Brief introduction of TripMonitor Software for quantitative Assessment of shutdown risk in Nuclear Power Plant

Jun Qi[a], Yi Zou[b], Johan Sörman[c] and Xuhong He [d]

[a] CNNP Nuclear Power Operations Management Co., Ltd, Haiyan, China, qij@cnnp.com.cn

[b] Lloyd´s Register, Beijing, China, yi.zou@lr.org

[c] Lloyd´s Register, Stockholm, Sweden, johan.sorman@lr.org

[d] Lloyd´s Register, Stockholm, Sweden, xuhong.he1@lr.org

Abstract: Following the implementation of risk monitors at nuclear stations in China, the concept of trip monitor was developed by the CNNP and Lloyd´s Register (LR). This paper outlines the findings in a project for developing a trip monitor for implementation at Qinshan nuclear stations, mainland China.

The criteria on a trip monitor are different to that of a risk monitor where the Probabilistic Safety Assessment (PSA) using Fault Tree and Event Tree analysis constitutes the basis and can as such be readily used for the purpose. A trip monitor requires building a new Fault Tree and Event Tree model with focus on representing availability for systems required for production.

In China, a lot of work in reducing the frequency of unplanned shutdown has been done. These efforts are carried out from a qualitative point of view, but there is little work to assess the risk of unplanned shutdown from a quantitative point of view.

With this background, CNNP and LR developed a trip monitor for Qinshan II, the first application in China to evaluate the risk of trip for a nuclear power plant from the point of view of quantitative analysis. The work includes software development, model development and verification of the rationality of the results.

1. BACKGROUND

Nuclear power plants can be divided into two parts:

- Nuclear Island: including reactors, safety systems, nuclear auxiliary systems, etc.
- Conventional island: including steam turbine and its auxiliary system, water supply system, power generation system, electricity transmission system, etc

The corresponding power loss of nuclear power plant comes from two aspects, nuclear island-reactor shutdown and conventional island-turbine trip. Shutdown means the loss of steam supply, so reactor shutdown will inevitably lead to turbine trip.

The nuclear island reactor is mainly controlled from the point of view of nuclear safety. If the parameter exceeds the safety limit, the reactor will be shut down to ensure nuclear safety. The conventional island is the same as the conventional power plant, from the point of view of equipment protection, once the parameter exceeds the limit, the steam turbine generator set trip.

For nuclear power plants, reactor shutdown and turbine trip will lead to power loss, affecting the economy and performance indicators of the power plant. In addition, due to the particularity of the nuclear power plant, the restart process of the unit after shutdown is more complex and longer than the conventional power plant. Therefore, for nuclear power plants, unplanned shutdown is required to avoid as much as possible. For this reason, nuclear power plants have done a lot of work to reduce the frequency of unplanned shutdown and trip. These works are mostly from the perspective of qualitative analysis, while the quantitative risk assessment is very little.

Under this background, Qinshan Nuclear Power Plant, taking Unit 1 of the second phase project as the example, has carried out the research of Trip Monitor, the first quantitative risk assessment tool for shutdown of nuclear power plant in China for a period of 4 years. The research draws lessons from the PSA Risk Monitor method, refers to EPRI guideline 1008121 Generation Risk Assessment Plant Implementation Guide [1]. The plant trip models are developed in RiskSpectrum PSA and Trip Monitor is implemented in RiskSpectrum RiskWatcher platform. At present, Trip Monitor has been used for the plant production planning and operation to evaluate the risk of reactor shutdown and turbine trip

In this paper the Trip Monitor function and user, interface, background model, the verification of the rationality of the results and the application to the equipment management.

