DRAFT July 12, 1999

PROBABILISTIC SAFETY ASSESSMENT
COOPER NUCLEAR STATION
ENGINEERING STUDY

RISK INFORMATION MATRIX

RISK RANKING OF SYSTEMS BY IMPORTANCE MEASURE

PSA-ES019

In support of
NRC REGULATORY
OVERSIGHT PILOT PROGRAM

Signature / Date

Preparation: Risk Management Senior Engineer — Kent Sutton

Review: Risk Management Senior Engineer — Franz Markowski

Approval: Risk Management Supervisor — Rick Wachowiak

Revisions:

Number	Description	Reviewed By	Reviewed Date	Approved By	Approved Date
	DRAFT Issue, For Comment				

1. Introduction

The results of the PSA model have been categorized for risk insights based on system, human error and recovery strategy by relative importance. These results are presented in the NRC RIM-2 format for Cooper Nuclear Station. This report documents CNS specific risk insights and was developed based on the results of the CNS 96a PSA model and IPEEE results.

2. Background

As part of the NRC Reactor Oversight Program, risk information matrices (RIMs) are tools to be used in determining which activities, systems, or components are to be inspected in the baseline inspection program. The matrices are to be used, along with other generic and site specific information, in planning the baseline program at the beginning of each planning cycle, scheduling inspections within each inspection area, and during inspections by guiding the inspector to select the more risk-significant inspection samples.

3. Discussion

The CNS total core damage frequency is comprised of the sum of various sequence cutsets. The sequence cutsets are defined as the product of system functional failures (reactivity control, pressure control, core cooling, containment cooling, ect.) and an initiating event (loss of offsite power, turbine trip, loss of service water, ect.). A typical sequence cutset can be represented as;

$$CS_{SEQ} = IE * SF1_{CFx} * SF2_{CFy} * SF3_{CFz} \quad (yr^{-1})$$

where:

- CS_{SEQ} - PSA cutset core damage frequency for the sequence,
- IE - initiating event frequency for the sequence being investigated,
- $SF1_{CFx}$ - system functional failure probability caused by component failure x,
- $SF2_{CFy}$ - backup system functional failure probability caused by component failure y,
- $SF3_{CFz}$ - redundant backup system functional failure probability due to component failure z.

For example, given that a DBA LOCA event occurs on loop A of RHR, and the sequence of failures that could lead to core damage are:

- IE - Large LOCA initiator (1.E-04/yr),
- $SF1_{CFx}$ - LPCI loop B failed due to MOV 253 failed closed (3.E-03),
- $SF2_{CFy}$ - Core spray train A failed due to MOV 12A failed closed (3.E-03),
- $SF3_{CFz}$ - Core spray train B out for test of maintenance (3.2E-03).
- CS_{SEQ} - PSA cutset core damage frequency: 2.88E-12 / yr.

The probability of core damage for this sequence of events is quantified to be 2.88E-12/yr. This sequence quantification process is repeated many times for the various system failure possibilities for all possible sequences resulting from all postulated initiators.

The concept of an initiating event is easily understood, but is reiterated here in the context that it is used in the PSA model. An initiating event is an upset in plant power operations that leads to emergency conditions such that plant systems are used to return the reactor to the safe stable shutdown state. The sequence of events which lead to the safe stable state must be achieved and maintained within 24 hours following the initiating event. This is known as the "24 hour mission time" PSA modeling objective used to evaluate potential component failure modes which may challenge continued operation of equipment. To estimate outcomes beyond 24 hour mission time, introduces modeling uncertainty which would mask results due to limitations in predicting the impact of human actions. Initiating events are plant specific, since some equipment failures can both result in upset plant conditions (results in eventual reactor scram) and by nature of the failure, render some plant systems and mitigating functions useless.

As indicated above, the primary consideration following the initiating event is the availability and reliability of systems to mitigate the event. The front line systems credited for successful mitigation of core damage are limited to those utilized within existing plant procedures (EOPs and supporting abnormal procedures.) In some instances where front line systems have failed, general recovery strategies were credited for system restoration due to the collective efforts of post-accident activities of the ERO. In addition, the systems credited for mitigation to each sequence are carefully selected based on best estimate thermal-hydraulic analysis of the ensuing upset plant conditions. For example, use of HPCI or RCIC for long term core cooling would not be viable for an initiator which causes depressurization of the RPV (stuck open SRV, large LOCA, etc.)

The system failures modeled for each system include those components and support systems that are required for the system to successfully meet its credited function following various initiating events. To quantify system reliability, failure probabilities were estimated using available CNS data and industry information. Also included is the likelihood that the mitigating system and/or its support systems are unavailable at the time of the initiator. Equipment unavailability occurs during routine maintenance and periodic testing evolutions and is modeled in terms of fractional time per year.

Therefore, each sequence is the frequency of the initiating event and the probability of failure of minimum system functions needed to prevent core damage. The sequence is made up of a number of "cutsets" that are unique sets of combinations that would have to occur in order to result in core damage.

4. Definitions

Risk Achievement Worth - Impact of Event Failure

Risk achievement worth (or risk increase importance measure) provides a ranking of events by those most crucial to "maintaining safety" at the current level. The importance value for each event indicates the potential increase to the core damage frequency if the event conditional failure probability is quantified as 1.0 (certain event failure.) This measure gives an indication of how much the core damage frequency can be increased (safety margin subdued or theoretical minima for system fault) if failure of an event was certain. The RAW importance ratio is defined as:

$$\text{RAW Importance} = \sum CS_{CF=1.0} / \sum CS_{Total}$$

where:

$\sum CS_{CF=1.0}$ Sum of all sequence cutsets which contribute to the total estimated core damage frequency, if the system component failure probability of interest is increased to 1.0.

$\sum CS_{Total}$ Sum of all sequence cutsets which contribute to the total estimated core damage frequency (CDF) for CNS. Current value is 1.33E-05/yr for the 96a model.

Fussell-Vesely - Impact of Event Success

Fussell-Vesely importance measure provides a ranking of events by their contribution to the core damage frequency by computing the potential to change the core damage frequency. The FV importance measure provides a ranking of events by those most crucial for "safety improvement" at the current level. The importance value for each event indicates the potential reduction to the core damage frequency for the event. This measure gives an indication of how much the core damage frequency might be reduced (safety margin augmented or theoretical maxima for system success) if an event was assured to occur when required, or dependability is 1.0 (unavailability and unreliability are 0.)

In addition, the FV importance ranking provides the relative impact of declining system or component performance. The importance value for each event indicates the potential increase to the core damage frequency due to that events contribution. This measure gives an indication of how much the core damage frequency would be effected (safety margin reduction for a given decline in system performance) for conditions degrading system dependability.

The FV importance ratio is defined as:

$$\text{FV Importance} = \sum CS_{SF} / \sum CS_{Total}$$

where:

$\sum CS_{SF}$ Sum of those sequence cutsets which contain failures for the system of interest.

5. Matrix Footnotes

1. Core damage frequency ranking for each system is determined by adding all sequence frequencies containing at least one failure component of the system and dividing the sum by the total core damage frequency for CNS (1.33E-5/yr.) This importance measures the relative risk impact that would be realized if the system dependability were to change. The CDF% numbers can be interpreted as the relative change that would be observed with changing system performance. In practice, this indicates how much risk reduction (or safety decrease) could be expected if the system were upgraded with more (downgraded with less) redundancy, diversity, quality, testing, maintenance, etc. Since multiple concurrent failures are associated with each core damage sequence, the sum of these percentages is not equal to 100%.

2. The system ranking using Risk Achievement Worth is based on system component RAW values greater than 10. This is estimated based on setting the system component failure rate to 1.0, and comparing the new CDF to the original CDF. This criteria (RAW>10) is typical of system level evaluations for importance rankings focused on "safety maintenance" due to CDF impact.

3. The human error ranking, both pre-accident and post-accident errors, is based on individual actions which comprise >1.5% of total CDF. This criteria is typical of component level evaluations for importance rankings focused on "safety improvement" due to CDF impact.

4. If the failure of the system has the potential to challenge the integrity of the reactor coolant pressure boundary or the primary containment, it is indicated in the Barrier column of the table by an RC or PC, respectively.

PSA Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station

CNS PSA Systems	Risk Significant Systems Ranking Safety Improvement Insights, CDF %[1] Reasons for Importance at CNS	Cornerstones		
		Initiating Events	Mitigating Systems	Barrier
Onsite Emergency AC Power Rank: #1 %CDF=50%	Onsite Emergency AC power as defined by the PSA model includes emergency diesel generators, and various buses (4160, 480 VAC) associated switch gear, breakers, motor control centers, etc. Dominant failures of the AC buses and circuitry are circuit breaker failure 32%, common cause failure of AC components 27%, relay failure 5% and bus unavailability due to test or maintenance which occurs in 4% of the loss of onsite AC power cutsets. Concurrent hardware failures of both buses occur in 2% of these sequences (excluding common cause failures), otherwise single bus random failure combined with support system failures (non-critical AC, 125VDC, room cooling) of the opposite bus contribute to 10% of the cutsets. There are no specific human errors nor recovery actions effecting the dependability of the AC hardware.	Loss of AC Bus F or G Transient PSA Sequences: T1, T2, T3C, TACF, TACG	The essential AC buses and the onsite AC emergency power (EDG) fulfill an important support system function.	
Emergency Diesel Generators Rank: #3 %CDF=45%	The dominant failures of the diesel generators are failure to start 37%, common cause failure of both emergency diesel generators 21%, unavailability due to test or maintenance 19%, and failure to run the duration of mission time 12% of the loss of AC power cutsets. Concurrent failures of both diesels occur in 15% of cutsets (excluding common cause), otherwise random single EDG failure combined with support system failures of the opposite EDG contribute to 73% of the failure results. Support system functions for dependable EDG operation include; DC power for breaker control and EDG starting, service water system cooling, HVAC ventilation of EDG rooms (and standby switch gear rooms) and associated instrumentation (NBI.) The failure to restore from testing is the dominant human error effecting EDG reliability, however this failure is limited to 2% of loss of onsite AC power sequences. Recovery of DGs occurs in 83% of all loss of onsite AC power sequences. The unavailability of one diesel generator either due to random failure or maintenance, combined with the failure of the other safety trains that are fed from the remaining emergency bus, have the potential to be a major contributor to risk. Therefore, configuration control is important during maintenance or emergent work on EDGs. These issues are individually covered by CNS Procedure 0.49 as part of plant risk management.			

PSA Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station

CNS PSA Systems	Risk Significant Systems Ranking Safety Improvement Insights, CDF %[1] Reasons for Importance at CNS	Cornerstones		
		Initiating Events	Mitigating Systems	Barrier
Offsite AC Power Rank: #2 %CDF=49%	The loss of offsite power (LOSP) is an important initiating event, if lasting beyond 60 minutes (core boil-off time assuming no LOCA and no core injection.) The LOSP event could occur as a result of adverse weather conditions (weather-centered LOSP), grid or switch yard activities (grid-centered LOSP), or on-site plant activities such as component failure, design inadequacy, or human error (plant-centered LOSP). Important design features include: The AC switchyard redundant design and diverse maintenance alignments contribute to the overall reliability of the AC power system. The number of offsite lines capable of providing critical loads (7MW) is 7. There are 5 lines at 345kV, 1 at 161kV and 1 at 69kV (capable of 10MW.) The switchyard design consists of a ring bus with 1½ breaker configuration which allows removal of any one 345kV line for maintenance without effecting the other lines on the ring. This configuration greatly enhances the availability and reliability of offsite AC power function. The individual contribution to LOSP frequency is dominated by weather-related events 34%, then onsite plant events 10%, followed by grid-related events 5%. Some losses of offsite power could be recovered by offsite utility actions (note: completion of these actions do not require CNS operator support.) The potential recovery of offsite power within 60 minutes is an important recovery strategy which is credited in all LOSP events.	Loss of Offsite (AC) Power PSA Sequences: T1, T1W, T1P, T1G, LOSP, LOSEP	Offsite AC power supply fulfills support system functions. Offsite AC power is considered recoverable in T1 sequences and initially available in all others.	
RCIC Rank: #4 %CDF=24%	The reactor core isolation cooling system PSA model consists of those components required to fulfill the core cooling function. This consists of RCIC turbine, pump, suction and injection flow paths and automatic level control. The use of RCIC for alternate boron injection during ATWS scenarios is not modeled since no credit is given for partial failure to scram events and operator response times exceed time available for alignment. The dominant failures of RCIC are turbine failures 56%, motor operated valves 18%, general system failures 14%, common cause failure 7% and unavailability due to test or maintenance 4%. Concurrent random failure of both RCIC and HPCI occur in 11% of the sequences with RCIC failure (includes cross-system common cause terms.) Support system functions for dependable RCIC operation include; DC power for motor operated valves and electric motors to support turbine operation and associated RPV instrumentation (NBI.) There is no AC dependency for RCIC; the HVAC cooling for the RCIC room during an SBO event is not necessary for successful RCIC operation during the 4 hour coping period (PSA model does not credit DC load shedding.) The initiators attributed with core damage due to RCIC failure are LOSP (T1) 57% , loss of condenser (T2) 21%, and loss of instrument air (TIA) 12%. The RCIC system importance for core cooling during Station Blackout (SBO) scenarios is amplified due to the room cooling dependency of HPCI.	PSA Sequences Not Credited: TDCB, Large LOCA Intermediate	High Pressure Core Cooling System	

PSA Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station

CNS PSA Systems	Risk Significant Systems Ranking Safety Improvement Insights, CDF %[1] Reasons for Importance at CNS	Cornerstones		
		Initiating Events	Mitigating Systems	Barrier
	There are no specific human errors nor recovery actions effecting the dependability of the RCIC system. If continued long term containment heat removal is not assured for an event sequence, continued RCIC injection could be challenged by either, NPSH and vortex requirements when taking suction from suppression pool, excessive RCIC turbine lube oil (cooled by suppression pool) temperatures and increasing containment pressure challenging RCIC operation due to turbine exhaust limitations (22 psig.)			
Primary Containment Venting Rank: #5 %CDF=22%	The primary containment venting serves as an alternate containment heat removal function. The venting function consists of various hardware, valve operators, accumulators and human actions needed to align the primary containment for venting from the torus airspace (hard pipe vent) or drywell airspace (purge line.) Dominant failures of the PCV function are failure to manually operate 58%, failure of valves to change position 42% and failure of rupture disk to open <1%. Support system functions for dependable PCV operation include; instrument air to air operated valves, SBNI provide alternate motive power to AOVs (using manual actions,) and AC power is required for motor operated valve operation. The hard pipe vent is not available during SBO events. The initiators attributed with core damage due to PCV failure are loss of condenser (T2) 22%, loss of service water (TSW) 22%, LOSP (T1) 19% and loss of instrument air (TIA) 9%. The importance of PCV function is amplified in scenarios where the condenser is unavailable There are no specific recovery actions effecting the dependability of primary containment venting. The use of torus venting is an effective means of avoiding catastrophic containment failure for the Mark I containment during loss of containment heat removal scenarios.		Containment Pressure Control System	PC
Reactor Protection System Rank: #6 %CDF=19%	The reactor protection system failure term used in the PSA consists of common cause failure of all electrical scram signals and common cause failure of the mechanical scram function. The two failure modes are mechanical failure of the control rod drive system following receipt of reactor scram signal and electrical failure of the scram circuitry which provides the scram signal. Mechanical CRD scram failure (hydraulic lock) leads directly to ATWS scenarios and constitutes 99.6% of the RPS failures leading to core damage. If reactor recirculation pumps trip (RPT), then manual boron injection using SLC and executing RPV water level control are credited as backup actions for mechanical failure of RPS. The remaining 0.4% of RPS failures are attributed to electrical component failure to transmit the RPS trip signal. In the event that electrical RPS failure occurs with RPT, alternate methods for reactor shutdown include; alternate rod insertion, initiate manual scram (separate RPS channel,) manual boron injection using	Anticipated Transient Without Scram	Reactivity Control Sys	

PSA Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station

CNS PSA Systems	Risk Significant Systems Ranking Safety Improvement Insights, CDF %[1] Reasons for Importance at CNS	Cornerstones		
		Initiating Events	Mitigating Systems	Barrier
	SLC and executing RPV water level control. These actions are credited in the ATWS event tree associated with independent human actions. Because of the redundancy in the number of RPS signals available to scram the reactor, the redundancy in available instrumentation for each measured parameter, the redundancy in scram pilot valves, and the fail safe design of the scram system upon loss of air or power, the failure probability of the RPS is dominated by common cause failures. Theses common cause failures are based on industry generic evaluation of RPS rather than CNS specific fault tree model development and quantification. The evaluation indicates that the level of redundancy RPS design is dominated by common cause failures of components, not surveillance testing or unavailability due to maintenance. The common cause failure values used in the 96a PSA are an order of magnitude higher than the results of the latest industry study. It is anticipated that RPS will become less important when these failure values are updated in the next revision to the PSA model.			
Nuclear Boiler Instrumentation (NBI) Rank: #7 %CDF=13%	The nuclear boiler instrumentation PSA model consists of the RPV instruments and circuitry required to support automatic core and containment cooling functions. The various components modeled include level sensors, level transmitters, pressure sensors and various associated relays, permissive signals and switches. The NBI model consists of three sensors systems, reactor level instrumentation (LIS 72s, LIS 101s, LT 52s), reactor pressure instrumentation (PS 52s), and drywell pressure instrumentation (PS 101s.) Dominant failures of the NBI function are LIS 72s unavailable following post maintenance (PM) testing 48%, random hardware failures within one of 4 redundant channels 22%, and common cause failure to restore PS 52s after PM testing 19% of all NBI cutsets. Support system functions for dependable NBI operation include divisional 125V DC power for NBI circuitry and sensors, less than 1% of the NBI random failure sequences coincide with failure of divisional DC power. Multiple random failures of NBI exist in 24% of the NBI failure sequences. The initiators attributed with core damage due to NBI failure are inadvertant open relief valve (T3C) 33%, turbine trip without bypass (T2) 28%, loss of instrument air (TIA) 13% and loss of offsite power (T1) 9%. The failure of the NBI function leading to failure of automatic low pressure ECCS systems resulting in core damage is amplified by scenarios where the condenser is unavailable. The NBI failures are dominated by pre-accident human errors involving instrument calibration errors following testing or maintenance. Typically there are no NBI system recovery strategies credited, other than those already included in the evaluation of instrument mis-calibration errors.		RPV Instruments Support Sys For Core Cooling	
Power Conversion	The power conversion system PSA model consists of those components required to fulfill three functions, high pressure core injection, low pressure core injection and decay heat removal function. This consists of multiple	Loss of Feedwater	RPV Pressure Control	

PSA Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station

CNS PSA Systems	Risk Significant Systems Ranking Safety Improvement Insights, CDF %[1] Reasons for Importance at CNS	Cornerstones		
		Initiating Events	Mitigating Systems	Barrier
System Rank: #8 %CDF=12% MSIV Rank: #17 %CDF=2%	PCS trains for feedwater injection, condensate injection and main steam lines to transport decay heat to the condenser. Major components include, main condenser, main steam lines, injection flow lines, motor driven and turbine driven pumps, air operated, motor operated and hydraulic valves and various instrumentation and control components. The dominant failures of the modeled PCS function are failure to recover BOP equipment within 1 hour following reactor trip 71%, human failure to initiate specific actions (failure to start mechanical vacuum pumps, open MO26, mode switch to shutdown) 16%, failure of high pressure feedwater injection 6%, and failure of valves to change position 5%, and failure to recover BOP equipment within 24 hours 2% of all PCS cutsets. The initiators attributed with core damage due to PCS failure are turbine trip without bypass (T2) 42%, loss of instrument air (TIA) 21%, inadvertant open relief valve (T3C) 16% and reactor scram with PCS initially available (T3A) 12%, and loss of feedwater (T3B) is < 0.1%. Loss of feedwater is not an important initiator for CNS. The use of alternate high pressure injection systems, such as HPCI, RCIC and CRD (enhanced flow) reduce the importance of this initiator. The loss of PCS occurs in 74% of ATWS events, which contributes to the importance of PCS, this includes T2 events, failure of RPS with PCS failure and failure of RPS with MSIVs isolated (human failure to bypass low RPV water level Group 1 isolation when executing RPV water level control.) The PCS failures are dominated by post-accident human errors involving failure to operate equipment. This is due to the level of equipment redundancy, the equipment is normally operating and is highly reliable, consequently typical common cause failures associated with standby equipment (excluding common cause human errors of operation) are not dominant contributors to PCS system failure. As indicated above, PCS recovery strategies are very important – combining for 73% of the PCS cutsets resulting in core damag.	Transient PSA Sequences: T2 TIA T3A T3B T3C ATWS	Core Cooling And Ultimate Heat Sink	
Service Water Rank: #9 %CDF=12% SW Cross-tie %CDF=0.2%	The service water (SW) system PSA model consists of those components required to fulfill the heat removal and core cooling function (service water cross-tie.) The SW system consists of pumps, piping, valves and associated components. The model includes components of the RHR service water booster system needed to support the equipment heat removal function. The RHR SW cross-tie system uses pumps and valves common to the SW, RHR (LPCI) and Reactor Recirculation Systems to inject service water into the RPV using the LPCI injection lines. The RHR SW water cross-tie has no automatic actuation and must be manually aligned and manually actuated. The cross-tie system consists of SW pumps, boosters, cross-tie valves and various valves to define the injection flow path, the remaining permissives, interlocks and isolations/trips are part of SW model. The dominant failures of SW system are non-recovery of SW failure 42%, general hardware failures 40%, human failure successfully operate booster pumps 12%, common cause failure 7%, various valve failures	Loss of Service Water Transient PSA Sequences: TSW	Support Sys Ultimate Heat Sink And Core Cooling	

PSA Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station

CNS PSA Systems	Risk Significant Systems Ranking Safety Improvement Insights, CDF %[1] Reasons for Importance at CNS	Cornerstones		
		Initiating Events	Mitigating Systems	Barrier
	7%, motor driven pumps fail 3% and unavailability due to test or maintenance <1%. Concurrent random failure of both SW trains occur in 10% of the sequences. Support system functions for dependable SW operation include; DC power for control logic (standby mode), AC power for valves, pump motors and associated equipment. Initiating events attributed with core damage due to SW failure are LOSP (T1) 48%, loss of service water (TSW) 42% , loss of condenser (T2) 3%, and transient with condenser (T3A) 2%. The failure of the SW support equipment can fail the diesel generators, turbine equipment cooling and reactor equipment cooling systems. The recovery strategy for SW failure has significant impact on system dependability. When combined with divisional random failure of EDGs, the SBO core damage sequences can be attributed to loss of SW 12%, DC power failure 5% and failure of NBI at 2%. The unavailability of one service water train due to random failure or maintenance, combined with the failure (or unavailability) of the other safety train that are service by the remaining train, have the potential to be a major contributor to risk. Therefore, configuration control is important during maintenance or emergent work on SW system. These issues are individually covered by CNS Procedure 0.49 as part of plant risk management.			
HPCI Rank: #10 %CDF=10%	The high pressure core injection system PSA model consists of those components required to fulfill the core cooling function. This consists of HPCI turbine, pump, suction and injection flow paths and automatic level control. The dominant failures of HPCI are turbine failures 56%, motor operated valves 34%, unavailability due to test or maintenance 10% and human errors contributions <1%. Concurrent random failure of both HPCI and RCIC occur in 26% of the sequences with HPCI failure (excludes RCIC common cause failures.) Support system functions for dependable HPCI operation include; DC power for motor operated valves and electric motors to support turbine operation and associated RPV instrumentation (NBI.) The room cooling for the HPCI quad during an SBO event is necessary for successful HPCI operation, therefore HPCI is not a viable long term SBO injection source. The initiators attributed with core damage due to HPCI failure are loss of condenser (T2) 45%, loss of instrument air (TIA) 20%, loss of Div I DC (TDCA) 16%, transient with condenser (T3A) 14% and LOSP (T1) 2%. The RCIC system importance for core cooling during Station Blackout (SBO) scenarios is amplified due to the room cooling dependency of HPCI. There are no specific recovery actions effecting the dependability of the HPCI system. If continued long term containment heat removal is not assured for an event sequence, continued HPCI injection could be challenged by either, NPSH and vortex requirements or turbine lube oil temperature limits when taking suction from suppression pool. Containment pressurization does not challenge HPCI operation during loss of containment heat removal due to the 135 psig HPCI turbine exhaust limit.		High Pressure Core Cooling System	

