

23. **ATTACHMENT 4 – RISK EVALUATION BB PRA-017.91B**

**PURPOSE**

This evaluation examines the risk significance associated with the failure to conduct a risk evaluation in accordance with the requirements of the Maintenance Rule section a(4) before removing power to 1SX033 and 1SX034 valves as part of maintenance activities during the refueling outage at Byron Unit 1. Byron Unit 2 was operating at power during the outage at Unit 1.

**BACKGROUND**

On April 6, 2008, Byron staff members were making preparations to replace the 1SX034 valve with a newer and improved valve. In the process of isolating SX flow to the valve, the 1SX033 valve was closed using its motor operator. Although closed, the 1SX033 valve did not provide a completely water tight seal sufficient to allow removal and replacement of the 1SX034 valve without water leakage into the work area. For large (36") butterfly valves of this type, small leakage is not an unusual occurrence.

A decision was made to use the manual operator for 1SX033 to tighten the seal between the butterfly and the seat by manually closing the valve operator further than the motor operator could. While manually tightening the closure of the valve, operators notice a "pop" noise followed by a decrease in torque needed turn the valve operator. At that point, the effort to replace 1SX034 was stopped and troubleshooting to determine the status of the 1SX033 operator was begun.

As part of the troubleshooting efforts, both the 1SX033 and 1SX034 valves were fully opened using their motor operators. Power was then removed from both valves as part of the effort to investigate the condition of the 1SX033 operator. The open position is the normal operating position of both the 1SX033 and 1SX034 valves. This alignment cross ties the SX pump supply to the A and B headers within Unit 1. This allows one SX pump to provide flow for both trains during normal operations.

However, operators failed to recognize that removal of power for these valves disabled the remote isolation capability normally relied on in the event of an auxiliary building flooding condition (IR # 759945 [8]). Abnormal Operating Procedure OBOA PRI-8 [1] directs operators to isolate the trains as part of steps to determine which train contains the leak so that it can be effectively isolated to limit the impact of flooding in the auxiliary building. Auxiliary Building flooding could impact both the unit in outage as well as the unit at power because of the nature of sharing inherent in the design of the SX system and the layout of the Auxiliary Building. Therefore, a risk evaluation for the condition should have been conducted for both the unit in outage and the unit at power

**METHOD and ACCEPTANCE CRITERIA**

An evaluation of the condition for both units should have been made prior to entering a condition where the both the 1SX033 and 1SX034 valves could not be isolated remotely from the control room in accordance with OBOA PRI-8. NRC Inspection Manual Chapter 0609 Appendix K [2] is the guiding document for conducting the significance determination process (SDP) for "findings related to licensee assessment and management of risk associated with performing maintenance activities under all plant operating or shutdown conditions".

In the event that no assessment of risk was performed prior to maintenance activities, App. K provides a flow chart to assess the impact of the failure to assess the risk

implications of the maintenance. Portions of that flow chart applicable to this occurrence are reproduced below.

App. K indicates that for cases where no risk assessment was performed, the risk deficit is defined as follows:

“If the licensee did not perform a risk assessment at all, the actual risk increase (ICDP<sub>actual</sub>) is the product of the incremental CDF and the annualized fraction of the duration of the configuration [i.e.,  $ICDP_{actual} = ICDF_{actual} \times (\text{duration in hours}) \div (8760 \text{ hours per reactor year})$ ], where  $ICDF_{actual} = CDF_{actual} - CDF_{zero-maintenance}$ ”

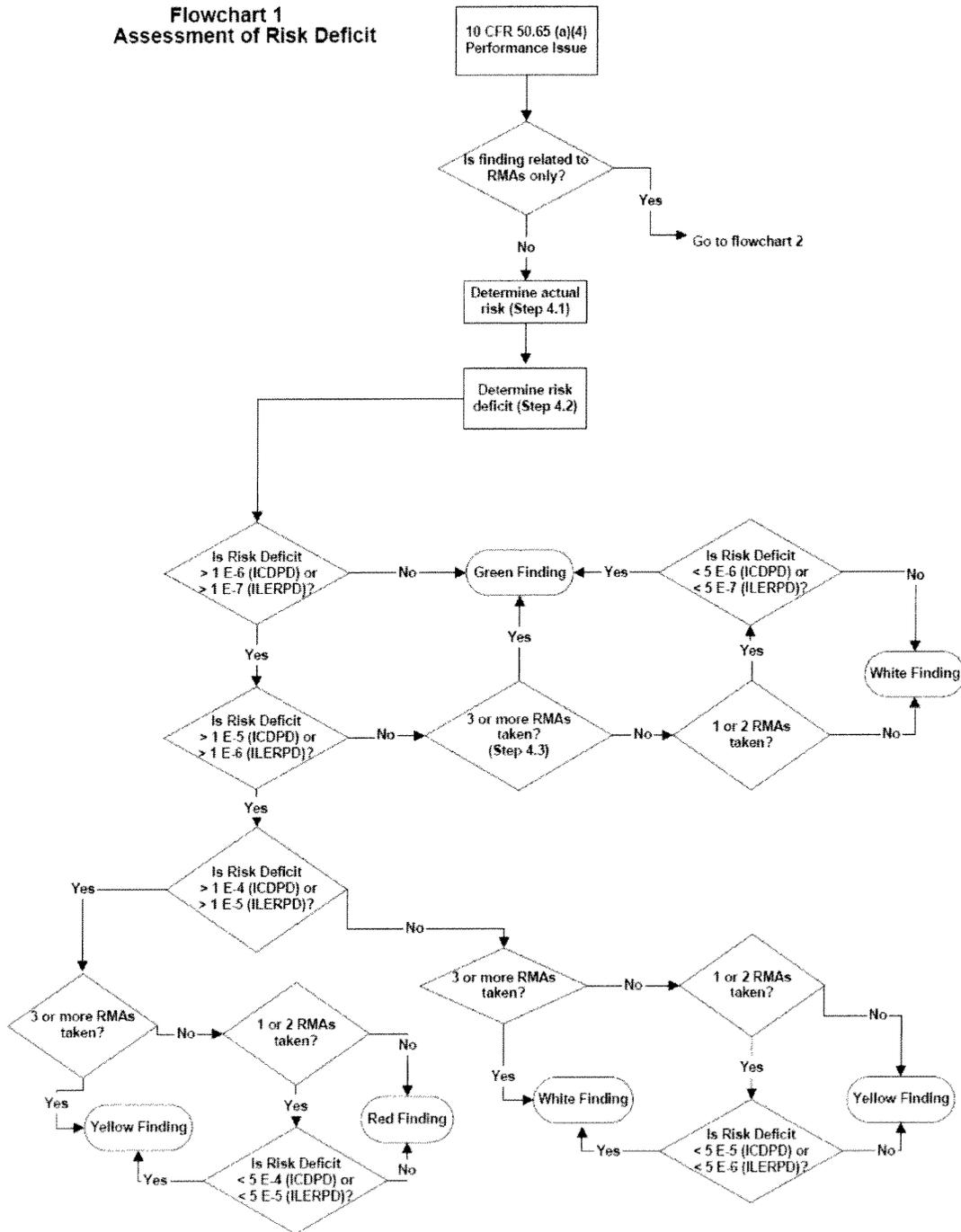
The risk deficit, ICDPD, is equal to ICDP when the licensee’s performance deficiency involves not conducting a risk assessment.”

