use the SDP Worksheets provided in this Chapter to aid in documenting the facts of the finding and their stated assumptions. Since the SDP result depends on these inputs, documenting them is necessary if the basis for the result is to be understood by others. The Phase 1 Worksheet is generic for all plant types and is included in this Appendix. The Phase 2 Worksheets are plant-specific to account for variations in available mitigation equipment and other plant-specific attributes. The Phase 2 Worksheets, identified as Table 3 are provided separately from this Appendix in plant-specific SDP Notebooks.

The Phase 1 and 2 Worksheets are not required to be included in the inspection report. However, any finding documented in an inspection report should be given sufficient detail to allow a knowledgeable reader to reconstruct the SDP determination. This is intended to provide a clear and objective basis for the significance determination of the finding. Further guidance on inspection report documentation is provided in IMC 0610*.

3. Treatment of Reactor Safety Inspection Issues Not Addressed By SDP Worksheets

Even if the SDP Worksheets do not explicitly address the inspection finding of concern, the basic probabilistic framework represented by SDP plant specific Tables 1, 2, and 3, and generic Tables 4 and 5 may be used to help develop a basis for potential significance. This is done by first identifying the core damage accident scenario of greatest concern. This will be the core damage scenario having the greatest increase in its likelihood of occurrence (i.e., estimated frequency) due to the effect of the inspection finding. If an inspector can identify candidate scenarios, then Table 1 can be used to help estimate the likelihood of the initiating events and Table 5 can be used to help estimate the Remaining Mitigation Capability to each failure event within the scenarios. SDP Table 4 can then be used with these inputs to estimate the change in core damage frequency represented by the identified scenario.

This process is basic to any probabilistic risk analysis and can be used for issues related to areas such as spent fuel pool cooling, low-power/startup issues, etc. This is essentially a Phase 3 analysis and the assistance of a risk analyst will be necessary. However, the inspector is encouraged to provide as much input as possible in the development of the scenarios of concern and to assist the risk analyst in identifying any conditions influencing the likelihoods of the failure events that constitute the scenarios.

DELETED GRAPH ELIMINATE THIS PAGE.

5. At-Power Internal Events Plant-Specific Reactor Safety SDP Basic User Procedure (Desk Aid)

It is important to remember that the objective of this SDP is to identify those at-power core damage accident sequences whose likelihood is increased due to the conditions described in the inspection finding and to estimate the resulting likelihood (i.e., frequency) of those sequences.

Phase 1 - Characterization and Initial Screening of Findings

Step 1.1 - Definition of the Inspection Finding and Assumed Impact

Using the Phase 1 Worksheets, fully and factually describe the known observations associated with the issue. Describe the assumed impact on affected plant safety functions. Do not include hypothetical conditions, e.g., single failure criteria. A bounding determination of significance may be made by assuming a worst-case condition (e.g., assume complete loss of function, even if unsupported by the facts known at that time). If a bounding determination results in greater than green, greater factual detail will be necessary to complete the SDP.

Step 1.2 - Initial Screening of the Inspection Finding

Use the decision logic in the Phase 1 Worksheets to determine if the issue can be characterized as green without the need for more detailed analysis of potential risk increase by Phase 2. Inspectors are encouraged to evaluate findings using Phase 2 even if they screen as Green in Phase 1. Doing so helps the inspector develop plant-specific risk insights and may alert the inspector to cases where multiple concurrent findings could have a significant risk impact.

Phase 2 - Initial Risk Significance Approximation and Basis

The Phase 2 process incorporates the following Tables.

Plant Specific Tables found in the individual Risk-informed Inspection Notebooks:

Table 1 "Categories for Initiating Events";
Table 2 "Initiators and System Dependency for XXX Plant";
Table 3 "SDP Worksheets for XXX Plant;

Generic version of Table 1 is incorporated into this document for information only.

Generic Tables located in this document to be used in conjunction with the Notebooks:

Table 4 "Risk Estimation Matrix";
Table 5 "Type of Remaining Capability".

Step 2.1 - Select or Define the Applicable Initiating Event Scenarios

Enter the plant-specific Table 2 "Initiators and System Dependency for XXX Plant" with the equipment or safety functions assumed to be affected and determine the initiating event scenarios that must be evaluated (i.e., the affected function plays some role in mitigating the initiating event scenario). This Table is provided in the plant-specific SDP notebook.

It may also be possible for an inspector to define core damage accident sequences that are not already represented in the plant-specific SDP notebook. If such sequences are identified, obtain the assistance of an NRC risk analyst to review the analysis.

Step 2.2 - Estimation of the Likelihood of Scenario Initiating Events and Conditions

From SDP Table 1 "Categories of Initiating Events" in this Appendix, select the appropriate Estimated Likelihood Ratings (i.e., A - H) for the initiating event scenarios identified in Step 2.1. At the top of the plant-specific Phase 2 Worksheets found in the SDP notebook for that plant, enter the Estimated Likelihood Rating information from Table 1 on each of the applicable Phase 2 Worksheets.

Step 2.3 - Estimation of Remaining Mitigation Capability

Step 2.3.1 The various safety functions needed to mitigate the specific initiating event are listed in the upper section of the applicable Phase 2 Worksheet. All of the creditable plant-specific capability that is potentially available to satisfy the safety function is listed on the right. Below the safety function section of the Worksheet is a listing of core damage sequences associated with the initiating event being evaluated. Circle the safety functions listed in these sequences that are affected by the inspection finding and consider ONLY those sequences in the following steps.

Step 2.3.2 Given the unavailability of the equipment or function as identified in the inspection finding, determine the remaining creditable mitigation capability for each affected sequence as follows:

Step 2.3.2.1 Determine if the nature of the degradation is such that an operator could recover the unavailable equipment or function in time to mitigate the assumed initiating event. A credit may be given in the designated column of the Phase 2 Worksheet *only* if such operator recovery action meets the five requirements specified on the Worksheet. Document any assumptions on the Worksheet.

Step 2.3.2.2 For the *affected* safety function in the sequence, determine the *remaining* capability. For the *unaffected* safety functions in the sequence, use the *full* capability as listed in the upper right section of the Worksheet. Document all remaining capability for each affected sequence in the space provided to the right. For each remaining capability credited, use Table 3 to determine the Remaining Capability Rating. Sum these ratings for the sequence. Any credited equipment must be monitored by the licensee under the provisions of 10 CFR 50.65 (the Maintenance Rule).

Step 2.4 - Estimating the Risk Significance of Inspection Findings

Step 2.4.1 For each affected sequence, enter Table 4 "Risk Significance Estimation Matrix" using the results from Table 1 (from step 2.2 above) and the total Remaining Capability Rating (from step 2.3.2 above). Determine the color and cell location in Table 4 for each sequence.

Step 2.4.2 For each row in Table 4, note the total number of "counts" in each cell (i.e., number of times a sequence result occurred in the cell). Determine the number of counts in Green cells that are adjacent (horizontally or vertically only) to White cells. If there are **three or more** counts in Green cells adjacent to White cells, then a Phase 3 review should be conducted to confirm the significance of the finding. Similarly, determine the number of counts in White cells that are adjacent to Yellow cells and apply the same rule as above for all cells, starting with White and working toward Red. The significance of the inspection findings for results greater than Green will be confirmed by a Phase 3 analysis.

Step 2.5 - Screening for the Potential Risk Contribution Due to External Initiating Events

The plant-specific SDP Phase 2 Worksheets do not currently include initiating events related to fire, flooding, severe weather, seismic, or other initiating events that are considered by the licensee's IPEEE analysis. If the inspection finding was sent to Phase 2 based on Phase 1 screening criteria that did not evaluate its potential effect on plant risk from external initiating events, it is possible that this effect may not be accounted for in the Phase 2 significance determination. Therefore, the finding should be screened for the potential additive effect of core damage sequences involving external initiating events that could increase the total change in core damage frequency to greater than 1E-6/yr (greater than Green). This should be done by the inspector using the following criteria:

1. If the licensee's current risk analysis for their plant incorporates external initiating events and the equipment or function being evaluated has been assigned a risk importance measure (e.g., RAW), based on this analysis, that would result in its unavailability causing an increase in core damage frequency of greater than 1E-6/yr, then identify the core damage scenarios of concern and provide this input for a Phase 3 analysis.

