Risk-Informed Review of Actual Maintenance Strategy at Paks NPP

Tibor Kiss[a], Zoltan Karsa[b]
[a] Paks NPP, Paks, Hungary
[b] NUBIKI, Budapest, Hungary

Abstract: A common pilot project was launched in April 2010 by the Hungarian Atomic Energy Authority (HAEA) and the Paks Nuclear Power Plant (Paks NPP) with technical support from NUBIKI Nuclear Safety Research Institute to enhance existing, and implement new Risk Informed Decision Making (RIDM) practices. In the framework of the project Risk Monitor (RM) was utilized, and risk-informed review of maintenance at Paks NPP was performed. Based on the operators' electronic logs information and using the Risk Monitor tool the annual risk profile of historical performance of the units could be visualized. Altogether 16 reactor-years risk profiles have been created including the operation and shut down operation modes. Later these risk profiles served as a basis for further assessment of recent maintenance strategy and formulating findings and recommendations. According to the existing regulation no preventive maintenance of the safety related SSCs is allowed during power operation. The investigation went into two directions. The first one is the risk-informed examination of the online maintenance of emergency diesel generators (DGs). As a result of this investigation it could be demonstrated that online maintenance of the DGs would reduce the annual cumulative risk and, at the same time, may result in economical benefit due to the potential reduction of the outage time duration. The aim of the second direction of investigation was to reduce risk by means of changing the actual maintenance strategy. Assessing the annual risk profile risk areas with an unavailable safety train could be identified during power operation due to the twin unit outage. Such a risk area can be explained by the design of the service water system, having common parts for two units. The outcome of this investigation was a recommendation to use the given unavailability timeframe to perform the maintenance of the components already unavailable including the related DG as well. Fortunately, at the end of the pilot assessment, the above mentioned activities could be harmonized and a new complex maintenance approach could be formulated motivating the licensee to operate more safely and more economically at the same time.

Keywords: PSA, Risk Monitor, Risk-Informed, Online maintenance

1. INTRODUCTION

Paks NPP is the only nuclear power plant in Hungary, running four VVER-440-213 type reactors with 500 MW electrical output each. The units started their commercial operation at the beginning of 80's. The operation and maintenance practice and the associated regulation practically remained unchanged, it reflects the safety philosophy of those times. Since the beginning of early 90's a very intensive safety assessment program has been lunched to evaluate the existing safety level of the plant. Information gathered from the safety assessment reports were used as a basis for several safety upgrading measures. In addition to the traditional deterministic evaluation, several new assessment techniques e.g. Probabilistic Safety Assessment (PSA) were applied. PSAs of comprehensive scope and significant depth have been completed and implemented for the Paks NPP. The PSAs analyze internal postulated initiating events (PIEs) including internal initiators and internal hazards (fire and flood) and external PIEs including seismic hazard. The PSAs address Level 1 and Level 2 for full power and shutdown modes of operation for all four NPP units. The major part of these models has already passed several internal and international reviews. Living PSA models provide a good basis for implementation of RIDM in Hungary. Nowadays high attention is paid to implementation of Risk Monitor at the Paks NPP. Understanding the important role of this tool in the safety and efficiency of the plant operation and maintenance, implementation and use of the RM became one of the strategic goals for the plant. In the framework of a RIDM pilot application the existing operational performance of the units from the point of view of safety and economic efficiency have been evaluated. Based on the findings a generally new maintenance strategy was formulated for the plant. This new maintenance

strategy promises benefits both for the overall safety and the economic efficiency of the plant. The paper presents the key elements of the assessment process and introduces the set of rules applied for the new maintenance strategy.

2. DESCRIPTION OF THE PRESENT REGULATION AND MAINTENANCE PRACTICE

2.1. Actual regulation

According to the existing regulation, no scheduled preventive maintenance activities are allowed for safety related SSCs during power operation. Only corrective maintenance of the failed component is allowed for a limited duration of time. In case if repair of the failed component expires this allowed outage time (AOT), the unit must be shut down. General value for AOT is common for different safety components and limited to 24 hours.
According to the regulatory requirements, in case if any technical and/or administrative modification related to the operation or maintenance is planned, its effect (positive or at most neutral impact on safety) must be demonstrated. Regulation in some countries allows to have a so called "allowed risk increase value" during power operation. Based on this value, the AOT and the time duration for online maintenance of the safety related components could be derived. Due to the lack of such an allowed risk increase value in the Hungarian regulation, different approach was used for establishing the possibility for the online maintenance. This new approach will be introduced in this paper.