App K identifies that the number of RMAs (risk management activities) is also a factor in determining the SDP “color”. The flowchart shows how the combination of the risk deficit and the number of RMAs taken affects the final SDP evaluation.

Byron does not use a quantitative shutdown risk model for assessing and managing risk for outage situations, but does use a risk model for assessing and managing risk for operations at power. App K notes that qualitative assessments are done for the former in a Note in prior to Section 4.0 which invokes the flowchart noted above.

**Note: This guidance does not apply to the following situations: (1) those licensees who only perform qualitative analyses of plant configuration risk due to maintenance activities, or (2) performance deficiencies related to maintenance activities affecting SSCs needed for fire or seismic mitigation. When performance deficiencies are identified with either 1 or 2 above, the significance of the deficiencies must be determined by an internal NRC management review using risk insights where possible in accordance with IMC 612, “Power Reactor Inspection Reports.”**

**Flowchart 1  
Assessment of Risk Deficit**



To evaluate the implications of having the 1SX033 and 1SX034 valves' power removed there are two analyses that need to be performed. The first one involves the impact on the unit in outage and the second for the unit at power. T&RM ER-AA-600-1041 [6] provides guidance for performing SDP analyses. T&RM ER-AA-600-1012 [3] provides the guidance for documenting this evaluation.

LERF values are more than an order of magnitude lower than CDF values for Byron. The specific failure modes of the 1SX033 and 1SX034 valves have no impact on the LERF except through their impact on CDF. Therefore, calculations based on CDF are the more limiting cases.

### **ANALYSIS INPUTS and RESULTS**

For unit 1 which was in a refueling outage at the time that the valves had power removed, a qualitative assessment is required. During this period, the reactor head was removed and was flooded up so that fuel could be moved back into the reactor. The spent fuel pool was at normal levels. Decay heat was being removed via the component cooling heat exchangers to the essential service water system.

According to the plant status reports prepared for each shift turnover during the outage in accordance with Attachment 1 to OU-BY-104 Revision 10 [7], there was in excess of 16 hours to core boiling in the event of a loss of cooling and over 24 hours to core damage. Even if one were to assume a total loss of essential service water due to an auxiliary building flooding event with failure of both 1SX033 and 1SX034 to close, the amount of water required to keep the core and spent fuel pool covered and cooled is minimal. Fire protection water, an alternate cooling water source, alone would be more than adequate for those purposes. In addition recent changes made in response to the NRC security orders under section B.5.b would also be available if needed. These are not included in this evaluation due to the sensitive nature of information related to those orders.

Given an SX leak in the Auxiliary Building at a rate of  $7.6E-04$  per year based on the flooding analysis notebook (BB PRA-012 Rev. 4 [4]) and a period of interest of 42.3 hours, the maximum frequency of loss of SX would be  $3.7E-06$  per year. Given the fact that the times to boil and uncover were very long, and that fire protection water was available (along with other sources identified as part of the recent security inspections associated with section B.5.b of the NRC orders following the 9/11 events), it is qualitatively presumed that the probability of core damage frequency deficit for the outage unit would be significantly below the  $1E-6$  value noted in the App. K flowchart. Based on these qualitative insights, the SDP assessment for the outage unit would be Green.

For the unit operating at power, there are two scenarios where the loss of integrity of SX piping in the Auxiliary Building could affect risk. These are risks associated with leaks (flow rate  $<2000$  gpm) and with ruptures (flow rates  $>2000$  gpm). In order to prevent core damage, the flooding analysis presumes that loss of the SX pumps and inability to maintain charging pump flow will lead to core damage. This is due to the potential reactor coolant pump (RCP) seal LOCA that could occur if charging (RCP seal injection) and component cooling water (CCW barrier cooling) were both lost. Flooding induced failures of the SX pumps could lead to the loss of the RCP thermal barrier cooling capability via loss of CCW cooling while inundation of the charging pumps would lead to failure of RCP seal injection. Loss of SX would also prevent operation of RCS injection systems so that a RCP Seal LOCA would eventually lead to core damage due to lack of injection.

The Flooding Analysis [4] indicates that the frequency of SX pipe ruptures (flow rates >2000 gpm) is  $9.6E-06$  per year. For the 42.3 hour duration, this is equivalent to a frequency of  $4.6E-08$  per year. Assuming that neither 1SX033 nor 1SX034 could be closed to isolate a rupture in accordance with OBOA PRI-8 in time to prevent loss of SX and loss of charging, the frequency would still indicate a Green condition per Appendix K of IMC 0609.

The frequency of leaks between 100 gpm and 2000 gpm is  $7.6E-04$  in the Flooding Analysis [4]. For the 42.3 hour duration when neither the 1SX033 nor the 1SX034 valves were capable of closure in accordance with OBOA PRI-8, this equates to a frequency of  $3.7E-06$ . However, even for the maximum flow rate among leaks (2000 gpm) it would take 10.8 hours to reach the point (1.29 million gallons per the Flooding Analysis) where the charging pumps would be inundated (215 hours at the minimum leakage rate). BOP SX-22 [5] provides the procedure for isolating SX leaks at specific locations in the Auxiliary Building.

The probability of failure to isolate a leak is low for several reasons:

1. The time to isolate is between 10.8 hours for a 2000 gpm leak and 215 hours for a 100 gpm leak.
2. A procedure exists to specify valves to isolate any particular piping segment in the Auxiliary Building. In addition, Operators are trained in use of P&IDs for troubleshooting problems with systems that are not functioning as would be expected in procedures such as OBOA PRI-8.
3. Complete isolation of the affected segment per BOP SX-22 is not needed in order to stop the flooding. The impact of failure of closing 1SX033 and 1SX034 is that the A and B supply for the unit 1 trains are cross tied. Other means exist to isolate the supply side of either the A or B train without having to perform the complete isolation of a leaking pipe segment. Isolation of five valves (1SX004, 1SX016A(B), 1SX013A(B), 1SX2103A (1SX173), and 1SX052A(B)) in the major supply headers downstream of 1SX012A(B) would accomplish the same function as closing 1SX033 or 1SX034 for train isolation purposes.
4. With unit 1 in a refueling outage, there were more people on-site and in the Auxiliary Building than normally would be the case. Therefore, detection of the leak location and availability of staff to perform isolation steps would be enhanced.
5. Additional staff through manning of the Outage Control Center (and TSC/EOF if needed) would be available in plenty of time to diagnose and effect isolation.