2. If the licensee's current risk analysis for their plant does NOT incorporate external initiating events, then determine if the affected equipment or function has been otherwise identified by the licensee as risk significant in their IPEEE. If possible, identify the core damage scenarios of concern. Provide this input for a Phase 3 analysis.
3. Review the external initiating event precursor screening criteria given in the Phase 1 Worksheet. If these criteria are met, then identify the core damage scenarios of concern and provide this input for a Phase 3 analysis.

Step 2.6 - Screening for the Potential Risk Contribution Due to LERF

If the Phase 2 analysis result is Green, but any of the core damage sequence types listed below result in a Green cell adjacent (horizontally or vertically only) to a White cell in SDP Table 2, then the finding should be screened for its potential risk contribution to LERF using IMC 0609 Appendix H.

ISLOCA, Transients, or Small LOCAs for all reactor containment types

ATWS for BWR Mark I reactor containment types

SGTRs for all PWR reactor containment types

Phase 3 - Risk Significance Finalization and Justification

When applied, Phase 3 is an important part of the SDP. Inspectors should provide as much risk insight as possible from the Phase 2 analysis described above to the NRC risk analyst for any inspection finding resulting in greater than Green or if either the Step 2.5 or Step 2.6 criteria require the finding to be analyzed in Phase 3. The final determination of finding significance is the responsibility of the NRC staff.

Step 3.1 - Human Reliability Analysis (HRA) Model

It is recognized that several HRA methods are available to quantify human error probabilities (HEPs) for use in probabilistic risk analysis (PRA) models. However, there is no general agreement among PRA experts as to which HRA method should be used for HEP quantification. For SDP Phase 3 evaluations, the HRA method used in a licensee's PRA model may be considered a reasonable basis for the significance determination of the inspection finding, provided that any significant concerns raised by the staff with the HRA method used in the licensee's PRA model (e.g., in the staff's review of the licensee's IPE submittal) have been corrected. If the analyst's significance determination uses the NRC's Standardized Plant Analysis Risk (SPAR) model, it would then be appropriate to use the Accident Sequence Precursor (ASP) Human Error Worksheet to derive the applicable HEPs. The analyst should always determine the adequacy of any influential assumptions used in any HEP analysis.

Step 3.2 - Initiating Event Frequency

NUREG/CR-5750, "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987 - 1995," provides updated generic frequency estimates for the occurrence of initiating events in U.S. nuclear plants. For SDP Phase 3 evaluations, risk analysts may use the frequency estimates of LOCA events as listed in NUREG/CR-5750. However, the initiating event frequency estimates used in the licensee's PRA model should be used if these estimates are more conservative (i.e., higher) than those listed in NUREG/CR-5750. If relevant factual evidence of plant conditions or characteristics are known and could increase these frequency estimates, then SPSB/NRR should be consulted to determine whether the factual evidence and its associated degree of uncertainty provides reasonable confidence that the frequency estimates do not significantly alter the significance characterization of the inspection finding.

Documentation

Each finding processed through the SDP must be given a color characterizing its significance. In addition, each colored inspection finding must be justified with sufficient detail to allow a knowledgeable reader to reconstruct the decision logic used to arrive at the final color. Further guidance on inspection report documentation is given in IMC 0610.

SDP PHASE 1 SCREENING WORKSHEET FOR IE, MS, and B CORNERSTONES

Reference/Title (LER #, Inspection Report #, etc):

Factual Description of Identified Condition (statement of facts known about the finding, without hypothetical failures included):

System(s) degraded by identified condition:

Train(s) degraded by identified condition:

Licensing Basis Function of System(s) or Train(s) (as applicable):

Other Safety Function of System(s) or Train(s) (as applicable):

Maintenance Rule category (check one): ___ risk-significant ___non-risk-significant

Time that identified condition existed or is assumed to have existed:

Functions and Cornerstones degraded as a result of this identified condition (check ✓)

INITIATING EVENT CORNERSTONE

_____ Transient initiator contributor (e.g., reactor/turbine trip, loss offsite power)

_____ Primary or Secondary system LOCA initiator contributor (e.g., RCS or main steam/feedwater pipe degradations and leaks)

MITIGATION SYSTEMS CORNERSTONE

_____ Core Decay Heat Removal Degraded

_____ Initial Injection Heat Removal Degraded

_____ Primary (e.g., Safety Inj)

____ Low Pressure

____ High Pressure

_____ Secondary - PWR only (e.g., AFW)

_____ Long Term Heat Removal Degraded (e.g., ECCS sump recirculation, suppression pool cooling)

_____ Reactivity Control Degraded

_____ Fire/Flood/Seismic/Weather Protection Degraded

BARRIERS CORNERSTONE

_____ RCS LOCA Mitigation Boundary Degraded (e.g., PORV block valve, PTS issue)

_____ Containment Barrier Degraded

_____ Reactor Containment Degraded

_____ Actual Breach or Bypass

_____ Heat Removal, Hydrogen or Pressure Control Degraded

_____ Control Room, Aux Bldg, or Spent Fuel Bldg Barrier Degraded

_____ Fuel Cladding Barrier Degraded

SDP PHASE 1 SCREENING WORKSHEET FOR IE, MS, and B CORNERSTONES

Check the appropriate boxes ✔

If the finding is assumed to degrade:

1. fire protection defense in depth (DID), detection, suppression, barriers, fire brigade, use IMC 0609 Appendix F
2. the safety of a shutdown reactor, use IMC 0609 Appendix G
3. the safety of an operating reactor, identify the degraded areas:

☐Initiating Event ☐Mitigation Systems ☐RCS Barrier ☐Fuel Barrier ☐Containment Barriers

4. **Two or more** of the above areas degraded → **Go to Phase 2**
5. If **only one** of the above areas is degraded, continue **only** in the **appropriate** column below.

Initiating Event	Mitigation Systems	RCS Barrier or Fuel Barrier	Containment Barriers
1. Does the finding contribute to the likelihood of a Primary or Secondary system LOCA initiator? ☐**If YES → Go to Phase 2** ☐If NO, continue 2. Does the finding contribute to both the likelihood of a reactor trip AND the likelihood that mitigation equipment or functions will not be available? ☐**If YES → Go to Phase 2** ☐If NO, continue 3. Does the finding increase the likelihood of a fire or internal/external flood? ☐**If YES** → Use the IPEEE or other existing plant-specific analyses to identify core damage scenarios of concern and factors that increase the frequency. Provide this input for **Phase 3** analysis. ☐If NO, screen as Green	1. Is the finding a design or qualification deficiency confirmed not result in loss of function per GL 91-18 (rev 1)? ☐**If YES** → screen as Green ☐If NO, continue 2. Does the finding represent an actual loss of safety function of a System? ☐**If YES → Go to Phase 2** ☐If NO, continue 3. Does the finding represent an actual loss of safety function of a single Train, for > its Tech Spec Allowed Outage Time? ☐**If YES → Go To Phase 2** ☐If NO, continue 4. Does the finding represent an actual loss of safety function of one or more non-Tech Spec Trains of equipment designated as risk-significant per 10CFR50.65, for >24 hrs? ☐**If YES → Go To Phase 2** ☐If NO, continue 5. Does the finding screen as potentially risk significant due to a seismic, fire, flooding, or severe weather initiating event, using the criteria on page 3 of this Worksheet? ☐**If YES** → Use the IPEEE or other existing plant-specific analyses to identify core damage scenarios of concern and provide this input for **Phase 3** analysis. ☐If NO, screen as Green	1. RCS Barrier **Go to Phase 2** 2. Fuel Barrier screen as Green	1. Does the finding only represent a degradation of the radiological barrier function provided for the control room, or auxiliary building, or spent fuel pool, or SBGT system (BWR)? ☐**If YES** → screen as Green ☐If NO, continue 2. Does the finding represent a degradation of the barrier function of the control room against smoke or a toxic atmosphere? ☐**If YES → Go to Phase 3** ☐If NO, continue 3. Does the finding represent an actual open pathway in the physical integrity of reactor containment or an actual reduction of the atmospheric pressure control function of the reactor containment? ☐**If YES → Go to Phase 2 in Appendix H of IMC 0609** ☐If NO, screen as Green Page 2 of 3

