Application of Risk-Informed Decision-Making Approach in Optimization of Online Maintenance for Safety Systems

WU Licun[a], DENG Wei[a], MA Chao[a]
[a]China Nuclear Power Engineering Co.,Ltd, Beijing, China

Abstract： To facilitate online maintenance for safety systems in TianWan nuclear power plant, the optimization measures for Technical Specifications are proposed in this paper, and risk-informed decision-making approach is used to demonstrate its feasibility. According to the analysis results, the optimization of Technical Specification meets the requirements of relative guides and deterministic analysis, and the impact on risk of plant is acceptable. Based on the optimization of Technical Specifications, it is feasible to carry out online maintenance for safety systems and corresponding support systems, which can effectively reduce workload during shutdown.

Keywords： Safety System; Online Maintenance; Risk-Informed Decision-Making

1. INTRODUCTION

There are two units under operation in TianWan NPP (nuclear power plant) applied VVER type PWR, which have four loops with four separate safety trains. However, limited by the stringent requirement from Technical Specification (TS), the preventable maintenance for safety systems have always been carried out during shutdown mode since the commercial operation, without taking advantage of the high redundancy of safety system. Compared to the plant with similar design, the requirement of Allowed Outage Time (AOT) and Surveillance Test Interval (STI) in TS for TianWan NPP is much more stringent. Meanwhile, according to the operating experience, the maintenance activities for safety systems and related support systems would be a heavy workload during refueling outage, which may cause extension of outage duration. Thus, to make full use of the redundancy design of safety systems, the optimization work is carried out to extend AOT and STI to facilitate the preventive maintenance for safety systems during power operation. By carrying out the online maintenance for safety systems, on the one hand, it can improve the flexibility for TianWan NPP operation and the quality of maintenance. On the other hand, it can reduce the work pressure and activity risk during shutdown mode.

The safety systems involved in TS optimization include high pressure safety injection system (JND), low pressure safety injection system (JNG-1), emergency boron injection system (JDH), containment spray system (JMN), emergency feedwater system (LAS/LAR) and related support systems.

2. OPTIMIZATION OBJECT AND METHODOLOGY

The current TS allow continued power operation with inoperability of a single train for a maximum of 30 days. Hence, if one train of safety system (e.g. JND) is inoperable due to corrective maintenance, the train must be restored within 30 days. If this train is not restored to an operable status within this period, other TS requirements would direct that the plant be placed, within a specified period, in an operating mode where alternate operability requirements for safety system are met. But the plant must immediately shut down in the conditions of two inoperable trains of safety system. Hence, if one train is inoperable due to preventive maintenance, meanwhile a random failure leads to another train inoperability, the plant must shut down even if there are still two redundant trains with 100% capability remaining operable. Thus, the extension for the current AOT is proposed in this paper. The proposed less restrictive AOT would allow the plant to complete maintenance activities at power while avoiding a potentially higher risk associated with plant shutdown.

According to the plant operation experience, the longest time of preventive maintenance for one train of safety system (e.g. JND) is 15 days. However, considering the STI requirements for safety system is one month, that is, all the periodic tests for the four trains of safety system need to be completed within one month, which means one train need to be performed periodic test every week (7 days). As a result, it is inevitable that one train will be tested in the process of online maintenance for another train. On one hand, this increase the work pressure and workload during the online maintenance, on the other hand, human errors may be introduced during the periodic test activity, resulting in a reduction in the redundancy of the safety system. Furthermore, too frequent periodic tests also have some negative effects on the equipment reliability. For example, too frequent start-stops in a short period of time can impact the equipment and accelerate equipment aging. Thus, an optimization of STI is also proposed to avoid the periodic test during online maintenance.

The approach used in this paper, to justify the proposed revision to AOT and STI are consistent with the guidance outlined in NNSA-0147 [1] and NNSA-0148 [2], which are compiled based on NRC guideline RG1.174 [3] and RG1.177 [4].