PSA Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station

CNS PSA Systems	Risk Significant Systems Ranking Safety Improvement Insights, CDF %[1] Reasons for Importance at CNS	Cornerstones		
		Initiating Events	Mitigating Systems	Barrier
Residual Heat Removal (RHR) Rank: #11 %CDF=7%	The residual heat removal (RHR) system PSA model consists of those components required to fulfill the containment heat removal and core cooling function. The RHR system consists of two trains with pumps, piping, valves and associated components. The model includes specific components of the RHR system for low pressure coolant injection (LPCI), suppression pool cooling (SPC), containment spray (CSS) and shutdown cooling (SDC) modes of operation. The LPCI mode provide core cooling, while SPC, SDC and CSS modes provide containment heat removal. The major commonalities for RHR operation are: 1) the RHR pumps are used in all modes, 2) heat exchanger cooling is used for CSS, SDC and SPC modes, and 3) the suppression pool suction valves (MO 13s) for each pump train are common to CSS, SPC and LPCI modes. The SPC, SDC and CSS modes of operation does not have automatic actuation and must be manually aligned and manually actuated. The dominant failures of RHR are common cause failure of motor driven pumps 49%, unavailability due to test or maintenance 32%, motor operated valve failure 10% and check valve failure 8%. Support system functions for RHR include: instrumentation, DC power and critical AC power (service water for heat removal function.) Initiating events attributed with core damage due to RHR failure are LOSP (T1) 41%, loss of condenser (T2) 28%, loss of instrument air (TIA) 8%, and loss of AC bus F (TACF) 5%. Individual core damage contribution for each mode of RHR is as follows: loss of heat removal 5.6% (SPC 3.8%, SDC 1.8%, DWS <0.0%) and loss of core cooling 3.5% (LPCI.) There are no specific recovery strategies for RHR failure. Human errors are not dominant contributors to core damage for any mode of the RHR system. On a transient with loss of containment cooling RHR and PCV, eventual containment failure is assumed which impacts long viability of mitigating systems located outside of containment within the reactor building due to harsh environments (steam, flood, etc.)		Core and Containment Cooling System	PC
Standby Liquid Control System (SLC) Rank: #12 %CDF=6.5%	The standby liquid control system PSA model consists of those components required to fulfill the reactivity control function. This consists of SLC pumps, tank, suction and injection flow paths. The SLC system must be manually actuated during an ATWS event. The dominant failures of SLC are common cause failures of explosive valves 28%, human error failure to operate within time frame required 28%, general system failures 18%, other common cause failures 8% and unavailability due to test or maintenance 8%. Support system functions for dependable SLC operation include; AC power and successful reactor water cleanup isolation. The SLC system provides important mitigating function during ATWS scenarios. This alternate reactivity control system is dependent on timely operator initiation during isolation ATWS events. Other important associated actions include RPV water level control during ATWS events to reduce heat loads.		Reactivity Control Sys	

PSA Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station

CNS PSA Systems	Risk Significant Systems Ranking Safety Improvement Insights, CDF %[1] Reasons for Importance at CNS	Cornerstones		
		Initiating Events	Mitigating Systems	Barrier
Automatic Depressurization System (ADS) Rank: #13 ADS %CDF=5.8%	The automatic depressurization system PSA model consists of those components required to fulfill the RPV pressure control function. The ADS system operates in conjunction with standby low pressure core injection systems for core cooling. The ADS system consists of safety relief valves, safety valves, SRV accumulators and inhibit function (no circuitry modeled.) The ADS system actuates automatically and is manually inhibited as directed by emergency operating procedures. The dominant failures of ADS are common cause failures of SRVs 52%, and human error failure to manually depressurize 48%. Support system functions for dependable ADS/SRV operation are critical DC power and instrument air. Failure of ADS is important for LOCAs that require depressurization 5% of these core damage cutsets involve failure of ADS. For transients with high pressure injection failure, operators must manually depressurize with ADS (assuming successful inhibit.) The transient initiating events attributed with core damage due to ADS failure are loss of condenser (T2) 32%, loss of instrument air (TIA) 28%, and loss of DC Div I (TDCA) 27%. For ATWS sequences failure to inhibit ADS contributes an additional 6% to the total CDF. This is an important human action which indicates the benefits of controlled RPV depressurization. Detailed studies of the tradeoff between automatic ADS actuation and ADS inhibit for CNS indicate that the overall core damage impact is well balanced between additional risk and safety benefit.	Inadvertant Open Relief Valve Transient PSA Sequences: T3C	RPV Pressure Control Sys	
HVAC Rank: #14 %CDF=5.6%	The heating, ventilation and air conditioning (HVAC) support system PSA model consists of those components required to maintain suitable temperatures in equipment rooms to preclude component failure. The extent of the HVAC model includes cooling to the AC critical switchgear rooms, diesel generator rooms and fan coil units for core spray, RCIC, RHR and HPCI pump rooms. The dominant failures of HVAC are failure of air operated dampers 57%, human error failure to initiate alternate room cooling 30% and supply/exhaust fan failures 13%. Initiating events attributed with core damage due to HVAC failure are loss of offsite power (T1) 66% and loss of service water (TSW) 23%. Alternate room cooling (recovery actions) following loss of HVAC is based on portable ventilation system (requires AC.)		Support Sys Room Cooling	
Turbine Equipment Cooling (TEC) Rank: #15 %CDF=3.8%	The TEC support system PSA model consists of those components required to transfer component heat energy to the service water system. The PSA model includes TEC backup capability of the reactor equipment cooling and service water systems where feasible. The dominant failures of TEC are unavailability of the standby pump (B). The primary initiating events attributed with core damage due to TEC failure is inadvertant open relief valve (T3C) 70% and turbine trip with condenser available (T3A) 19%. The loss of TEC is an initiating event for CNS which leads to loss of various important PCS functions, main condenser heat sink and loss of	Loss of TEC Transient PSA Sequences:	Heat removal support system	

PSA Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station

CNS PSA Systems	Risk Significant Systems Ranking Safety Improvement Insights, CDF %[1] Reasons for Importance at CNS	Cornerstones		
		Initiating Events	Mitigating Systems	Barrier
	feed /condensate injection capability.	TTEC		
DC Electrical Power (Buses, components) Rank: #16 %CDF=2.8%	The DC support system PSA model consists of those components required to provide adequate DC power to equipment used for safe shutdown functions. The dominant failures of DC are common cause failure of the batteries and related hardware failures. The primary initiating event attributed with core damage due to DC failure is loss of offsite power (T1) 90%. Loss of DC buses is an important initiator since it can cause reactor trip and compromise the operation of the mitigating systems. DC power is required for operation of the AC independent systems (e.g. RCIC and ADS or SRVs). Battery depletion times for CNS is 4 hours, no credit is taken for load shedding in the CNS PSA to extend depletion time (this could provide more time for recovery of AC power.)	Loss of DC Bus A or B Transient PSA Sequences: T1 TDCA/B	The essential DC buses are support systems	
Control Rod Drive System (CRD) Rank: #17 %CDF=1.6%	The control rod drive system is modeled as an alternate RPV injection system when used in the enhanced flow alignment. CRD enhanced flow is capable of 240 gpm at low RPV pressure (<300 psi) and 180 gpm at high RPV pressure. The dominant failures of CRD are human error failure to successfully maximize flow to the RPV within the time allowed in the sequence. The primary initiating events attributed with core damage due to DC failure is turbine trip with loss of condenser (T2) 83%.		High Pressure Core Cooling System	
Primary Containment Features Rank: # 18 %CDF=0.6%	The Mark I primary containment can effect the outcome of transient and accident sequences due to passive features which may become challenged. Since ECCS systems can align suction from the torus, the possibility of common cause failure of the ECCS suction strainers (such as plugging or structural limitations) contributes to 0.55% of the CDF. In addition, failure of the initial primary containment pressure suppression function during LOCAs can challenge core cooling due to equipment exposure to harsh environment in the reactor building. Failure of pressure suppression function has two primary causes: either 1) one or more drywell to wetwell vacuum breaker is fail to close, or 2) one or more downcomers rupture in the wetwell airspace during the LOCA event. This type containment failure occurs in 0.1% of the CDF. Loss of this function leads to containment failure which in turn leads to eventual core damage. In this case containment failure occurs prior to core damage, and is the failure of the final fission product barrier – primary containment.		Support System	PC
Instrument air (IAS) Rank: # 19 %CDF=0.5%	The IAS distribution to pneumatic instruments and control components is modeled. The notable failures of IAS include human error failure to align backup dryer or compressor cooling and random failure of compressors. The loss of instrument air is included in CNS PSA model due to its impact on front line systems. The of loss of IA contributes to 6% of the total CDF for CNS.	Loss of Instrument Air Transient TIA	Support System	
Core Spray System (CS)	The CS low pressure core cooling function is modeled. The notable failures of CS include common cause failure of CS pumps and motor operated valve failure. The initiators attributed with CS failure resulting in core		Low Pressure Core Cooling	

Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station

CNS PSA Systems	Risk Significant Systems Ranking Safety Improvement Insights, CDF %[1] Reasons for Importance at CNS	Cornerstones		
		Initiating Events	Mitigating Systems	Barrier
Rank: #20 %CDF=0.2%	damage are fairly distributed, all LOCAs combined are 12%, remaining are transients. The importance of CS is reduced due to the redundancy and diversity of available low pressure coolant injection systems.		System	
Recirculation Pump Trip (RPT) Rank: # 21 %CDF=0.1%	Field breakers to the reactor recirculation pumps fail to open upon scram signal. Momentum of RRMG sets during coast down impacts core reactivity during initial phases (first 10 minutes) of ATWS scenarios. Failure of the RPT can also contribute to the failure of the reactor coolant pressure boundary for very specific sequences, with the most limiting event being the MSIV closure, high flux scram event.		Support System	RC
Reactor Equipment Cooling (REC) Rank: # 22 %CDF<0.1%	The loss of REC is an initiating event for CNS. In addition, loss of REC leads to loss of various important ECCS functions. However due to the cross-tie capability between trains and backup capability with SW, REC failure has negligible risk significance.	TREC	Heat removal support system	
Alternate Rod Insertion (ARI) Rank: # 23 %CDF<0.1%	The loss of the alternate rod insertion capability of CNS has negligible risk significance. The ATWS sequences at CNS are dominated by mechanical failure of the scram function, not electrical failure. The electrical RPS scram signal, the operator action to manually scram and ARI signal all serve to ensure the core is shutdown such that heat loads are reduced to radioactive decay and sensible heat of RPV internals.		Reactivity Control Sys	

PSA Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station

CNS PSA Systems	Risk Significant Systems Ranking Safety Maintenance Insights, Risk Achievement Worth [2] Reasons for Importance	Cornerstones		
		Initiating Events	Mitigating Systems	Barrier
RPS/CRDMs Rank: #1 RAW: 19000	The possibility of common cause failure of the control rod drive system hydraulics has the potential to discount the highly reliable RPS scram signal. Mechanical failure of CRD hydraulics occurs following successful RPS electrical signal. The mechanical failure includes SOV-127 scram valve failure to open, making CRD hydraulic binding possible. The mechanical failure of CRD scram function is the dominant contributor to ATWS CDF scenarios at 99.6% and electrical failure of RPS occurs in only 0.4% of ATWS sequences.		Reactivity Control	
Service Water System Rank: #2 RAW: 5980	The possibility of common cause failure of 3 out of 4 motor driven service water pumps has the potential to impact the reliability of the service water system. This type failure contributes to 0.52% of the core damage frequency. The loss of service water leads to containment heatup and eventual failure which in turn results in core damage. Therefore this failure has an impact on a fission product barrier – containment.	TSW	Heat Removal Support Sys	PC
Electrical DC Power Rank: #3 RAW: 1080	The common cause failure of various DC components could compromise the operation of front-line mitigating systems. At CNS this is dominated by common cause failure of 125V batteries, which contribute to 0.87% of the core damage frequency.	TDCA TDCB	Electrical Support	
Nuclear Boiler Instrumentation Rank: #4 RAW: 500	The common cause failure or unavailability of NBI components could compromise the operation of automatic mitigation functions, such as core injection. At CNS this is dominated by common cause failure of PS52 pressure switches due to failure to restore to service following testing. The signal provides the low reactor vessel pressure permissive signal for low pressure ECCS injection valves to open.		RPV Instruments	
Torus Suction Strainers Rank: #5 RAW: 380	The common cause failure of ECCS suction strainers in the primary containment torus could render all ECCS functions ineffective. Only a factor for limited sequences, such as emergency condensate tank inventory not available, PCS not available. This possibility contributes to 0.55% of the CDF. (Note: This model still has the old strainers.)		RPV Injection Heat Removal	
Electrical AC Power Rank: #6 RAW: 260	Failure or unavailability of AC components could result in loss of offsite power and compromise the operation of mitigating systems. At CNS is this dominated by common cause failure of circuit breaker and other fast transfer components.	TACF TACG	Electrical Support Sys	
Wetwell Vacuum Breakers Rank: #7 RAW: 100	Failure of the initial primary containment pressure suppression function. The failure implies one or more drywell to wetwell vacuum breaker is fail to close or one or more downcomers rupture in the wetwell airspace. The failure contributes occurs in 0.1% of the CDF. Loss of this function leads to containment failure, which results in eventual core damage. Therefore this failure has an impact on a fission product barrier – containment.		Containment Pressure Control (passive)	PC

PSA Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station				
CNS PSA Systems	Risk Significant Systems Ranking Safety Maintenance Insights, Risk Achievement Worth Reasons for Importance	Cornerstones		
		Initiating Events	Mitigating Systems	Barrier
Automatic Depressurization System (ADS) Rank: #8 RAW: 130	Failure of ADS signal to open the associated SRVs to depressurize the RPV prior to core damage at high pressure. At CNS is this dominated by common cause failure of SRVs to open on demand. In addition, operator failure to manually open SRVs to depressurize after inhibiting ADS is the second most important event (RAW: 110.)		RPV Pressure Control	
Residual Heat Removal System (RHR) Rank: #9 RAW: 59	Common cause failure of motor driven RHR pumps. Contributes 3.5% to core damage frequency.		RPV Injection Heat Removal	
Primary Containment Vent (PCV) Rank: #10 RAW: 14	Failure of valve actuators associated with Primary Containment venting. Also included, are; failure of the operator to manually initiate venting prior to containment challenge and, operator failure to bypass the primary containment isolation interlocks associated with venting . Combined these events contribute to 2.6% of CDF. Loss of this function leads to containment failure which in turn results in core damage. Therefore this failure has an impact on a fission product barrier – primary containment.		Containment Pressure Control (active)	PC

PSA Risk Important Systems, Human Errors and Recovery Strategies at CNS				
CNS PSA Actions	**Risk Significant Human Errors** **Safety Improvement Insights, CDF%[3]** **Reasons for Importance**	**Cornerstones**		
		Initiating Events	**Mitigating System**	**Barrier**
Containment Venting Rank: #1, 5, 7	During a transient sequence, with failure of the PCS , containment temperature and pressure increase due to SRV discharge. Operator action is required to remove decay heat using containment vent (alternate systems are either unavailable or failed) before high pressure challenges containment integrity. The dominant contributor is failure to operate valve MOV 233, which occurs in 7.6% of the core damage frequency. Loss of venting leads to containment failure which in turn results in core damage. Therefore this failure has an impact on a fission product barrier – primary containment.		Containment Pressure Control (active)	PC
Mis-calibration of RPV Level Transmitter Rank: #2	During routine calibration activities, technicians mis-calibrate the RPV (LT73) level transmitters which are provide critical water level indication. In the CNS PRA this comprises 6.3% of CDF.		RPV Instruments	
Level Control in ATWS Rank: #3, 9	Effective Rx Vessel level control is needed during an ATWS in order to reduce core power prior to containment challenge on temperature and pressure. Failure of the operator to establish timely level control appears in 5.7% of CDF.		Reactivity Control	
Prevent RPV Overfill in ATWS Rank: #4	Effective reactivity control is needed during an ATWS in order to maintain the reactor shutdown. Failure of the operator to prevent boron depletion during later stages of ATWS appears in 5.1% of CDF cutsets.		Reactivity Control	
Restore pressure switches Rank: #6	Following testing or maintenance activities, technicians fail to restore the RPV pressure switch instrumentation to service (part of the NBI instrumentation.) In the CNS PRA this appears in 2.5% of CDF cutsets.		RPV Instruments	
Perform Manual Depressurization Rank: #8 (non-ATWS)	On selected sequences, depressurization is required after failure of high pressure injection systems to allow for injection with low pressure systems. A complicating factor is that the EOPs may initially direct the operator to inhibit ADS during the event. In the CNS PRA this appears in 2.2% of CDF cutsets.		RPV Pressure Control	

PSA Risk Important Systems, Human Errors and Recovery Actions at CNS				
CNS PSA Actions	**Risk Significant Human Errors** **Safety Improvement Insights, CDF%[3]** **Reasons for Importance**	**Cornerstone**		
		Initiating Events	**Mitigating System**	**Barrier**
Maintain Condenser Available Rank: #10,11	Following reactor trip, the operator fails to take action to maintain the PCS as the heat sink. Two independent actions are important: bypass MSIV low water level interlock to keep flowpath open and start the mechanical vacuum pumps needed to maintain a vacuum in the condenser. In the CNS PRA these actions appear in 1.9% and 1.8% of CDF results, respectively.		Heat Removal	PC
Provide Alternate Room Cooling (In Event of Loss of HVAC) Rank: #12	On transient sequences, loss of HVAC (due to various reasons) can jeopardize ECCS equipment operation. The operators may be able to take actions to provide alternate room cooling, such as opening doors and providing blowers. In the CNS PRA this appears in 1.7% of CDF cutsets.		Heat Removal	
Initiate SLC Rank:#13	Manual initiation of Standby Liquid Control (SLC) system early during ATWS scenarios. In the CNS PRA this appears in 1.6% of CDF.		Reactivity Control	

PSA Risk Important Systems, Human Errors and Recovery Actions at CNS				
CNS PSA Recovery	**Risk Significant Recovery Strategies** **Safety Maintenance Insights, CDF% Ranking** **Reasons for Importance**	**Cornerstones**		
		Initiating Events	**Mitigating Systems**	**Barrier**
Recover Offsite Power Rank: 1 of 5 %CDF: 49%	Some losses of offsite power could be recovered by offsite utility actions (note: completion of these actions do not require operator support.) The recovery of offsite power within 60 minutes is an important post-event recovery action.	T1	Offsite AC power supply is a support system.	
Recover EDG Rank: 2 of 5 %CDF: 41%	Station Blackout sequences occur due to EDGs unavailability or failure to start or run. The importance of recovery of EDGs depends on the failure mode and the time available before they fail after loss of cooling. Some of these are possible just from the main CR, while others require maintenance activity.	T1	EDG electrical support system.	
Recover Power Conversion Rank: 3 of 5 %CDF: 8.5%	The importance of recovery of PCS depends on the cooling requirements of the core and the time available for recovery of PCS before containment fails. Some of these actions are possible just from the main CR, while others require local operator actions.	T2	PCS heat sink and press control	PC
Recover Service Water Rank: 4 of 5 %CDF: 5.2%	The importance of recovery of SW depends on the cooling requirements of mitigating systems and the time available before they fail after loss of cooling. Recovery is also needed to allow adequate removal of decay heat using the RHR heat exchangers. Some of these are possible just from the main CR, while others require local operator actions.	TSW	SW provides heat sink and press control	PC
Recover DC Power Rank: 5 of 5 %CDF: 2.4%	The loss of DC power support system results in failure of mitigating systems. The importance of recovery of DC depends on the failure mode and the time available before the core is adversely effected. Some of these are possible just from the main CR, while others require local activities in the plant.	TDC	EDC electric support system	

CNS Risk Significance Determination Screening

Initial Review PIR # _____

COMPLETE ALL INITIAL REVIEW SECTIONS (1A - 1C)

Section 1A - Cornerstone Evaluation

1. Does the PIR affect any Cornerstone ?

_____ Initiating Events _____ Mitigating Systems _____ Barrier Integrit _____ Emergency Preparedness

_____ Occupational Radiation Safet _____ Public Radiation Safet _____ Physical Protectio

☐ YES ➡ A Level 1 Screen is Required. ☐ NO ➡ Continue ⇓

2. Does the PIR affect any Structure System or Component that is used as a compensatory measure in any open OD/OE, OWA or TCC ?

☐ YES ➡ Continu ⇓ ☐ NO ➡ Non-Risk Significant, No Cornerstone is Affected.

3. Does the open OD/OE, OWA or TCC affect any Cornerstone ?

_____ Initiating Events _____Mitigating Systems _____ Barrier Integrit _____ Emergency Preparedness

_____ Occupational Radiation Safet _____ Public Radiation Safet _____ Physical Protectio

☐ YES ➡ A Level 1 Screen is Required. ☐ NO ➡ Non-Risk Significant, No Cornerstone is Affected.

Section 1B - Cross Cutting Issues Evaluation - Answer All Questions

4. Does the PIR indicate a programmatic breakdown in any area of the CAP process ?

☐ YES ➡ Perform an Apparent Cause Review ☐ NO

5. Does the PIR indicate a condition of ineffective or untimely corrective action for an RCR or SCR ?

☐ YES ➡ Perform an Apparent Cause Review ☐ NO

6. Does the PIR identify a recurring human performance issue that was previously a Condition Adverse to Quality condition in the past 6 months ?

☐ YES ➡ Perform an Apparent Cause Review ☐ NO

7. Does the PIR identify a human performance issue that caused failure of equipment, failures of multiple 10CFR50, Appendix B criteria or result in personnel injury ?

☐ YES ➡ Perform an Apparent Cause Review ☐ NO

IF all Questions 4 through 7 are marked NO, then no Cross Cutting Issues have been identified and no additional corrective ac[illegible]quired for the Cross Cutting Issues. If any Question 4 through 7 is marked YES, then process the PIR as directed.

IF ALL QUESTIONS 1 THROUGH 7 ARE MARKED NO, PLACE THE PIR INTO THE NORMAL CAP PROCESS.