SDP PHASE 1 SCREENING WORKSHEET FOR IE, MS, and B CORNERSTONES
Seismic, Fire, Flooding, and Severe Weather Screening Criteria

1. Does the finding involve the loss or degradation of equipment or function **specifically** designed to mitigate a seismic, flooding, or severe weather initiating event (e.g., seismic snubbers, flooding barriers, tornado doors)? (Equipment and functions for the mitigation or suppression of fire initiating events, such as thermal wrap or sprinkler systems, should be evaluated using IMC 0609 Appendix F and are not evaluated here)

   ☐ **If YES** → continue to question 2

   ☐ If NO → skip to question 3

2. If the equipment or safety function is assumed to be completely failed or unavailable, are ANY of the following three statements TRUE? The loss of this equipment or function by itself, during the external initiating event it was intended to mitigate

   a) would cause a plant trip or any of the Initiating Events used by Phase 2 for the plant in question;

   b) would degrade **two or more** Trains of a multi-train safety system or function;

   c) would degrade one or more Trains of a system that supports a safety system or function.

   ☐ **If YES** → the finding is potentially risk significant due to external initiating event core damage sequences - return to page 2 of this Worksheet

   ☐ If NO, screen as Green

3. Does the finding involve the loss of any safety function, identified by the licensee through a PRA, IPEEE, or similar analysis, that contributes to external event initiated core damage accident sequences (i.e., initiated by a seismic, fire, flooding, or severe weather event)?

   ☐ **If YES** → the finding is potentially risk significant due to external initiating event core damage sequences - return to page 2 of this Worksheet

   ☐ If NO, screen as Green

Result of Phase 1 screening process: ☐screen as Green ☐ **go to Phase 2** ☐ input to Phase 3

Important Assumptions (as applicable):

Row	Approx. Freq.	Example Event Type	Estimated Likelihood Rating		
I	>1 per 1-10 yr	Reactor Trip Loss of Pwr Conv Sys (loss of condensor, Closure of MSIVs, Loss of feedwater)	**A**	**B**	**C**
II	1 per 10-10^2 yr	Loss of Offsite Power Small LOCA (BWR) (Stuck open SRV only) MSLB (outside cntmt)	**B**	**C**	**D**
III	1 per 10^2-10^3 yr	SGTR Stuck open PORV (PWR) Small LOCA (PWR) (RCP seal failures and stuck open SVs only) MFLB MSLB(inside PWR cntmt)	**C**	**D**	**E**
IV	1 per 10^3-10^4 yr	Small LOCA(RCS rupture) Med LOCA (RCS rupture)	**D**	**E**	**F**
V	1 per 10^4-10^5 yr	Large LOCA (RCSrupture) ATWS-BWR	**E**	**F**	**G**

VI	<1 per 10^5 yr	ATWS-PWR (mech only) ISLOCA Vessel Rupture	F	G	H
			> 30days	30-3days	<3 days
			Exposure Time for Degraded Condition		

Table 1 - Generic Example - Categories for Initiating Events

Initiating Event Likelihood	Remaining Mitigation Capability Rating (with Examples)						
	6	5	4	3	2	1	0
	3 diverse trains OR 2 multi-train systems OR 1 train + 1 multi-train system + recovery of failed train	1 train + 1 multi-train system OR 2 diverse trains + recovery of failed train	2 diverse trains OR 1 multi-train system + recovery of failed train	1 train + recovery of failed train OR 1 multi-train system OR Operator action + recovery of failed train	1 train OR Operator action OR Operator action under high stress + recovery of failed train	Recovery of failed train OR Operator action under high stress	none
A	Green	White	Yellow	Red	Red	Red	Red
B	Green	Green	White	Yellow	Red	Red	Red
C	Green	Green	Green	White	Yellow	Red	Red
D	Green	Green	Green	Green	White	Yellow	Red
E	Green	Green	Green	Green	Green	White	Yellow
F	Green	Green	Green	Green	Green	Green	White
G	Green	Green	Green	Green	Green	Green	Green
H	Green	Green	Green	Green	Green	Green	Green

Table 4 - Risk Significance Estimation Matrix

Type of Remaining Capability	Remaining Capability Rating
Recovery of Failed Train Definition: Operator action to recover failed equipment that is capable of being recovered after an initiating event occurs that requires the equipment (e.g., equipment was unavailable due to a switch misalignment). Action may take place either in the control room or outside the control room and is assumed to have about a 1E-1 probability of failing when credited as "remaining mitigation capability".	1
1 Automatic Steam-Driven (ASD) Train Definition: A collection of associated equipment that includes a single turbine-driven component to provide 100% of a specified safety function. The probability of such a train being unavailable due to failure, test, or maintenance is assumed to be about 1E-1 when credited as "remaining mitigation capability".	1
1 Train (diverse as compared to other trains) Definition: A collection of associated equipment (e.g., pumps, valves, breakers, etc.) that together can provide 100% of a specified safety function and for which the probability of being unavailable due to failure, test, or maintenance is assumed to be about 1E-2 when credited as "remaining mitigation capability". Two or more trains are diverse if they are not considered to be susceptible to common cause failure modes.	2
1 Multi-Train System Definition: A system comprised of two or more trains (as defined above) that are considered susceptible to common cause failure modes. Such a system is assumed to have about a 1E-3 probability of being unavailable, regardless of how many trains comprise the system, when credited as "remaining mitigation capability".	3
2 (diverse) Trains [adding example] (2 diverse trains are assumed to have a combined 1E-4 probability of being unavailable)	4 (=2+2)
1 Train + Recovery of Failed Train [adding example] (1 train plus recovery of failed train is assumed to have a combined 1E-3 probability of being unavailable or failed)	3 (=2+1)

Table 5 - Remaining Capability Rating Values

6. Detailed Guidance

Step 1.1 - Definition of the Inspection Finding and Assumed Impact

It is of utmost importance that inspection findings be well defined in order to consistently execute the logic required by this process. The process can be entered with inspection findings associated with performance deficiency(s) that involve one or more degraded

conditions concurrently influencing any mitigation equipment and/or initiating event frequency. The definition of the finding should be based on the known existing facts and should NOT include hypothetical failures such as the one single failure assumed for licensing basis design requirements.

The significance of certain types of inspection findings cannot be estimated using this SDP and will require a Phase 3 analysis. One example is the case where a system is designed with two or more pumps capable of meeting 100% of a function within a single train and two such trains are provided (e.g., service water or cooling support systems). If one of the pumps is found to be unavailable, the function of the train is unaffected, but it reliability has been significantly reduced. Whether this is a greater than Green condition depends on the particulars of the system function at that plant. However, the Phase 1 and Phase 2 SDP would not address a 100% capable train that remains 100% capable, but with reduced reliability, given a degraded component. Therefore, the inspector may consider the entire train with the degraded component as unavailable for the purpose of "bounding" the significance determination. If this "bounding" result is Green, it may not be worth expending further inspection effort in this area. If it is greater than Green, a Phase 3 analysis will be necessary.

When the scenario includes the identification of a condition under which a function, a system, or a train becomes unavailable, then this fact must be factored into the assessment. It is not appropriate to assume that the affected function, system, or train is unavailable. At this point, it is necessary that a risk analyst assess the probability of the condition, in order to adjust the likelihood of the initiating event (or events) by the appropriate amount. For example:

> A finding is that if a control valve in the instrument air system fails it could lead to overpressure of a low-pressure part of the system, thereby leading to the failure of the equipment controlled by the air system. The probability of interest is that of the failure of the valve during the mission time, which depends on the impact of the failure. For example, if the valve failure would lead to a reactor trip in addition to failing some mitigating equipment, the mission time is 1 year, and the initiating event frequency would be the probability of failure of the valve in one year. If the impact is simply on the mitigating systems for a LOCA, the mission time is that time required to place the plant in a safe, stable state. In this case, the LOCA frequency would be adjusted by the probability that the valve failure would occur during the mission time.