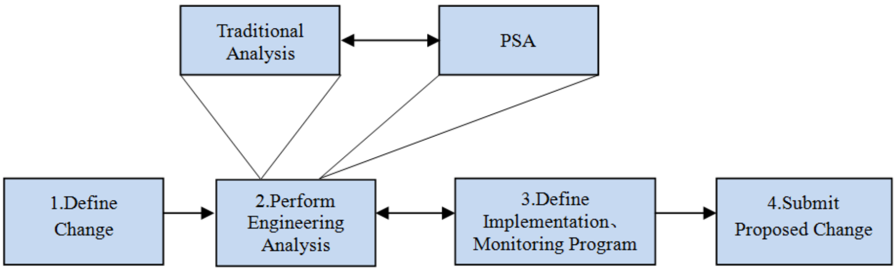
Traditional Analysis
PSA
1.Define Change
2.Perform Engineering Analysis
3.Define Implementation、Monitoring Program
4.Submit Proposed Change

Figure 1: Principle Elements of Risk-informed, Plant-Specific Decision-making

According to the principle of risk-informed decision-making discussed in these documents, the four-element approach, which Figure 1 presents graphically, is used to justify the proposal.

3. PROPOSED CHANGE

As discussed above，the safety train (e.g. JND) still has the capability to perform its safety function when two trains inoperable. Therefore, a less restrictive AOT would be more appropriate for TianWan NPP to complete maintenance activities at power. According to comparing the TS requirements with other type of NPPs (as showed in Table 1), it is easy to find that AOT requirements in Tianwan NPP are too conservative. Thus, it can be considered to make appropriate adjustments on AOT based on the decision-making approach. According to the operation experience and engineering judgement, the AOT is proposed to extend to 3 days to address cases where two trains are declared inoperable. Meanwhile, the other requirements in TS are not expected to be modified. The intent of AOT optimization is to enhance overall plant safety by avoiding potential unscheduled plant shutdowns, and to provide more flexibility in maintenance and surveillance scheduling.

Table.1 Comparison of TS requirement between several types of NPPs

NPP	System Configuration	Event	Consequence	TS Requirement
M310	2×100%	One train inoperable	Loss of redundancy	Entry into shutdown mode in 3days
STS	2×100%	One train inoperable	Loss of redundancy	3 days for maintenance
EPR	4×100%	Two trains inoperable	Loss of redundancy	Entry into shutdown mode in 3 days
VVER	4×100%	Two trains inoperable	Loss of redundancy	Immediately shutdown

The similar logic is used for extending the STI of safety systems from 1 month to 2 months, which means one train need to be performed periodic test every two weeks (14 days). It can avoid one train is under test in the process of online maintenance for another train.

4. TRADITIONAL ENGINEERING EVALUATION

4.1. Defense-in-Depth

According to NNSA-0147, the engineering evaluation conducted should determine whether the impact of the proposed AOT and STI change are consistent with the defense-in-depth philosophy. It is an effective way to account for uncertainties in equipment and human performance, in particular, to account for the potential for unknown and unforeseen failure mechanisms or phenomena, which neither the PSA nor traditional analyses reflect. It is acceptable for a licensee to use the seven defense-in-depth considerations described in NNSA-0147 to evaluate the impact of a proposed licensing basis change on defense in depth.

- The proposed change (extension of AOT and STI) doesn’t significantly reduce the effectiveness of the layer of defense that exists in the plant design to the extent that the layer no longer provides an acceptable level of defense. First, it doesn’t significantly increase the likelihood of initiating events or create new significant initiating events. Second, it doesn’t significantly impact the availability and reliability of safety systems providing the safety functions because there are 4 trains with 100% capability in safety systems of TianWan NPP, which means it still meet the single failure criterion in case of 2 trains inoperable. Third, the change doesn’t significantly impact the containment function or SSCs supporting that function. Fourth, the change doesn’t significantly reduce the effectiveness of the emergency preparedness program. Thus, a reasonable balance of the layers of defense (i.e., minimizing challenges to the plant, preventing any events from progressing to core damage, containing the radioactive source term, and emergency preparedness) are preserved.

- Since compensatory measures are not compulsory to support the changes, the adequate capability of design features could be preserved without an overreliance on programmatic activities as compensatory measures.