Section 1C - Initial Evaluation Results

☐ Level 1 S[illegible]een Required. Perform a Level 1 Screen Beginning with Section 2

☐ RCR / Apparent Cause Review Required ☐ Normal CAP ☐ Work Item ☐ Root Cause Review ☐ Other: _____

Cross Cutting Issues Identified: ☐ Human Performance ☐ CAP ☐ Safety Conscious Work Environment

Comments:

Performed By: (Print) _____ (Sign) _____ Date _____

Initiating Events

- Turbine Trip with Bypass Initially Availabl
- Turbine Trip with Bypass Initially Unavailable (e.g. Group I, Loss of Circ Water, Ruptured Condenser)
- Loss of Feedwater
- Inadvertent Open Relief Valve
- Loss of Service/Instrument Air
- RCS Leak within Capacity of 1 CRD pump
- Loss of Offsite Power with Emergency Transformer Availabl
- Loss of a 125V DC Division
- LOCA Outside Containment
- Loss of Offsite Power with Emergency Transformer Unavailabl
- Loss of TEC System
- Loss of NBPP
- Loss of REC System
- Loss of a 4160V AC Division
- Small LOCA (RCIC has sufficient capacity and the break will not depressurize the RPV)
- Loss of the Service Water System
- Medium LOCA (HPCI has sufficient capacity and the break will not depressurize the RPV) (Note 1)
- Large LOCA (RPV will depressurize via the break and allow LP systems to inject prior to core damage, and the LP system will be abl to refill the core above the top of fuel) (Note 2)
- Anticipated Transient without Scram (Note 3)
- Interfacing System LOCA
- DBA type LOCA (Double ended break of a Recirc Line)
- Vessel Ruptur

Note 1: CNS PSA rev 96a evaluates medium LOCA, but latest analysis shows that breaks larger than RCIC capacity will depressurize the RPV similar to the large LOCA

Note 2: The DBA type LOCA is a subset of this initiator and is categorized separately. A large LOCA will depressurize slowly (on the order of minutes rather than seconds), allowing time for the DGs to slow start and other non-DBA valves to realign LP systems

Note 3: ATWS is not really an initiator, but it can be treated as such for these analyses

Mitigating Systems

- ARI
- Containment Vents
- Core Spray
- HPCI
- RCIC
- REC (Quad Cooling, CRD Cooling)
- RHR - LPCI, Containment Sprays, Torus Cooling, Shutdown Cooling
- RHR Service Water Booster System (LPCI, Containment Sprays, Torus Cooling, Shutdown Cooling)
- SBLC
- Service Water (Including Cross-Tie to REC and Alternat Injection
- SRVs (Relief Mode and Manual Actuation) (Open & Closed)
- Torus to Drywell Vacuum Breakers

- Circ Water (For Main Condenser Heat Removal)
- Condensate / Feedwater
- CRD - Mechanical (Including HCU's) and Hydraulic (Including Flow to the RPV)
- Instrument and Service Air
- Main Condenser (As a Heat Sink)
- Main Turbine Bypass Valves (Open -Main Condenser Heat Removal)
- MSIVs (Open -Main Condenser Heat Removal) (Closed - Primary Containment Integrity)
- TEC
- Nuclear Boiler Instrumentation (Pressure, Level)

- RPS
- Emergency Diesel Generators
- 4160 VAC Essential & Non-Essential (For Equipment & Systems Listed Above)
- 125 VDC (For Equipment & Systems Listed Above)
- 250 VDC (For Equipment & Systems Listed Above)
- 120 / 240 VAC Instrument Power (For Equipment & Systems Listed Above)
- No-Break Power (For Equipment & Systems Listed Above)
- RPT Logic

CNS Risk Significance Determination Screening

Level 1 Screen PIR # _____

Section 2 - Description

Summary Description of Issue / Condition:

System(s) and/or Trains with Degraded Equipment:

Licensing Basis and/or Technical Specification Requirement Not Met:

Maintenance Rule Risk Significant: ____ Yes ____ No

Time Degraded Condition Existed or Estimated to Exist:

Section 3 - Cornerstones and Functions Affected / Degraded by the Issue / Condition

(Mark each applicable condition)

3A - INITIATING EVENTS

☐ Transient initiator contributor (e.g. Rx Scram, Turbine trip, Loss of Offsite Power, CSCS Initiation)

☐ Primary System LOCA initiator contributor (e.g. RCS or Main Steam / Feedwater leaks or pipe degradation)

3B - MITIGATING SYSTEMS

Core Decay Heat Removal

- ☐ ECCS Systems (e.g. LPCI, CS, HPCI, RCIC)
- ☐ BOP Systems (e.g. Main Condenser, Cond/Feed, CRD)

☐ Long Term Decay Heat Removal (e.g. Shutdown Cooling, SRVs, Torus Cooling)

☐ Reactivity Control (e.g. CRD, SLC, RWCU, RCIC)

3C - BARRIER INTEGRITY

☐ RCS LOCA Mitigation Boundary degraded (Unidentified Leakage > 25% TS Limit)

Primary Containment Integrit

- ☐ Breach or Bypass of Primary Containment (e.g. PCIV not isolable)
- ☐ Heat Removal or Pressure Control degraded or not functional (e.g. drywell cooling, drywell / torus sprays, vent and purge capability)
- ☐ Fuel Cladding degraded (Also review Public Rad Safety Cornerstone)

Continue on Page 4 for additional Cornerstone areas

Section 3 - Cornerstones and Functions Affected / Degraded by the Issue / Condition (continued)

(Mark each applicable condition)

3D - EMERGENCY PREPAREDNESS

Violation or Potential Violation of 10 CFR or of the Emergency Plan

- ☐ Failure to meet or implement Planning Standards (Refer to 10 CFR 50.47(b) and Appendix E)

Problem Identification Issue

- ☐ Failure to identify a problem during a drill or exercise
- ☐ Failure to resolve or resolve in a timely manner a problem identified during a drill or exercise

3E - PUBLIC RADIATION SAFETY

Rad Material Control

- ☐ Radwaste Shipping Problem (This includes 10 CFR 61 requirements, shipping records, etc.)
- ☐ Radwaste Processing (This includes sampling and characterization)
- ☐ Contamination Monitors for material exiting the RCA

Effluent Release Program - Gaseous and Liquid Effluents

- ☐ Releases above 10CFR50, Appendix I limits
- ☐ Unmonitored or potentially unmonitored releases
- ☐ Effluent monitoring rad monitors and Count Room instrumentation operation and calibration (This includes verification of ventilation flowrates)

Environmental Monitoring Progra

- ☐ Sample Collection, Measurement and Analysis
- ☐ Calibration and Operations of Meteorological and Counting instrumentation

3F - OCCUPATIONAL RADIATION SAFET

ALARA Progra

- ☐ Actual job dose greater than estimated (Actual exceeded Estimated by 25% or more)
- ☐ Unintended Contamination of a previously clean area

Unintended Exposure

- ☐ Exposure of >50 mrem that is not intended

Substantial Potential Exposure

- ☐ Violation of a Locked High Rad Area or Very High Rad Area (e.g. High Rad Door checks)

Dose Assessment

- ☐ Inability to determine or assess dose
- ☐ Radiation Monitoring instrumentation problems (Including PAM instruments, Containment Rad Monitors and ARMs)

3G - PHYSICAL PROTECTION

- ☐ Access Authorization
- ☐ Access Control
- ☐ Physical Protection Systems
- ☐ Response to Contingenc

Continue to Page 5 for Level 1 Screening

CNS Risk Significance Determination Screening (Continued)

Level 1 Screen PIR # _____

Section 4 - LEVEL 1 SCREENING PROCESS (Mark all boxes that apply from Section 3)

☐ **INITIATING EVENT** ☐ **MITIGATING SYSTEMS** ☐ **BARRIER INTEGRITY** ☐ **EMERGENCY PREPAREDNESS**

☐ **OCCUPATIONAL RADIATION SAFETY** ☐ **PUBLIC RADIATION SAFETY** ☐ **PHYSICAL PROTECTION** ☐ **NONE**

If more than one Cornerstone is marked, a Level 2 screen is required. If **NO** Cornerstone is affected, then the concern screens OUT as "**GREEN**". No further assessment is required.

If only one Cornerstone is affected, continue in the appropriate section below.

Section 4.A INITIATING EVEN

1. Does the issue / condition contribute to the likelihood of a Primary System LOCA?

☐YES ➡ Level 2 Screen Required ☐NO ➡ Continue ⇓

2. Does the issue / condition contribute to both the likelihood of a reactor SCRA AND the likelihood that mitigation systems / equipment will not be available ?

☐YES ➡ Level 2 Screen Required ☐ NO ➡ Screen OUT as **GREEN**

Section 4.B MITIGATING SYSTEMS

1. Does the issue / condition concern a Design or Qualification issue that is still Operable per GL 91-18 (rev 1) ?

☐YES ➡ Screen OUT as **GREEN** ☐NO ➡ Continue ⇓

2. Does the issue / condition represent an actual Loss Of Safety Function of a Mitigating System ?

☐YES ➡ Level 2 Screen Required ☐NO ➡ Continue ⇓

3. Does the issue / condition concern TS equipment or systems ?

☐YES ➡ Continue to Question 4 ⇓ ☐NO ➡ Continue to Question 5 ⇓

4. Does the issue / condition represent an actual Loss of Safety Function for a single train of a multi-train system for greater than TS LCO?

☐YES ➡ Level 2 Screen Required ☐NO ➡ Screen OUT as **GREEN**

5. Does the issue / condition affect equipment designated as risk-significant under the Maintenance Rule ?

☐YES ➡ Level 2 Screen Required ☐ NO ➡ Screen OUT as **GREEN**

Section 4.C BARRIER INTEGRITY

1. Does the issue / condition identify a failure or potential failure of the RCS boundar

☐YES ➡ Level 2 Screen Required ☐NO ➡ Continue ⇓

2. Does the issue / condition concern fuel barrier integrity ?

☐YES ➡ Screen OUT due to the condition being monitored ☐NO ➡ Continue ⇓
by the Performance Monitoring Progra .

3. Does the issue / condition concern a failure or potential failure of Primary Containment integrity ?

☐YES ➡ Contact Risk Management for an evaluation. ☐ NO ➡ Screen OUT as **GREEN**

Continue to Page 6 for Level 1 Screening of additional Cornerstone areas.

Section 4.D EMERGENCY PREPAREDNESS

1. Does the issue / condition concern identify a violation or potential violation of regulatory requirements for Emergenc Planning ?

☐YES ➡ Level 2 Screen Required ☐NO ➡ Continue ⇓

2. Does the issue / condition identify a failure to implement or meet an Emergency Planning requirement during a drill / exercise or during a real event ?

☐YES ➡ Level 2 Screen Required ☐NO ➡ Continue ⇓

3. Does the issue / condition identify either a failure to identify an Emergency Planning issue OR resolve an identified Emergency Planning issue OR resolve an identified Emergency Planning issue in a timely fashion ?

☐YES ➡ Level 2 Screen Required ☐ NO ➡ Screen OUT as **GREEN**.

Section 4.E PUBLIC RADIATION SAFETY

1. Does the issue / condition concern Rad Material Control ?

☐YES ➡ Level 2 Screen Required ☐NO ➡ Continue ⇓

2. Does the issue / condition concern the Effluent Release Progra ?

☐YES ➡ Level 2 Screen Required ☐NO ➡ Continue ⇓

3. Does the issue / condition concern the Environmental Monitoring Program ?

☐YES ➡ Level 2 Screen Required ☐ NO ➡ Screen OUT as **GREEN.**

Section 4.F OCCUPATIONAL RADIATION SAFETY

1. Does the issue / condition concern the ALARA program ?

☐YES ➡ Level 2 Screen Required ☐NO ➡ Continue ⇓

2. Does the issue / condition concern an Unintended Exposure ?

☐YES ➡ Continue ⇓ ☐NO ➡ Go to Question 4 ⇓

3. Did an Overexposure occur ?

☐YES ➡ Level 2 Screen Required ☐NO ➡ Continue ⇓

4. Does the issue / condition concern a Substantial Potential Exposure ?

☐YES ➡ Level 2 Screen Required ☐NO ➡ Continue ⇓

5. Does the issue / condition compromise the ability to assess dose ?

☐YES ➡ Screen OUT as WHITE ☐ NO ➡ Screen OUT as **GREEN.**

Section 4.G PHYSICAL PROTECTION

1. Determine the risk of Radiological Sabotage based on the issue / condition:

☐SOME RISK ➡ Level 2 Screen Required ☐LOW RISK ➡ Screen OUT as **GREEN**.

Continue to Page 7 for Level 1 Screening Evaluation results.

Section 5 - Level 1 Screening Results

Result of Level 1 Screening Process: ☐ Screen OUT as **GREEN** ☐ Level 2 Screen Required

List assumptions made for the evaluation (as applicable):

Section 6 - Cross Cutting Issues

List any aspects of the PIR that may imply a failure or degraded condition in any of the cross cutting issues:

(Mark all that apply)

☐ Corrective Action Progra ☐ Human Performance ☐ Safety Conscious Work Environment

Section 7 - Screening Performed By

Name: (Print) _____ (Sign) _____ Date _____

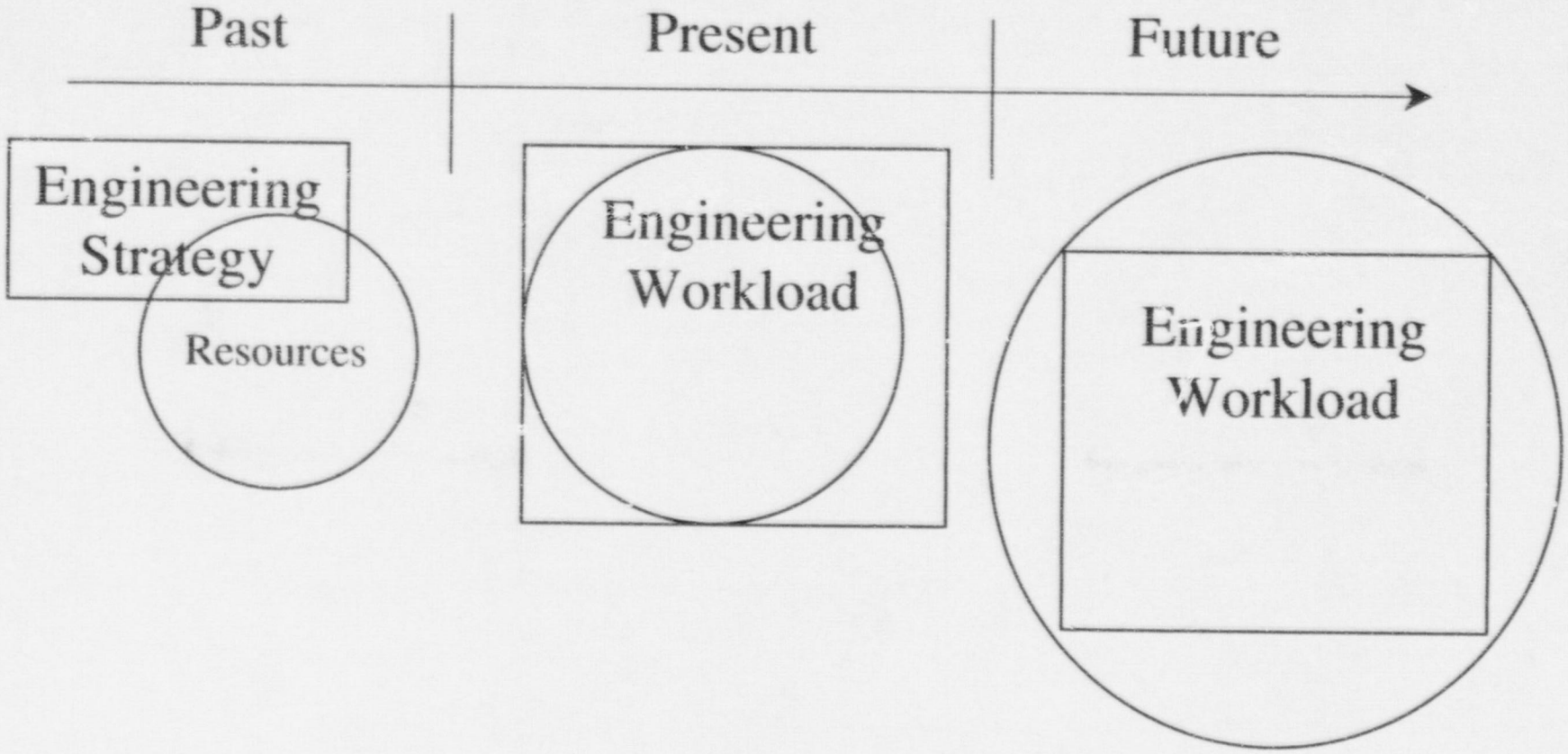
Using Risk Information to Prioritize Engineering Work

Rick Wachowiak
Nebraska Public Power District

presented at

Region IV PRA Conference

Engineering Resources
at CNS

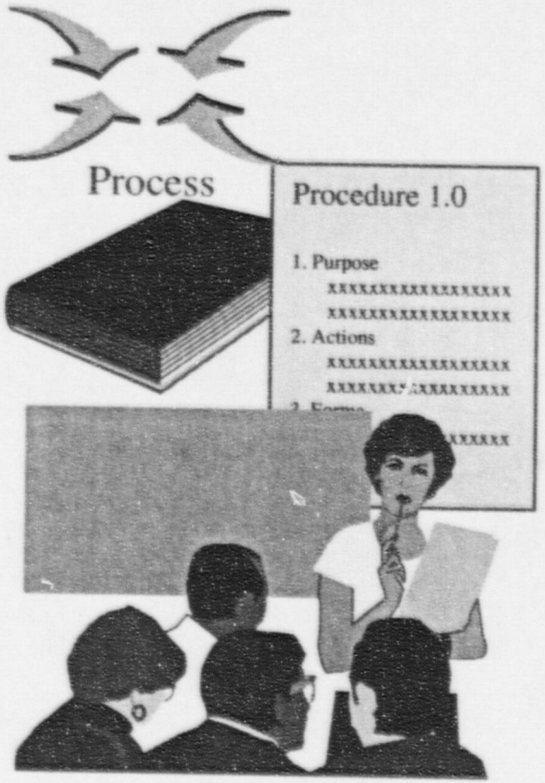


- Scope not defined
- Resources mis-applied

- Scope defined
- Resources insufficient

- Scope doesn't decrease
- Resources more effective
- Result of RI and training

Risk Informed Engineering



- Not intended to be an integrated approach
- Helps optimize medium/large projects
- Focused
- Gets Risk Information into the hands of the Engineers

Match Risk Information to the Project

- Type of risk information needed will vary
- Determine figure of merit
  - CDF
  - LERF
  - Other
- Determine Importance Measure
- Does not need to be quantitative
- Maintenance Rule ranking is usually overkill

Match Risk Information to the Project

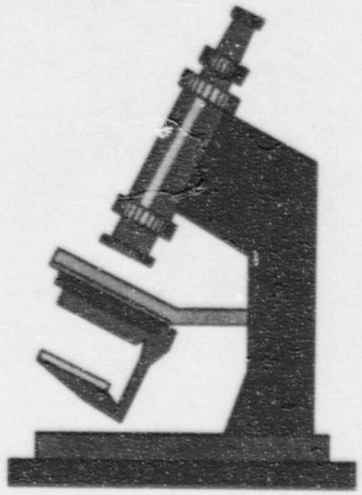
Always look at

- Common Cause
- Human Actions
- Recoveries

for applicability

Match Risk Information to the Project

Look at the critical characteristics



- **Valve Program:**
  - Adjusts reliability about a mean
  - FV dominates
  - Must consider common cause failures

- **Past Modification Review**
  - Determine if system will perform its function
  - RAW dominates
  - Human actions may be important

CNS Examples

Severe Accident Management Implementation

- Project designed to incorporate Risk Information
- Started with a list of IPE/IPEEE insights
  - 11 initial issues
  - 10 determined not to be significant
  - 1 incorporated, but as a procedure change rather than a modification
- One additional insight discovered
  - For human actions, the decision phase is much more important than the execution phase

CNS Examples

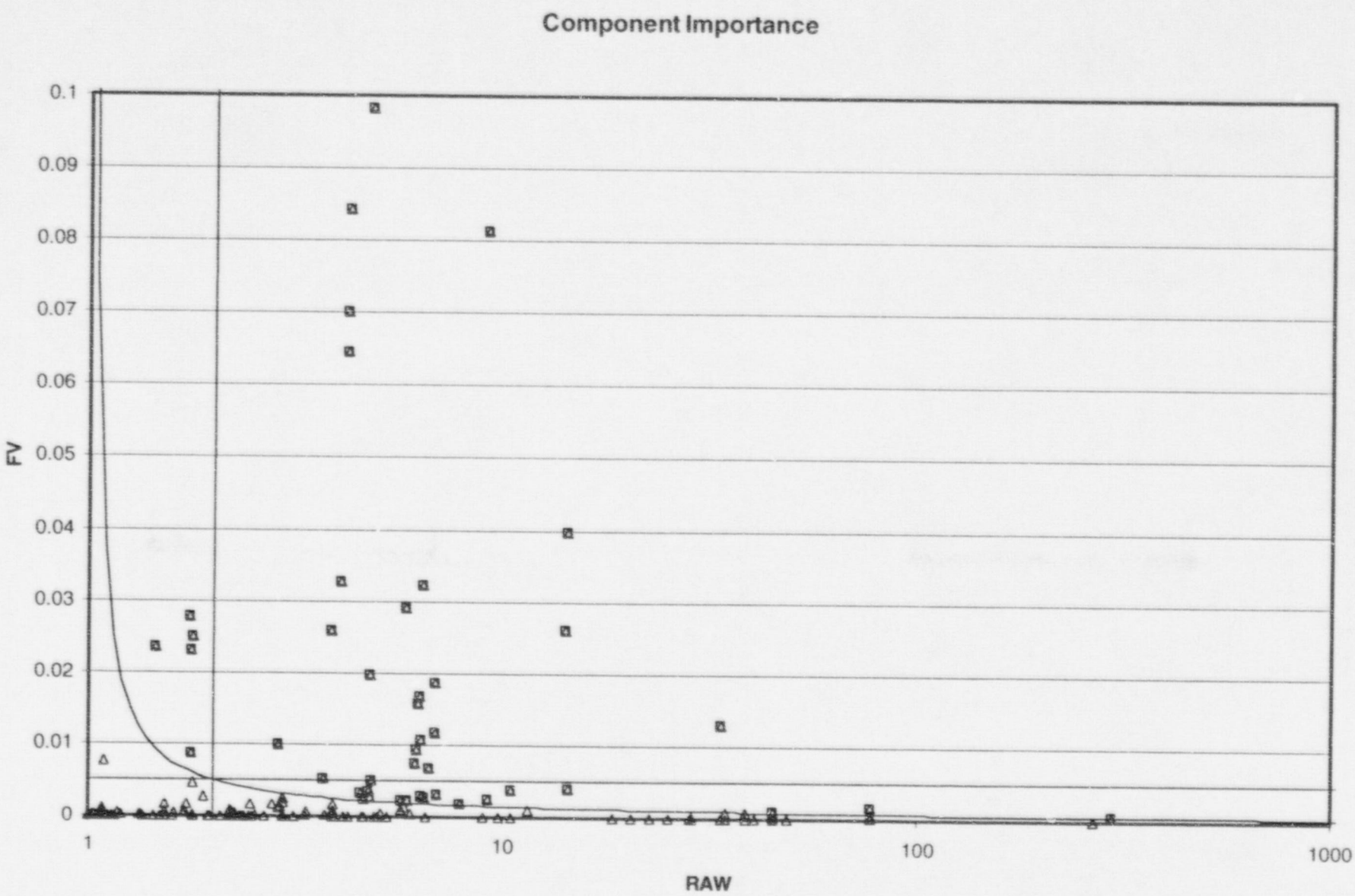
Past Modification Review

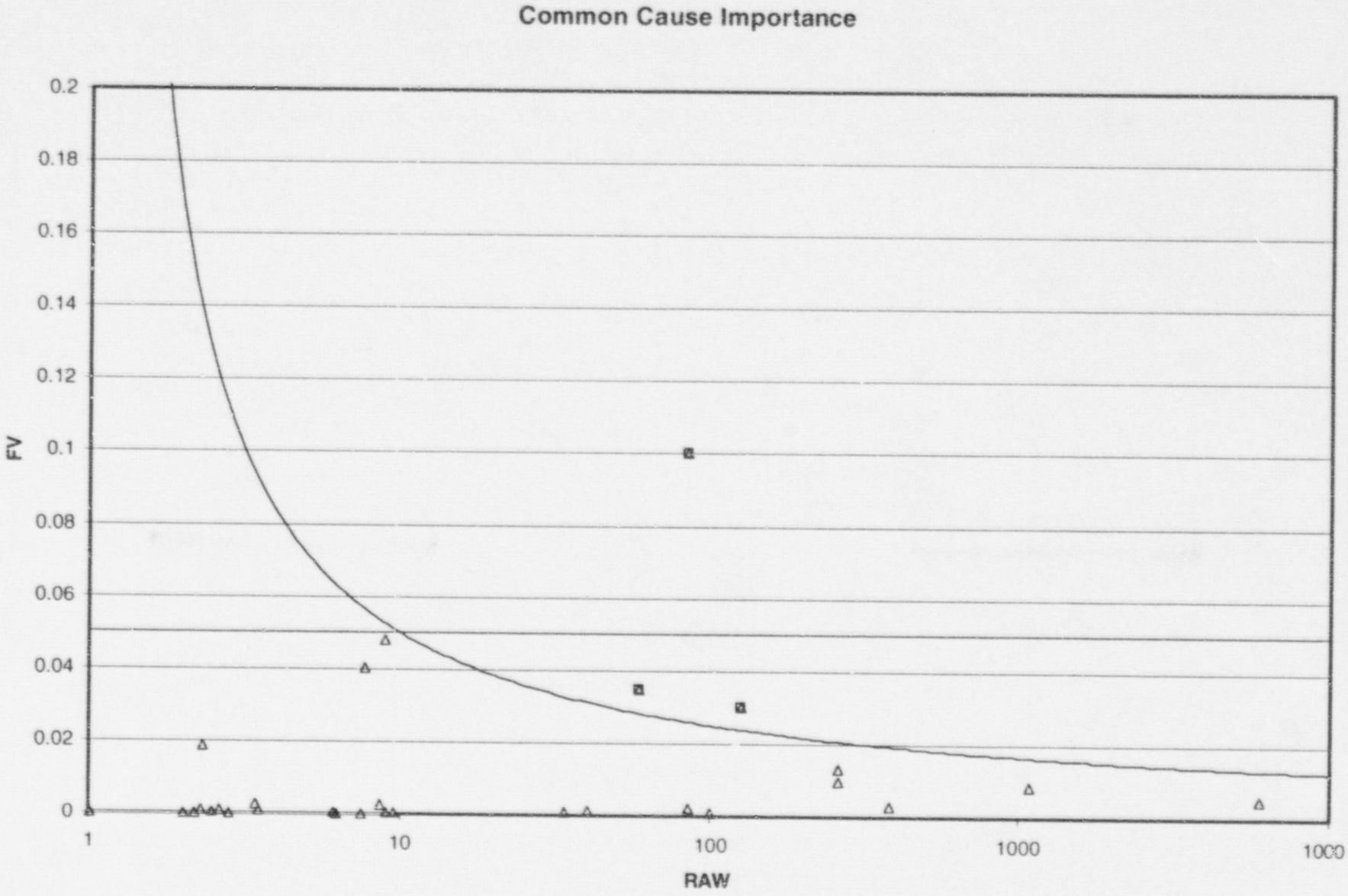
- Objective to ensure low probability of significant findings
- Limit population to systems with potential to have significant findings
- Resulted in higher confidence that there were no significant findings