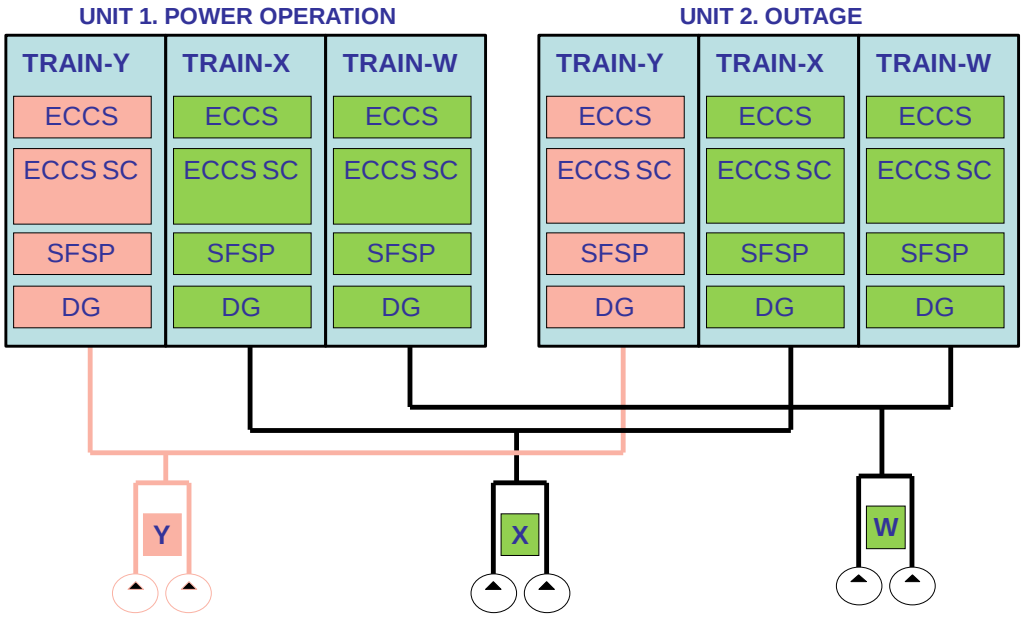
2.2. Actual maintenance practice, unavailability of safety systems

As it was described above, at present no online maintenance activities are allowed during power operation. All maintenance activities of the safety systems and components are performed during the refueling outage. Unit outages are scheduled sequentially, normally only one unit is in shutdown mode at once. Each unit has three identical (designated as Y, X, W) safety trains with 100% redundancy. This means that according to the design, one successfully operating train is sufficient to cope with the design basis accidents. According to the present practice all the three safety trains are maintained during each refueling outage sequentially. The average maintenance of one safety train takes 5-6 days and this duration is dominated by the diesel generator maintenance activities. Supposing a hypothetical case of not performing the DG maintenance, this 5-6 days unavailability duration of the safety train could be reduced down to 3 days! The maintenance of the safety trains has a high influence on the total duration of the outage, these activities are on the so called critical path in the maintenance schedule. Reduction of the maintenance length of the safety trains thus could result in the reduction of the outage duration in total. Naturally, the licensee is fully interested in the reduction of outage duration because of its economical interest.

In addition to the unavailabilities of the safety trains due to preventive maintenance during outage, there is another type of unavailability of the safety trains that is of a plant specific nature. It is related to the maintenance of the Essential Service Water System (ESWS). To understand the importance of and the unavailabilities caused by this system a short technical description follows. ESWS cools several important safety components like DGs, Emergency Core Cooling System (ECCS) pumps, ECCS Sump Coolers (SC), Spent Fuel Storage Pool (SFSP) etc. The units were designed in "twin units" concepts, which means that units 1 and 2 - similarly units 3 and 4 – have some shared systems like ESWS. Water taken directly from the Danube river is charged into the common ESWS discharge line. This common discharge line branches off and both units have their own separate ESWS lines distributing cooling water between consumers. This construction is the same for all the three redundant ESWS trains. The schematic of the ESWS and its consumers is presented in Figure 1. Maintenance of the common ESWS line (presented in pink in Figure 1.) is allowed when one of the twin units is shut down and the other is in power operation mode. In this case the operating unit runs with only 2 instead of 3 available safety system trains due to unavailability of one ESWS train. The risk increase caused by unavailability of one ESWS train is limited to 5 days/system/unit/year by the Technical Specifications. Considering all the 3 ESWS trains per unit, the total allowed "one train

unavailability" per unit during power operation is 3 x 5 days = 15 days altogether. This number is doubled due to the twin unit unavailabilities (the same unavailability configuration is allowed when the other unit is shut down), so the total allowed "one train unavailability" duration is 30 days. Thus, according to the present regulation, a 30 days timeframe is allowed for the state, when one of the twin units runs with reduced safety capabilities.