2. THE TRIP MONITOR FUNCTIONS AND ITS USERS

The Trip Monitor is used to quantitatively evaluate the risk of shutdown and trip in nuclear power plants. The function mainly includes six aspects:

1. Calculation and display of quantitative risk of unit shutdown and trip, including current risk and historical risk.
2. When an equipment is out of operation, the system status display directly or indirectly affected by it.
3. Sometimes a single failure of equipment of the unit, will not lead to trip, but the superimposed failure of equipment will cause shutdown or trip. Therefore, the second and most important function of Trip Monitor is to identify which equipment must be available when one or more equipment are unavailable, otherwise the superimposed failure of equipment will cause shutdown or trip. A more typical example is shutdown logic 2/4, where there are four related instruments. When one instrument is not available, the other three must be available, otherwise 2/4 logic triggers the shutdown. The Trip Monitor can automatically identify these three instruments.
4. When multiple equipment are unavailable, the priority of equipment recovery is given, that is, which equipment should be restored to be available first and which equipment can be restored later.
5. Automatically identify the daily production plan and give the total shutdown/trip risk of the planned unavailable equipment, and equipment and give a list of equipment that must be available. Provide decision support for planner and operator.
6. Provide browsing function for each page of Trip Monitor.

2.1. Users

Corresponding to the function, the users of Trip Monitor are divided into three categories: MCR operators, daily production planners and other employees of the power plant. The authorities and responsibilities of the three categories of personnel in Trip Monitor are as follows:

1. MCR operators:

   Through the Trip Monitor it is possible to intuitively understand the downtime risk caused by the current equipment failure and maintaining equipment of the power plant.
2. Input equipment defects in Trip Monitor, quantify the risk, and identify the devices that need to be paid attention.
3. Daily production planner
    1. Input the daily plan (three-day upcoming plan), assess the shutdown/trip risk of the planned work, and the equipment to focus on.
    2. Adjust the plan according to the analysis results.
4. Other employees of the power plant. Browse the Trip Monitor web pages to understand the risk of the units.

3. THE TRIP MONITOR INTERFACE

3.1 The Risk Graph

Figure 1. Quantified shut down risk

In Figure 1, the Operator screen of RiskSpectrum RiskWatcher is shown with three measures highlighted:

1: Shutdown/trip risk. In this case, the shutdown/Trip risk is 1.72E-04, its unit is times per hour. If converted into a year, it is 1.507 times per year, that is, under the current unit system configuration, the risk of shutdown/trip in one year is 1.507 times.

2: In this field the current level of Trip risk is indicated. In this case, the risk is medium. The risk level of Trip Monitor is divided into three levels, high, medium and low, corresponding to red, yellow and green respectively. For different risk levels, power plants have different countermeasures and management requirements.

3: Identify the changing trend of unit risk over a period of time. As can be seen from the picture, from 10:47 on March 6th, due to the equipment out of operation, the risk of the unit has increased slightly. The equipment has not been restored so the risk persists.