Using the SPAR-H methodology, the value for probability of failure to isolate would be about  $6.0E-02$  (Attachment 2). When combined with the frequency of the condition (leaks between 100 and 2000 gpm with failure of 1SX033 and 1SX034 for 42.3 hours) the result is about  $2.2E-07$ . When combined with the rupture failure to isolate probability of  $4.6E-08$ , the total for leaks and ruptures that could not be isolated would be  $2.7E-07$  which is well below the  $1.0E-06$  value in Appendix K.

Using the nominal HRA methodology for Byron and Braidwood which involves the cause based decision tree (CBDT) method combined with the Accident Sequence

Evaluation Program (ASEP) time response curves for cognitive error and the Technique for Human Error Prediction (THERP) method for execution errors, the probability of failure to isolate for leaks would be about 2.3E-02 (Attachment 1). This would further reduce the frequency of failure to isolate for leaks but would have no impact on failure to isolate for ruptures. This results in the actual incremental CDF of 8.4E-08 from the leaks. Thus, the combined value for leaks and ruptures would be about 1.3E-07 (4.6E-08+8.4E-08) which is well below the 1.0E-06 threshold in Appendix K.

## **SUMMARY**

Operators failed to perform a risk evaluation prior to engaging in maintenance activities that rendered portions of the SX system incapable of being used for isolating potential leaks or ruptures. In this condition, neither the 1SX033 nor 1SX034 valves could be operated remotely for purposes of train isolation in accordance with OBOA PRI-8. The plant was in the condition where both valves were open and incapable of remote operation for 42.3 hours. Assuming that SX piping ruptures (>2000 gpm) could not be isolated by other means and assuming that operators could potentially isolate leaks (between 100 gpm and 2000 gpm) before core damage would be assured, the actual core damage frequency associated with this configuration is about 1.3E-07 which is well below the 1.0E-06 threshold of Appendix K to IMC 0609 Figure 1 for evaluating the risk significance of such events. Therefore, the risk significance of this condition should be assessed as Green.

## **REFERENCES**

1. Byron Abnormal Operating Procedure OBOA PRI-8, Revision 0.
2. USNRC Inspection Manual Chapter 0609 Appendix K.
3. T&RM ER-AA-600-1012, Rev. 7, Risk Management Documentation.
4. BB PRA-012 Rev, 4, Internal Flooding Analysis Notebook. March 2008.
5. Byron Operating Procedure BOP SX-22, Revision 1.
6. T&RM ER-AA-600-1041, Rev. 6, Risk Metrics – SDP & Event Analysis.
7. T&RM OU-BY-104, Rev. 10, Shutdown Safety Management Program Byron/Braidwood Annex.
8. IR # 759945.

**Attachment 1:  
HEP for Isolation Failure for Leaks  
When 1SX033 and 1SX034 Fail**

Ref	Description	HEP		
DSX-SX22ISO-HVOA	Operators Fail to Isolate Leak per SX-22 when 1SX033 and 1SX034 fail to close	2.33E-02		
<b>Boundary Condition</b>				
<p>Following a leak (100-2000-gpm) in the SX system in the Auxiliary Building during one-unit-in-outage, failure of SX033 or SX034 to close prevents train isolation due to cross tie on the supply side to both SX trains. OBOA PRI-3 Step 3 calls for identification of which train the leak is coming from and isolation of that train by closing the SX033 and SX034 valve to separate A and B train supplies. BOP SX-22 provides specific valve lists to isolate particular break location L. In this case, only the supply side for the affected train needs to be isolated because the train isolation of the discharge path via 1/2 SX011 is presumed successful. There are five valves in each train downstream of the SX033 and SX034 valve which can accomplish this function. They are SX004 and SX015(A/B) which are MOVs operable from the control room and SX013(A/B), SX052(A/B), and SX2103 A( SX173 ) which are manual valve operable locally. More than 10 hours are available to take this action before charging pumps are inundated.</p>				
<b>Evaluation of p<sub>c</sub></b>				
Causal Factor	HEP-Num	Compensating Factor(s)/Comments	Non-Recover	HEP-Final
p a 2	1.00E-04	Recovery factor/ Extra crew	5.00E-01	5.00E-05
p b 8	1.00E-08	Recovery factor/ Self-recovery and STA-recovery	5.00E-02	5.00E-10
p c 1	5.00E-04	Recovery factor/ STA-recovery	1.00E-01	5.00E-05
p d 4	5.00E-02	Recovery factor/ Extra crew and STA-recovery	5.00E-02	2.50E-03
p e 8	1.30E-02	Recovery factor/ Self-recovery, Extra crew, and STA-recovery	2.50E-02	3.25E-04
p f 3	3.00E-02	Recovery factor/ Self Recovery, Extra crew and STA-recovery	2.50E-02	7.50E-04
p g 10	1.00E-03	Recovery factor/ Extra crew and STA-recovery	5.00E-02	5.00E-05
Total p <sub>c</sub> (Unrecover)	9.45E-02		p <sub>c</sub> (BD TM)	3.73E-03
		T <sub>w</sub> < 10-hr	p <sub>c</sub> (ASEP)	1.00E-04
<b>Evaluation of p<sub>c</sub></b>				
Procedure(s) Step	Description	HEP	HEP Variable	HEP
OBOA PRI-3 Step 1a Determine source and severity of flooding	Skip step (Table 20-7-6)		20 7 4	1.25E-02
BOP SX-22 Step F.1 Utilize the following table for isolation of SX system leakage	Skip step (Table 20-7-6)		20 7 4	1.25E-02
Close SX004 and SX015(A/B)	Select wrong control (Table 20-12-1) X 2 Turn control in wrong direction (Table 20-12-6) X 2		20 12 1 20 12 4	7.50E-03 2.66E-03
Close SX013(A/B), SX052(A/B), and SX2103A (SX173)	Fail to close valve (Table 20-13-1) X 3		20 13 1	3.75E-03
	Recovery inside CR		r <sub>1</sub> c	5.00E-01
	Recovery outside CR		r <sub>2</sub> l c	5.00E-01
			Total p <sub>c</sub>	1.95E-02

