# RISK INFORMED UNAVAILABILITY MANAGEMENT (INTRODUCING BALANCE TIME INSTEAD OF AOT)

Tibor Kiss[1], Zoltán Karsa[2]

*[1] MVM Paks NPP Ltd.:H-7031 Paks, P.O.B.71, Hungary, kisst@npp.hu*
*[2] NUBIKI Nuclear Safety Research Institute: Konkoly-Thege Miklos str.29-33., Budapest, Hungary, 1121, nubiki@nubiki.hu*

*Thanks to several year systematic PSA development nowadays Paks NPP has a comprehensive picture of different potential risks related to the operation of the nuclear facility. Beside the normal full power and shut down operation modes, these risk assessment studies cover the risks associated with the unplanned, forced shut down modes, as well. Extensive knowledge of probabilistic aspects of the plant risks gives a good basis for changing the clearly deterministic based regulation into a risk-informed one. As a move forward with this process the new version of the Hungarian Nuclear Safety Regulation requests justification of Allowed Outage Times (AOT) for the safety related systems and components. Based on the risk-informed decision making principles a new method for the management of component unavailabilities has been introduced. Instead of the traditional "rectangle" method which has obvious deficiencies in determining AOTs a new risk-informed approach has been developed. The basic concept of the method is based on the comparison of risks associated with the possible ways of managing the situation caused by unavailabilities of safety related components. Basically, management of an unavailability is possible either by continuous operation of the unit with the parallel repair of the failed component, or by shutdown of the unit until the component restoration. The new method compares the risks associated with these possible solutions. Based on the risk importance of the failed component in full power and different forced shutdown plant operational states (POSs), and also information on the possible restoration time, the optimal risk-informed solution on unavailability management can be made.*

*The method was used for evaluation of components having limiting conditions of operation. A set of so called balance times were determined for these components. It can generally be stated that the results show the possibility of significant extension of limiting time condition for the components with no risk increase or relaxation. The method fulfills the requirement of the Hungarian Nuclear Safety Regulation on consideration of risks caused by shutdown and startup maneuvers of the unit in connection with the unavailability. The new approach will be applied in the revision of existing Technical Specifications and submitted for regulatory approval.*

*The new approach to managing risk associated with component unavailabilites fully fits the risk-informed decision making implementation concept for Paks NPP. The method supports the selection of the way with optimal risk to handle situations when safety components become unavailable. The advantage of the new approach in comparison with traditional ones is that there is no need for a predefined allowed risk increase value (e.g. CCDP<1E-6), instead, the optimal cumulative risk can be reached. Thus it can be applied in countries (like Hungary) where a predefined risk increase value does not exist in the regulatory requirements.*

## I. INTRODUCTION

The limiting time conditions of unavailability of components are prescribed in the Technical Specification (TS) for Paks NPP Hungary. These limitations are primarily based on either some past engineering judgment or maintenance capacity of the repair staff. According to the recently issued version of the Nuclear Safety Regulation, the limiting time conditions of the TS must be revised and established with the assistance of modern assessment tools. The determination method of the limiting condition times must consider the risks caused by the potential shutdown and startup of the unit. This is a difficult task due to the fact that the Hungarian Regulation neither defines nor allows the predefined risk increase value.

## II. METHODS FOR DETERMINATION OF LIMITING CONDITION TIMES

### II.A. Conventional Methods

The basis of the conventional unavailability management relies on the predefined risk increased value (e.g. CCDP<1E-6). The risk associated with the unavailability of the given safety component can be determined by a multiplication of the core damage frequency (ΔCDF) increment and the time elapsed. The traditional "rectangle" method (see Fig. 1) represents the Allowed Outage Time (AOT) as a ratio of the allowed risk increase against the CDF increment.