3.2 System state view

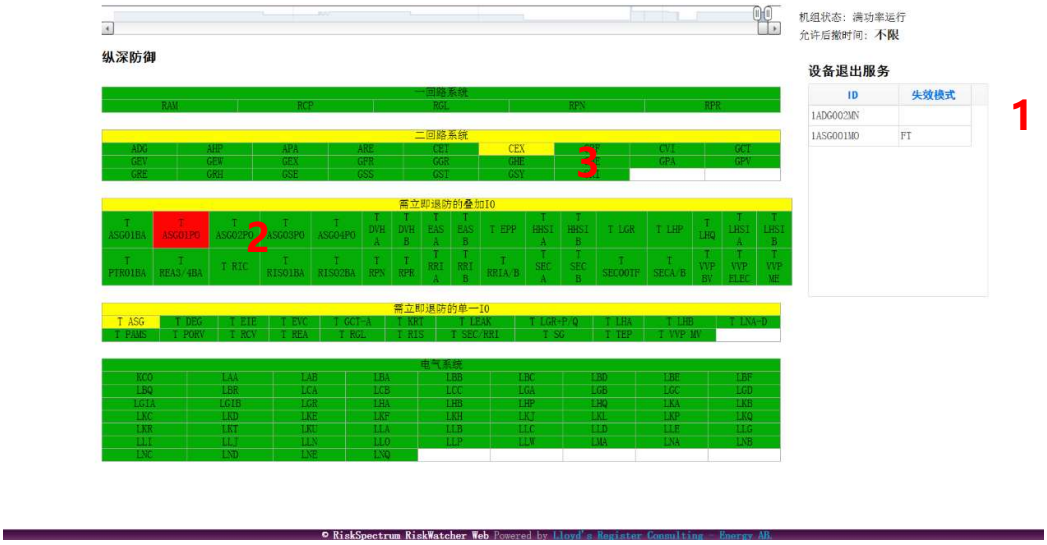

Figure 2. The system state diagram

The system state diagram shows the state of systems related to shut down indicated by the colours red, yellow and green. The state diagram includes a primary loop (nuclear island) and a second loop (conventional island) and an electrical system. In addition, it also contains the requirements in the operation technical specification for the operation of the nuclear power plant, including "……Superimpose I0"and "……Single I0" two modules.

Due to the particularity of nuclear safety, nuclear power plants have strict regulations on equipment availability related to nuclear safety, and corresponding requirements will be made when the equipment is not available. Some of these requirements will force the unit to shut down manually when some equipment is not available in order to protect nuclear safety. These requirements are expressed as I0. The two modules of I0 in the figure above are equipment related to forced manual shutdown.

In Figure 2, a System State Diagram of RiskSpectrum RiskWatcher is shown with three measures highlighted:

1: Indicates the equipment that is unable to perform its functions normally due to maintenance/tests or defects. In this example, two equipment are out of operation 1ADG002MN and 1ASG001MO. The former is the water level gauge of the deaerator in the water supply system, which is involved in controlling the opening of the regulating valve of the condensate water system (CEX system). If the water level gauge is out of operation, it will affect the control of the condensate water flow, and there is a potential risk of shutdown. The latter is the motor for the auxiliary feedwater system (ASG system) electric pump, the failure of which will render the corresponding pump unavailable. The ASG system does not directly participate in the operation of the unit, and its system failure will not directly lead to the shutdown of the unit. However, the ASG system is one of the special safety systems to nuclear power plants, which affects the cooling of the core after an accident in the nuclear power plant, so it has high requirements for the availability of its system. Only one ASG electric pump is unavailable, and the unit will not be forced to shut down. But if there are other ASG pumps at the same time, or some other nuclear safety-related equipment is unavailable, the stacking of unavailable equipment will force a shutdown.

2: T ASG001PO has become red, as an effect of that ASG001PO is unavailable due to ASG001MO unavailable, and related I0 takes effect.

3: CEX has become yellow, as an effect of that ADG002MN is unavailable, which affects the normal performance of the system's functions.

3.3 Equipment importance

Figure 3. The equipment importance view

The equipment importance view includes two parts: "Risk Increase Factor (RIF)" and " Restoration Worth Factor (RWF)". The "RIF" indicates, in the current configuration and equipment availability/unavailability, the factor with which the available equipment would increase the risk for shut down if they were made unavailable. The "RWF" indicates which of the equipment that are out of service, at the moment, should be restored first.

1: Due to that equipment 1ASG001MO and 1ADG002MN are out of service, the equipment in the list has a RIF factor of a very high number, i.e. must be available in order to prevent the unit from shutting down automatically or manually

2: When the equipment 1ASG001MO and 1ADG002MN are out of service, 1ASG001MO should be the first one to restore, i.e. would reduce the risk for shut down slightly more than compared to 1ADG002MN

4. THE TRIP MONITOR MODEL

The RiskWatcher Trip Monitor interface is the where the human-computer input and output of information takes place. The calculation of results is realized through the shutdown/trip model linked to the application.

The shutdown/trip model is represented in fault trees, using shutdown/trip as the top event, and systems, equipment and instruments will be deduced and analysed step by step from top to bottom, to identify the condition that will cause shutdown/trip. In Figure 5, below is an example of a system fault tree with one subtree.