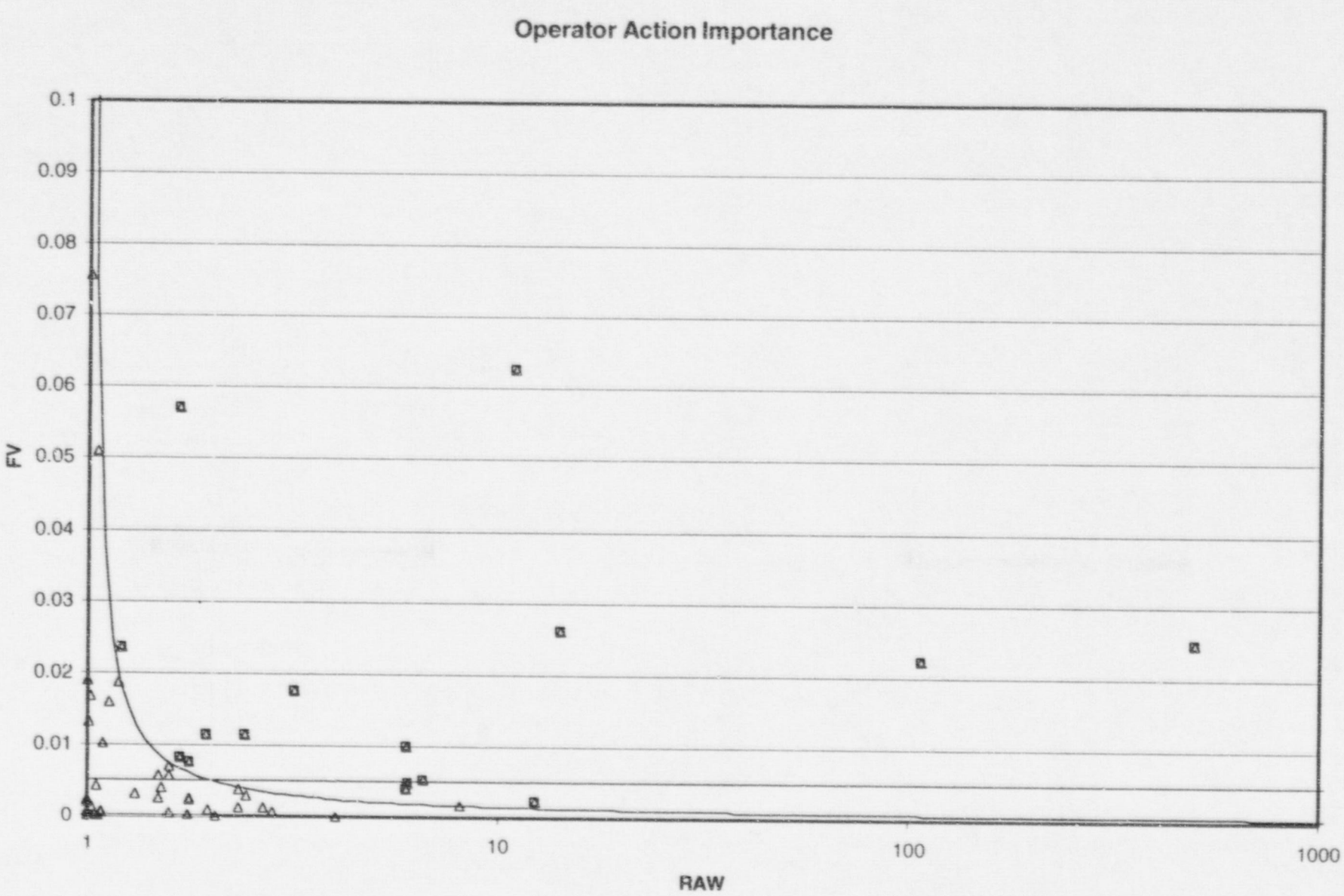
CNS Examples

FSAR Reconstitution

- Several attempts at prioritizing
- Periodically screened open items for significance
- Mainly used to sequence the the completion of the sections
- If the information in a chapter is important, put it earlier in the sequence
- All importance measures have a place in this project
- Attempt to combine FV and RAW measures on a single scale


Component Importance
0.1
0.09
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0
FV
1
10
100
1000
RAW


Common Cause Importance
0.2
0.18
0.16
0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
FV
1
10
100
1000
1000
RAW


Operator Action Importance
0.1
0.09
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0
FV
1
10
100
1000
RAW

CNS Examples

Instrument Uncertainty for Indications

- Instruments where surveillance acceptance and Tech. Spec. limits are the same
- From a core damage Risk perspective, how much margin do we have
  - Is it significant if the function is lost?
  - What is the PRA success criteria vs. the Tech Spec
- A couple of significant parameters identified, but these have no specific PRA success defined

CNS Examples

Classify Risk of Issues Early

- Developed because CNS is a pilot plant in the new oversight process
- Risk Management Group is involved in classification of all plant issues
- Risk Management Group is involved in all reportable issues
- Risk Management Group is involved in all equipment related Significant Conditions Adverse to Quality

CNS Examples

Classify Risk of Issues Early (continued)

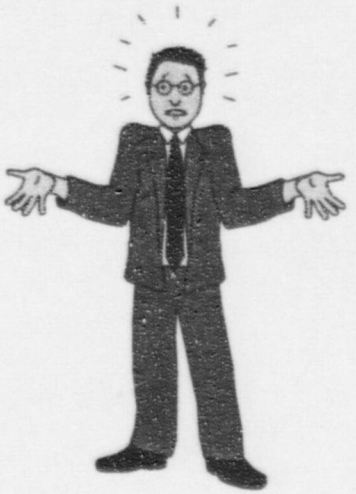
- Developing plant specific Risk Matrices
- Developing plant specific Risk basis document
- Developing templates for performing Risk reviews
- Developing Risk insight training for OPS, Licensing, QA, CAP, Engineering, etc

Example Page from Plant Specific Risk Matrix

PSA Risk Important Systems, Human Errors and Recovery Strategies at Cooper Nuclear Station				
CNS PSA Systems	Risk Significant Systems Ranking Safety Improvement Insights, CDF % Reasons for Importance at CNS	Cornerstones Initiating Events	Mitigating Systems	Barrier
Onsite Emergency AC Power Rank #1 %CDF=50%	Onsite Emergency AC power as defined by the PSA model includes emergency diesel generators, and various buses (4160, 480 VAC) associated switch gear, breakers, motor control centers, etc. Dominant failures of the AC buses and circuitry are circuit breaker failure 32%, common cause failure of AC components 27%, relay failure 5% and bus unavailability due to test or maintenance which occurs in 4% of the loss of onsite AC power cutsets. Concurrent hardware failures of both buses occur in 2% of these sequences (excluding common cause failures); otherwise single bus random failure combined with support system failures (non-critical AC, 125VDC, room cooling) of the opposite bus contribute to 10% of the cutsets. There are no specific human errors nor recovery actions effecting the dependability of the AC hardware.	Loss of AC Bus F or G Transient PSA Sequences: T1, T2, T3C, TACF, TACG	The essential AC buses and the onsite AC emergency power (EDG) fulfill an important support system function.	
Emergency Diesel Generators Rank #3 %CDF=45%	The dominant failures of the diesel generators are failure to start 37%, common cause failure of both emergency diesel generators 21%, unavailability due to test or maintenance 19%, and failure to run the duration of mission time 12% of the loss of AC power cutsets. Concurrent failures of both diesels occur in 15% of cutsets (excluding common cause); otherwise random single EDG failure combined with support system failures of the opposite EDG contribute to 71% of the failure results. Support system functions for dependable EDG operation include: DC power for breaker control and EDG starting, service water system cooling, HVAC ventilation of EDG rooms (and standby switch gear rooms) and associated instrumentation (NBI). The failure to restore from testing is the dominant human error effecting EDG reliability, however this failure is limited to 2% of loss of onsite AC power sequences. Recovery of DGs occurs in 83% of all loss of onsite AC power sequences. The unavailability of one diesel generator either due to random failure or maintenance, combined with the failure of the other safety trains that are fed from the remaining emergency bus, have the potential to be a major contributor to risk. Therefore, configuration control is important during maintenance or emergent work on EDGs. These issues are individually covered by CNS Procedure 0.49 as part of plant risk management.			
Offsite AC Power Rank #2 %CDF=49%	The loss of offsite power (LOSP) is an important initiating event, if lasting beyond 60 minutes (core boil-off time assuming no LOCA and no core injection.) The LOSP event could occur as a result of adverse weather conditions (weather-centered LOSP), grid or switch yard activities (grid-centered LOSP), or on-site plant activities such as component failure, design inadequacy, or human error (plant-centered LOSP). Important design features include: The AC switchyard redundant design and diverse maintenance alignments contribute to the overall reliability of the AC power system. The number of offsite lines capable of providing critical loads (7 MW) is 7. There are 5 lines at 345kV, 1 at 161kV and at 69kV capable of 10MW). The switchyard design consists of a ring bus with 1½ breaker configuration which allows removal of any one 345kV line for maintenance without effecting the other lines on the ring. This configuration greatly enhances the availability and reliability of offsite AC power function.	Loss of Offsite (AC) Power PSA Sequences: T1, T1W, T1P, T1G, LOSP, LOSEP	Offsite AC power supply fulfills support system functions. Offsite AC power is considered recoverable in T1 sequences and initially available in all	

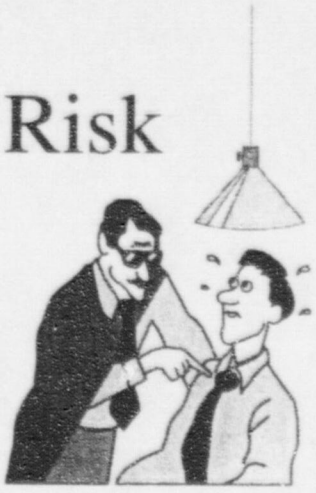
Prioritizing Modifications

- So far, we have not been able to influence
- Driven by OPS and Budget
- Three key items to consider
  - Does it reduce Risk?
  - Can it be designed to reduce Risk?
  - How can installation minimize Risk?
- New oversight process should help
  - OPS and Engineering need to be able to discuss Risk with the regulator



Have We Reduced Engineering Resource Requirements?

- It's too early to tell
- There is increased awareness that Risk insights are available
- PRA staff is in great demand
- Feedback indicates that the Risk information tools are being applied and are useful



Proposed Issues

- NRC envisioned benefits from certification
- PRA Model Living Programs
- Risk informed submittals - experience
- Maintenance Rule (a)(4)
- Insights from NRC Region IV evaluations of shutdown risk

PROBABILISTIC RISK ASSESSMENT ACTIVITIES

GARY M. HOLAHAN, DIRECTOR
DIVISION OF SYSTEMS SAFETY AND ANALYSIS
OFFICE OF NUCLEAR REACTOR REGULATION
U.S. NUCLEAR REGULATORY COMMISSION

PROBABILISTIC RISK ASSESSMENT ACTIVITIES

REGION IV RISK-INFORMED
COUNTERPART WORKSHOP
JULY 20-21, 1999

GARY M. HOLAHAN, DIRECTOR
DIVISION OF SYSTEMS SAFETY AND ANALYSIS
OFFICE OF NUCLEAR REACTOR REGULATION
U.S. NUCLEAR REGULATORY COMMISSION

RISK-INFORMED INITIATIVES OVERVIEW

- Activities Are Underway in a Number of Areas to Take a Risk-Informed Approach to Regulation in Both Plant-Specific and Generic Activities:
  - Rulemaking (Risk-Informing Part 50)
  - Licensing Activities (Risk-Informed License Amendments)
  - Plant Oversight (Inspection, Assessment, Enforcement)
  - Events Assessment/Generic Issues

ROUNDTABLE DISCUSSION

NRC/INDUSTRY INTERFACE ISSUES

Potential Roundtable / Interface Topics

Maintenance Rule (a)(4) changes for on-line maintenance risk assessments

Review of submittals - cost and response time

PRA Model Living Programs - NRC and Industry expectations

Shutdown Risk

General contact list issues
- periodicity of updates
- methodology to keep NRC updated (i.e. lines of communication, email, etc.)
- threshold of NRC interest for risk related issues

Status of information provided to the NRC
- FOIA
- Proprietary issues
- Docketing status

Risk Characterization of Inspection Findings (Significance Determination Process)

Pilot Plant Inspection Process

Regulatory Impact of SRA Activities
- Regulatory Impact of this meeting
- Potential for future meetings, industry group, etc.
- Management conference calls to understand plant configurations, events, etc.

Use of Risk Information in LERs, Inspection Reports, other correspondence

Use of Risk Information in the Operator Licensing arena

Role of the Region (and the SRAs) in Licensing activities

Use of Risk in the Notice of Enforcement Discretion (NOED) process

Protocols for providing risk information on short notice/real-time
- NOEDs, Events, etc.

SRA site visits
- Feedback from initial site visits
- Feedback from outage assessment visits
- Potential for future visits

Bill Jones' trip to France
- Use of risk information by the French

Proposed Issues

- NRC actions to redirect a licensee submittal to require risk informed addition
- PWR SG tube risk assessment
- Changes to 10CFR50
- Fire Analysis

OBJECTIVES FOR RISK-INFORMED REGULATION

- Improve Safety Decisions
- Efficient Use of NRC Resources
- Reduce Unnecessary Industry Burden
- These Objectives are Equivalent to the Concept of "Focusing NRC and Licensee Resources on Those Issues and Activities Most Importance to Public Health and Safety"

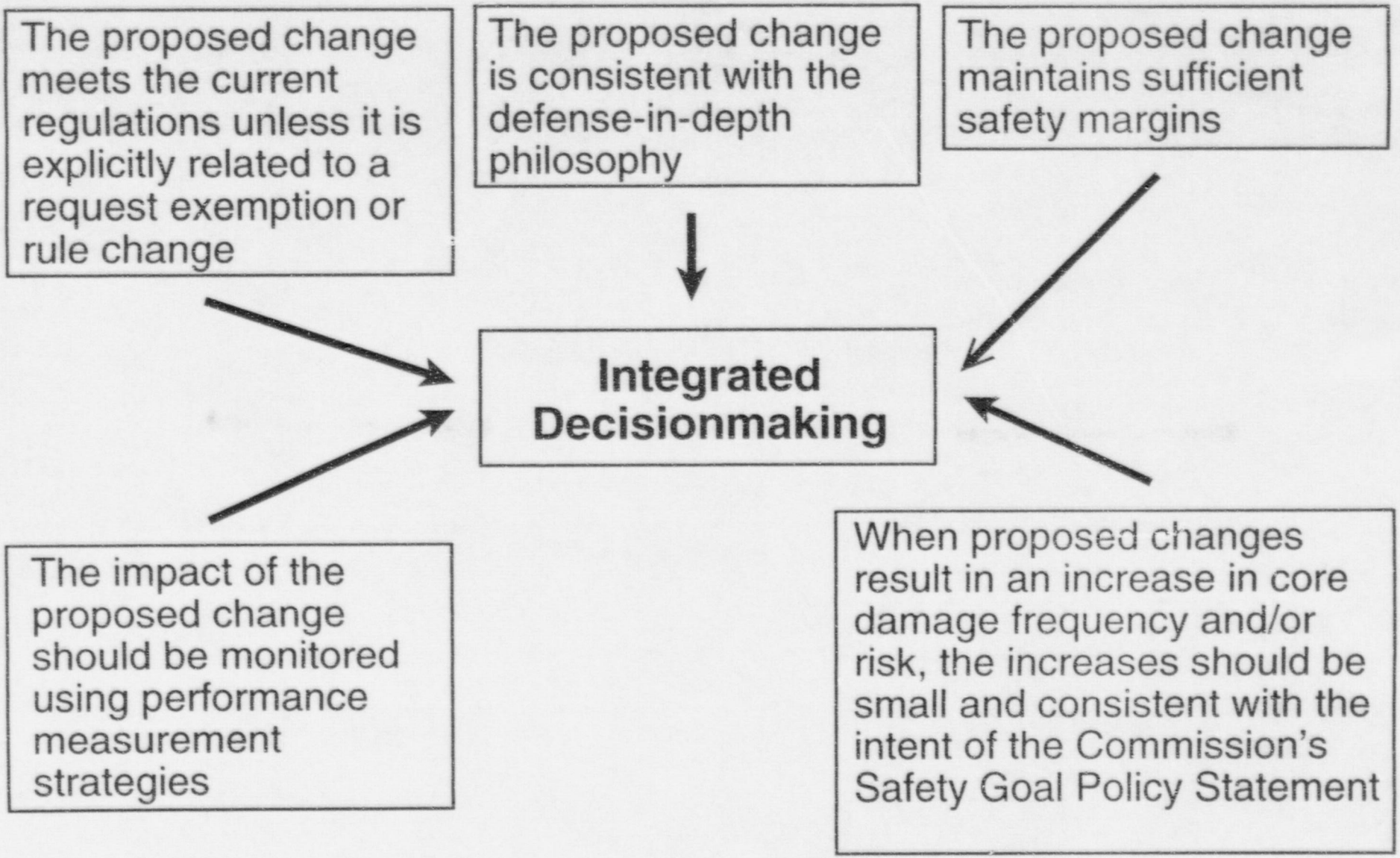
RISK-INFORMED REGULATORY GUIDANCE

Risk-Informed Regulatory Guides and SRPs

Regulatory Guide 1.174 -General Guidance to Licensees	SRP Chapter 19, Revision P - General Guidance to Staff
RG 1.175 - Application Specific Guidance on Inservice Testing (IST)	SRP Section 3.9.7 - Application Specific Guidance on IST
RG 1.178 - Application Specific Guidance on Inservice Inspection (ISI)	SRP Section 3.9.8 - Application Specific Guidanceon ISI
RG 1.176 - Application Specific Guidance on Grade Quality Assurance (GQA)	GQA Inspection Guidance -Under Development
RG 1.177 - Application Specific Guidance on Technical Specifications (TS)	SRP Section 16.1 - Application Specific Guidance on TS

RISK-INFORMED REGULATORY GUIDANCE

Principles of Risk-Informed Decisionmaking



SPECIFIC RISK-INFORMED ACTIVITIES PROGRESS AND STATUS

- Inservice Inspection:
  - Safety Topical Report Issued -December 14, 1998
- Evaluation on Westinghouse Owners Group
  - Safety Evaluation of EPRI Methodology Underway
  - Vermont Yankee, Surry, Arkansas Nuclear One Safety Evaluation Reports Issued
- Inservice Testing:
  - Comanche Peak Safety Evaluation Report Issued August 14, 1998
  - Staff Evaluating Lessons Learned From Pilot Plants

SPECIFIC RISK-INFORMED ACTIVITIES PROGRESS AND STATUS (Continued)

- Graded Quality Assurance:
  - South Texas Proposed GQA Program Approved November 1997
  - South Texas Project Experienced Barriers to Full Implementation
  - Part 50 Rulemaking Would Address the Major Issues
  - Draft GQA Inspection Procedure Undergoing Management Review and Resolution of CRGR Comments
    - Staff Responding to CRGR Issues and Internal Review Comments

SPECIFIC RISK-INFORMED ACTIVITIES PROGRESS AND STATUS (Continued)

- Technical Specifications:
  - Several Topical Reports From CEOG and WOG Approved
  - Plant-Specific Allowable Outage Time Extensions Approved
- Other Licensing Initiatives
  - BWR Vessel Shell Weld Inspections - SER Provided to Commission
  - Whole Plant Study, Task 0:
    - ANO Hydrogen Monitoring SER Completed and Issued
    - San Onofre Hydrogen Recombiner Application Under Staff Review (SER due 6/30/99)

OTHER RISK-INFORMED ACTIVITIES
PRA QUALITY

- PRA Quality
  - PRA Certification Programs (e.g., BWROG)
  - PRA Standards (e.g., ASME Standards)

RISK-INFORMED MODIFICATIONS TO 10 CFR PART 50

- SECY-98-300 Proposed a Two-Phase Review and Modification of 10 CFR Part 50:
  - Changes to Scope, Definitions, and Processes
  - Modifications to Specific Regulations
  - Clarification of Staff Authority

RISK-INFORMED MODIFICATIONS TO 10 CFR PART 50 - OBJECTIVES

- Specific Objectives of 10 CFR Part 50 Modification:
  - Enhance Safety by Focusing NRC and Licensee Resources in Areas Commensurate With Their Importance to Health and Safety
  - Provide NRC With the Framework to Use Risk Information to Take Action in All Regulatory Matters
  - Allow Use of Risk Information to Provide Flexibility in Licensing and Operational Areas

RISK-INFORMED 10 CFR PART 50 OPTIONS

OPTION 1

- Continue Only Ongoing Rulemakings to Change Parts of 10 CFR Part 50 (e.g., 50.59, 50.65, 50.72/73) and Voluntary License Amendment Requests Under Risk-Informed Regulatory Guides

OPTION 2

- Continue Option 1 Activities
- Develop Risk-Informed Definitions, Processes, and Scope Changes to Systems, Structures, and Components Needing Special Treatment in Terms of Quality. Utilize Maintenance Rule as a First Step
- Utilize Industry Pilot Studies to Assist in Scope and Definition Revisions
- Staff Recommends Implementation

RISK-INFORMED 10 CFR PART 50 OPTIONS (Continued)

OPTION 3

- Modification of Specific Regulations to Make Them Risk-Informed:
  - "Acceptable Alternative" Provisions in Selected Regulations
  - Modification of Technical Content to be Risk-Informed
  - Deletion of Regulations With Little Safety Significance
- Utilize Industry Pilot Studies to Assist in Development
- Staff Recommends Further Study

RISK-INFORMED 10 CFR PART 50 POLICY ISSUES

- Voluntary or Mandatory Conformance with Modified 10 CFR Part 50
  - Staff Recommends Voluntary
- Exemptions for Pilot Plants
  - Staff Recommends Use of Exemptions for Pilot Plants
- Modification of Maintenance Rule Scope
  - Continue Near Term Rulemaking
  - Staff Recommends Utilizing Maintenance Rule as an Initial Step in Revising the Scope Under Option 2
- Clarification of Staff Authority for Risk-Informed Decision Making
  - Staff Recommends Development of Guidance to Clarify Application of Risk-Informed Decision Making

BACKGROUND
RISK-INFORMED REGULATION EXPECTATIONS

Expectations (Process)

- Proposed Changes are Evaluated in an Integrated Fashion That Ensures That All Principles are Met.

- All Safety Impacts of the Proposed Change are Evaluated in an Integrated Manner as Part of an Overall Risk Management Approach in Which the Licensee is Using Risk Analysis to Improve Operational and Engineering Decisions Broadly by Identifying and Taking Advantage of Opportunities for Reducing Risk, and Not Just to Eliminate Requirements the Licensee Sees as Undesirable.

- The Use of Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) as Bases for Probabilistic Risk Assessment Guidelines is an Acceptable Approach to Addressing Risk Impact and Consistency with the Intent of the Commission's Safety Goal Policy Statement.

- Increases in Estimate CDF and LERF Resulting from Proposed CLB Changes are Limited to Small Increments, and the Cumulative Effect of Such Changes Should be Tracked and Considered in the Decision-Making Process.

BACKGROUND
RISK-INFORMED REGULATION EXPECTATIONS

Expectations (Analysis)

- The Scope and Quality of the Engineering Analyses (Including Traditional and Probabilistic Analyses) Conducted to Justify the Proposed CLB Change Should be Appropriate for the Nature and Scope of the Change and are Based on the As-Built and As-Operated and Maintained Plant, Including Reflecting Operating Experience at the Plant.

- Appropriate Consideration of Uncertainty is Given in Analyses and Interpretation of Findings, Including Using a Program of Monitoring, Feedback, and Corrective Action to Address Significant Uncertainties.

- The Plant-Specific PRA that is Used to Support Licensee Proposals has Been Subjected to Quality Controls Such as an Independent Peer Review or Certification.