Figure 1: ESWS for twin units



3. RISK ASSESSMENT OF THE NEW MAINTENANCE STRATEGY

3.1. Information and tools

As a first step of the review, all the necessary information regarding the existing maintenance practice, actual regulation and system unavailabilities were gathered. In the second phase of the project the risk associated with the unavailabilities were evaluated and, based on the available assessment tools, the basics of a new maintenance strategy were laid. During the elaboration of the new strategy the principle of Risk-Informed Decision Making Process was followed [1]. This paper presents only the risk considerations of this process. For the purpose of risk evaluation the PSA and RM tools were used. As it has already been described above, PSA analyses of comprehensive scope and significant depth were available for the Paks NPP. RM is a relatively new tool for Paks, but as it will be shown below it is a very powerful tool in the risk evaluation process.

3.2. Risk assessment of the present and proposed maintenance strategies

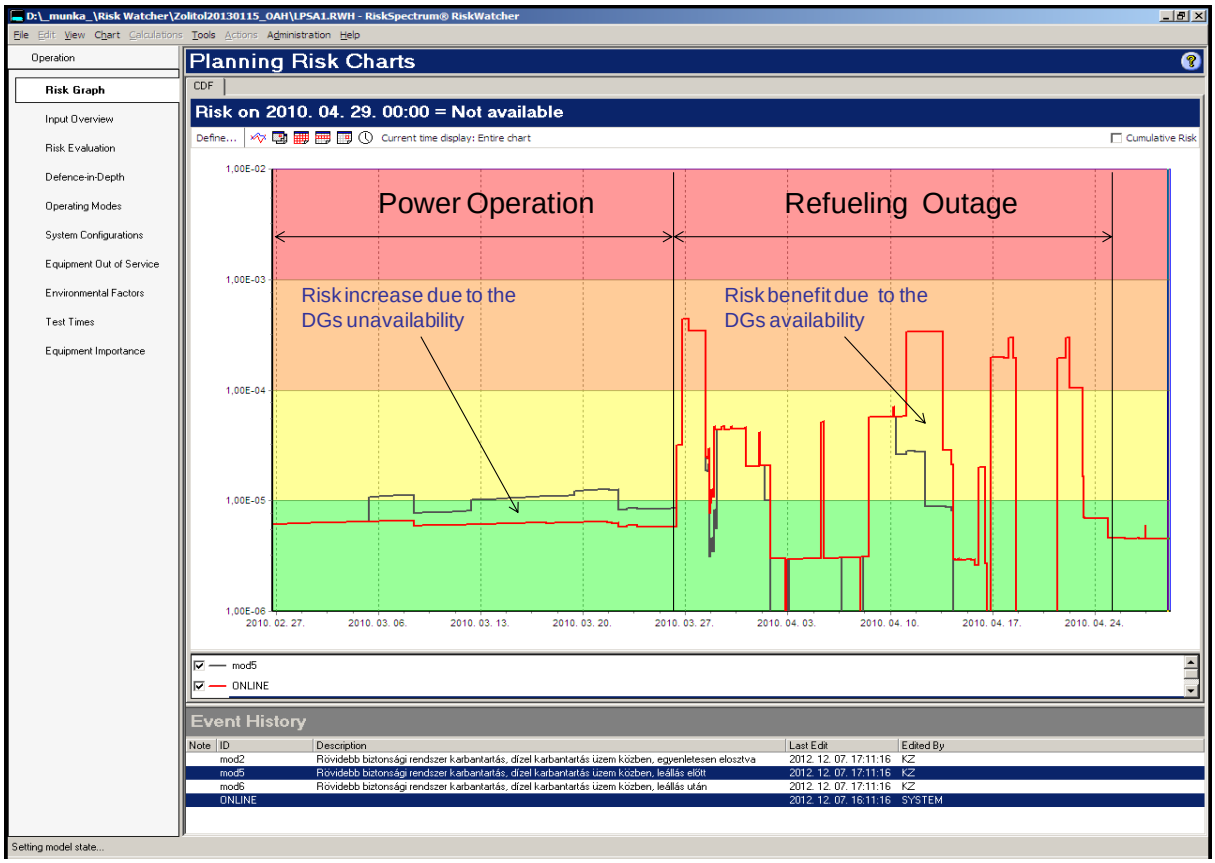
During the review of annual performance of SSCs regarding the unavailability, two major areas were identified. The first area is connected to the preventive maintenance activities of the safety systems during refueling outages, the second area is related to the ESWS unavailability during power operation. In the second case the unavailability is induced by the unavailability of the ESWS common line, when the twin unit is shut down. In the next 2 paragraphs the basic concept and assessment approaches related to the DGs and ESWSs online maintenance will be introduced.