- Due to there are 4 trains with 100% capability in safety systems of TianWan NPP, the proposed changes don’t significantly reduce the redundancy, independence, or diversity of safety systems. Even one train is inoperable due to online maintenance and other train is identified as failure in periodic test, it still has two remaining trains and is consistent with the assumption in the plant’s safety analysis.

- Since the proposed changes don’t involve any hardware changes, and still maintain the original operating requirement for accident response. Therefore, the proposed change neither introduce a new potential CCF cause or event or coupling factor, nor increase the probability or frequency of a cause or event that could cause simultaneous multiple component failures. Thus, adequate defense against potential CCFs are preserved.

- The proposed changes neither create a significant increase in the likelihood or consequence of an event that simultaneously challenges multiple barriers nor introduce a new event that would simultaneously impact multiple barriers. Therefore, multiple fission product barriers are maintained.

- Since the proposed changes will facilitate online maintenance (i.e. transferring scheduled preventive maintenance (PM) from shutdown to power operation), it can effectively reduce work pressure on maintenance personnel during refueling outage stage, reducing the possibility of human error at that stage. For online maintenance, since maintenance personnel have enough time to perform maintenance and post-maintenance verification, it at least will not increase the probability of existing human errors.

- Since the changes don’t significantly compromise the ability to meet the intent of the plant’s design criteria, so it continues to meet the intent of the plant design criteria.

4.2. Safety Margin

The proposed changes are not in conflict with approved codes and standards relevant to these systems, and it meet the safety analysis acceptance criteria in final safety analysis report (FSAR). For example, for JND, based on the thermal-hydraulic considerations, the plant design basis requires that the plant be able to cope with the full spectrum of LOCAs. Design basis calculations indicate that the requirements can be met with a minimum of one JND train (plus other ECCS components dependent on break size) respond to all LOCAs, and one JND train is sufficient to accomplish adequate core heat removal in feed-bleed cooling stage. Thus, the proposed changes provide sufficient margin to meet the acceptance criteria in FSAR. Further, the restriction of proposed changes is not more relaxed than the engineering practice in other types of NPPs listed in Table.1. Thus, it can be found that the proposed changes are consistent with the principle that sufficient safety margins are maintained.

4.3. Compliance with Current Regulations

Changes regarding TS of safety systems meet regulatory requirements to meet HAD103/01 “Nuclear Power Plant Operating Restrictions ,Conditions and operating procedures” and other regulatory requirements.

5. ASSESSMENT OF RISK

5.1. Methodology

1) The evaluation of the impact on plant risk of the proposed AOT change is expressed by the incremental conditional core damage probability (ICCDP), and the incremental conditional large early release probability (ICLERP). According to the NNSA-0148, an ICCDP of less than 1E-6 and an ICLERP of less than 1E-7 are considered small for a single TS condition entry. The evaluation utilizes the following risk measures:

Conditional Core-Damage Frequency (CCDF): The CCDF is the CDF conditional upon some event, such as the outage of equipment. It is calculated by re-quantifying the PSA model after adjusting the unavailability of those basic events associated with the inoperable equipment. For the JND system:

$$\Delta CDF = CCDF_{\text{(JND inoperable)}} - CCDF_{\text{(JND operable)}} \qquad (1)$$

ICCDP is calculated as ICCDP = ΔCDF * ΔT, where ΔT equals to AOT.

ΔLERF has the similar expression, and ICLERP is calculated as ICLERP = ΔLERF * ΔT, where ΔT equals to AOT.

2) The evaluation of the impact on plant risk of the proposed STI change is expressed by ΔCDF and ΔLERF.

5.2. PSA Model Modification

1) For AOT change, it is necessary to assess the risk of a plant configuration where the two trains of safety system are not available for 3 days. According to NUREG-5485 [5], the CCF parameters should be adjusted for evaluating the risk of maintenance.