When determining the risk associated solely with the licensee performance problem, it is not necessary to include equipment that is out of service for routine maintenance or testing. The impact of the likelihood of this equipment not being available for mitigation purposes due to plant maintenance or surveillance testing is included in the licensee's baseline PRA equipment unavailability values. However, for the purpose of initial NRC response to degraded conditions when the reason for equipment unavailability is unknown, a preliminary SDP analysis may assume the entire plant configuration, including out-of-service equipment for routine maintenance or testing. This approach allows the NRC to validate that the other out-of-service equipment was not a result of performance problems. The final SDP determination must still be made only from identified licensee performance deficiencies.

The statement of the finding should clearly identify the equipment potentially or actually impacted, as this will be used in the risk characterization process. In some cases, the impact of the finding can be stated unambiguously in terms of the status of a piece of equipment, for example, whether it is functional or not. In other cases, the finding may specify conditions under which a piece of equipment becomes unavailable. In cases

involving degraded conditions, the impact may not have been determined, and assumptions will have to be made for the purposes of assessing the "bounding" risk significance.

Any explicitly stated assumptions regarding the effect of the finding on the safety functions should initially be conservative (i.e., force a potentially higher risk significance) because the final result will always be viewed from the context of those assumptions. Subsequent information or analysis from the licensee or other sources is expected, in many cases, to reduce the significance of the finding, with an appropriate explicit and defensible rationale. Findings must also be well defined because the assumptions can be modified to examine their influence on the results and thereby gain risk sensitivity insights. The general rule is that the definition of the finding must address its safety function impact and any assumptions regarding other plant conditions. Examples include the following:

1. The following situations represent two different findings: a motor-operated valve (MOV) in a pressurized-water reactor (PWR) auxiliary feedwater (AFW) system is found with hardened gearbox grease (i.e., is degraded); and an MOV in the AFW system is found with a broken wire that renders it non-functional. For the purposes of assessing the risk significance, the impact of both could be characterized conservatively as "MOV does not perform its safety function of opening to provide flow to the steam generators." In the first case, it is necessary to assume that the hardened grease makes the valve unavailable, while in the second it is not.

2. A finding involving a deficiency in the design of the plant could be stated as follows: "Equipment/System/Component X would not perform its safety function of .... under conditions. ..." For example, a remote shutdown panel that might be rendered inhabitable during a cable spreading room fire that causes a loss of offsite power due to inadequate heating, ventilation, and air conditioning (HVAC) dispersion of the resulting smoke, would be characterized conservatively as "plant cooldown not possible from control room or remote shutdown panel during a loss of offsite power (LOOP) caused by cable spreading room fire due to inhabitability from resulting smoke and loss of power to remote shutdown panel HVAC."

Step 1.2 - Initial Screening of the Inspection Finding

For the sake of efficiency, the initial screening is intended to screen as Green any findings that have minimal impact on risk early in this process. The screening guidelines are linked to the cornerstones as follows: If there is negligible impact on meeting the reactor safety cornerstone objectives, the finding can be identified as having minimal impact on risk and should be considered as a Green finding to be corrected under the licensee's corrective action process. Inspectors are encouraged to use the Phase 2 process at any time they wish to analyze the sensitivity of an issue and are not prohibited from doing so just because the issue screens as Green in Phase 1.

The decision logic for the Phase 1 screening is given on the Phase 1 Worksheet provided in this Chapter. Page 1 of the Phase 1 Worksheet provides space to document important facts needed to screen the finding. The lower section of page 1 also aids in determining which cornerstone is affected so that the appropriate screening questions can be applied.

Page 2 of the Phase 1 Worksheet starts by identifying other SDPs that should be used for specific findings (i.e., fire barrier or suppression degradation, or shutdown safety issues). If more than one cornerstone is affected, then the screening requires the next level of analysis (Phase 2) because of the potential risk significance of two or more defense-in-

depth attributes being degraded. If only one cornerstone is affected, screening questions are asked that directly relate to the specific cornerstone.

The purpose of the Initiating Event screening questions is to identify findings for further review that are more significant than a finding that increases the likelihood of an uncomplicated plant trip. The third question screens for findings that could increase the likelihood of external initiating events, since these are not currently included in the SDP Phase 2 Worksheets. Only fire and flooding are considered by this screening question since seismic and severe weather initiating event frequencies cannot be influenced by a licensee performance deficiency.

The Mitigation Systems screening questions follow a similar logic to those used by the NRC Accident Sequence Precursor Program described in NUREG/CR-4674 (series) to screen LERs for possible risk significance. The first question screens to Green findings that represent deficiencies that do not impact operability. Questions 2 and 3 examine whether an actual loss of safety function (i.e., the safety function is certain to fail if demanded), as defined by the inspector on Page 1, has occurred. The fourth question is intended to catch any non-Tech Spec equipment identified as risk-significant under the Maintenance Rule and therefore would not be caught under Question 3 which relates only to Tech Spec equipment. Question 5 is included to identify any potential for risk significance related to the influence of external initiating events which are not addressed by the Phase 2 process (i.e., seismic, fire, flooding, or severe weather). Note that the fire screening question at the top of Page 2 deals ONLY with degraded fire *barrier or suppression features*. Alternatively, question 5 under Mitigation Systems is intended to address the front-line or support systems themselves which become risk significant due to the reactor safety functions they provide in mitigating fire scenarios.

The RCS Barrier screening is directly to Phase 2 due to the potential risk associated with LOCA events or failure to mitigate LOCA events. The Fuel Barrier screening is always Green, based on the existence of a Performance Indicator that continuously monitors fuel performance through the magnitude of RCS radioactivity known to originate within the fuel.

The Containment Barrier screening question 1 results in Green based on the low probability of a core damage event coincident with containment failure impacting the control room barrier, the low probability of a release of source term from the spent fuel pool, and because auxiliary building barrier deficiencies are considered non-reactor safety related and covered under the Occupational or Public Radiation Safety cornerstone. If inspection findings can be identified that represent a departure from these assumptions and that potentially increase the LERF by greater than 1E-7/yr, then they should be forwarded to an NRC risk analyst for Phase 3 evaluation. Question 2 acknowledges that the control room barrier also functions to maintain a breathable atmosphere for operators during events more likely to occur than core damage coincident with reactor containment failure. The failure of this barrier during such events could significantly increase the core damage risk, but this is highly dependent upon human reliability analysis and requires risk specialist expertise in this area. Question 3 screens findings for potential increases in LERF that are considered in Appendix H to this Chapter.

The Page 3 screening questions for seismic, fire, flooding, and severe weather test two categories of finding. The first category is that in which the degraded equipment is specifically intended to mitigate a particular external initiating event. In this case (question 2), the finding is assumed to be "worst-case" (i.e. complete failure of the degraded equipment's function) and tested against four questions intended to reveal any potential for risk significance. The second category (question 3) is that in which the degraded equipment provides a reactor safety function during seismic, fire, flooding, or severe

weather initiating events. In this case, the only known method that reveals potential for risk significance is a risk analysis that accounts for core damage sequences beginning with these external initiating events. Each licensee has conducted an IPEEE in response to NRC Generic Letter 88-20 Supplement 4. Some licensees have incorporated external initiating events into their current PRAs. At a minimum, the IPEEE should provide qualitative insights that can possibly be supplemented by a licensee PRA staff knowledgeable of its results. In addition, the NRC is completing Staff Evaluation Reports (SERs) and Technical Evaluation Reports (TERs) on every IPEEE, which could provide inspectors with either qualitative or quantitative external event risk insights. Although these SERs and TERs do not approve the IPEEE for any particular use, they may provide a condensation of important risk insights reported by the licensee. In answering question 3 on page 3, inspectors are not expected to fully understand all relevant IPEEE details, but rather should obtain from the licensee or NRC SER/TER any available qualitative or quantitative risk insights, equipment lists, or other information to determine the most significant external event initiated core damage accident sequences whose frequency could be increased by the inspection finding. If the finding is related to such an identified sequence, then a Phase 3 review by an NRC risk analyst will be necessary to determine if the increased sequence frequency exceeds the Green band.