3.2.1. Diesel generator online maintenance

Based on the operators' electronic logs information and with the help of the Risk Monitor tool the annual risk profile of historical performance of the units could be visualized. Altogether 16 reactor-

years risk profiles have been created including the operation and shut down operation modes. According to the maintenance schedulers information the 16 reactor-years historical data were modified hypothetically in such a way that the time windows of the preventive maintenance of the DGs was relocated from outage period to power operation mode. Loading this information into the RM, it was possible to compare the original risk profiles with the hypothetical ones (DGs online maintenance). The evaluation of the yearly risk profiles shows that additional risk increase appears when DGs become unavailable during power operation and risk reduction can be observed during outage, when unavailability of safety trains become shorter. These risk profiles are presented in Figure 2.

Figure 2:Risk profiles with different DG maintenance schedule



The risk balance of the risk increase and risk reduction effects in the different operational modes determines the final, cumulative effect on risk. The comparison of the annual cumulative risks easily provides this information. All the 16 reactor-years of operational experience was modified hypothetically and the results demonstrate that DG online maintenance has a positive impact on the safety, i.e. annual cumulative core damage probability decreased in all cases. Sensitivity studies were performed in two directions. In the first case the sensitivity of the results against the online scheduling time was verified. It was shown that changing the DG online maintenance schedule during the campaign does not change the positive outcome. In the second case the duration of DG online maintenance was varied between 7 and 10 days. The results of the investigation showed that extension of DG unavailability due to online maintenance up to 10 days is still acceptable and does not change the positive effect of the DG online maintenance. It is noted that 3 safety trains multiplied by this value gives 30 days of operation in this mode. This 30 days timeframe is one of the key elements of the new strategy and it is reflected in the proposed set of rules as “DG-30” rule.

3.2.2. New preventive maintenance strategy for the ESWS and its consumers

In paragraph 2.2 above the unavailability and the associated risk due to the maintenance of the common part of the ESWS was described. As it was explained, the case when one of twin units operates with one unavailable system has a duration of 2 units x 3 ESWS train x 5 days = 30 days. According to the existing Technical Specifications this risk increase is acceptable. From the point of view of risk there is no difference between the cases when the component is unavailable due to either the support system's unavailability (e.g. service water) or because of preventive maintenance. The question could be raised why not use the given (allowed) ESWS unavailability for maintenance purposes. Most likely the answer is that the 5 days portions are too short to finish the preventive maintenance activities on a safety system train with high confidence. According to the existing regulation exceeding the 5 days limit means that the operating unit must be shut down. In such circumstances the licensee is not encouraged to do any preventive maintenance activities during power operation. The possible solution to motivate the licensee would be the cancellation of train level limitations and having a common 30 days "risk credit" that could be used and distributed freely between safety system trains. Paks units have practically identical safety system trains (3 x 100% redundancy), which means that the actual safety level of the units is determined by the number of available safety trains. It is practically indifferent from the risk point of view, which specific train is really unavailable. For example risk increase caused by 5 days unavailability of safety train "Y" plus unavailability of safety train "X" for 3 days is equivalent to 8 days unavailability caused by "any" safety train unavailability (e.g. "Y"). Based on the above risk considerations it is proposed to use the 30 days risk credit without any prescribed subdivisions. PSA was used to evaluate the applicability of such an approach. The main benefit of this approach is that the plant may increase the overall safety and reduce the refueling outage duration at the same time without modifying the allowed 30 days "one train unavailability". This double positive effect can be explained by the following:

- The ESWS made already unavailable can be maintained during this unavailability. The risk associated with the preventive maintenance of ESWS during refueling outage may disappear, the system may be available during outage.
- Components supplied by the ESWS including DG may be maintained during ESWS unavailability. Thus safety system components may have longer availability during outage.