- Data, Methods, and Assessment Criteria Used to Support Regulatory Decision Making are Clearly Documented and Available for Public Review.

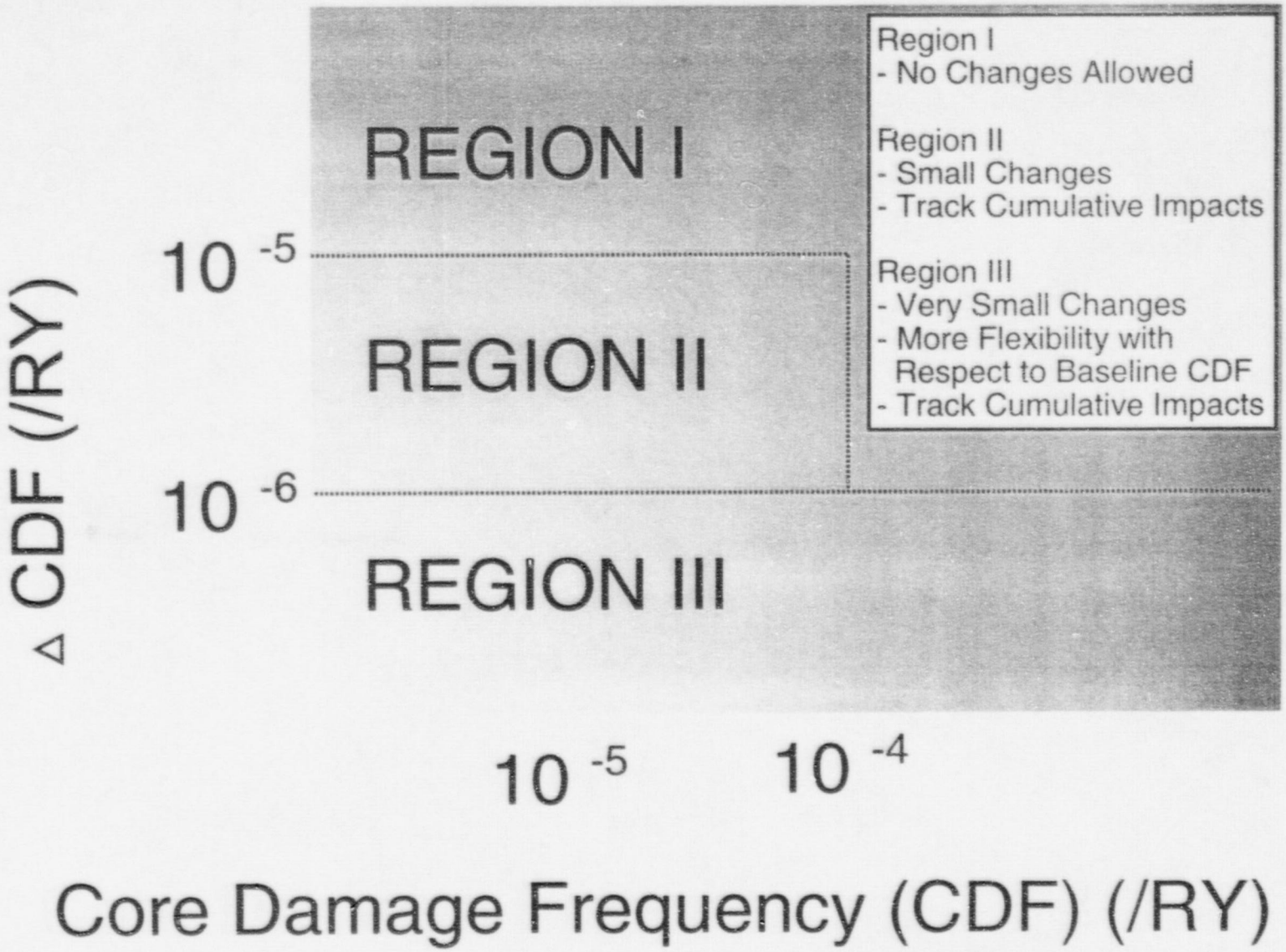
BACKGROUND
DEFENSE-IN-DEPTH PHILOSOPHY

- In Demonstrating that the Proposed Change Maintains the Defense-In-Depth Philosophy, it is a Staff Expectation that:
  - A Reasonable Balance Prevention of Core Damage, Prevention of Containment Failure, and Consequence Mitigation is Preserved;
  - Over-Reliance on Programmatic Activities to Compensate for Weaknesses in Plant Design is Avoided;
  - System Redundancy, Independence, and Diversity are Preserved Commensurate with the Expected Frequency and Consequences of Challenges to the System and Associated Uncertainties;
  - Defenses Against Potential Common Cause Failures are Preserved and the Potential for Introduction of new Common Cause Failure Mechanisms is Assessed;
  - Independence of Barriers is not Degraded;
  - Defenses Against Human Errors are Preserved; and
  - The Intent of General Design Criteria in 10 CFR Part 50, Appendix A is Maintained.

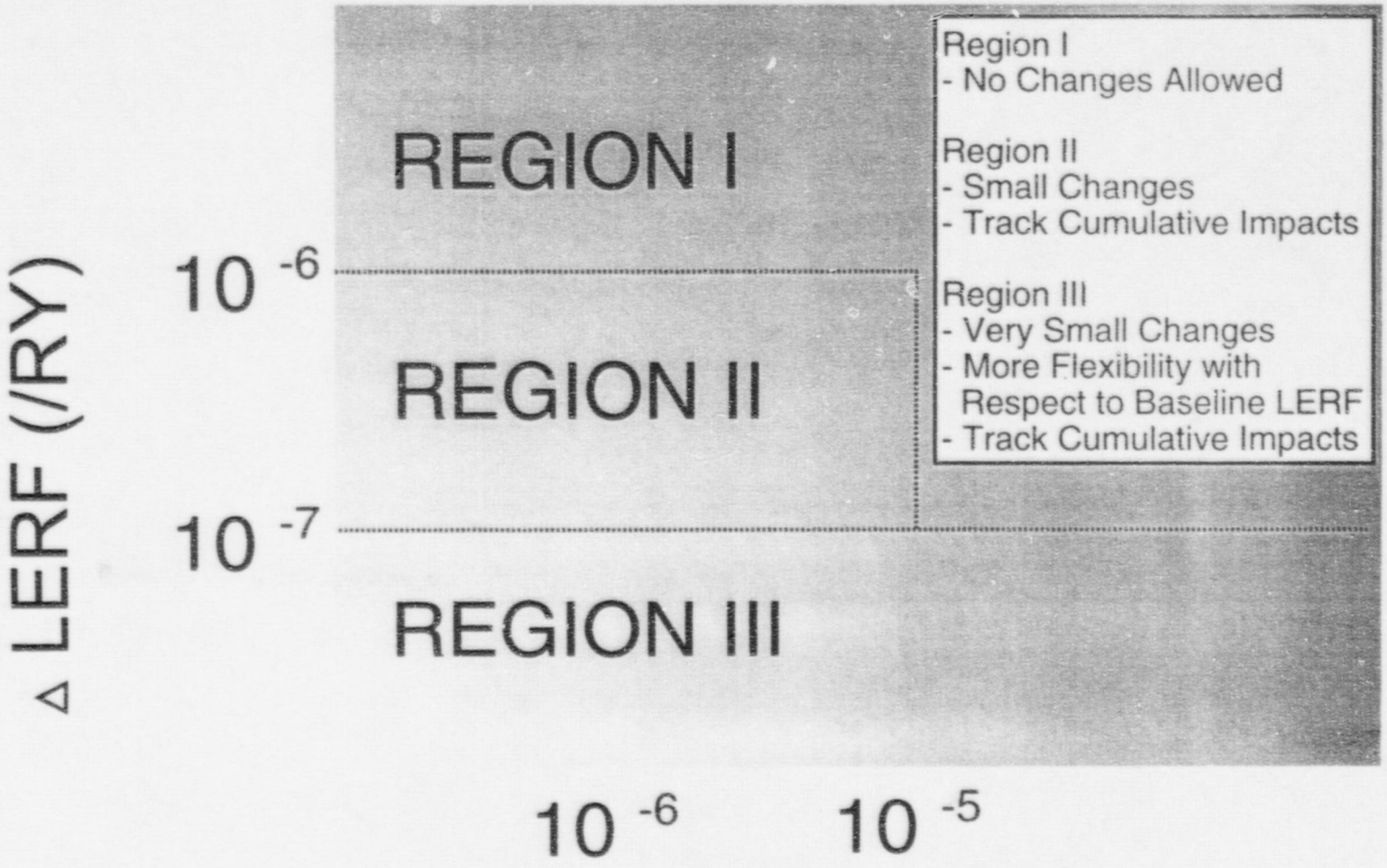
BACKGROUND
SUFFICIENT SAFETY MARGINS

- Sufficient Safety Margins are Maintained:
  - Engineering Codes and Standards or Alternatives Approved for Use by the NRC are Met; and
  - Safety Analysis Acceptance Criteria in the Current Licensing Basis (e.g., FSAR, Supporting Analyses) are Met, or Proposed Revisions Provide Sufficient Margin to Account for Analysis and Data Uncertainty.
- The Level of Justification Required for Changes in Margin Should Depend on:
  1. How Much Uncertainty is Associated with the Performance Parameter in Question,
  2. The Availability of Mechanisms to Compensate for Adverse Performance, and
  3. The Consequences of Functional Failure of the Affected Elements.

CDF ACCEPTANCE GUIDELINES



LERF ACCEPTANCE GUIDELINES



REVISION TO 10CFR 50.65
THE MAINTENANCE RULE

CONTACT:

RICHARD CORREIA, NRC/NRR/DIPM/IQMB, 415-1009, RPC@NRC.GOV

BACKGROUND

- SECY 97-055 (3/97) - described problems with rule language (...assessment "should" be taken into account...")

- SRM 97-055 (4/97) - staff to consider clarifying (a)(3) and provide examples of weak programs found during baseline inspections (MRBI)

- SECY 97-173 (8/97) - provided three options for (a)(3): (1) no changes; (2) change "should" to "shall" only; (3) comprehensive change

  - staff recommended option (2)

PROPOSED RULE CHANGE
ISSUED FOR PUBLIC COMMENT (SECY 98-165)

"Before performing maintenance activities on structures, systems or components within the scope of this section, (including but not limited to, surveillance testing, post-maintenance testing, corrective maintenance, performance/condition monitoring, and preventive maintenance), an assessment of the current plant configuration as well as expected changes to plant configuration that will result from the proposed maintenance activities shall be conducted to determine the overall effect on performance of safety functions. The results of this assessment shall be used to ensure that the plant is not placed in risk significant configurations or configurations that would degrade the performance of safety functions to an unacceptable level."

REASONS FOR RULE CHANGES

- Industry increasing amount and frequency of maintenance at power
- Inadequacies found with (a)(3) assessments during baseline inspections
- Technical specifications generally not intended to address removal of multiple equipment out-of-service simultaneously
- (a)(3) assessment is a recommendation, therefore is not enforceable

PUBLIC COMMENT CATEGORIES

- Terms need to be defined (e.g., "risk significant configuration")
- Assessments should only be required for SSCs that are *removed* from service
- (a)(4) requirement duplicates technical specification requirements (e.g., Configuration Risk Management Program - CRMP)
- (a)(4) assessments should not be required for non or low safety significant SSCs
- Regulatory Guide needs revision to include information on:
  - when assessments would not be required
  - type of assessments during shutdown conditions
  - documentation for assessments

STAFF RESPONSES TO PUBLIC COMMENTS

- (a)(4) language revised to clarify the use of assessments
- Assessments must be performed for all maintenance activities that could impact plant safety (e.g., transient initiators)
- Technical specifications were generally not intended to address multiple equipment out-of-service simultaneously
- Requests for deletion of Technical Specification Configuration Risk Management Program (CRMP) will be processed after 50.65(a)(4) becomes effective
- Combinations of out-of-service low safety significant SSCs must be evaluated for the impact on plant safety
- Regulatory Guide 1.160 revision to incorporate implementation guidance for (a)(4) assessments, including shutdown and documentation

REVISED (a)(4) PROVISION

(after addressing public comments - April 1999)

Before performing maintenance activities (including but not limited to surveillances, post-maintenance testing, and corrective and preventive maintenance) on structures, systems, or components within the scope of this section, the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities.

MODIFIED (a)(4) PROVISION
(Approved by the Commission June 18, 1999)

Before performing maintenance activities (including but not limited to surveillance, post-maintenance testing, corrective and preventive maintenance), the licensee shall assess and manage the increase in risk that may result from the proposed maintenance activities. The scope of the assessment may be limited to structures, systems or components that a risk-informed evaluation process has shown to be significant to public health and safety.

DRAFT REGULATORY GUIDE DG-1082

"ASSESSING AND MANAGING RISK BEFORE MAINTENANCE ACTIVITIES AT NUCLEAR POWER PLANTS"

Assessments for Maintenance Activities

- Review the current plant configuration and changes expected to the plant configuration from the proposed maintenance activities
- Assessment method commensurate with complexity of the maintenance configuration
- Make assessments scrutable and repeatable

ASSESSMENTS DURING POWER OPERATION

- Maintenance on a Single SSC

  - Qualitative assessment by a licensed operator trained in Maintenance Rule implementation

  - TS allowed outage time

  - Operator awareness of the SSC's risk significance

  - Awareness of potential impacts of external conditions

  - Re-evaluate risk impact due to emergent failures

ASSESSMENTS DURING POWER OPERATION (Continued)

- Maintenance on Two SSCs

  - Qualitative assessment by a licensed operator trained in Maintenance Rule implementation
  - TS allowed outage time
  - Operator awareness of the SSC's risk significance
  - Qualitative or quantitative assessment
  - Use pre-analyzed configurations (e.g., two-dimensional matrix)
  - Awareness of potential impacts of external conditions
  - Re-evaluate risk impact due to emergent failures
  - Expert panel or risk analyst evaluation of configurations beyond the capability of assessment tool

ASSESSMENTS DURING POWER OPERATION (Continued)

- **Maintenance on More Than Two SSCs**

  - PRA insights

  - Use previously assessed configurations when available

  - Expert panel or risk analyst evaluation of configurations beyond the capability of the assessment tool

  - Awareness of potential impacts of external conditions

  - Re-evaluate risk impact due to emergent failures

Methods commonly used to evaluate risk of maintenance configurations

- Technical Specifications and operator judgment

- Two-dimensional matrix of pre-analyzed configurations

- Pre-calculated set of configurations

- Risk monitor

ASSESSMENTS DURING SHUTDOWN CONDITIONS

- Quantitative assessment using shutdown PRA model when available

- Otherwise, qualitative assessment of degradation of key safety functions

  - Key safety functions are decay heat removal, reactor coolant inventory control, electrical power availability, reactivity control, and containment closure (primary and secondary)

RISK-SIGNIFICANT CONFIGURATIONS

- Concurrent equipment outages whose incremental contribution to annual risk is substantial, or would significantly affect the performance of safety functions
- Risk of maintenance activity depends on the configuration and its duration
- Risk metrics* are (1) increase in core damage probability (delta CDP), and/or (2) large early release probability (delta LERP)
- Configuration is risk significant when delta CDP (or LERP) exceeds a predetermined level allowed for a temporary condition

* Reference: Regulatory Guide 1.177, Section 2.4

PRA MODEL USED FOR ASSESSMENTS

- Should reflect the as-built and as-operated plant
- Should reflect actual plant performance
- Process to periodically evaluate and update PRA
  - Design modifications
  - Changes in operational practices
  - Changes in equipment reliability and unavailability

Assessment Scope (optional)

- SSCs modeled in PSA
- SSCs considered to be high safety-significant (HSS) by licensee's Expert Panel
- Low Safety Significant SSCs

  - Support systems
  - Systems with interdependencies

Assessment Scope (continued)

LSS SSCs (support and interdependent):

- **LSS support systems for HSS SSCs**
  (ECCS room HVAC; SBO DG; certain 480VAC load centers)

- **LSS SSCs w/interdependencies w/other LSS SSCs**
  (Instrument and service air)

- **LSS SSC failure could increase the likelihood of an initiating event**
  (Turbine-Gen. Aux. Systems; EHC; stator water cooling; lube oil)

- **LSS SSCs in low frequency cutset(s) that increase CDF (or LERF) significantly when multiple SSCs are out of service**
  (Instrument and service air)

EXAMPLES OF LSS SSCS NOT MODELED IN PSA THAT MIGHT BE EXCLUDED FROM SCOPE OF ASSESSMENTS:

- Emergency DC Lighting
- Communication systems
- PASS Hydrogen Concentration Monitoring
- PASS Water Level Indication
- Annunciators
- Post Accident Hydrogen System
- Gaseous Waste Processing System

MANAGING RISK

- Scrutable process to identify, assess, and control risk of maintenance activities

- If a proposed configuration exceeds risk-acceptance guidelines, a licensee should implement prudent actions:

  - Senior plant management involvement prior to entering configuration
  - Minimize duration of the maintenance activity by preplanning and pre-staging necessary equipment
  - Compensatory actions and contingency plans implemented
  - Site personnel at a heightened state of risk awareness

INTERACTIONS WITH STAKEHOLDERS

- REVISIONS TO SECTION 11 TO NUMARC 93-01
- TWO PUBLIC MEETING TO DISCUSS CHANGES
- AREAS UNDER DISCUSSION:
  - SCOPING CRITERIA
  - RISK METRICS
  - RISK SIGNIFICANCE OF SSCs FROM FIRES
- REVISIONS UNDERWAY..SUBMITTAL TO NRC & INDUSTRY BY 7/23/9
- SUBMITTAL TO NRC FOR ENDORSEMENT BY 8/31/99
- MAINTENANCE RULE WORKSHOP 9/13-14/99

Rule in effect' 120-days

FIRE PROTECTION RISK SIGNIFICANCE SCREENING METHODOLOGY

Probabilistic Safety Assessment Branch
&
Plant Systems Branch

Office of Nuclear Reactor Regulation, NRC

(*Presented at Region IV PRA Workshop; July 20,1999*)

OBJECTIVES

- Focuses resources on monitoring performance and effectiveness of fire protection mitigation features important to risk

- Provides a two-phase method for characterizing the risk significance of inspection findings - screens out findings with minimal or no risk significance

- Fits into plant oversight assessment process, thus recommending a regulatory response due to the potential risk significance of fire protection inspection findings

OVERVIEW

Phase 1

- Screen out individual inspection findings not affecting DID
- Primary user is resident inspector
- Does not require fire protection DID to be evaluated fully for fire area

Phase 2

- To be entered if finding(s) do not screen in Phase 1, OR during fire protection triennial inspection
- Primary user is Region
- Evaluate DID fully for fire area to assess ΔCDF.

PHASE 1

Two-Step Process for Phase 1 Screening

- Step 1: Impact on function of DID, relationship to AOT
- Step 2: SSD for the fire area, fire protection scheme
  - All equipment and cables in fire area are assumed failed
  - If DID principle not evaluated, it is assumed to have a low degradation

PHASE 2

- Is Conservative. If a fire scenario can be developed, then
  - All equipment and cables in room where fire initiates is failed. The barrier is challenged, and if failed, all equipment and cables in adjacent room are failed too.
  - Characterization of DID degradation due to inspection findings is conservative.
- Is Qualitative
  - Degradations in DID are categorized as High, Medium, or Low

PHASE 2 (cont.)

- Views inspection findings collectively
  - Synergistic impact on risk of a fire area
- Feeds into "Inspection Finding Risk Characterization Process" (SECY-99-007A, attachment 2)
  - Fire mitigation frequency (IF, AS, MS, FB) integrated with SSD mitigation capability from SDP tool to approximate Δ CDF
  - Therefore, produces risk significance categories which are consistent with regulatory response thresholds used in NRC licensee performance assessment process.

UNDERLYING QUANTITATIVE FOUNDATION

- Failure probabilities developed for qualitative degradations in DID
- Product of ignition frequency and failure probabilities for DID produces CDF
- Dependencies between auto-suppression and manual suppression modeled
  - Since auto-suppression only controls fire, credit for auto-suppression adjusted with fire brigade high degradation
  - Common mode failures of water based auto-suppression and fire brigade included

FAILURE PROBABILITIES FOR DID

(excluding SSD)

Level of Degradation	3 Hour Barrier	1 Hour Barrier	Auto-Suppress	Fire Brigade	
				non-CR	CR
High	0	0	0	-0.25	-0.5
Medium	-1	-0.5	-0.75	-0.5	-1
Low	-2 (door)	-1	-1.5	-1	-1.5

ADJUSTMENTS DUE TO DEPENDENCIES

Auto-Suppression Degradation	Fire Brigade Degradation	Adjustment
Medium	High	+0.75
Low	High	+0.50
Low (Sprinklers only)	Low	+0.25

Fire Protection Risk Significance Screening Methodology

Example of its Application

TRANSFORMER VAULT ROOM

Room Protection - 3-Hour Rated Room (doors/dampers/penetration seals)

Startup and Unit Auxiliary Transformers Housed in the Room

Redundant Post-Fire Safe Shutdown Located in the Room

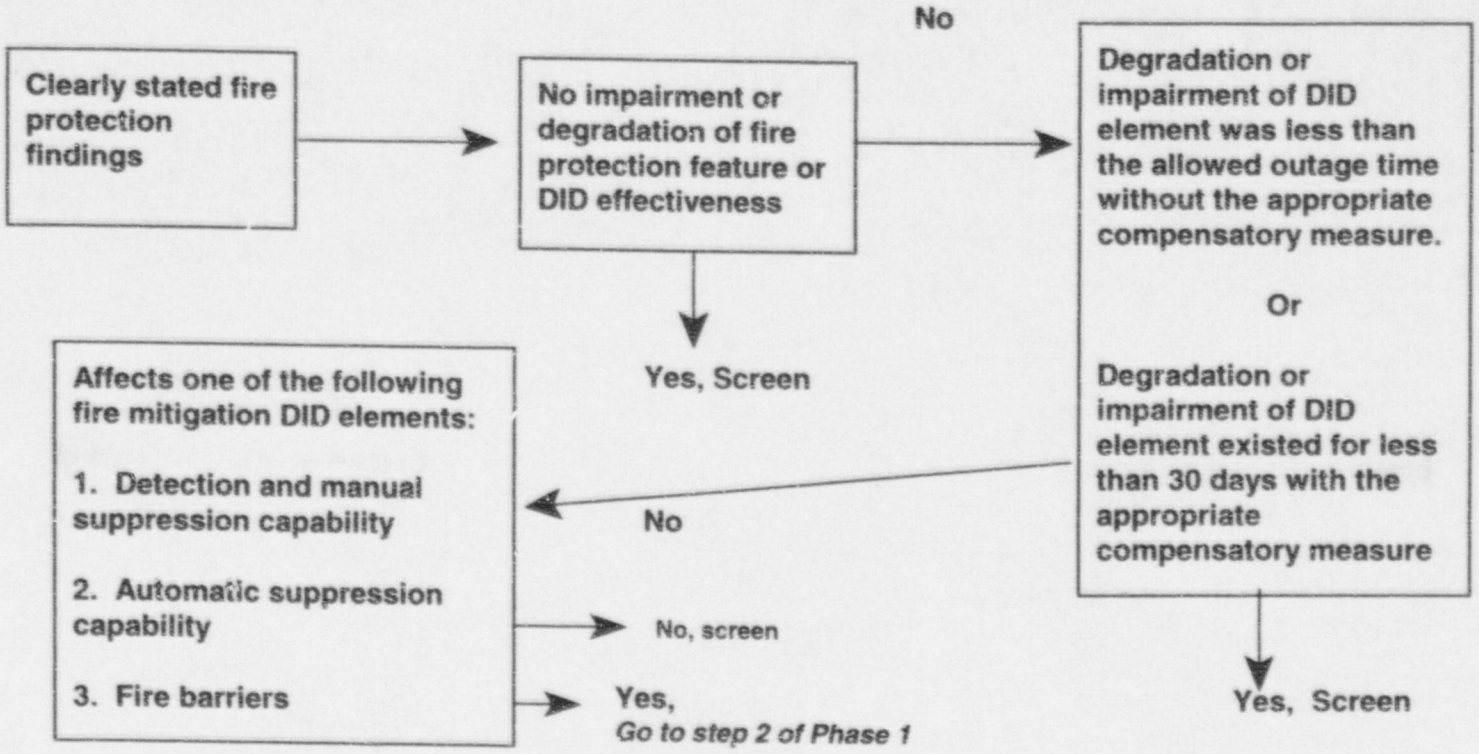
- **SW Pumps (power and control cables)**
- **CCW Pumps (power and control cables)**
- **125 Vdc Power Distribution Cables**

Fire Protection

- **Oil Containment Curb Around Transformers**
- **Automatic Water Spray System Actuated by Cross Zone Fire Detection Provided For Transformers**
- **1-Hour Fire barrier Provided for One Train of Post Fire Safe Shutdown Functions**

Screening Process Phase 1 (Step 1) Figure 4-1

For a given fire area, zone, or room under consideration



Step 2 of Phase 1

SSD system with redundancy is located in the area, zone, or room of concern. Remaining mitigation capability is a system with redundancy which is physically independent of the fire area, zone, or room of concern and is manually actuated under time constraints.