<b>CBDT Justifications</b>	
<b>P<sub>c</sub>A</b>	<b>Data Not Available. Branch #2 (variable name is '_p_a_2') is chosen because the procedures for isolating Auxiliary Building Flooding per BOA PRI-8 and BOP SX-22 are relatively new and limited training opportunities have been undertaken.</b>
<b>P<sub>c</sub>B</b>	<b>Data Available But Not Attended To. The workload is assumed high due to the fact that one unit is in a refueling outage. Branch #8 is selected since Auxiliary Building flooding is alarmed via sump level alarms.</b>
<b>P<sub>c</sub>C</b>	<b>Communications issues. Branch #1 is a default for all HEP assessments. The Byron and Braidwood control room layouts have been subjected to formal human factors review &amp; validation . The plant policy is to emphasize 3-way communications; this is stressed in all training.</b>
<b>P<sub>c</sub>D</b>	<b>Available Information Misleading &amp; Misinterpreted. Branch #4 is chosen because of the procedures are relatively new and training on them is limited.</b>
<b>P<sub>c</sub>E</b>	<b>Skipping the Relevant Step in the Procedure. Branch #8 is selected (Multiple procedures, E-0 and OA PRI-8, and BOP SX-22). With one exception, there is no requirement for using any place keeping aids. The exception is the use of Status Trees (ST). Except for 'boxed' procedure steps (immediate, memorized steps), and steps identified by 'diamond symbol' (for continuous actions), the procedure design does not include any feature that would prevent the operators from overlooking a procedure step - not "graphically distinct."</b>
<b>P<sub>c</sub>F</b>	<b>Misinterpretation of the Instruction. Branch #3 is selected because determination of the actual break location is a function of the ability of the staff in the Auxiliary Building to locate the leak and communicate that to the control room. Also, training on the relatively new BOA PRI-8 and BOP SX-22 is limited.</b>
<b>P<sub>c</sub>G</b>	<b>Error in Interpreting the Decision Logic. This CDBT is concerned with presence of logic statement(s) in procedure. Branch #10 is selected since the cited procedure steps include any written logic statements. Furthermore, it is assumed that the operators have received limited training on this action.</b>

**Attachment 2: SPAR-H Estimate of HEP**

- 23.1. 0SX-SX22ISO-HVOA, Operators Fail to Isolate Leak per SX-22 when 1SX033 and 1SX034 fail to close

**Basic Event Summary**

<b>Analyst:</b>	DEM
<b>Rev. Date:</b>	06/16/08
<b>Reviewer:</b>	
<b>Cognitive Method:</b>	SPAR-H
<b>Analysis Database:</b>	no33-34.HRA (06/16/08, 507904 Bytes)

**Table 1: 0SX-SX22ISO-HVOA SUMMARY**

<b>Analysis Results:</b>	Cognitive	Execution
<b>Failure Probability</b>	4.8e-02	1.2e-02
<b>Total HEP</b>	6.0e-02	

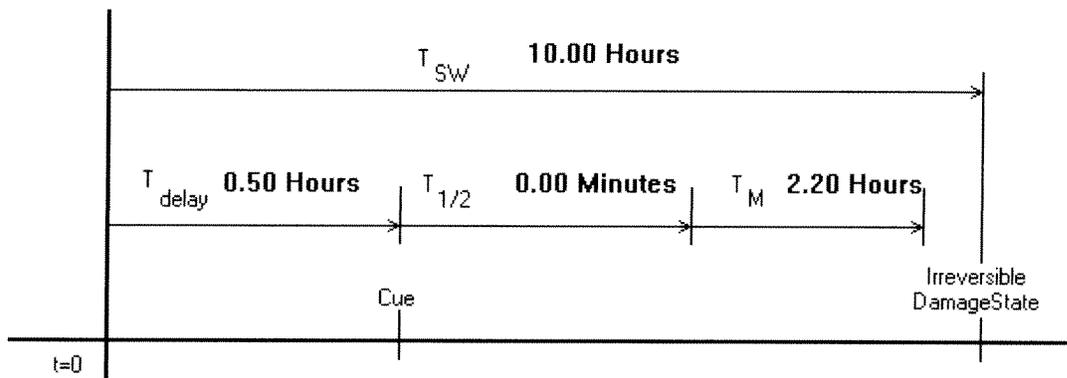
**Plant:**  
Byron

**Initiating Event:**  
SX flood leak (100-2000 gpm)

**Basic Event Context:**

Following a leak (100-2000 gpm) in the SX system in the Auxiliary Building during one unit in outage, failure of 1SX033 and 1SX034 to close prevents train isolation due to cross tie on the supply side to both SX trains. OBOA PRI-8 Step 7 calls for identification of which train the leak is coming from and isolation of that train by closing the 1SX033 or 1SX034 valves to separate A and B train supplies. BOP SX-22 provides specific valve lists to isolate particular break locations, but no guidance related to addressing failures of particular isolation valves. However, the operators are trained to address SX leak isolation through review of the P&IDs to identify and secure isolation points. In this case, only the supply side for the affected train needs to be isolated because the train isolation of the discharge path via 1/2SX011 is presumed successful. There are five valves in each train downstream of the 1SX033 and 1SX034 valves which can accomplish this function. They are SX004 and SX016(A/B) which are MOVs operable from the control room and SX013(A/B), SX052(A/B), and SX2103A (SX173) which are manual valves operable locally. More than 10 hours are available to take this action before charging pumps are inundated.

**Timing:**



**Timing Analysis:** Assuming isolation of a manual valve requires 20 minutes and that 1 minute is needed for a valve in the MCR, the 5 additional valve isolations that would be required to make up for 1SX033 or 1SX034 failure would contribute 62 minutes to the manipulation time if the valves were addressed sequentially. Most other isolation cases include only a few manual valve manipulations and 1 hour would be a reasonable manipulation time for those valves. There are some cases, however, that require as many as 10 local valve closures. In these cases, 3.3 hours would be required to isolate them sequentially. For this case, minimal parallel work is assumed: the 4.3 hours of ex MCR work is assumed to be split among two crews so that it could be completed in about 2.2 hours. The MCR isolations are considered to be completed in parallel with the ex-MCR work and no additional time is added to address those actions.

The system window of 10 Hours is based on the time needed to reach critical flood volume 2 in the Flooding Analysis in BB PRA-012 Revision 3 for the worst leak rate (2000 gpm). For the smallest leak size (100 gpm) it would take about 215 hours to reach that level.

The delay time of 30 minutes, which is the length of time to the cue, is based on the time to reach sump alarm levels with minimum leak flow, but would more likely be much earlier due to visual identification from a crew member due to the fact that one unit was in a refueling outage and numerous staff were in the Auxiliary Building.