Any inspection finding that is NOT screened as green by the above-mentioned decision logic should be assessed using the Phase 2 or Phase 3 process described in this Chapter.

Note that the SDP can be an important inspector tool to better understand the sensitivity of various assumptions regarding plant capability to the change in plant risk. For example if an inspection finding screens as Green in Phase 1, it may still be useful to use the SDP Phase 2 process to examine the effect of other plant equipment being unavailable or degraded simultaneously with that of the finding. If the outcome of the SDP can be significantly influenced by the unavailability of other equipment (e.g. if a "combined" finding could be characterized as White or greater), then inspection effort may be warranted to verify the assumption that this equipment was available.

Phase 2 - Risk Significance Approximation and Basis

Step 2.1 - Define or Select the Applicable Scenarios

Once an inspection finding passes into Phase 2, it is evaluated in a more detailed manner. The first step in Phase 2 is to ask the question "Under what core damage accident scenarios would the finding, as defined in Step 1.1, increase risk?" That is, the inspector must determine which core damage scenarios are made more likely (i.e., greater estimated frequency) by the finding.

Determining which scenarios make an inspection finding risk important may not always be intuitive. Therefore, high level (functional) plant-specific scenarios taken from PRAs have been provided as a set of Phase 2 Worksheets for each plant design. The worksheets are Table 3 in the plant specific Risk-informed Inspection Notebooks. Additionally, documents such as current plant-specific PRA insights, safety analysis reports, Tech Spec bases, and emergency operating procedures may be reviewed as needed to ensure that all applicable events and circumstances are considered. Identifying the scenarios begins with identifying the equipment and the assumed or actual impact of the finding, and takes into consideration the role the equipment plays in either the continued operation of the plant or the response to an initiating event. This step leads to an identification of the role of the finding in either contributing to an initiating event or affecting a mitigating system, or both. For the mitigating systems, the impact may be one of two kinds: the finding results in the

equipment function being degraded or the finding relates to the identification of a condition under which the function would become degraded.

In the first of these two cases, the function can be assumed to be lost, and the scenario of interest begins with the initiating event for which the equipment is required and the remaining equipment that, by design, can provide the same function as that which has been lost. For the second case, the scenario definition must also include the condition under which the function would become degraded.

For example, if the finding is that while performing the switchover to recirculation in a PWR, the safety injection (SI) pumps could be irreparably damaged due to cavitation, the scenario definition includes the loss of coolant accident (LOCA) initiating event, the failure of the charging system (if it is a viable alternative means of providing sump recirculation), and also the human error (which represents the condition under which the pumps would fail). If the finding were that the SI pumps could never be aligned properly for some reason (this extreme case is an example to demonstrate a point only), the scenario definition would involve only the LOCA and the charging system failures.

During this phase of the process, inspectors may determine that several different scenarios are affected by a particular inspection finding. This determination can occur in one of two ways:

First, the finding may be related to an increase in the likelihood of an initiating event, which may require consideration of several scenarios resulting from this initiating event.

Second, the finding may be related to a system required to respond to several initiating events. For example, the discovery of a degraded instrument air system could affect plant response to both a loss of offsite power and a LOCA. Each of these two initiating events must be considered separately.

In identifying possible core damage accident scenarios, consideration must also be given to the role of support systems as well as the primary system. For example, if a particular initiating event can be mitigated by more than one system providing the same safety function, but all such systems are dependent on a single train of a support system (e.g., service water or emergency ac power), the limiting scenario may involve the failure of the single train of the support system rather than the individual primary system trains. Therefore, for findings involving support system functional degradation, each scenario given on the Phase 2 Worksheet must be examined for the impact of this degradation on the primary system functions and the user may need to create a new scenario by collapsing multiple primary system functions into a single associated support system failure.

Step 2.2 - Estimation of the Likelihood of Scenario Initiating Events and Conditions

In Step 2.1, sets of core damage accident scenarios were determined that could be made more likely by the identified inspection finding (degraded condition). This identifies one or more initiating events with each followed by various sequences of equipment failures or operator errors. To determine the most significant scenarios, perform the following analysis for <u>each</u> set of scenarios having a common initiating event.

If the finding does not relate to an increased likelihood of an initiating event, the initiating events for which the affected SSC(s) are required are allocated to a frequency range in accordance with guidance provided in the left-hand column of Table 1 herein. Table 1 is entered from the left column, using the initiating event frequency, and from the bottom,

using the estimated time that the degraded condition existed, to arrive at a likelihood rating (A - H) for the combination of the initiating event and the duration of the degraded condition. For a Phase 2 analysis, only these initiating event frequencies should be used, with the exception of a plant-specific LOOP frequency that is greater than that given in Table 1. Some plants have had sufficient numbers of LOOPs and partial LOOPs to justify a higher than 1 every 10 year average frequency. In such cases, it is appropriate to use the higher LOOP frequency. Plants in this category will be identified on the plant-specific Phase 2 LOOP Worksheet in the SDP Notebooks.

If the finding relates to an increased likelihood of a specific initiating event, the likelihood of that initiating event may be increased according to the significance of the degradation. For example, if the inspection finding is that loose parts are found inside a steam generator, then the frequency of a steam generator tube rupture (SGTR) for that plant may increase to the next higher frequency category, and Table 1 is entered accordingly. The degree of increase during Phase 2 can only take place as an order-of-magnitude (factors of 10) change and is made on the basis of judgement alone.

The definition of the finding and the selection of core damage accident scenarios should be strictly based on the known existing facts and should NOT include hypothetical failures, such as the one single failure assumed for licensing basis design requirements. However, the selection of scenarios need NOT be restricted only to those described in the SDP worksheets and tables. The SDP provides a simplified risk framework to examine all possible scenarios based on plant-specific design. Inspectors should recognize that reasonable probabilities must be assigned to each failure event in any scenario they may postulate and should seek risk analyst assistance when attempting to construct such scenarios.

The determination of Degraded Condition Exposure Time for entry into Table 1 should be the best estimate time based on all known information. Any assumptions made regarding this should be documented on the Worksheet. If no information is known regarding when the failure or unavailability occurred, then one-half the time since the last demonstrated successful operation should be used. This is consistent with the rule used to calculate unavailability for the Performance Indicators used in the Reactor Oversight Process. In addition, it is not appropriate to subtract the Technical Specification LCO time (i.e., allowed outage time) from the degraded condition exposure time used for entry into Table 1. This is because the SDP is designed to estimate the *additional* core damage frequency risk due to *unintended* and *unexpected* deficiencies in licensee performance. Therefore, *all* of the exposure time for such a condition has added to the otherwise expected annualized plant risk.

Use of Table 1 should result in one or more initiating events of interest with an associated likelihood rating ("A" through "H") for each.

Step 2.3 - Estimation of Remaining Mitigation Capability

The initiating event scenarios of interest have now been identified, and Table 1 has been used to estimate associated initiating event frequencies and to combine them with degraded condition exposure time to arrive at an estimate of the likelihood of the initiating events. Following an initiating event, core damage will result from a series of system, component, or operator failures. In this step, the inspector will approximate the probability of failing to mitigate the core damage scenarios associated with the condition identified by the finding. Findings defined in Phase 1 will generally identify the potential for degrading a particular function. Therefore, the probability of preventing the scenarios that include this

degraded function will depend on the extent of remaining mitigation capability for providing the function.