Consider a common cause component group consisting of four JDN pumps, denoted by A, B, C, D respectively. Assuming component D is unavailable due to online maintenance (i.e., preventive maintenance) and that it is not in a failed state. Furthermore, assuming component C is failed and need to be taken corrective maintenance while component D is unavailable due to online maintenance, which leads to two trains inoperable. We need to calculate the risk impact of component C failure given component D under online maintenance. According to the formula derivation in NUREG-5485, the failure probability of the remaining pumps and common cause failure in terms of alpha factor model can be given by following equations:

$$P[A_I] = P[B_I] = Q_1 \qquad (2)$$

$$P[CCF] = Q_1\alpha_2 + Q_1{}^2\alpha_2 + Q_1\alpha_3 + 1/3\alpha_3 + \alpha_4 \qquad (3)$$

Where A_I and B_I represent the independent failure of pump A and B, and CCF represents the probability of common cause failure for remaining pumps.

2) For STI change, the impact is mainly reflected in the start-up failure possibility of the safety system during the interval between two periodic tests. From the point of view of PSA modeling, interval changes will have a direct impact on the reliability parameters of related equipment, and indirectly affect the equipment common cause groups and frequency of some initiating events.

5.3. Risk Insight

1) After changing the PSA model in the way as discussed above, we could get risk of a plant configuration where the two trains of safety system are not available for 3 days. Since several safety systems (JND, JNG-1, JMN, etc.) are also involved in AOT extension. The risk insight will be discussed using the JND as an example.

The risk of a plant configuration where the two trains of JND inoperable for 3 days are showed in Table 2. We can get ΔCDF=1.08E-06/r*y and Δ LERF=3.3E-08/r*y.

Because it is proposed to extend AOT to 3 days, the value of Δ T equals to 3. According to the formula of ICCDP and ICLERP, we can get ICCDP=1.17E-08 and ICLERP=3.03E-10, which are much less than the threshold of a “small” risk described in NNSA-0148.

Table 2: Change in CDF and LERF

	CDF(/r*y)	LERF(r*y)
Baseline	1.16E-06	4.61E-08
2 trains inoperable*	2.44E-06	7.91E-08

*One train is under online maintenance, and other train is failed.

The JND system plays an important role in managing plant risk. If two JND train are declared inoperable, the plant staff should manage the risk and define compensatory measures, as appropriate. Risk insights suggest typical administrative actions that may be taken during "at power" include the following:

- For TianWan NPP, the JND system may be used for Once-Through-Core Cooling and therefore can back up the auxiliary feedwater system in satisfying the RCS heat removal safety function. Thus, concurrent maintenance on the JND and auxiliary feedwater system should be carefully controlled. This risk insight applies to all operating modes where the steam generator is used for heat removal. This guidance will be captured in plant administrative controls.

- Prior to entry into the extended AOT, risk management actions should be considered, as appropriate, utilization of non-safety equipment and/or temporary procedures to control risks. These actions could include procedures returning the affected JND train to functional use, if not fully operability, if the need arises. For example, for failure of one JND HVAC cooling train, measures should be taken for establishing temporary cooling.

- Include a risk assessment as an integral part of the work control process. Using risk-informed assessment tools to assess the actual maintenance risk based on the combined plant configuration.

2) The increase in CDF and LERF for proposed STI changes are show in Table 3 and 4. △CDF is less than 1E-06/r*y and △LERF is less than 1E-07/r*y. According to acceptance guidelines in NNSA-0148, it can be concluded that the increase in risk are acceptable.

Table 3: Increase in CDF due to STI Change

STI	CDF at power（/r*y）	LPSD CDF（/r*y）	Total CDF（/r*y）
1 month	1.16E-06	1.68E-07	1.328E-06
2 months	1.33E-06	2.03E-07	1.533E-06
△CDF	1.70E-07	3.50E-08	2.05E-07

Table 4: Increase in LERF due to STI Change

STI	LERF at power（/r*y）	LPSD LERF（/r*y）	Total LERF（/r*y）
1 month	4.61E-08	6.68E-09	5.278E-08
2 months	5.18E-08	7.91E-09	5.971E-08
△LERF	5.70E-09	1.23E-09	6.93E-09