Time available for recovery: 438.00 Minutes

SPAR-H Available time (cognitive): 438.00 Minutes

SPAR-H Available time (execution) ratio: 4.32

Minimum level of dependence for recovery: ZD

## PART I. DIAGNOSIS

PSFs	PSF Levels	Multiplier for Diagnosis
Available Time (recommended choice based on timing information in bold)	Inadequate Time	P(failure) = 1.0
	Barely adequate time (~ 2/3 x nominal)	10
	Nominal time	1
	Extra time (between 1 and 2 x nominal and > 30 min)	0.1
	Expansive time (> 2 x nominal and > 30 min)	X 0.01
	Insufficient Information	1
	<i>Based on the timing analysis, "expansive" time is available.</i>	
Stress	Extreme	5
	High	X 2
	Nominal	1
	Insufficient Information	1
	<i>The long time available before negative consequences will reduce the stress for the scenario.</i>	
Complexity	Highly complex	X 5
	Moderately complex	2
	Nominal	1
	Obvious diagnosis	0.1
	Insufficient Information	1
Experience/Training	Low	X 10
	Nominal	1
	High	0.5
	Insufficient Information	1
	<i>Procedures OBOA PRI-8 and BOP SX-22 are relatively new and limited training has occurred due to their recent implementation. In addition, the operators would be required to use P&amp;IDs and information from plant staff to identify the location of the leak and means of isolating the condition when 1SX033 and 1SX034 failed to close. Therefore, a decrement to Low was chosen.</i>	
Procedures	Not available	50
	Incomplete	20
	Available, but poor	X 5
	Nominal	1
	Diagnostic/symptom oriented	0.5
	Insufficient Information	1

PSFs	PSF Levels		Multiplier for Diagnosis
	<i>The procedure BOP SX-22 identifies appropriate isolation points for leaks in the SX system. When multiple isolation valves fail to operate in accordance with OBOA PRI-8, the operators would rely on their training to help the isolate the leak using alternate valves. No procedure can be written to address all failure cases and they are not expected to do so, but a degraded condition is used to account for the difficulties associated with dynamically identifying new isolation points.</i>		
Ergonomics/HMI	Missing/Misleading		50
	Poor		10
	Nominal	X	1
	Good		0.5
	Insufficient Information		1
Fitness for Duty	Unfit		P(failure) = 1.0
	Degraded Fitness		5
	Nominal	X	1
	Insufficient Information		1
Work Processes	Poor		2
	Nominal	X	1
	Good		0.8
	Insufficient Information		1

**Diagnosis HEP:**

4.8e-02 [Adjustment applied:  $1.0E-2 * 5.0e+00 / (1.0E-2 * (5.0e+00 - 1) + 1)$ ]

24. **PART II. ACTION**

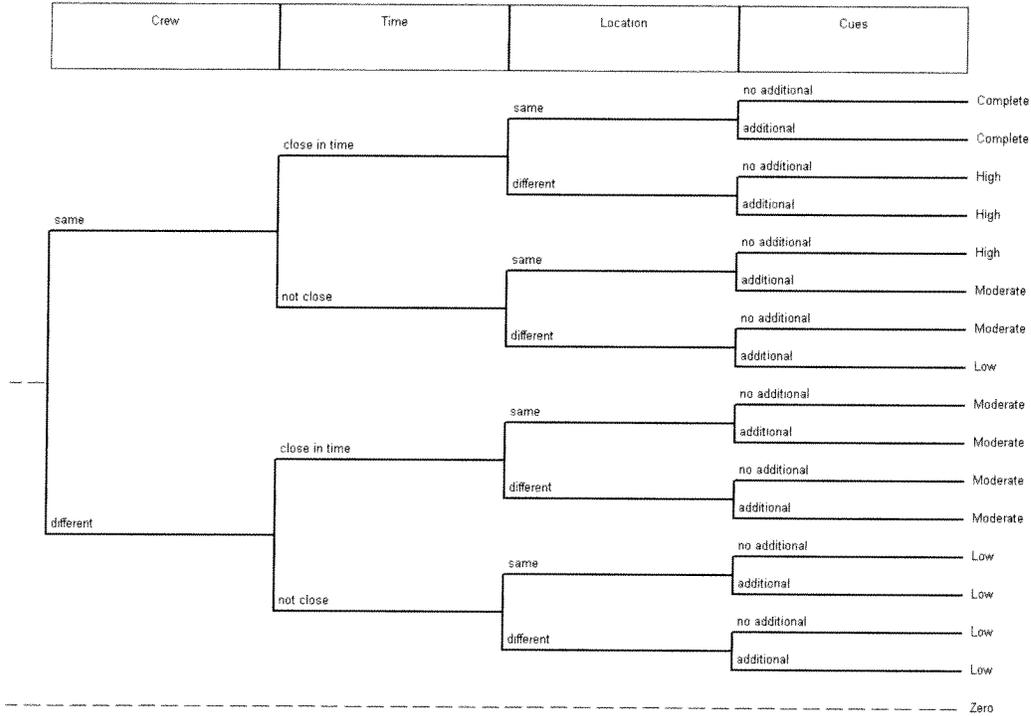
PSFs	PSF Levels		Multiplier for Diagnosis
Available Time (recommended choice based on timing information in bold)	Inadequate Time		P(failure) = 1.0
	Time available is ~ the time required		10
	Nominal time	X	1
	Time available $\geq 5x$ the time required		0.1
	Time available $\geq 50x$ the time required		0.01
	Insufficient Information		1
Stress/Stressors	Extreme		5
	High	X	2
	Nominal		1
	Insufficient Information		1

PSFs	PSF Levels		Multiplier for Diagnosis
Complexity	Highly complex		5
	Moderately complex	X	2
	Nominal		1
	Insufficient Information		1
Experience/Training	Low	X	3
	Nominal		1
	High		0.5
	Insufficient Information		1
Procedures	Not available		50
	Incomplete		20
	Available, but poor		5
	Nominal	X	1
	Insufficient Information		1
Ergonomics/HMI	Missing/Misleading		50
	Poor		10
	Nominal	X	1
	Good		0.5
	Insufficient Information		1
Fitness for Duty	Unfit		P(failure) = 1.0
	Degraded Fitness		5
	Nominal	X	1
	Insufficient Information		1
Work Processes	Poor		5
	Nominal	X	1
	Good		0.5
	Insufficient Information		0.5

**Action Probability:**

1.2e-02 [Adjustment applied:  $1.0E-3 * 1.2e+01 / (1.0E-3 * (1.2e+01 - 1) + 1)$ ]

25. **PART III. DEPENDENCY**



**Task Failure WITHOUT Formal Dependence:**

6.0e-02

**Task Failure WITH Formal Dependence:**

6.0e-02

**STATION: Byron**

**UNIT(S) AFFECTED: UNITS 1 and 2**

**TITLE:**

Byron SDP Evaluation of Failure to Conduct a Risk Evaluation  
Prior to Disabling 1SX033 and 1SX034 Remote Isolation Capability

**SUMMARY** (Include UREs incorporated):

**This document evaluates the risk significance of operator failure to conduct a risk evaluation in accordance with Maintenance Rule section a(4) prior to beginning maintenance on the 1SX033 and 1SX034 valves. Both valves were opened and power was removed by opening their supply breakers. This disabled the ability to close the valves in response to SX floods in the Auxiliary Building.**