In addition to the positive impact on the safety this may have economic benefits as well due to reduction of the preventive maintenance work volume during outage, which may result in reduction of the outage duration. Realization of the above described approach in practice would be based on the following principles. Unavailability of ESWS common part could only be set up when both the twin units are in the power operation mode. One of the ESWS trains could be unavailable at once. During the unavailability of the ESWS on both units preventive maintenance activities of the ESWS components and of the components supported by ESWS could be started. Finishing the preventive maintenance on the system surveillance test would be performed and duration of the total unavailability of the train would be recorded and added to the cumulative time already spent on similar maintenance activities before. This cumulative time must be always checked against the time credit remaining from the 30 days/year. Preventive maintenance of the next ESWS train can only be started when all safety trains are available and there is sufficient cumulative time credit remained to finish the preventive maintenance.

3.3. Set of rules

For practical use of the above described approach a set of rules must be formulated which would serve as the basis for preparing the regulation documents and administrative actions. These rules have to consider the risk based limitations introduced earlier, and also the plant maintenance needs and possibilities. Before introducing the proposed set of rules some preconditions should be considered as follows:

- During online maintenance both the twin units must be in operation.
- The annual cumulative risk caused by the proposed online preventive maintenance of DG must not exceed the present value.
- The risk caused by the proposed strategy of ESWS unavailability during power operation must not exceed the recently allowed risk level derived from the recent regulation (2 units x 3 trains x 5 days/twins).
- Components supported by the ESWS should be maintained during the ESWS unavailability both technically and administratively as much as possible.
- DG and ESWS maintenance should be possible to separate in time.

Based on these preconditions, a set of rules was created making it possible to realize the proposed new online maintenance strategy. The set of rules consists of three major parts.

Rule №1 One DG unavailability status during power operation must not exceed 30 days/unit/campaign (Rule called: DG-30)

Rule №2 One ESWS unavailability status during power operation must not exceed 30 days/twin units/campaign (Rule called: ESWS-30)

Rule №3 DG must be considered unavailable when the related ESWS system is unavailable.

The explanation of Rule №1 comes from paragraph 3.2.1. It was demonstrated that the risk associated with the online maintenance of DG does not exceed the recent risk level associated with the DG maintenance performed during outage. The 30 days limitation refers to one unit. Rule №2 limits the risk caused by the unavailability of the ESWS during power operation and keeps it under the level allowed by the recent regulation. This rule is specific for a twin-unit and the cumulative time spent in this status must be recorded and controlled against the time left from the limiting 30 days. Rule №3 establishes the bridge between the first two rules. Availability of the DG is assumed when its supporting ESWS is available. This means that in case if ESWS system is unavailable (e.g. for the purpose of preventive maintenance) the allowed DG unavailability time is also running out (see Rule №1). For example, 10 days ESWS unavailability reduces the 30 days credit for ESWS (see Rule №1) by 10 days, and also reduces 30 days credit for DG unavailability time (see Rule №1) on both the twin-units by 10 days independently on whether the DG maintenance is performed during this time or not. Rule №3 thus motivates the utility to schedule DG preventive maintenance for the time when the ESWS is unavailable.

4. CONCLUSION

Risk-informed review of the actual maintenance strategy of Paks NPP has been shown. Based on the risk evaluation of the present maintenance practice, a new strategy could be formulated. For the new strategy it is fundamental not to exceed the present risk caused by direct or indirect unavailability due to preventive maintenance activities. For risk evaluation the PSA models and RM tools were used intensively. The new maintenance strategy was formulated in the form of a set of rules. This set of rules motivates the licensee to schedule maintenance of all ESWS related components for the time when the ESWS is unavailable. The proposed strategy motivates the licensee to optimize his maintenance schedule and promotes risk-informed thinking. Moving maintenance activities from refueling outage to power operation mode decreases the annual cumulative risk. In addition to the positive aspects on the annual risk, an economic benefit may be realized via reduction of outage duration time. Thanks to the set of rules established, the licensee may become motivated to enhance the safety of the plant which coincides with its economical interests.

References

[1] IAEA, A Framework for an Integrated Risk Informed Decision Making Process, INSAG-25, Vienna 2011, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1499_web.pdf