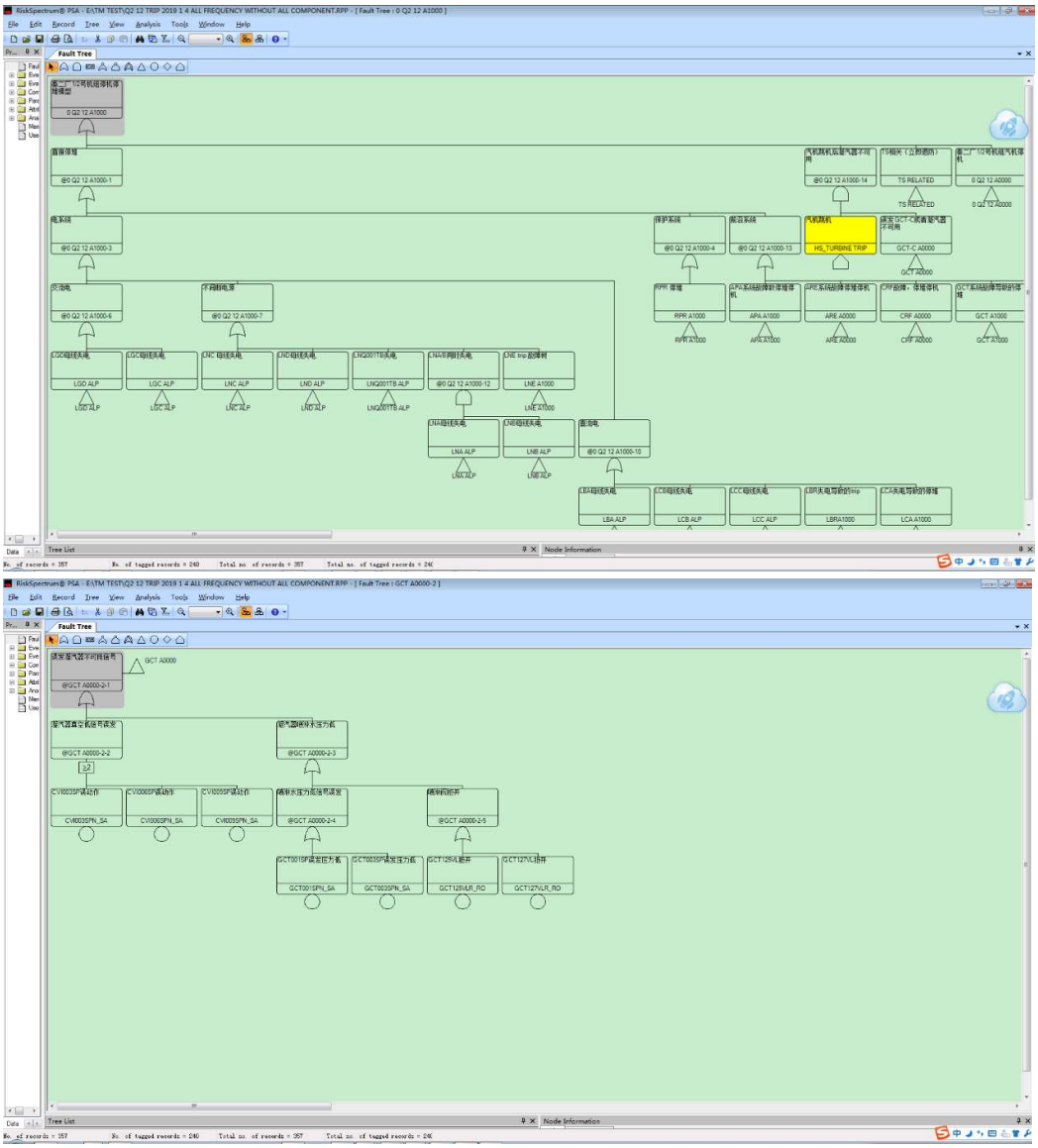

Figure 4. Fault trees representing faulure of systems that can cause Shut down/trip

4.1 Fault tree modelling

The fault tree model was realized by 7 Main Control Room engineers of which 2 had prior experience in Fault tree modelling. The whole project, without any reference model, took 4 years to develop following American EPRI GRA guidelines.