**Number of pages:** Total 73 pages, including this page.

**RM Document Level:** Category 2, per ER-AA-600-1012.

Review required after periodic Update

Internal RM Documentation

External RM Documentation

**Electronic Calculation Data Files: (Program Name, Version, File Name extension/size/date/hour/min)**

**Method of Review:**  Detailed  Alternate  Review of External Document

**This RM documentation supersedes: \_\_\_\_\_ in its entirety.**

**Prepared by:** Steven E. Mays / \_\_\_\_\_ / 6/19/08

Print

Sign

Date

**Reviewed by:** Young In / \_\_\_\_\_ / 6/19/08

Print

Sign

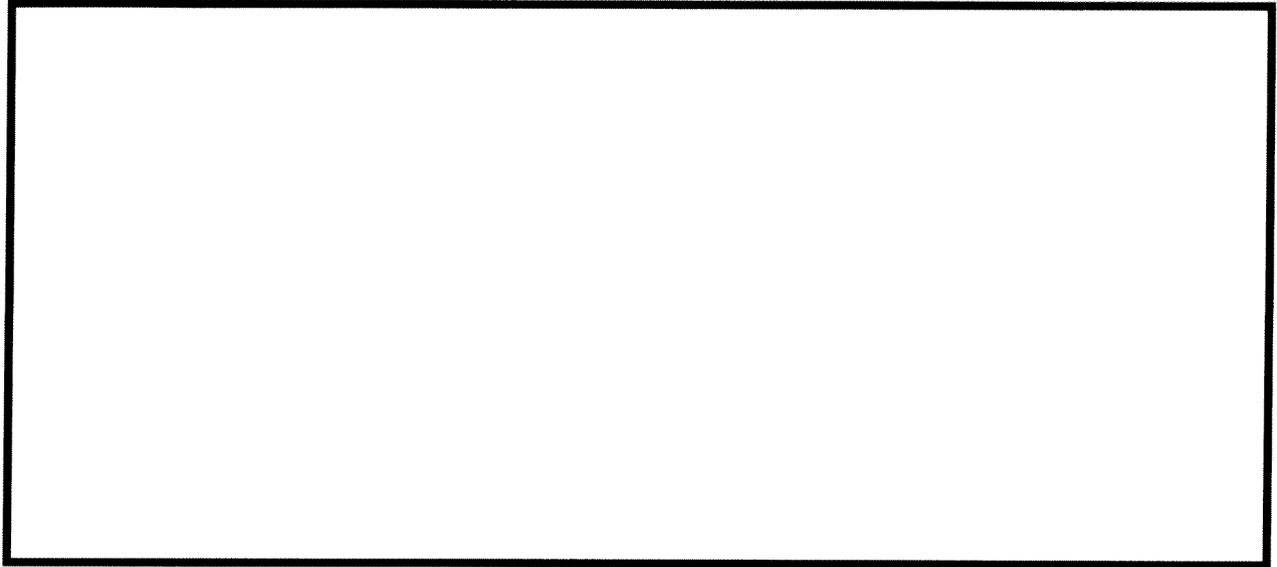
Date

**Approved by:** Barry Sloane / \_\_\_\_\_ / 6/19/08

Print

Sign

Date



26.

**ATTACHMENT 5 -- CAUSE AND EFFECT ANALYSIS -- GENERIC**  
**Knowledge Based Decision Required**  
**Understanding Needs Improvement**

EFFECT/SYMPTOM	Why	CAUSE/REASON
<ul style="list-style-type: none"> <li>• CO notes require SRO to evaluate for Technical Specifications at time CO is placed; no reference to risk.</li> <li>• U2 OLR not evaluated for configuration change.</li> <li>• Cycle Manager 2 wasn't concerned with 1SX033 and 1SX034 availability to position from the MCR until Risk Engineer stated.</li> </ul>	→ ↙	Personnel do not recognize the potential risk significance of the 1SX033 and 1SX034 related to Auxiliary Building internal flooding. (Dual Function high risk components) Knowledge based understanding required.
Personnel do not recognize the potential risk significance of the 1SX033 and 1SX034 related to Auxiliary Building internal flooding. (Dual Function high risk components) Knowledge based understanding required.	→ ↙	Process -- no flag or warning to alert personnel dual function high-risk components being used as isolation points on COs or WOs.  Training – less than adequate understanding of dual function high-risk components as they affect OLR.  Training – less than adequate understanding of Auxiliary Building internal flooding as related to plant risk.
Process -- no flag or warning to alert personnel dual function high-risk components being used as isolation points on COs or WOs.  Training – less than adequate understanding of dual function high-risk components as they affect OLR.  Training – less than adequate understanding of Auxiliary Building internal flooding as related to plant risk.	→ ↙	Process -- Dual function high-risk components are not identified in rule-based guidance available to Shift Managers, SROs, Cycle Managers, and Work Week Managers.  Training – licensed operator training learning objectives, lesson plan content does not address dual function high-risk components and their potential affect on OLR.  Training – less than adequate review of auxiliary building internal flooding for plant processes and procedures.

EFFECT/SYMPTOM	Why	CAUSE/REASON
<p>Process -- Dual function high-risk components are not identified in rule-based guidance available to Shift Managers, SROs, Cycle Managers, and Work Week Managers.</p> <p>Training – licensed operator training learning objectives, lesson plan content does not address dual function high-risk components and their potential affect on OLR.</p> <p>Training – less than adequate review of auxiliary building internal flooding for plant processes and procedures.</p>	<p>➔</p>	<p>Ineffective risk management program administration oversight.</p>

Conclusions – Causes:

1. Dual function high-risk components are not identified in rule-based guidance.
2. Licensed operator training learning objectives and lesson plan content does not address dual function high risk components and their potential affect on OLR.
3. Less than adequate review of auxiliary building internal flooding for plant processes and procedures.
4. Ineffective risk management program administration oversight.