To count remaining mitigation capability in a probabilistically consistent manner, systems are considered to be either single train or redundant. A redundant system is a system that has more than one identical train, where the loss of one train does not lead to a loss of function. However, all trains of a redundant system are subject to a possible common-cause failure. Successful mitigation may be provided by each train of diverse single-train systems (e.g., high-pressure injection in a boiling water reactor (BWR) for a loss of feedwater transient may be provided by the high-pressure coolant injection (HPCI) and reactor core isolation coolant (RCIC) systems, both single train systems), or by diverse redundant systems (e.g., low-pressure injection may be provided by the low-pressure core spray (LPCS) and the LPCI systems in a BWR-4, both multi train systems), or by mixtures of single-train and redundant systems. In some cases there may be time to recover the function or train that has been lost, which can be credited under certain conditions.

In determining the remaining available mitigation capability for a scenario affected by the degradation assumed by the finding, the inspector must select the most appropriate column of Table 4, "Risk Significance Estimation Matrix," for each affected core damage sequence. Each column in Table 4 represents one order of magnitude difference from adjacent columns in the failure probability of remaining mitigation capability, and the descriptions in the column headings are intended as non-inclusive examples of mitigation methods that can typically be assumed. Site or design specific information has been provided in the Phase 2 Worksheets (Tables 3 in the site specific Notebooks) for basic information on the number of trains and redundant systems. Table 5 of this procedure also provides guidance on how to apply mitigation credit. In addition, the following rules and guidelines apply:

Only equipment that the licensee has scoped into the maintenance rule (10 CFR 50.65) may be credited for remaining mitigation capability. This provides a minimum level of assurance that credited equipment meets pre-established reliability goals or performance criteria.

The potential for common-cause failure of the remaining mitigation capability is accounted for by this process. However, any actual evidence of a common-cause failure must be included in the definition of the inspection finding.

Credit for recovery may be taken if there is a possibility of restoration of the equipment or function that has been assumed lost due to the condition identified by the finding. Recovery actions should be credited only if there is sufficient time available, environmental conditions allow access, they are covered by operator training and written procedures, and necessary equipment is available or appropriately staged and ready for use. For recovery actions that are relatively complex, and/or require actions outside the control room, it is particularly important that the actions required are feasible within the time available to prevent core damage. If there is no remaining mitigation capability other than restoring the failed equipment, and the above conditions are met, then use of the "recovery of failed train" column on the Phase 2 Worksheet will credit this recovery. For example, consider an inspection finding involving a potentially recoverable system failure, such as a failed automatic start feature. If status indication exists and operator action would reasonably be able to start the equipment within sufficient time to provide the system function, then credit can be given to recovery.

Major actions by operators during accident scenarios are credited using four categories of Human Error Probabilities (HEPs). They are termed operator action=1 (representing

an error probability of 5E-2 to 0.5), operator action=2 (error probability of 5E-3 to 5E-2), operator action=3 (error probability of 5E-4 to 5E-3), and operator action=4 (error probability of 5E-5 to 5E-4). A human action is assigned to a category bin, based on a generic grouping of similar actions among a class of plants. The details on credits for operator actions are incorporated into the site specific Risk - Informed Inspection Notebooks.

Sometimes full mitigation credit for a safety function is given on the event-specific Phase 2 Worksheet as a combination of equipment and operator action. However, the most limiting reliability is used to credit this as remaining mitigation capability. For example an ECCS recirculation function might be credited as: 1 / 3 charging trains taking suction from 1 / 2 LPSI trains using manual operation actuation (operator action). This states that the plant has three 100% charging trains (i.e., only 1 of 3 are required to provide the full safety function), two 100% LPSI trains, and operator action required. It is also clear that the function cannot be satisfied by any less than one charging train, one LPSI train, and successful operator action. Using Table 5, the charging and LPSI trains would each be given a credit of three (3) because they are both multi-train systems. These credits could not be added together because the failure of either system fails the function, just as if there were only one multi-train system providing the function. However, if operator action is only given a credit of two, since failure of operator action is required to satisfy the function, it is the most limiting credit and is therefore given as the maximum credit allowed for satisfying the function. If an inspection finding involves the unavailability of one train of LPSI, for example, that would leave one train remaining (credit of 2). But this still is not more limiting than operator action, so there is no change to the credit for the recirculation function. If both trains of LPSI were unavailable, then the function could not be satisfied at all and zero credit would be allowed (other than possibly for manual recovery action).

When all scenarios have been identified and the associated initiating event likelihoods and remaining mitigation capability estimated, then Table 4 "Risk Significance Evaluation Matrix" described in the next section can be used to estimate the potential significance of the degraded condition, within the context of all assumptions made to this point.

Step 2.4 - Estimating the Risk Significance of Inspection Findings

The last step of the Phase 2 assessment process is to estimate the relative risk significance of the finding. The risk is estimated by employing an evaluation matrix (Table 4), which utilizes the information gained from Steps 2.1 through 2.3. This matrix combines the scenario likelihood derived in Step 2.2 with the remaining mitigation capability determined in Step 2.3 and establishes an estimated risk significance for the particular finding. One of only four possible results can be obtained: Green, White, Yellow, or Red. These results are comparable to those used for PIs. The user must complete this assessment process for <u>each</u> scenario affected by the inspection finding before determining the scenario of highest significance.

The scenarios resulting in the highest significance will be used to establish the initial relative risk-significance of the finding. The Phase 2 process does not "sum" the changes in core damage frequency of multiple low-significance scenarios. Therefore, a simple summing rule is used to capture this potential effect.

Step 2.5 - Screening for the Potential Risk Contribution Due to External Initiating Events

The plant-specific SDP Phase 2 Worksheets do not currently include initiating events related to fire, external flooding, severe weather, seismic, or other initiating events that are considered by the IPEEE analysis requested in NRC Generic Letter 88-20 Supplement 4. An inspection finding could increase the frequency of certain of these core damage sequences sufficiently to be greater than green, either independent of the internal initiating event sequences or in combination with them. The influence of external initiating events on core damage risk is contained in the licensee's IPEEE submittal, but may not be quantitative. Therefore it may not be possible to directly obtain a color result from reactor safety SDP Table 4. However, some licensee's may have quantified portions of the external initiating event sequences in their PRA models and may have risk importance measures (e.g., Risk Achievement Worth) for modeled equipment that account for their influence. The rationale and basis for the fire and seismic screening questions follow from NUREG/CR-6544 "A Methodology for Analyzing Precursors to Earthquake-Initiated and Fire-Initiated Accident Sequences".

Step 2.6 - Screening for the Potential Risk Contribution Due to LERF

This step is related to the Containment Barrier SDP in Appendix H. Certain core damage sequences can result in a breach of the reactor vessel with the RCS at high pressure. If this occurs, the impact on containment is substantially worst due to direct corium heating of the containment walls. This increases the likelihood of containment failure. Therefore, if any of these sequences are affected by the finding and result in a Green next to White change in core damage frequency, there could be a corresponding change in LERF. Since the significance thresholds for changes to LERF are one order-of-magnitude lower than for CDF, changes to CDF in the Green next to White range could become a White effect on LERF. Thus, the finding should be evaluated using Appendix H for its affect on LERF.

Phase 3 - Risk Significance Finalization and Justification

If necessary, Phase 3 is intended to refine or modify the earlier screening results from Phases 1 and 2. Phase 3 analysis will utilize current PRA techniques and rely on the expertise of knowledgeable risk analysts.

Although licensee risk perspectives and related information are considered by the SDP, the NRC staff always retains the final and sole responsibility for determining the risk significance of a finding and will provide its written justification in an inspection report. When licensee assumptions or perspectives regarding the significance characterization are known to differ from those of the staff, the staff should explicitly address these differences in its written justification.

The NRC will consider licensee perspectives until such time as the NRC makes its final and docketed determination of significance. Once the final NRC determination is made and the finding is given a "color" in a docketed transmittal to the licensee, the question of risk significance is closed and any additional NRC inspection activities should proceed on a schedule commensurate with the significance determination inputs to the NRC Action Matrix assessment of licensee performance.