By comparing the dominant sequences before and after the STI change, it can be seen that the dominant sequences are exactly the same. From the numerical point of view, the largest increase in frequency after STI extension is the sequence related to loss of offsite power (i.e., 4 emergency diesel generator sets fail to start or run, and 4/4 SG water supply side or steam side operation failure after loss of offsite power), which shows that the STI extension of emergency diesel generator has an impact on the mitigation ability for loss of offsite power accident. The second is related to the small breaks and the minimum breaks. It means the STI changes of JND and JNG-1 have an impact on the ability to mitigate the accidents regarding small breakage and minimal breakage. Considering the absolute value of frequency change, the maximum frequency increase in these dominant sequences is 4E-08/r*y, which only accounts for 3.45% of the CDF at power. Therefore, the STI changes of the safety systems have very little impact on the accident mitigation ability. Risk insights suggest typical administrative actions that may be taken during periodic test include the following:

- If one train failed in the test, especially for emergency diesel generator, the potential for the failure mechanism to similarly impact redundant components in remaining two trains should be assessed. This effort should be performed early in the repair process as practical and may include risk analyses or testing of other redundant equipment.

3) Before TS change, the maintenance of safety systems is arranged in the Cold Shutdown condition. Starting from the normal Cold Shutdown, preventive maintenance is carried out on each of the four safety trains respectively, so that there is always a train inoperable at the Cold Shutdown condition. After conducting on-line maintenance activities based on proposed TS changes, the schedule for preventive maintenance activities will be adjusted from the Cold Shutdown condition to the power operation period, so that all four trains are available under Cold Shutdown condition, reducing risk at that period. From the analysis result showed in Table 5, it can be found that performing online maintenance could effectively decrease the risk in Cold Shutdown condition.

Table 5: The Risk Decreased due to Online Maintenance

	Normal Cold Shutdown	Maintenance Cold Shutdown
Before	1.04E-07（/r*y）	6.11E-08（/r*y）
After	7.42E-08（/r*y）	4.76E-08（/r*y）
ΔCDF	2.98E-08（/r*y）	1.35E-08（/r*y）
Change Rate	28.65%	22.09%

6. MONITORING PROGRAM

To ensure no adverse safety degradation occurs because of the changes on TS, and the conclusions that have been drawn from the evaluation remain valid, it is necessary to have a long-term monitoring program after the proposal approved.

Configuration risk management is needed to ensure that the risk impact of out-of-service equipment is appropriately assessed and managed. And risk monitor will play an important role to assess the actual maintenance risk based on the combined plant configuration.

To ensure the TS change does not degrade capability of safety systems over time, the performance or condition of equipment affected by TS changes should meet its performance criteria. If there is a negative performance trend for the equipment, the corrective action should be taken. Such corrective action could include consideration of another TS change to shorten the revised AOT or STI, or imposition of a more restrictive administrative limit.

7. CONCLUSION

This paper provides the results of an evaluation to modify TS for safety systems in TianWan NPP, which allows consideration of extending AOT to 3 days in the condition of two trains of safety system inoperable, and extending the STI from 1 month to 2 months. The TS changes are sought to provide needed flexibility in the performance of both corrective and preventive maintenance during power operation. Justification of this request is based on the risk-informed decision-making approach. Results of this study demonstrate that the proposed TS changes provide plant operational flexibility while simultaneously allowing continued plant operation with an acceptable level of risk.

The proposal based on this study and analysis has already been approved as the first China's Risk-Informed on-line maintenance, and the totally outage duration is shortened to 27.2 days in 10th refueling outage for Unit 1, in which Risk-Informed on-line maintenance plays an important role.

References

[1] Approach for Using Probabilistic Risk Assessment in Risk-Informed Decision Making on Plant-specific Changes to Licensing Basis, NNSA-0147, 2012.
[2] An Approach for Plant-Specific Risk-Informed Decision making: Technical Specifications, NNSA-0148, 2012.
[3] An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decision Making on Plant- specific Changes to Licensing Basis, Regulatory guide (RG) 1.174, 1998.
[4] An Approach for Plant-Specific Risk-Informed Decision making: Technical Specifications, Regulatory guide (RG) 1.177, 2011.
[5] Guidelines on Modeling Common-cause Failure in Probabilistic Risk Assessment, NUREG/CR-5485, November 1998.