In order to ensure the correctness of the model, a large number of data have been consulted in the process of development. including: system flow chart, system operation manual, relevant operation procedures, power plant operation technical specifications, system logic diagram, primary wiring diagram, secondary wiring diagram, some equipment ex-factory data, relevant historical modifications, relevant historical condition reports and defects of each system.

Before the fault tree is built, the development team carries out FMEA (failure mode impact analysis) on every equipment in the system related to shut down.

In order to find suitable reliability data for the equipment in the model, all the relevant maintenance records of the target unit are specially collected, evaluated and the reliability data of the equipment are generated. In addition, for nuclear island equipment, the relevant reliability data used in the PSA model is used. For some equipment without available data source, engineering judgment is used to derive the reliability data.

5. VERIFICATION OF RESULTS

The core of Monitor is the shutdown/trip model. Whether the model is reasonable and whether the result is credible is verified from two aspects:

1) Is the result of risk quantification reasonable?

According to the operation history of the target unit, the average unplanned shutdown frequency from 2012 to 2018 is 1.14 times per year. Using the trip model in RiskWatcher the trip risk was 1.30 times per year. Power plant operators was asked to comment on the results, based on the operation experience, and they affirmed that the results were reasonable and slightly conservative.

2) Is the equipment identified by the model reasonable?

This was evaluated from two aspects:

a) The shutdown events of similar units (M310 units) in China from 2002 to 2018 were compared and analyzed. There had been a total of 53 shutdown events, of which 35 events was identified in in RiskWatcher. The reasons for the other 18 events which were not included in the model are:

- 5 events are not relevant because of design change and improvement
- 11 events are not in modelling scope (e.g., pipe break, software failure, human error, design flaws, etc.)
- 8 events are not represented in the model, which lead to later model update

b) Ranking of equipment importance

Random sampling tests was carried out for the equipment in the model, and the calculated equipment importance is in line with the operation experience and design logic. At the beginning of the test, a lot of model errors were found. The error was analyzed and corrected.

Through the above verification, it was believed that the rationality of the model and the credibility of the results were relatively high.

6. EQUIPMENT MANAGEMENT APPLICATION

The Trip Monitor model is one big fault tree. Except the calculation of the risk of shutdown/trip,and the RIF/RWF mentioned above, the cutsets are used as the input of the SPV equipment and temporary SPV equipment.

SPV equipment are equipment which failure will force the unit to shutdown/trip. Temporary SPV (T-SPV) equipment are equipment which failure does not lead to trip, but superimposed with other failure equipment will force shutdown/trip. For the trip model, the first order cutsets are corresponding to the SPV equipment. The second order cutsets are T-SPV.

The common method of SPV/T-SPV equipment identification is FMEA. The FMEA method is suitable for SPV equipment identification, but not suitable for T-SPV. The T-SPVs are difficult to identify using FMEA methodology, especially for equipment that are in different systems. The Tripmodel however is based on the deduction method using Fault trees makes it suitable for T-SPV equipment identification.

Using the trip model in RiskWatcher, about 20 new SPV equipment and 1032 new T-SPV equipment were discovered. The results have been analysed and confirmed by the equipment management department.

7. SUMMARY

The paper gives a comprehensive introduction to TripMonitor. At present, TripMonitor has been online in Qinshan Nuclear Power Plant, and the main users are production planners and main control operators. In combined with the work of equipment reliability management in nuclear power plant, the depth of Trip model will be deepened from the current equipment level to the possible component level to improve the quality and application in the future.

References

[1] EPRI 1008121. *"Generation Risk Assessment Plant Implementation Guide"*, (2004).