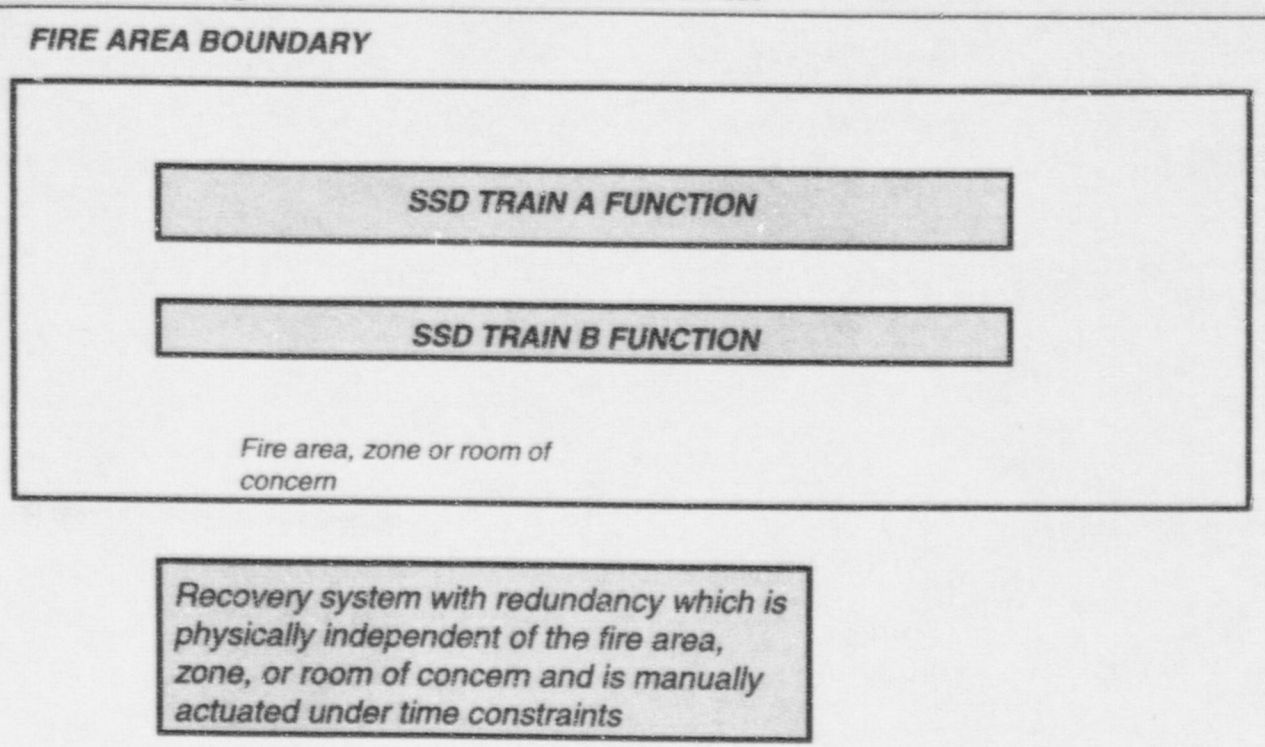


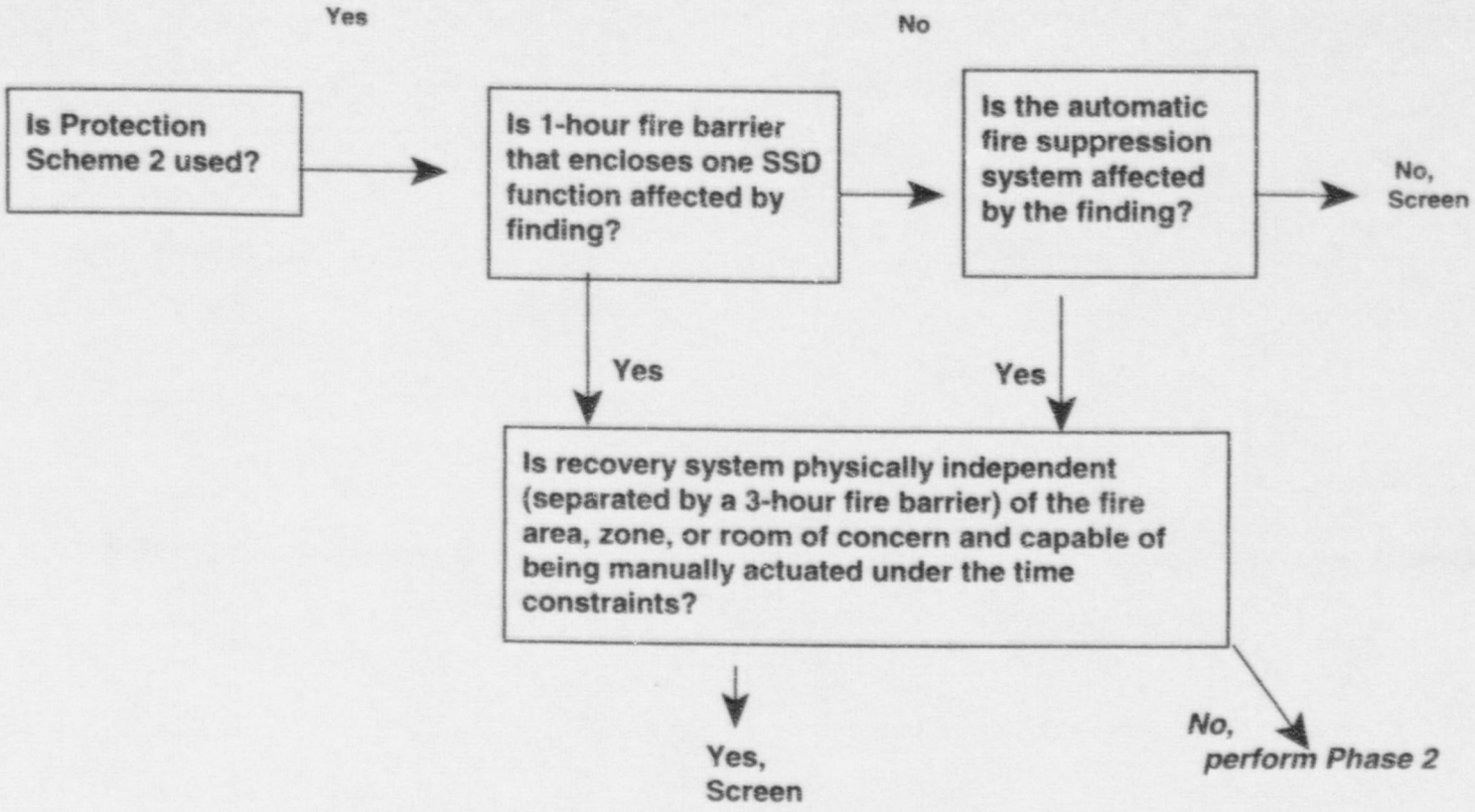
Figure 4-4

Fire Protection Schemes (Appendix R of 10 CFR Part 50, Section III.G.2)

Scheme 1 **Provide a 3-hour fire barrier separation which either encloses one SSD train or provides wall to wall and floor to floor separation between the redundant trains; or**

Scheme 2 **Provide a 1-hour fire barrier enclosing one of the SSD trains. The area shall be protected by automatic fire detection and suppression; or**

Scheme 3 **Provide greater than 20 feet of horizontal separation between the redundant SSD trains. The spacial separation between the two trains shall be free of intervening combustibles. The area shall be protected by automatic fire detection and suppression.**


Yes
No
Is Protection Scheme 2 used?
Is 1-hour fire barrier that encloses one SSD function affected by finding?
Is the automatic fire suppression system affected by the finding?
No, Screen
Yes
Yes
Is recovery system physically independent (separated by a 3-hour fire barrier) of the fire area, zone, or room of concern and capable of being manually actuated under the time constraints?
Yes, Screen
No, perform Phase 2

FPRSSM - Phase 2

Methodology Steps

- Grouping of findings
- Define fire scenario
- Qualitative evaluation of findings
- Assignment of quantitative values
- Determination of fire ignition frequency
- Integrated assessment of DID findings and fire ignition frequency
- Integration of adjusted Fire Mitigation Factor (FMF) with safe shutdown
- General rules for applying FPRSSM

INSPECTION FINDINGS (Step 1) (Example 1)

WATER SPRAY SYSTEM

- Re-assembly after startup transformer modificaticns Relocate spray nozzles so that thy were not aimed at the hazard
- Masking tape from prior system painting found covering the orifice openings on some nozzles
- 3 of 6 rate compensated fire detectors on the startup transformer had their outer shell (metal tube) dented. The tubes had through wall cracks (possibly affecting the outer shell's expansion coefficient)

ELECTRICAL RACEWAY FIRE BARRIER SYSTEM

- 1-hour Fire Barrier Conduit Protection on Sw Cables Has Through Barrier Opening

MANUAL FIRE FIGHTING EQUIPMENT

- No Apparent Problems with the Hose Station Equipment or Extinguishers

FIRE BRIGADE DRILL OBSERVATIONS

- No radio communications (used cell phones - phones did not work)
- Hose deployment problems, hose not long enough to reach the fire
- Turnout protective clothing not properly protecting personnel
- Use of personal protective equipment not adequate (didn't use SCBA, clothing not donned properly)
- Fire attack techniques were not proper, pre-fire plans did not have a smoke control plan
- Did not bring proper equipment

POSTULATED FIRE SCENARIO (Step 2)

Fire Likelihood Not Assessed

Define a Fire Condition in the Room That Is Capable of Developing a Hot Gas Layer or a Direct Exposure to Critical Systems, Equipment, or Components (Significant Fire)

A Possible Fire Condition

- **Fault offsite cause a fault and failure of the startup transformer**
- **Transformer housing fails and releases burning oil**

Post-fire Safe Shutdown - Possible Impact

- **Loss of off site power (due to loss of switchyard)**
- **Loss of Service Water to the EDGs and CCW**

EXAMPLE 1

- **FB (1 hour) = High, AD/AS = High, D/MS = High** (Steps 3 and 4)
- **IF > 1E-3/yr** (Step 5)
- **Fire Mitigation Factor (FMF) = IF+ FB + MS +AS+CC (when appropriate)**

  Where **IF = Fire Ignition Frequency**
  FB = Fire Barrier
  MS = Manual Suppression/Detection
  AS = Automatic Suppression/Detection
  CC = Dependencies/Common Cause Contribution

- **FMF = IF + FB + AD/AS + D/MS** (Step 6)
  -2 + 0 + 0 + -0.25 = -2.25
- **$-2 \geq FMF > -3$ (1 per 10^2 to 10^3)**
- **Condition greater than 30 days (estimated likelihood rating C)**
- **Risk significance estimation = RED** (Step 7)

Table 5.6 Association of FMF to Table 5.7 (SDP Table 1) approximate frequencies for Calculation of Delta CDF	
Fire Mitigation Frequency (FMF)	**Table 5.7 - Approximate Frequencies**
FMF > -2	**1 per 10 to 10^2**
-2 ≥ FMF >-3	**1 per 10^2 to 10^3**
-3 ≥ FMF >-4	**1 per 10^3 to 10^4**
-4 ≥ FMF >-5	**1 per 10^4 to 10^5**
-5 ≥ FMF >-6	**1 per 10^5 to 10^6**
FMF ≤ -6	**Less than 10^6**

Table 5.7 (Same as SDP Table 1)
Estimated Likelihood Rating for Initiating Event Occurrence During Degraded Period (taken from NUREG/CR-5499)

Approx. Freq.	Example Event Type	Estimated Likelihood Rating		
>1 per 1 - 10 yr	Reactor Trip Loss of condenser	A	B	C
1 per 10 - 10^2 yr	Loss of Offsite Power Total loss of main FW Stuck open SRV (BWR) MSLB (outside cntmt) Loss of 1 SR AC bus Loss of Instr/Cntrl Air Fire causing reactor trip	B	C	D
1 per 10^2 - 10^3 yr	SGTR Stuck open PORV/SV RCP seal LOCA (PWR) MFLB MSLB inside PWR cntmt Loss of 1 SR DC bus Flood causing reactor trip	C	D	E
1 per 10^3 - 10^4 yr	Small LOCA Loss of all service water	D	E	F
1 per 10^4 - 10^5 yr	Med LOCA Large LOCA (BWR)	E	F	G
1 per 10^5 -10^6 yr	Large LOCA (PWR) ISLOCA Vessel Rupture	F	G	H
<1 per 10^6yr		G	H	H
		> 30 days	30-3days	<3 days
		Exposure Time for Degraded Condition		

Table 5.8 (Same as SDP Table 2) - Risk Significance Estimation Matrix

Initiating Event Likelihood (From Step 2.2 of SDP)	Remaining Mitigation Capability (From Step 2.3 of SDP)						
	≥3 diverse trains OR 2 systems each with redundancy (1)	1 train + 1 system with redundancy OR 2 diverse trains + recovery of failed train (2)	2 diverse trains OR 1 system with redundancy + recovery of failed train (3)	1 train + recovery of failed train OR 1 system with redundancy (automatic initiation or no time constraints) (4)	1 train OR 1 system with redundancy (manual actuation under time constraints) (5)	Recovery of failed train (6)	none (7)
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

INSPECTION FINDINGS (Example 2)

No Apparent Problems with the Water Spray System

1-hour Fire Barrier Protecting Post Fire Safe Shutdown Functions had mechanical damage that reduced the barrier's wall thickness by 30%

No Apparent Probiems With the Hose Station Equipment or Extinguishers

Fire Brigade (effectiveness and efficiency) Drill Observations

- Poor radio communications (Radios did not work properly)
- Hose deployment problems
- Turnout protective clothing not properly protecting personnel
- Minor fire attack techniques problems

EXAMPLE 2

- **FB (1 hour) = Medium, AD/AS = Low, D/MS = Medium** (Steps 3 and 4)
- **IF > 1E-3/yr** (Step 5)
- **FMF = IF + FB + AD/AS + D/MS** (Step 6)
  -2 + -0.5 + -1.5 + -0.5 = -4.5
- **$-4 \geq$ FMF > -5 (1 per 10^4 to 10^5)**
- **Condition greater than 30 days (estimated likelihood rating E)**
- **Risk significance estimation = WHITE** (Step 7)

INSPECTION FINDINGS (Example 3)

No Apparent Problems with the Water Spray System

No Apparent Problems with the Fire Barrier Systems Protecting Safe Shutdown Functions

No Apparent Problems With the Hose Station Equipment or Extinguishers

Fire Brigade (effectiveness and efficiency) Drill Observations

- **Poor radio communications (Radios did not work properly)**
- **Hose deployment problems**
- **Turnout protective clothing not properly protecting personnel**
- **Minor fire attack techniques problems**

EXAMPLE 3

- **FB (1 hour) = Low, AD/AS = Low, D/MS = Medium** (Steps 3 and 4)
- **IF > 1E-3/yr** (Step 5)
- **FMF = IF + FB + AD/AS + D/MS** (Step 6)
  -2 + -1 + -1.5 + -0.5 = -5.0
- **$-5 \geq$ FMF > -6 (1 per 10^5 to 10^6)**
- **Condition greater than 30 days (estimated likelihood rating F)**
- **Risk significance estimation = GREEN** (Step 7)

SUMMARY

Example 1

- **FB (1 hour)= High, AD/AS = High, D/MS = High**
- Potential Risk Significance (with recovery of a train) = **Red**
  (without recovery of a train) = **Red**

Example 2

- **FB (1 hour) = Medium, AD/AS = Low, D/MS = Medium**
- Potential Risk Significance (with recovery of a train) = **White**
  (without recovery of a train) = **Yellow**

Example 3

- **FB (1 hour) = Low, AD/AS = Low, D/MS = Medium**
- Potential Risk Significance (with recovery of a train)= **Green**
  (without recovery of a train) = **White**

Risk-informed Changes to the Inspection Program and Assessment Process Improvements

Peter Wilson

Office of Nuclear Reactor Regulation

Nuclear Regulatory Commission

Washington, D.C.

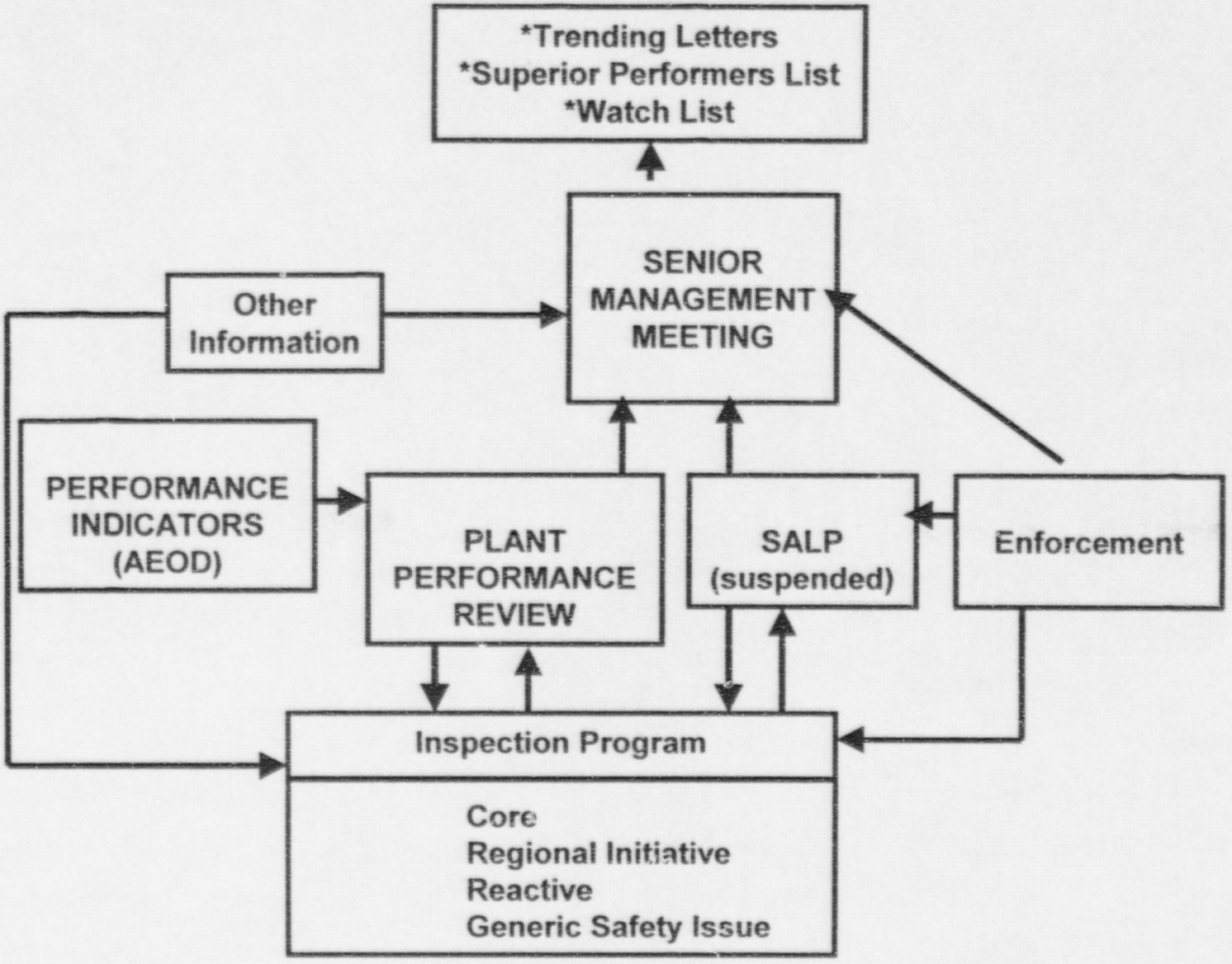
Forces Influencing Transition

* Maturing industry
* Maturing technology
* Improved plant performance
* Improved regulatory tools
* Environmental Factors:

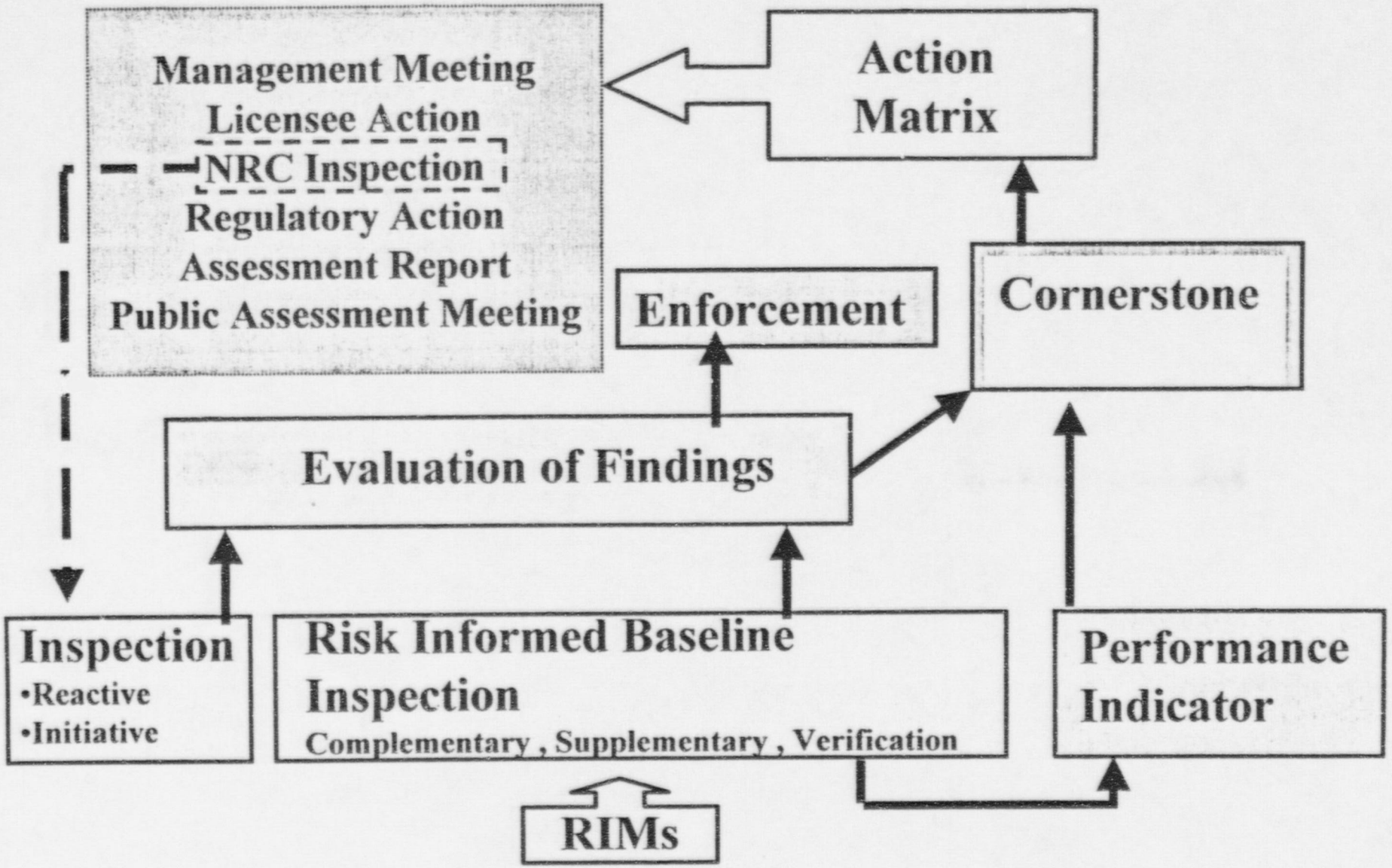
  deregulation, stakeholder input
* Internal Factors:

  reduced resources, improved internal processes

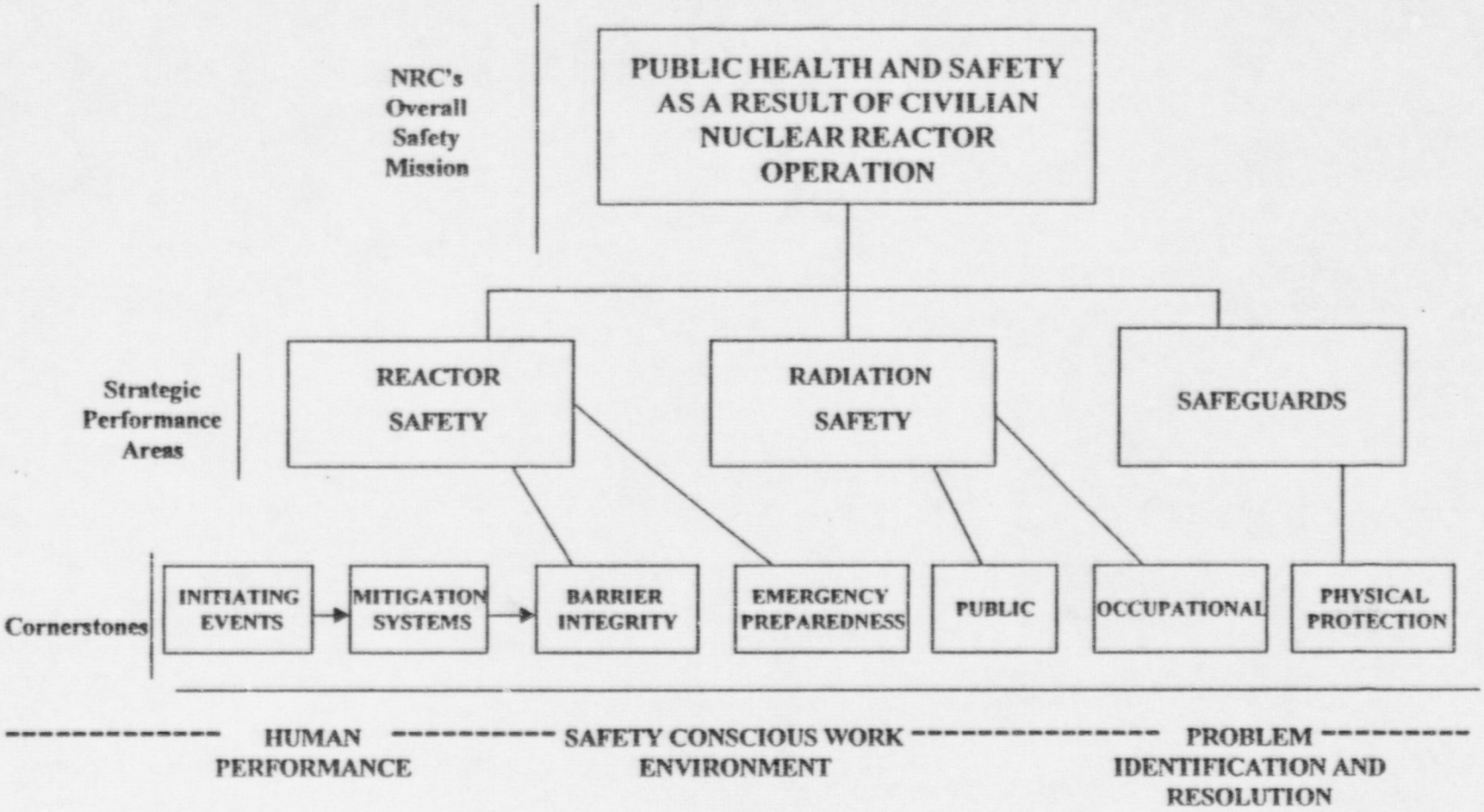
CURRENT OVERSIGHT PROCESS



Plant Oversight Process



REGULATORY FRAMEWORK



- PERFORMANCE INDICATOR
- INSPECTION
- OTHER INFORMATION SOURCES
- DECISION THRESHOLDS

Key Oversight Principles

* Maintain Risk-informed baseline inspection program
* Safety Cornerstones and Performance Indicators established
* Risk-informed Thresholds establish NRC response
* Assessment include PI's and Inspections
* Enforcement based upon regulations

PERFORMANCE INDICATORS					
Cornerstone	**Indicator**		**Thresholds**		
			Increased Regulatory Response Band	**Required Regulatory Response Band**	**Unacceptable Performance Band**
Initiating Events	Unplanned Scrams per 7000 Critical Hours (automatic and manual scrams during the previous four quarters)		>3.0	>6.0	>25.0
	Scrams with a Loss of Normal Heat Removal (over the previous 12 quarters)		>4.0	>10.0	>20.0
	Unplanned Power Changes per 7000 Critical Hours (over previous four quarters)		>8.0	N/A	N/A
Mitigating Systems	Safety System Unavailability (SSU) (average of previous 12 quarters)	**All Plants**			
		Emergency Power	>3.8%	>5.0%	>10.0%
		>2EDG	>3.8%	>10.0%	>20.0%
		BWRs			
		HPCI	>4.0%	>12.0%	>50.0%
		HPCS	>1.5%	>4.0%	>20.0%
		RCIC	>4.0%	>12.0%	>50.0%
		RHR	>2.0%	>5.0%	>10.0%
		PWRs			
		HPSI	>2.0%	>5.0%	>10.0%
		AFW	>2.0%	>6.0%	>12.0%
		RHR	>2.0%	>5.0%	>10.0%
	Safety System Functional Failures (over previous four quarters)		>5.0	N/A	N/A

EVALUATING LICENSEE PERFORMANCE INDICATORS: CONCEPTUAL MODEL

GREEN

Licensee Response Band

Cornerstone objectives fully met. Nominal risk with normal deviation from expected performance.

WHITE

Increased Regulatory Response Band

Cornerstone objectives met with *minimal* reduction in safety margin.

Changes in performance consistent with $\Delta CDF < E\text{-}5$ ($\Delta LERF < E\text{-}6$)

YELLOW

Required Regulatory Response Band

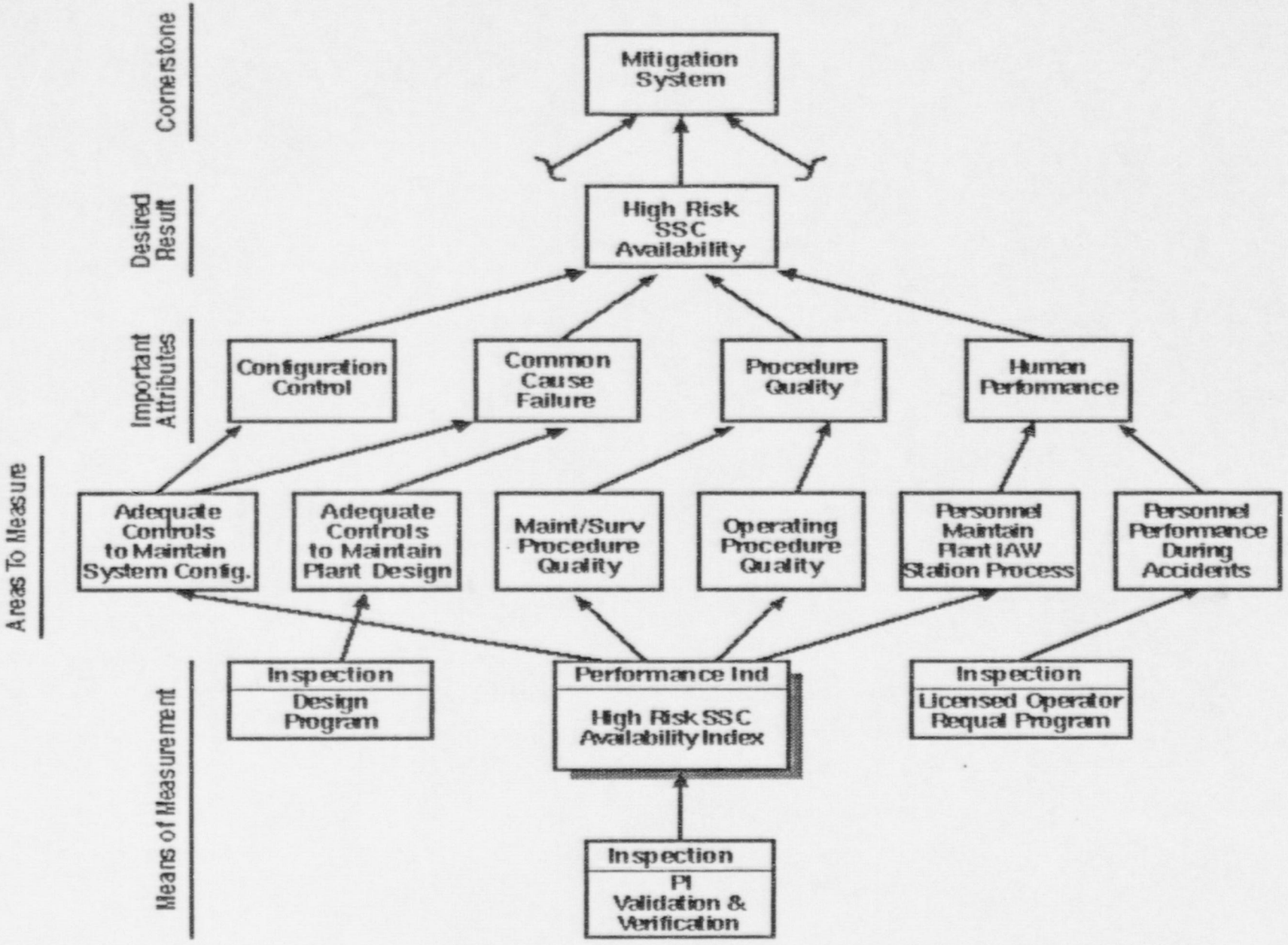
Cornerstone objectives met with *significant* reduction in safety margin.

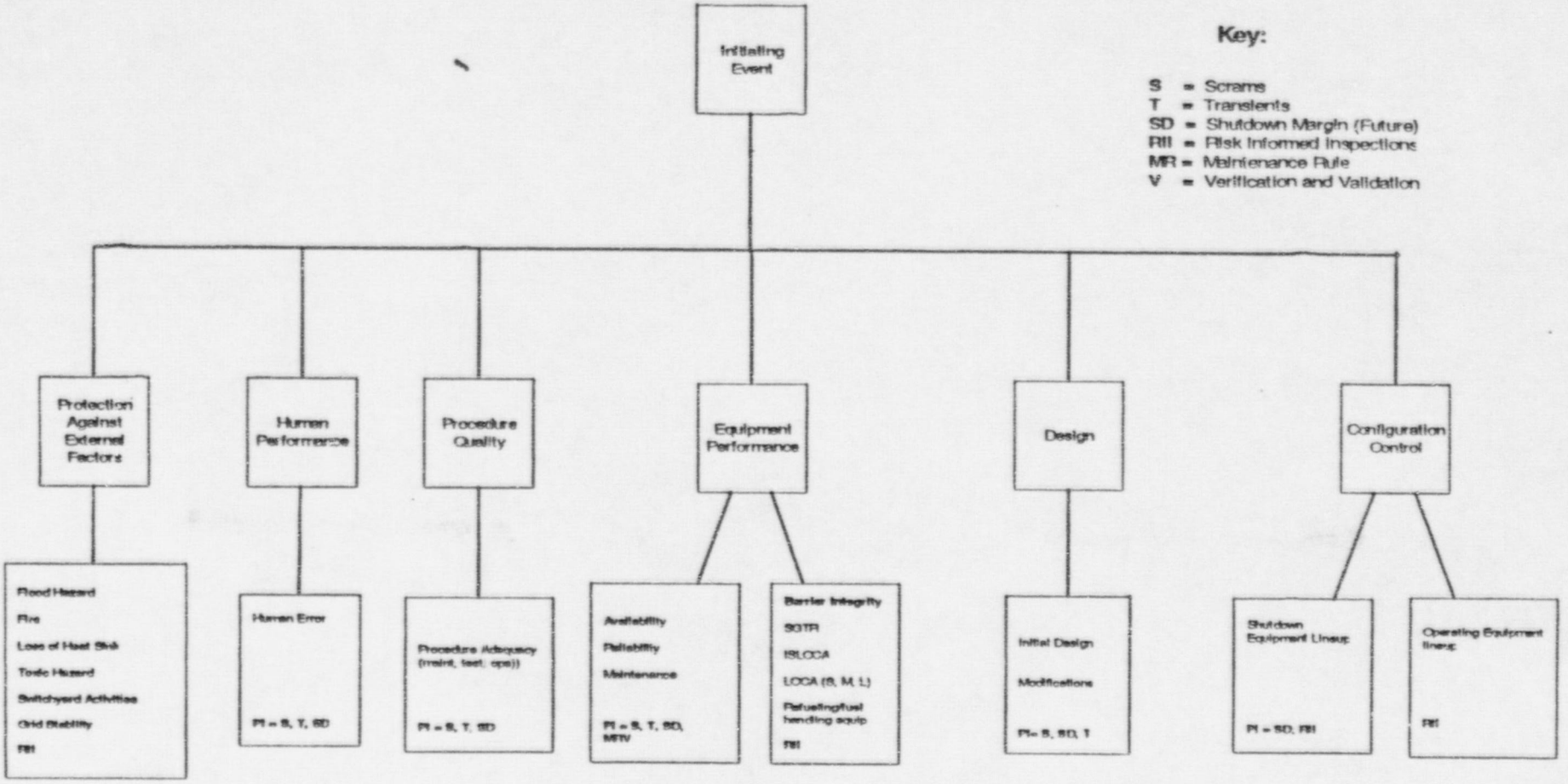
Changes in performance consistent with $\Delta CDF < E\text{-}4$ ($\Delta LERF < E\text{-}5$)

RED

Plants not permitted to operate within this Band

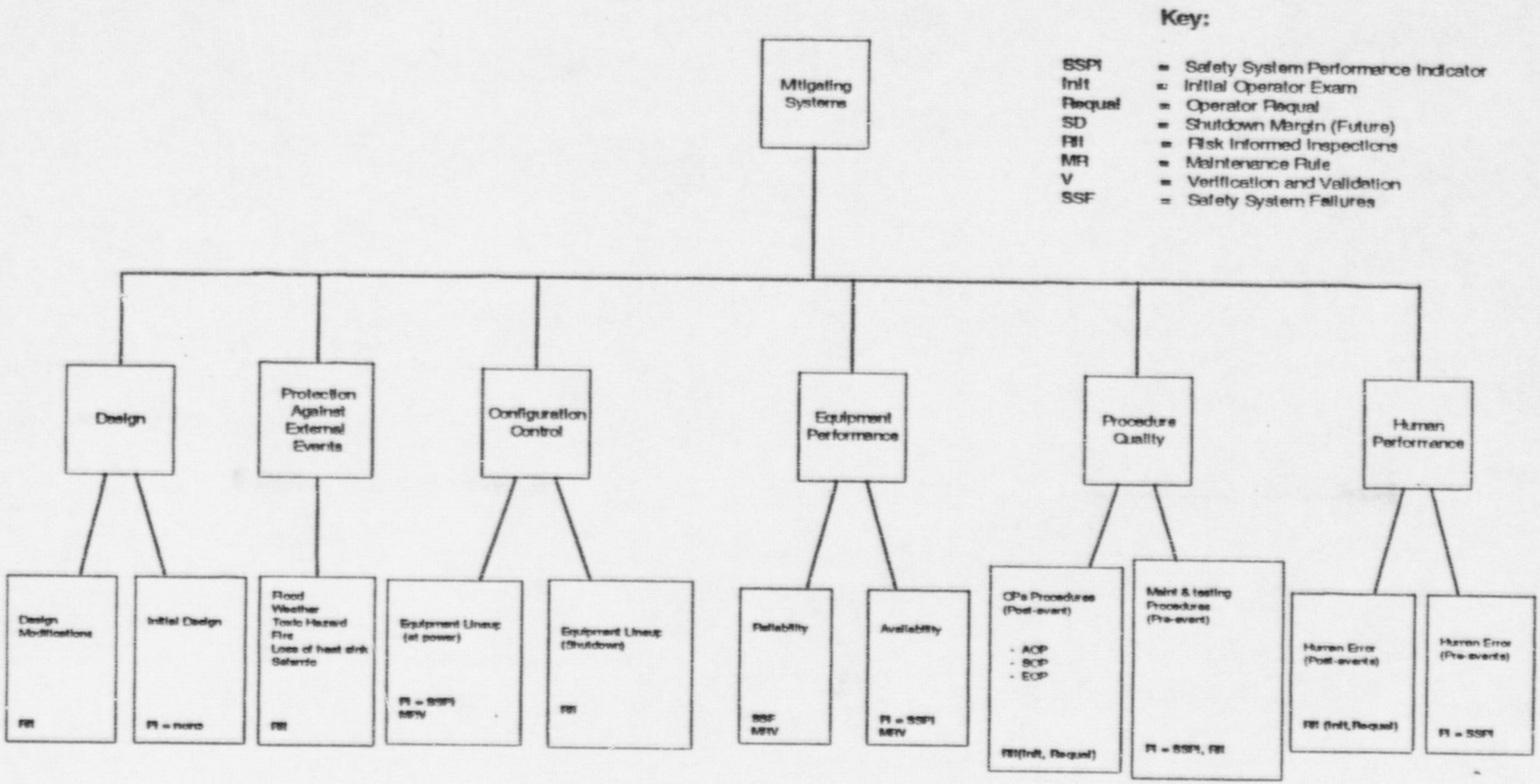
Plant performance significantly outside design basis. Loss of confidence in ability of plant to provide assurance of public health and safety with continued operation. Unacceptable margin of safety.


Cornerstone
Desired Result
Important Attributes
Areas To Measure
Means of Measurement
Mitigation System
High Risk SSC Availability
Configuration Control
Common Cause Failure
Procedure Quality
Human Performance
Adequate Controls to Maintain System Config.
Adequate Controls to Maintain Plant Design
Maint/Surv Procedure Quality
Operating Procedure Quality
Personnel Maintain Plant IAW Station Process
Personnel Performance During Accidents
Inspection
Design Program
Performance Ind
High Risk SSC Availability Index
Inspection
Licensed Operator Requal Program
Inspection
PI Validation & Verification



December 2, 1998

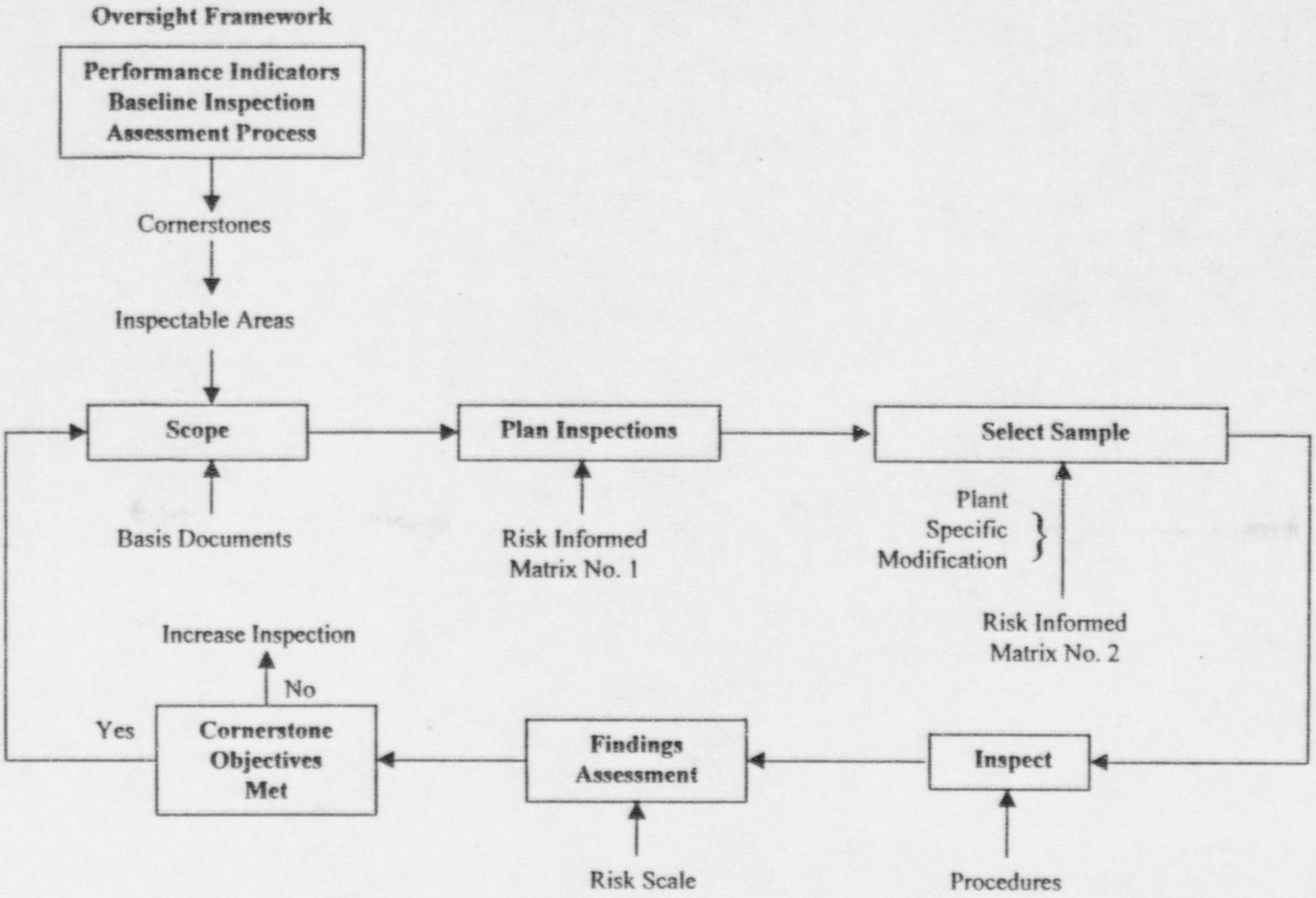
jdfiota.cdr



December 2, 1998

jdfig3a.cdl

RISK INFORMED BASELINE INSPECTION PROGRAM



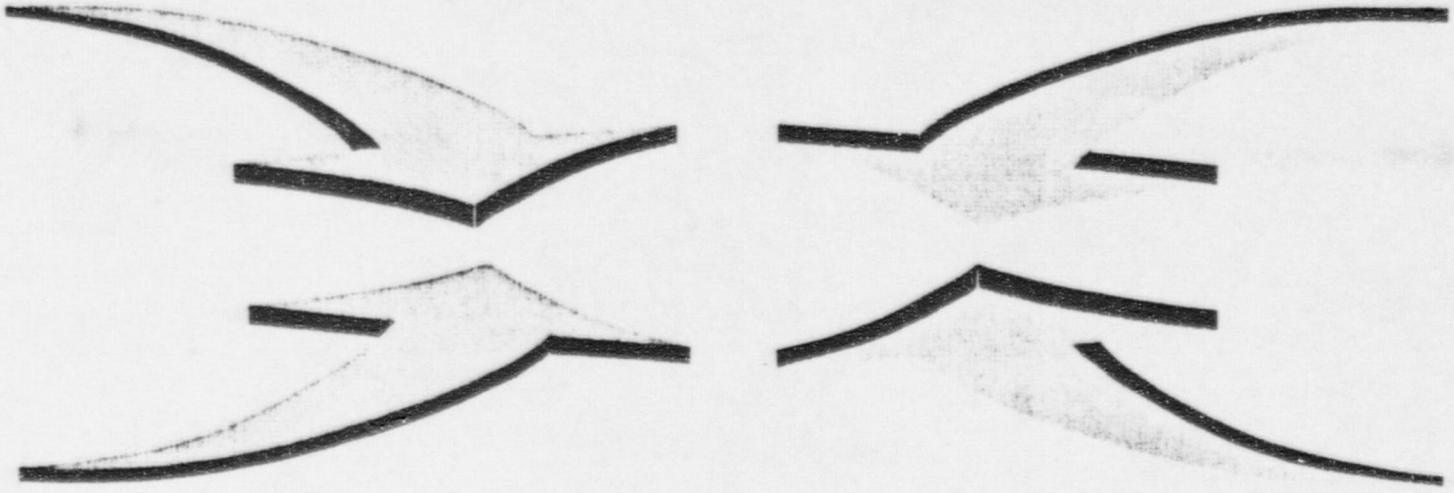
INSPECTION PROGRAM TRANSITION

From:

Diagnostic Emphasis

To:

Indicative Emphasis



NRR

Industry

Inspectable-Area Procedures Have Been Developed for These Areas

Number	Title
71111- 01	Adverse Weather Preparations
71111- 02	Changes to License Conditions and Safety Analysis Report
71111- 03	Emergent Work
71111- 04	Equipment Alignment
71111- 05	Fire Protection
71111- 06	Flood Protection Measures
71111- 07	Heat Sink Performance
71111- 08	Inservice Inspection Activities
71111- 09	Inservice Testing of Pumps and Valves
71111- 10	Large Containment Isolation Valve Leak Rate & Status Verification
71111- 11	Licensed Operator Requalification

Inspectable-Area Procedures Have Been Developed for These Areas

Continued

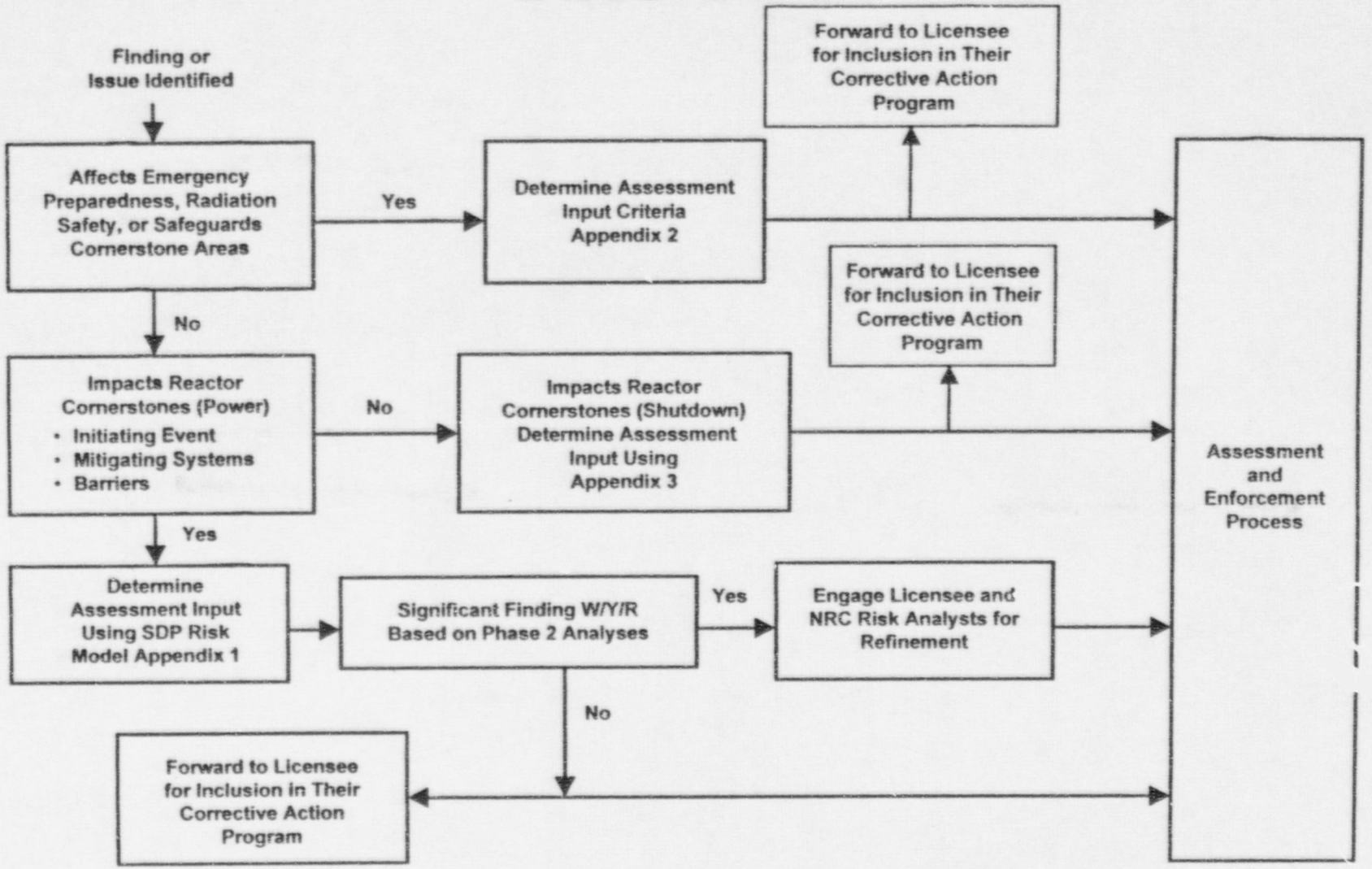
Number	Title
71111-12	Maintenance Rule Implementation
71111-13	Maintenance Work Prioritization & Control
71111-14	Nonroutine Evolutions
71111-15	Operability Evaluations
71111-16	Operator Workarounds
71111-17	Permanent Plant Modifications
71111-19	Post Maintenance Testing
71111-20	Refueling and Outage Activities
71111-21	Safety System Design and Performance Capability
71111-22	Surveillance Testing
71111-23	Temporary Plant Modifications

Significance Determination Process

The Why, for Whom, and Its Bases

- Needed to Align Inspection Finding to PIs for Plant Assessment
- Intended for Use by Field Inspectors
- Used Old Enforcement Criteria as Bases whenever Possiable for the Non-Reactor Cornerstone Areas
- For the Reactor Area, Risk values (Colors) Based on ReGuide 1.174, Screening Criteria Based on ASP Criteria, Initiating Event Frequency Based on NUREG -5499, and Typical PRA Equipment and Human Performance Reliability were Used

SIGNIFICANCE DETERMINATION PROCESS



The Reactor Safety Procedure Includes All Inspectable Areas Under the I, M, & B Cornerstones

I: Initiating Events

M: Mitigating Systems

B: Barrier Integrity

SIGNIFICANCE DETERMINATION PROCESS
INITATING EVENT, MITIGATING SYSTEMS & BARRIER CORNERSTONES AT_POWER

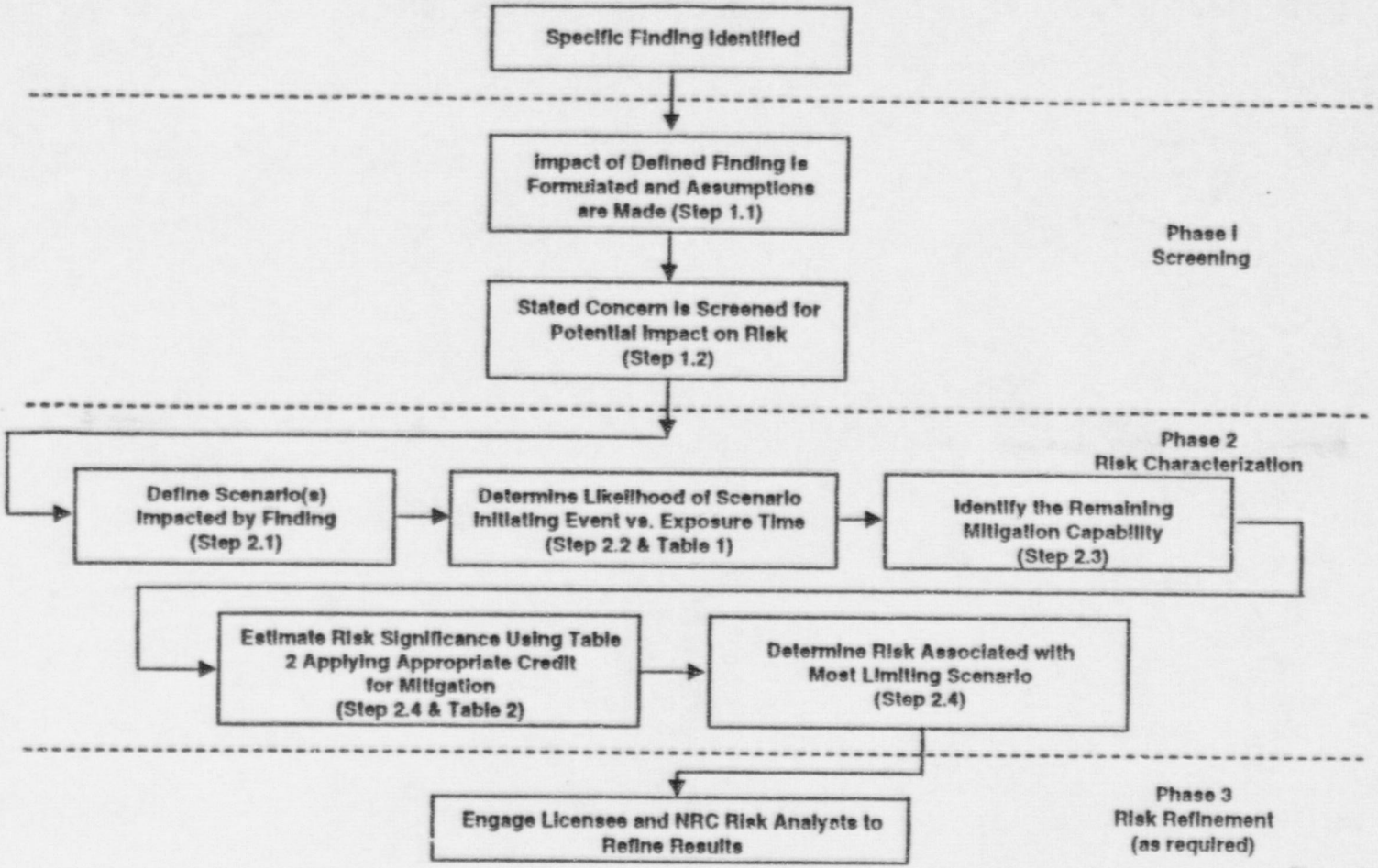
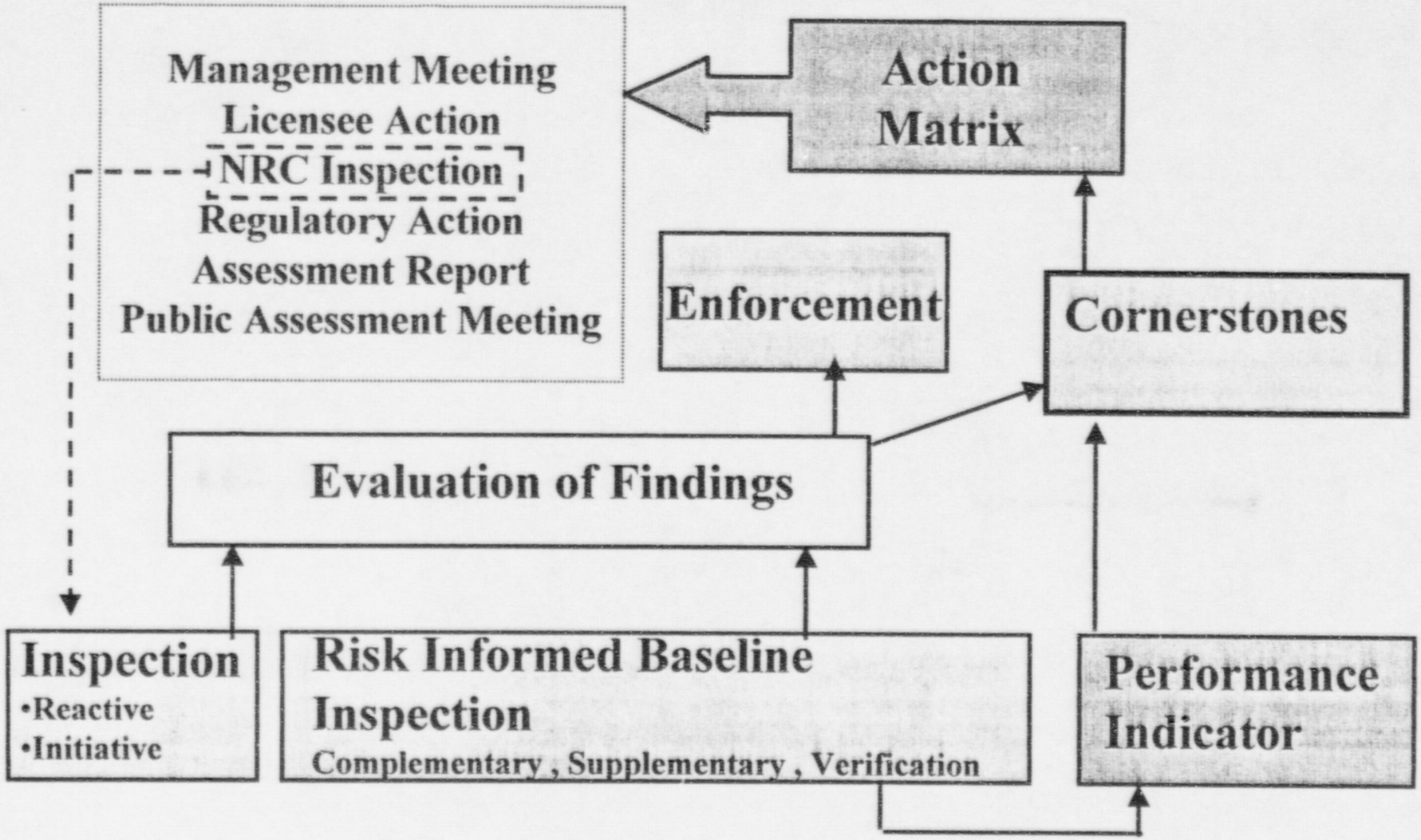


Figure 1

ACTION MATRIX

		LICENSEE PERFORMANCE INCREASING SAFETY SIGNIFICANCE --------->				
RESULTS		All Assessment Inputs (Performance Indicators (PIs) and Inspection Findings) Green; Cornerstone Objectives Fully Met	One or Two White Inputs (in different cornerstones) in a Strategic Performance Area; Cornerstone Objectives Fully Met	One Degraded Cornerstone (2 White Inputs or 1 Yellow Input) or any 3 White Inputs in a Strategic Performance Area; Cornerstone Objectives Met with Minimal Reduction in Safety Margin	Repetitive Degraded Cornerstone, Multiple Degraded Cornerstones, Multiple Yellow Inputs, or 1 Red Input[1]; Cornerstone Objectives Met with Longstanding Issues or Significant Reduction in Safety Margin	Overall Unacceptable Performance; Plants Not Permitted to Operate Within this Band, Unacceptable Margin to Safety
RESPONSE	Regulatory Conference	Routine Senior Resident Inspector (SRI) Interaction	Branch Chief (BC) or Division Director (DD) Meet with Licensee	DD or Regional Administrator (RA) Meet with Licensee	EDO (or Commission) Meet with Senior Licensee Management	Commission meeting with Senior Licensee Management
	Licensee Action	Licensee Corrective Action	Licensee Corrective Action with NRC Oversight	Licensee Self Assessment with NRC Oversight	Licensee Performance Improvement Plan with NRC Oversight	
	NRC Inspection	Risk-Informed Baseline Inspection Program (Baseline)	Baseline and Inspection Follow-up	Baseline and Inspection Focused on Cause of Degradation	Baseline and Team Inspection Focused on Cause of Degradation	
	Regulatory Actions	None	Document Response to Degrading Area in Inspection Report	Docket Response to Degrading Condition	-10 CFR 2.204 DFI -10 CFR 50.54(f) Letter - CAL/Order	Order to Modify, Suspend, or Revoke Licensed Activities
COMMUNICATION	Assessment Report	DD review/sign assessment report (w/ inspection plan)	DD review/sign assessment report (w/ inspection plan)	RA review/sign assessment report (w/ inspection plan)	RA review/sign assessment report (w/ inspection plan) Commission Informed	
	Public Assessment Meeting	SRI or BC Meet with Licensee	BC or DD Meet with Licensee	RA Discuss Performance with Licensee	EDO (or Commission) Discuss Performance with Senior Licensee Management	Commission Meeting with Senior Licensee anagement
		<---------- Regional Review / Agency Review ----------				

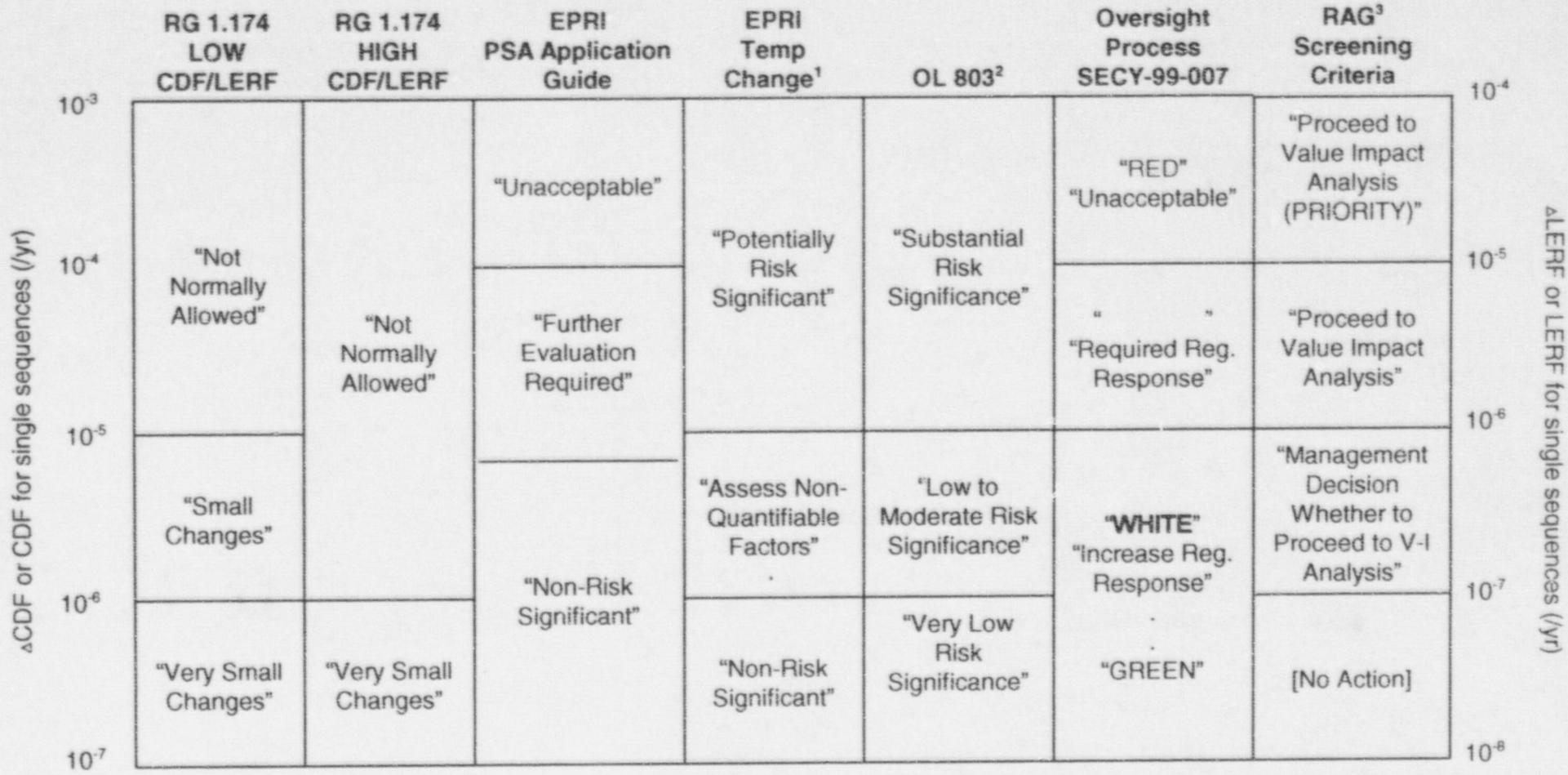
Plant Oversight Process



Reactor Oversight Process

- Integrates risk-informed measurement and inspection
- Consistent with established regulatory criteria (RG: 1.174)
- Provides consistency
- Differentiates levels of safety performance
- Rewards timely licensee trending and corrective activity
- Allows for plant specific design differences

USE OF RISK INFORMATION IN NRC AND INDUSTRY PROGRAMS



---

[1] ΔCDP ~ ΔCDF if used ~ 1/yr

[2] Office Letter 803 Reference to 10/30/98 Guidance Memo

[3] Regulatory Analysis Guidelines NUREG/BR-0058 for CCFP.1 to 1

Shutdown PSA at River Bend Station

Thomas L. Hunt

Entergy - River Bend Station

Purpose of RBS Shutdown PSA

- *Common Risk Assessment Tool for At-Power and Shutdown Operations*
- *Component Level Model More Flexible for Shorter Outages*
- *Suppression Pool Cooling & Cleanup / ADHR System Added*

Shutdown PSA End States

- End States
  - RCS Boiling
  - Core Damage (includes SFP Damage)
  - Fuel Pool Boiling
- Other NSAC-175L End States
  - LTOP - RBS LOCA Initiator
  - Prompt Criticality - Maintain SDM
  - Exposed Bundles - OPDRV Initiator /IFTS
  - Containment Performance (Shutdown Level 2)

Shutdown PSA Challenges

- *Initiating Events*
- *Success Criteria Changes*
- *Human Reliability Analysis*
- *Recovery Actions*
- *Defense-in Depth Modeling*
- *EOOS Development*

Phased Mission Model

- Plant Configuration Changes
  - Systems Running
  - Systems Out of Service
  - Success Criteria Changes
- Plant State Changes
  - Decay Heat Level
  - RPV Water Level
  - Containment Status
- RBS had ~65 Flags to Handle ~62 Plant Configurations

Fault Tree Changes

- *Five New Fault Trees Created*
- *Six Existing Fault Trees Changed*
- *Separated Demand and Run Failures in Certain Fault Trees to Account for Changes in System Status*

Shutdown PSA Quantification

- *No Baseline CDF or Boiling Risk*
- *Quantification Done for All Combinations of Flag Settings*
- *Sequence Quantification Done for Model Testing and Enhancement*
- *Schedule Quantification Done Through EOOS*

Human Reliability Analysis

- *Procedure Applicability*
- *Limited Procedural Guidance*
- *Indications Available*
- *More Time Available (and Less Stress)*
- *Applicable HRA Methodologies*

Operator Recovery Actions

- *Recovery of Off-site Power*
- *Recovery of Decay Heat Removal*
- *Recovery of Spent Fuel Pool Cooling*
- *Recovery from OPDRV/OPDRC*
- *Recovery Data from NSAC Documents*

Operator Recovery Times

- Decay Heat Level
  - High Decay Heat (Days 1-4)
  - Medium Decay Heat (Days 5-18)
  - Low Decay Heat (After Day 18)
- RPV Level
  - Normal RPV Level
  - RPV Level > 23 feet above Flange

Defense-In Depth Logic

- SSFAT Logic not Well Documented
- Force Color Code with Fault Tree
- Develop Consistent Color Codes Based on Technical Specifications
  - Green - Exceed LCO Requirements
  - Yellow - Meet LCO Requirements
  - Orange - In LCO Action Statement
  - Red - Tech. Spec. Violation

RCS Boiling Results

- RCS Boiling Frequency is High at the Beginning of the Outage (0.72/yr)
- RCS Boiling Frequency is High during RPV Hydrostatic Testing (0.7/yr)
- High RCS Boiling Frequency Does Not Imply High Core Damage Frequency

Core Damage Results

- Core Damage Frequency Driven by Support System Maintenance
- Highest for Maintenance not Allowed At-Power (DC Power, Off-site AC)
- Core Damage Frequency Cannot be Directly Tied to Any Defense-in-Depth Status Measure

Spent Fuel Pool Boiling

- Fuel Pool Boiling is Very Low Frequency Event (10^{-9}/Yr)
- Fuel Pool Boiling Risk Negligible Before Fuel Movement
- Not a Dominant Contributor to Fuel Damage (Except for Full Core Offload)

Shutdown PSA Limitations

- *Difficult to Perform Sensitivity and Uncertainty*
- *No Overall Importance Ranking*
- *Must Check Alignment before Performing SHEOOS Run*
- *No Simple Results*

Results and Conclusions

- *Shutdown PSA is Viable, but much more Dynamic than At-Power PSA*
- *No Baseline Risk Number*
- *Shutdown Risk Driven By Schedule*
- *Human Reliability Analysis and Operator Recovery Important*
- *Defense-In Depth Does Not Imply Low Shutdown Risk*

Results and Conclusions

- *Shutdown Risk Comparable to At-Power Risk*
- *Limitations to Short Outages without Impacting Outage Risk*
- *Can Be Physical Limitations for Short Outages*

Results and Conclusions

- *Shorter Outage = Higher Average Risk, but possibly Lower Overall Outage Risk.*
- *Can Determine the Impact of Moving Activities from Outage to At-Power*
- *Can Reduce Overall Risk By Doing More On-Line Maintenance*