A basis for any preliminary or final SDP assessment should be included in an inspection report. Inspectors and regional management should have engaged the licensee in discussions of the basis for characterizing a finding throughout the Phase 1 and Phase 2 significance determinations. During all interactions with the licensee, the staff's primary interest is in confirming and fully understanding all the facts associated with the issue. Where a licensee provides alternative risk or engineering analysis methods in support of reducing the significance of an issue, and such methods have not been previously

reviewed by the staff, the staff may conclude that the resources (both staff and licensee) that would be spent on ascertaining the adequacy and influence of the alternative methods would be greater than the resources required for licensee correction and staff verification of the corrective actions for the identified deficiencies. In such cases, the staff may decline to review the licensee analysis and should proceed with its final significance determination. At the conclusion of this interaction (i.e., one docketed letter from the licensee and one management meeting, as needed), the NRC staff must make its final significance determination and document it in an inspection report or other official document and, if necessary, address any docketed licensee perspectives.

Limiting licensee input to one docketed response and one management meeting provides adequate "due process" while avoiding protracted dialogue over probabilistic methods that already acknowledge uncertainty in either direction (i.e., allowing for the possibility of increases or decreases in the risk estimation).

In the case of a potential "red" significance determinations, the staff may determine that additional docketed information and meetings (beyond one each) are appropriate to allow more detailed consideration of the risk analysis basis. It remains the staff's obligation to fully disclose and document its basis for any significance determination.

If a licensee discovers new factual information that was not previously available regarding a finding, it may be forwarded on the docket to the appropriate Regional Administrator for consideration. In such cases, the region will respond in writing either modifying or upholding the earlier decision and will provide its basis.

A process to appeal the staff's final determination of significance is described in Attachment 2 to this Chapter.

Documenting the Results

The results of the Phase 2 risk estimation will be communicated to the licensee through the inspection report process. It is expected that risk-significant or controversial findings will require obtaining licensee risk perspectives and will most likely prompt a Phase 3 review. If the inspectors, and appropriate regional and Headquarters staff (when necessary), agree with the results of the Phase 2 assessment, the final results will be documented in an inspection report. The extent of documentation should include all information needed to reconstruct the Phase 2 analysis. Although licensee perspectives will be considered, the NRC staff will retain the final responsibility for determining the risk significance of a finding and will provide its justification in an inspection report or other appropriate document. The staff should explicitly address in the inspection report its justification for not using docketed licensee assumptions or perspectives when those differ from the staff's. Any Phase 3 analysis should utilize the following documentation format (use each major heading only as applicable to the analysis being described).

Identification information (date, inspection report number, enforcement action number, etc)

I. Background

A brief overview of the need for the analysis and any information to help clarify the subsequent paragraphs.

II. Safety Impact

A discussion of the influence that the issue under analysis has on contributors to plant risk or degradation to plant defense-in-depth characteristics.

III. Risk Analysis/Considerations

Detailed discussion of the important and influential factors that affect the outcome of this analysis. As appropriate, a discussion of the greatest uncertainties and their importance to the conclusions or recommendations.

IV. Calculations

As needed, a detailed description of the calculations used to support the conclusions and recommendations.

V. Conclusions/Recommendations

VI. References

6. Use of SDP for Event Response

The plant-specific reactor safety SDP has been designed to give results in terms of the change in CDF per year. This risk metric was chosen because it is most reflective of licensee performance alone and further because inspection findings that are assessed using this risk metric can be combined with the performance indicator (PI) information which uses the same metric to establish its thresholds for NRC response via the NRC Action Matrix. Conditional Core Damage Probability (CCDP) has been chosen to help guide NRC responsiveness to events or conditions. By using CCDP for this purpose, the NRC responds to events or conditions with a level of inspection effort that is related to the actual risk increase (in core damage probability terms) based on all plant configuration conditions at the time of the event or deficient condition.

Deficient conditions that exist for a period of time can generate additional CCDP over that which would have otherwise existed. The same value of CCDP can be generated by a high change in CDF over a short period of time or conversely by a low change in CDF over a longer period of time. If the SDP inputs consider all plant configurations during the time period of the deficient condition, then the SDP result can be viewed as this type of CCDP. However, an event CCDP is calculated for the instant in time of the event and the SDP is not designed to perform this calculation. Thus these two CCDPs do not represent identical risk metrics. For the purposes of determining an appropriate level of NRC responsiveness to events, the CCDP metric must be calculated by a risk analyst.

Operating events happen infrequently enough and are of sufficient potential significance that initial NRC determination of the appropriate level of inspection response will almost always involve risk analysts. The role of an on-site inspector will generally be to provide information to the risk analyst, and other agency personnel, that quickly develop the best possible understanding of the sequence of events and any equipment malfunctions, operator errors, or other complications. The risk analyst will use the best available risk methods and information to estimate the event CCDP. However, if the event corresponds to a particular SDP Phase 2 worksheet (e.g., transient, LOOP), an inspector can gain useful qualitative insights into aspects of the event that could help reveal its risk significance. If equipment malfunctions or operator errors have occurred, the inspector can identify the sequences represented on the Phase 2 worksheet that include failure of that equipment or function and can note the remaining mitigation capability being relied upon

to ensure reactor safety. It may be appropriate for the inspector to determine whether the remaining mitigation capability was truly available during the event. If it were not, the event could be potentially even more risk significant.

In summary, SDP Phase 2 worksheets can be used by inspectors to gain qualitative insights into the estimated significance of an event. The worksheets can be used to identify the most likely core damage sequences given the known complications. Once these sequences are identified, inspectors can question the availability and reliability of other components that could increase the likelihood (and thereby the risk significance) of the sequences of concern.

END

BASIS INFORMATION

THE UNDERLYING PHILOSOPHY AND REASONING BEHIND WHY CDF AND NOT CDP IS THE APPROPRIATE MEASURE OF SIGNIFICANCE FOR THE REACTOR SAFETY SIGNIFICANCE DETERMINATION PROCESS

The SDP was designed to estimate the *increase* in annualized CDF risk due to identified deficiencies in licensee performance that lead to unavailability of equipment or safety functions. This increase is measured from the normal annualized CDF that results from routine plant operation. The additional risk contributions caused by deficient licensee performance (as characterized by the SDP) are assumed to be additive to this normal annualized CDF which already includes the risk contribution due to the probabilities of equipment failures expected occasionally for industrial facilities of this size and complexity. Another contribution to normal annualized CDF is caused by planned preventive maintenance and testing activities which cause the CDF at any particular moment in time to fluctuate dependent upon the changes in plant equipment status. The additional annualized CDF risk due to deficient licensee performance must be dependent only upon the performance issue itself and not the particular plant configurations during which the issue occurred. Therefore, if a degraded equipment or function is identified to exist simultaneously with equipment outages for preventive maintenance or testing, the SDP inputs cannot include the contribution of the maintenance or testing, since this is already included in the normal annualized CDF against which the change is being measured. This non-consideration of routine maintenance and testing is a departure from the traditional enforcement practice of including the consideration of any additional equipment unavailability that made the loss of function due to a deficiency more severe, even if the added unavailability were due to routine maintenance.

The SDP can be used to estimate either CDF or the conditional core damage probability (CCDP) given any plant configuration, which may include a combination of degraded equipment/functions and equipment outages for maintenance. This CCDP could potentially render results of higher significance than the use of change in CDF whenever maintenance was involved. The staff recommends the use of the estimated change in CDF instead of CCDP to characterize licensee performance deficiencies for the following reasons.

a. The objective of using the SDP to characterize the significance of inspection findings is to compare these findings with a licensee's performance indicators in an additive manner within the NRC Action Matrix. The reactor safety cornerstone performance indicator thresholds were developed based on the increase to annualized CDF represented by the value of the indicators. Thus, in comparing and "adding" the effects of PIs and inspection findings within the Action Matrix, it is necessary to use the same risk metric.

b. If CCDP were used to characterize licensee performance, the result would be inconsistent as it is influenced as much by timing (i.e., plant configuration) as by deficient performance. Additionally, it would penalize licensee's for their performance of maintenance which is an acceptable practice when 10 CFR 50.65 requirements are met.

c. Deficient licensee performance often causes equipment unavailability over periods of time extending to days and months. Using CCDP to characterize licensee performance would require historical analysis of all plant maintenance configurations that existed concurrently with the degraded equipment.