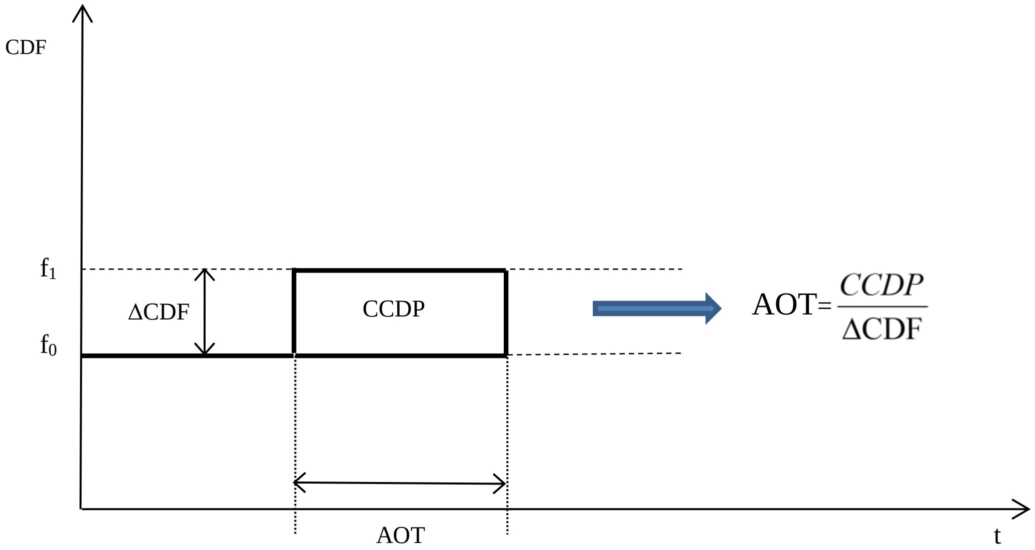


Fig. 1. Conventional determination of allowed outage time

Based on the significance of the components, the AOTs differ from component to component. The most important advantage of this method is the simplicity and relative easiness of implementation. These very facts explain its widespread application all over the word. Besides the advantages of this method, some deficiencies could be listed:

- The method requests the predefined allowed risk increase value. Nuclear regulation of some countries disowns such a value. Their reason for this is that the licensee must strive to minimize the operational risk all the time.
- It does not consider the shutdown and the startup risks of the unit.
- The decision made by means of probabilistic considerations in the past may change gradually over time, because the probabilistic values turn into reality, so the former probability assumption may become true or false. This means that the estimation and decision made at the beginning of the unavailability of the component may not match conditions at the time point when the AOT expires. (E.g. let us suppose the restoration of the component availability by the end of AOT is unsuccessful. According to the original decision the unit must be shutdown, however, if looked into the future the situation would be the same as it was when the failure was discovered. From risk point of view, in this case the shutdown of the unit cannot be verified.)
- Handling of multiple unavailabilities is a real challenge.

### II.B. Introducing the "Balance Time" Method

The method to be introduced now is based on the approach which aims at reaching a minimal level of cumulative risk caused by component unavailability. In case of random failure of the component, the risk of the possible interventions should be considered (e.g. transient risk due to change of Plant Operating State (POS)). According to the current TS, in case of expiration of the AOT the unit must be driven into the safer shutdown state. At the end of the component repair the unit will be restarted and will be driven back to the normal power operation. Fig. 2 shows the possible change of risk in general. The cumulative risk caused by the unavailability of the component could be understood as the territory below the risk curve between the time points $t_1$ and $t_5$. The cumulative risk i.e. the cumulative Core Damage Probability ($CDP_{Unav}$) due to the unavailability can be calculated according to the formula (1). As it can be seen from the formula, for determination of the cumulative risk in general we need the following data:

- CDF at the beginning (power operation) and final (target) shutdown POSs with the unavailable component.
- CDF at the shutdown transient POSs with unavailable component.
- CDF at the startup transient POSs with recovered component.
- Time durations in the transient POSs.

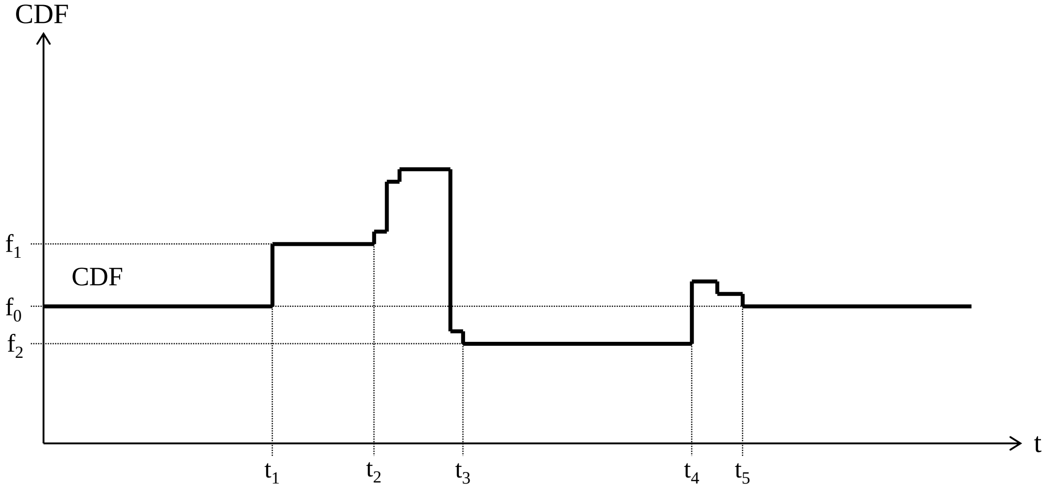


Fig. 2. CDF change due to the safety component unavailability

Notations of the Fig. 2:

- $f_0$ - Nominal CDF (power operational mode);
- $f_1$ - CDF in case of component failure (power operational mode);
- $f_2$ - CDF in shut down mode with the unavailable component;
- $t_1$ - Beginning time of the component unavailability;
- $t_2$ - The end of the allowed outage time, beginning of the shutdown ($t_2$-$t_1$=AOT);
- $t_3$ - Getting the target shut down mode (from $t_2$ to $t_3$ is the duration of the shutdown transient);
- $t_4$ - The end of the component repair, beginning the startup of the unit ($t_4$-$t_1$=$T_{repair}$, repair time);
- $t_5$ - Getting back to the power operation (from $t_4$ to $t_5$ is the duration of the startup transient).

$$CDP_{Unav} = f_1 \cdot AOT + \sum_{i=1}^{N_{SD}} f_{SD,i} \cdot T_{SD,i} + f_2 \cdot \left( T_{repair} - AOT - \sum_{i=1}^{N_{SD}} T_{SD,i} \right) + \sum_{j=1}^{N_{SU}} f_{SU,j} \cdot T_{SU,i} \qquad (1)$$

$N_{SD}$ – The number of shutdown transient POSs;
$f_{SD,i}$ – The CDF of the shutdown transient with the unavailability of the component in the POS named “i”. These POSs are represented between the time points $t_2$ and $t_3$;

$T_{SD,i}$ – Duration of the shutdown transient POS named “i”, $\sum_{i=1}^{N_{SD}} T_{SD,i} = t_3 - t_2$

$N_{SU}$ – The number of startup transient POSs;
$f_{SU,j}$ – The CDF of the startup transient with the recovered component in the POS named “j”. These POSs are represented between the time points $t_4$ and $t_5$;

$T_{SU,j}$ – Duration of the startup transient POS named “j”, $\sum_{i=1}^{N_{SU}} T_{SU,i} = t_5 - t_4$

Fig. 2 and formula (1) are only valid for the case, when the repair time of the component exceeds the AOT ($T_{repair}$>AOT). If the repair time is less than *the* AOT the shutdown of the unit is not considered. In this case cumulative core damage probability depends on the beginning POS and can be calculated by formula (2):

$$CDP_{Unav} = f_1 \cdot T_{repair} \qquad (2)$$

In general the beginning and the target (safe shutdown) plant operating states should be considered as a variable and they determine the transient POSs. Furthermore, during the evaluation, the AOT and the repair time ($T_{repair}$) are also considered as variables.

When the unavailability of the component or system occurs, there are two potential alternative actions that could be considered:

1. Further power operation with the parallel repair of the failed component or system
2. Shutting down the unit and driving to a safer plant operational mode. Following the component repair startup of the unit, it will be driven back to the power operation mode.

In case of the first option (power operation) after the component repair the risk level will be reduced to the nominal level $f_0$. In case of the shutdown option the shutdown and startup risks should be considered. According to the risk based decision principle the case with the smaller risk should be selected ($R_{Power}$ vs. ($R_{SD}$+ $R_{SU}$)). Decision made between these two options (further operation vs. shutdown) highly influence the component repair time. If the failed component can be repaired relatively fast, there is no reason to select the shutdown – startup option, because at the power operation mode - due to the short time - the accumulated risk is also small. In this case the risk is obviously less than in case of unit shutdown. The shutdown and startup processes always mean some extra risk due to the transient situation that have to be considered. Generally, with increasing repair time the shutdown - startup option tends to be seen more reasonable. It is obvious that there exists a certain repair time duration, when the risk of the two alternatives becomes equal. This time is named as “risk balance time” ($T_{balance}$). The determination of the $T_{balance}$ will be introduced by formula (3) by modifying the general formula (1). The left side of the equation represents the risk in case of power operation. On the right side of the formula we set the AOT=0 and instead of $T_{reapir}$ it is substituted with $T_{balance}$, because in case of AOT>0, the calculation of the $T_{balance}$ gives the overestimated value by AOT. This means the cumulative balance risk will not be minimal.