27. ATTACHMENT 8

**Barrier Analysis Simplified  
Unplanned OLR Change to Orange**

Barrier	Expected	Failed/ Successful	Comments
<b>Job Site Conditions</b>			
1. Procedure content and usability WC-AA-101, Online Work Control Process	Y	S	<p>Step 4.5.11 <b>Shift Operations</b> – Is assessment of Risk acceptable? Does reassessment of risk against the ongoing workweek risk file result in a green or yellow risk color as prescribed in Attachment 3? (The following requirement shall not delay nor impede restoration of the plant to a stable condition).</p> <p>Shift Operations must reassess risk and document the result of the evaluation (risk color), even if there is no corresponding change in risk status, in the Shift Manager log.</p> <p>Step 4.5.12 <b>Shift Manager</b> – Take appropriate actions to mitigate risk. If emergent condition results in an orange or red risk color, or risk results are unavailable, the following compensatory measures must be enacted to mitigate the risk until such time as risk is reduced to an acceptable level.</p> <p>If risk is indeterminate or PRA results are unavailable as described within Attachment 3, the site risk management engineer must be contacted to evaluate the risk. The site risk management engineer may provide a preliminary verbal evaluation based upon qualitative judgment pending completion of a quantitative risk assessment.</p>

- Y = Viable Barrier
- N = Non-viable Barrier
- F = Barrier Failed
- W = Barrier Weak
- S = Barrier Satisfactory
- \* = Primary Barrier

NA = Not Applicable

Barrier	Expected	Failed/ Successful	Comments
			Procedure steps adequate; this is an execution issue.
2. Procedure content and usability WC-AA-101-1002, Online Scheduling	Y	S	<p>Step 4.7.3.1, Evaluate any priority work that has been proposed to be added to the schedule. Evaluate impact on scheduled work and plant configuration. Determine if the work can be added to the schedule or should be rescheduled. Also evaluate the addition of Carryover, Short Cycle, or Sponsored Work. (Cycle Manager) E-9 to 6.</p> <p>Step 4.7.4.1, Evaluate any priority work that has been proposed to be added to the schedule. Evaluate impact on scheduled work and plant configuration. Determine if the work can be added to the schedule or should be rescheduled. Also evaluate the addition of Carryover, Short Cycle, or Sponsored Work. (WWM.WEC) E-5 to 1.</p> <p>Step 4.7.4.13, Evaluate any priority work proposed to be added to the schedule. Evaluate impact on scheduled work and plant configuration. Determine if the work can be added to the schedule or should be rescheduled. Also evaluate the addition of Carryover, Short Cycle, or Sponsored Work. (WWM and WEC) end of E-1</p> <p>Step 4.7.5.1, Evaluate work and assess risk. (WWM) E-0. Screening committee or shift manager identifies any additional emergent item. WWM will evaluate for impact on the schedule and ensure risk assessment is performed by Operations.</p>

Y = Viable Barrier  
N = Non-viable Barrier  
F = Barrier Failed  
W = Barrier Weak  
S = Barrier Satisfactory  
\* = Primary Barrier

NA = Not Applicable

Barrier	Expected	Failed/ Successful	Comments
			Procedure steps adequate; this is an execution issue.
3. Procedure content and usability WC-AA-104, Review and Screening for Production and Atmospheric Risk.	N	NA	NA
4. Procedure content and usability OP-AA-109-101, Clearance and Tagging	Y	W	Step 8.2.4.4. C/O's that result in Online Risk changing to Orange or Red.  Step 10.3.1.8 VERIFY On-line Risk, Shutdown Risk and any applicable databases are updated as required.  Attachment 5, Clearance Preparation/Approval Checklist Attachment 8, Clearance Authorization Checklist Attachment 10, Clearance Manipulation Prejob Brief Checklist
5. Knowledge and Skills of workers* Shift Managers Shift Supervisors Cycle/Work Week Managers	Y	F	Knowledge weaknesses identified with shift managers and supervisors and to some extent cycle and work week managers.
6. Attitudes of employees towards hazards*	Y	F	Risk not valued as high priority when plant manipulations are made under the clearance order process.
7. Tools/Equipment Paragon	Y	S	Paragon modeled appropriately with more than usual conservatism built in regarding auxiliary building flooding.
8. Work Place Environmental Conditions	N	NA	NA
9. Individual Readiness	N	NA	NA
10. Fitness for Duty	N	NA	NA

Y = Viable Barrier  
N = Non-viable Barrier  
F = Barrier Failed  
W = Barrier Weak  
S = Barrier Satisfactory  
\* = Primary Barrier

NA = Not Applicable

Barrier	Expected	Failed/ Successful	Comments
11. Staffing Levels	N	NA	NA

Y = Viable Barrier  
 N = Non-viable Barrier  
 F = Barrier Failed  
 W = Barrier Weak  
 S = Barrier Satisfactory  
 \* = Primary Barrier

NA = Not Applicable

<b>Organizational Processes and Values</b>			
<b>Barrier</b>	<b>Expected</b>	<b>Success/ Failure</b>	<b>Comments</b>
12. Roles, responsibilities, and expectations*	Y	F	Operating personnel do not effectively own OLR risk as procedures suggest. Much reliance on work management and risk engineer.
13. Training Programs*	Y	F	Limited focus on risk background contained in operator initial and continuing training programs.  No formal training for work management personnel
14. Self Assessment and Corrective Action Program	N	NA	NA
15. Operating Experience Program	N	NA	NA
16. Job Scheduling	Y	F	Outage schedule allowed configuration to exist that adversely affected Unit 2 OLR.
17. Staffing Levels	N	NA	NA
18. Management Monitoring	Y	F	Inadequate oversight of OLR for operating unit when opposite unit is in a refuel outage.
<b>Worker Behaviors</b>			
<b>Barrier</b>	<b>Expected</b>	<b>Success/ Failure</b>	<b>Comments</b>
19. Personnel actions consistent and appropriate	Y	F	Operating personnel do not effectively own OLR risk as procedures suggest. Much reliance on work management and risk engineer. Similar to roles, responsibilities, and expectations

Y = Viable Barrier  
N = Non-viable Barrier  
F = Barrier Failed  
W = Barrier Weak  
S = Barrier Satisfactory  
\* = Primary Barrier

NA = Not Applicable

<b>Barrier</b>	<b>Expected</b>	<b>Success/ Failure</b>	<b>Comments</b>
			related to risk management.
20. Self Checking	N	NA	NA
21. Peer Checking	Y	F	Defense not effectively used to independently validate plant conditions such an accurate risk analysis could be performed.
22. Conservative Decision Making	Y	S	When risk was analyzed the worst cases were evaluated that eventually led to the identification of the condition.
23. Task Preview	N	NA	NA
24. Procedure Use and Adherence	Y	W	Procedure use level 3; procedure not required to be in hand. Steps generic in nature but do outline the steps necessary to be successful. However, applicable procedures not executed effectively to ascertain an accurate picture of OLR.
25. Stop Work When Uncertain	Y	S	Compensating actions are taken when the affect on OLR related to plant configuration is recognized.
26. Problem Reporting	N	NA	NA
27. Quality Control Hold Points	N	NA	NA
<b>Plant Results</b>			
<b>Barrier</b>	<b>Expected</b>	<b>Success/ Failure</b>	<b>Comments</b>
28. Equipment Works as Planned*	Y	F	Isolation of 1SX034 was aborted by the failure of 1SX033 to provide adequate isolation subsequently resulting in removal of work from the outage.
29. Sustained, superior Error-free Operations	N	NA	NA

Y = Viable Barrier  
N = Non-viable Barrier  
F = Barrier Failed  
W = Barrier Weak  
S = Barrier Satisfactory  
\* = Primary Barrier