The CCDP metric is considered useful as an input to the decision of how the NRC staff should follow up on a reactor event or an identified degraded condition. This use of CCDP will be made part of the staff's internal guidance for event responses.

A more detailed mathematical treatment of this question is given below.

In developing the new performance assessment process one of the tasks was to establish risk-informed thresholds for PIs and corresponding thresholds for inspection findings, so that indications of performance degradation obtained from inspection findings and from changes in PI values could be put on an equal footing. The basis documents for establishing risk guidelines were Reg Guide 1.174, which bring in the Regulatory Analysis Guidelines, and the Safety Goal Policy Statement. The metrics that have been adopted in RG 1.174 for the characterization of risk are core damage frequency (CDF) and large early release frequency (LERF). These are essentially surrogates for health effects, which are the principal metrics in the Safety Goal Policy Statement, and, in addition, they are consistent with the metrics used in the Regulatory Analysis Guidelines. In RG 1.174, acceptance guidelines were established for assessing changes to the licensing basis of a plant. Acceptance is predicated on increases in CDF and LERF implied by the change to the licensing basis being small.

The philosophy behind the establishment of the thresholds on PIs and inspection findings was essentially to assume that an increase in PI values or conditions indicated by the finding, would, if their root causes were uncorrected, be equivalent to accepting a de facto increase in the CDF and LERF metrics. This is clearer for the PIs than it is for the inspection findings, which may relate to a time limited undesired condition. For such cases, the model used here is that the event is indicative of an underlying performance issue that, if uncorrected, would be expected to result in similar occurrences with the same frequency.

Therefore, the challenge is how to calculate the impact of changes in PI values and inspection findings on these metrics. Since PIs correspond (at least in some approximate sense) to parameters of PRA models, it is relatively straightforward to make the connection between changes in PI values to changes in risk. The thresholds were established by taking a set of PRA models, and varying the parameter that corresponded to the PI until the change in CDF became 1E-05 or 1E-04/ry, and these values were chosen as the thresholds for the white/yellow and yellow/red thresholds. Therefore, the risk significance of an inspection finding should be measured in the same way. When the impact of the finding can be characterized in terms of the unavailability of an SSC for some specified duration, then the SDP gives an estimate of the change in CDF (see Attachment 1 for a finding affecting a single SSC).

However, a finding that is associated with one SSC may be compounded by another SSC being out for routine maintenance or being in a (unrevealed) failed state. Enforcement has apparently, in the past, typically escalated enforcement for such coincidences, even though, performing maintenance is a necessary and beneficial operating practice. Also, failures will, and should be expected to, occur, and if they are unrevealed even though the licensee is following acceptable practices, it does seem harsh to penalize the licensee for a truly random occurrence, i.e. beyond the licensee's control. The ASP process does include the additional failure or unavailability in its assessment of "the event". Therefore

the question has arisen whether when applying the SDP, the failed or unavailable SSC that is not related to the finding per se should be treated as a failed or unavailable SSC.

In assessing the risk significance of the finding on the same basis as the PIs, it has to be remembered that the metric is CDF (LERF), and that CDF is an estimate based on a weighted average of all possible outcomes. Thus the key issue is how the finding is defined. If the finding relates to a specific reason that a particular SSC is, or has the potential to be, unavailable, for example a failure to follow a particular procedure, then it should, for the purposes of the SDP, be irrelevant whether another SSC is failed or is unavailable because it has been taken out of service for routine or scheduled maintenance, unless the cause of the failure or the reason for the maintenance is also related to deficient licensee performance. If the condition of independence holds, the finding has only by chance occurred when the second SSC was failed or unavailable, and the occurrences are uncorrelated. The chance that the events could have occurred simultaneously is accounted for in the SDP by using unavailability values for the redundant or diverse trains or systems that reflect the probability that they are unavailable.

However, the finding could be related to the component taken out of service. For example, if the reason the second component were taken out of service at the same time as the first component were unavailable is that a required check on operability of the first was not performed, the finding relates to the failure of the administrative process. The finding would relate to the second component, i.e. that which was taken out of service, and the failure of process being addressed could have and, given the assumption that, if uncorrected, it more than likely could have occurred when the first component was available. Therefore, in assessing the significance of the failure to follow the administrative process in the SDP, the first component should not be regarded as having failed. Instead, the SDP would be entered with the second component out of service as the condition of degradation, and the first component treated as being an alternate train. This is a somewhat contrived example which raises other questions in that if it were a generic degradation of the adherence to administrative procedures rather than for a specific procedure this would be impossible to analyze with the SDP.

Including the plant configuration as part of the finding is equivalent to risk tracking, as captured by a safety monitor for example, and is a record of one sample of all the possible outcomes, or a snapshot of the condition of the plant. It is however, not directly related to the estimate of the risk impact in the sense required for calculating ΔCDF. It is more accurately characterized as a measure of the margin to core damage, which could be measured as a conditional core damage probability, CCDP (for plant trip events), or a conditional core damage frequency (CCDF). There are currently no acceptance guidelines for CCDF or CCDP. Note that the ICCDP in RG 1.177 could be interpreted as an estimate of ΔCDF, in the same way as discussed above and in Attachment 1. However, we do not have a criterion for either CCDP or CCDF.

Suppose we were to derive appropriate criteria, we would still have to answer the question of how to interpret the data to generate a useful measure of the margin to core damage. If some of the failures that contribute to a high CCDP or CCDF are truly random, then does it make sense to penalize the licensee because they occur? It could be argued that since failures can and do occur, and as long as the indicators associated with those SSCs are acceptable, then the licensee could have done little to avoid this situation. What makes much more sense is to track the residual CCDP or CCDF with respect to the deliberate changes to plant configuration, i.e., those unavailabilities over which the licensee has direct control.

Mathematical demonstration that, for a simple unavailability, ΔCDP equates to ΔCDF over one year.

We want to show that, for a given basic event representing unavailability of an SSC, that the following holds:

$CDF = [T_0/(T_0 + T_1)].CDF_0 + [T_1/(T_0 + T_1)].CDF_1$,

where T_0 is the time when the SSC is available, and T_1 the time when it is not, CDF_0 is the CDF evaluated with the SSC available (i.e., unavailability = 0), and CDF_1 is the CDF calculated with the SSC unavailable, (i.e., unavailability = 1). $T_0 + T_1 = 1$ year.

That is, the addition of a CDP coming from a particular unavailability finding equates to an increase in CDF.

Note that the cutsets for CDF can be split into two groups, those that do not contain the SSC , which therefore corresponds to CDF_0 , and those that contain the SSC. These cutsets would typically be of the form x.y.z.U, where U is the unavailability of the SSC in question.

CDF_1 then is $CDF_0 + \Sigma(x.y.z.U)$ with the value of U set to 1.

Thus the equation above becomes

$CDF = CDF_0 + [T_1/(T_0 + T_1)].\Sigma(x.y.z.U)$ with the value of U set to 1.

Now, if we replace the value of U by $[T_1/(T_0 + T_1)]$, we get the usual CDF expression.

Thus, while what we are doing when applying the Tables 1 and 2 of the SDP is evaluating a CDP, i.e., an integral under a CDF spike, it translates to an increase in CDF for the year in which the finding occurred.

END

Attachment 3

RISK INFORMED INSPECTION NOTEBOOKS - PHASE 2 SITE SPECIFIC WORKSHEETS.

Site specific worksheets will be published through March 2001, at a rate of approximately 20 documents per month. As they get issued, each notebook will be sent to the licensees through the project managers and will be placed on the NRC web site and into ADAMS. The web site addresses and the ADAMS accession numbers will be provided to the inspectors and will be incorporated into this attachment.