NA = Not Applicable

30. Technical Specification Surveillance Requirements	N	NA	NA
<b>Barrier</b>	<b>Expected</b>	<b>Success/ Failure</b>	<b>Comments</b>
31. Technical Specification Limiting Conditions of Operation	N	NA	NA
32. Equipment Interlocks/alarms	N	NA	NA
33. Engineered Controls	N	NA	NA

Y = Viable Barrier  
 N = Non-viable Barrier  
 F = Barrier Failed  
 W = Barrier Weak  
 S = Barrier Satisfactory  
 \* = Primary Barrier

NA = Not Applicable

**Attachment 8  
Barrier Analysis**

FAILED OR INEFFECTIVE BARRIER	HOW BARRIER FAILED	WHY BARRIER FAILED	CORRECTIVE ACTION TO RESTORE BARRIER TO EFFECTIVENESS
1. Procedure content and usability	OP-AA-109-101, Clearance and Tagging weak in content to effectively ensure that CO are evaluated for OLR prior to execution.	No requirement exists to document the affect of the CO on OLR or SDR.  Procedure guidance is generic in nature and does not discuss dual function risk components.	Revise OP-AA-109-101, Clearance and Tagging.  Consider creating guidance that lists dual function risk components that if unavailable in conjunction with its redundant component would result in an orange or red condition.
2. Knowledge and Skills of workers	Knowledge weaknesses identified with shift managers and supervisors and to some extent cycle and workweek managers. Weaknesses related to recognition of dual function risk components that if unavailable in conjunction with its redundant component would result in an orange or red condition. Moreover, knowledge gaps were identified in the basis for risk changes based on plant configurations	Inadequate task analysis resulting in incomplete training material content or lack of training for specific work groups.	Perform task analysis and modify applicable training program content using the SAT process.
3. Attitudes of employees towards hazards	Risk not treated as an appropriate priority when plant manipulations are made under the clearance order process.	Inadequate perception of roles, responsibilities, and expectations with regard to priority of OLR.	Set expectations that include clear direction on roles and responsibilities for shift managers, shift supervisors, cycle/work week managers.
4. Roles, responsibilities, and expectations (Personnel actions consistent and appropriate)	Operating personnel do not effectively own OLR risk as procedures suggest. Much reliance on work management and risk engineer.	Inadequate perception of roles, responsibilities, and expectations with regard to priority of OLR.	Reinforce expectations through training.

FAILED OR INEFFECTIVE BARRIER	HOW BARRIER FAILED	WHY BARRIER FAILED	CORRECTIVE ACTION TO RESTORE BARRIER TO EFFECTIVENESS
5. Training Programs	<p>Limited focus on risk background contained in operator initial and continuing training programs.</p> <p>No formal training for work management personnel</p>	<p>Inadequate task analysis resulting in derisory training frequency and content in operator training programs.</p> <p>No formal mechanism in place to ensure that adequate transfer of knowledge related to OLR/SDR when personnel changes are made</p>	<p>Perform a formal task analysis to include not only the use of Paragon but more importantly the basis behind dual function components how they affect risk. Design, develop, implement and evaluate training using the SAT process.</p> <p>Develop a formal mechanism to ensure adequate transfer of knowledge related to OLR when personnel changes are made.</p> <p>Consider sending cycle and workweek managers to operator training related to OLR.</p>
6. Job Scheduling	<p>Outage schedule allowed configuration to exist that adversely affected Unit 2 OLR.</p>	<p>Outage scheduler did not fully realize the OLR implications encountered by 1SX033/34 configuration changes.</p> <p>OU-AP-104, Shutdown Safety Management Program Byron/Braidwood Annex, and OU-AA-101-1005, Exelon Nuclear Outage Scheduling are silent on opposite unit OLR considerations.</p>	<p>Develop a formal mechanism to ensure adequate transfer of knowledge related to SDR when personnel changes are made.</p> <p>Consider sending applicable outage scheduling personnel to operator training related to OLR.</p> <p>Consider revising OU-AA-101-1005 and/or OU-AP-104 to include references to consideration of opposite unit OLR.</p>

FAILED OR INEFFECTIVE BARRIER	HOW BARRIER FAILED	WHY BARRIER FAILED	CORRECTIVE ACTION TO RESTORE BARRIER TO EFFECTIVENESS
7. Management Monitoring	Inadequate oversight of OLR for operating unit when opposite unit is in a refuel outage as indicated by the lack of observation data related to OLR/SDR activities.	<p>Majority of management focus is on the outage unit because of the massive amounts of activities being performed.</p> <p>Little documented management observation of OLR/SDR activities.</p> <p>FMS data was queried for Byron from 01/01/08 to 07/01/08 that identified ~ 12300 fundamentals scored. A keyword search was performed using "risk" that identified 19 observations for either OLR or SDR. This represents ~ 0.15 % of the population. The median value for this population is 0.4% with the average value being 1.1%.</p> <p>Upon further review of FMS a task does not exist to assign OLR or SDR observations to.</p>	<p>Set expectations for observation of OLR/SDR activities and communicate to operations and work management.</p> <p>Consider adding a task related to OLR/SDR to the FMS activity menu.</p>
8. Peer Check	Defense not effectively used to independently validate plant conditions such an	Work management performs peer check of OLR values, however, an	Training and roles/responsibilities/ expectations actions listed above should address the underlying issue.

FAILED OR INEFFECTIVE BARRIER	HOW BARRIER FAILED	WHY BARRIER FAILED	CORRECTIVE ACTION TO RESTORE BARRIER TO EFFECTIVENESS
	accurate risk analysis could be performed.	adequate check was not made by shift operations to ensure OLR accounts for the present plant configuration. This is due in part to lack of knowledge and roles/responsibilities/expectations issues relate to OLR management.	Consideration should be given to institutionalize peer checks into OLR management activities for shift operations personnel.
9. Procedure use and adherence	Procedure use level 3; procedure not required to be in hand. Steps generic in nature but do outline the steps necessary to be successful. However, applicable procedures not executed effectively to ascertain an accurate picture of OLR.	This is due in part to lack of knowledge and roles/responsibilities/expectations issues relate to OLR management. Procedure guidance is generic in nature and do not discuss dual function risk components.	Training and roles/responsibilities/expectations actions listed above should address the underlying issue. Consider creating guidance that lists dual function risk components that if unavailable in conjunction with its redundant component would result in an orange or red condition. Consider identifying dual function risk components that if unavailable in conjunction with its redundant component would result in an orange or red condition in passport.
10. Equipment works as planned	Isolation of 1SX034 was aborted by the failure of 1SX033 to provide adequate isolation subsequently resulting in removal of work from the outage.	Unforeseen failure of isolation valve during manipulation.	Consider adding contingency actions if major isolation valves fail to perform their function project plans/fragnets/schedules.