$$f_1 \cdot T_{balance} = \sum_{i=1}^{N_{SD}} f_{SD,i} \cdot T_{SD,i} + f_2 \cdot \left( T_{balance} - \sum_{i=1}^{N_{SD}} T_{SD,i} \right) + \sum_{j=1}^{N_{SU}} f_{SU,j} \cdot T_{SU,i} \qquad (3)$$

From the Eq. (3) the $T_{balance}$:

$$T_{balance} = \frac{\sum_{i=1}^{N_{SD}} f_{SD,i} \cdot T_{SD,i} - f_2 \cdot \sum_{i=1}^{N_{SD}} T_{SD,i} + \sum_{j=1}^{N_{SU}} f_{SU,j} \cdot T_{SU,i}}{f_1 - f_2} \quad (4)$$

For all components (included in the PSA) this risk balance time can be calculated. If the estimated actual repair time exceeds the calculated risk balance time value, the shutdown option will be preferable, because the cumulative risk of the shutdown - startup process is less than that of the power operation. Practically the risk balance time for all components could be calculated using PSA in advance. The balance time for the component can be calculated by the equation Eq. (4). For the calculation of the risk balance time the PSA model is needed for the power, administrative shutdown and startup operational modes. The administrative shutdown and startup operational modes can be different from the outage shutdown and outage startup. During the outage shutdown, there can be different tasks (e.g. decontamination), which are not performed in case of administrative shutdown. Also the durations of the similar actions can be different. These risk balance times for the safety related components could be introduced in the Technical Specification. The actual restoration time for the component is determined by the failure mode. For the best approximation of the repair time in the actual situation the involvement of the maintenance personal is preferable. If the approximated repair time is less than the predefined risk balance time, the restoration of the component is preferable by further operating the unit, otherwise the shutdown option would cause smaller risk increase. This approach is entirely different from the conventional determination of allowed outage time methods. According to the conventional approach the repair works start at the power operation, and in case of success it finishes in the time frame of AOT.

In case of extension of the repair works beyond the AOT the administrative shutdown of the unit is initiated. According to the balance time approach both the decision and the action are made immediately, either for the repair of the component with further power operation or for repair with immediate shutdown of the unit. The new method has the following benefits:

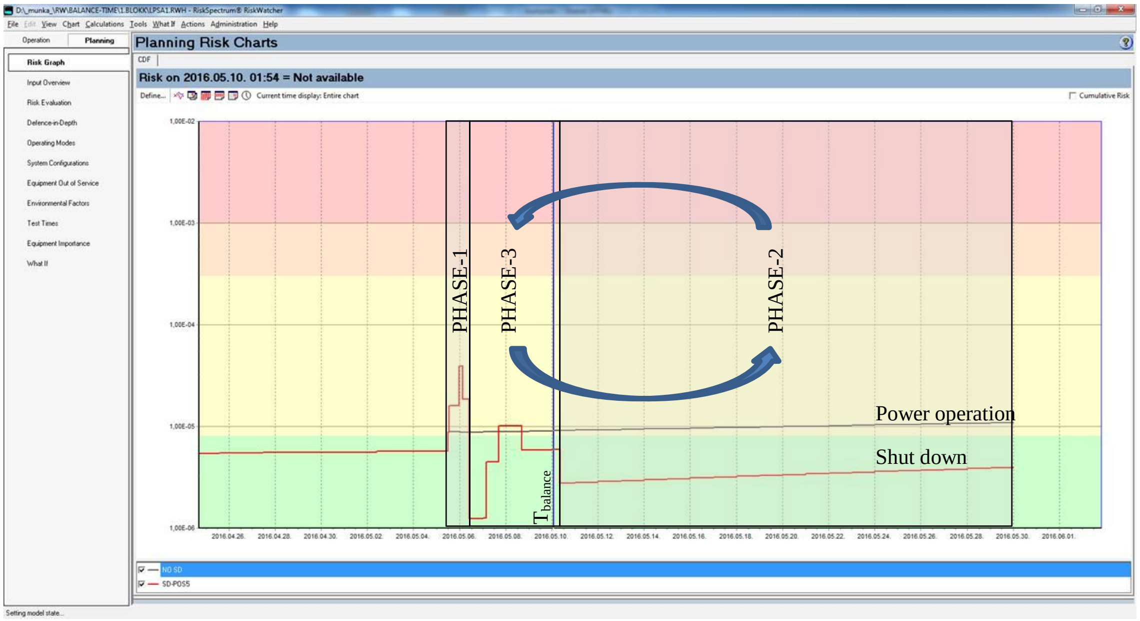
- The predefinition of the allowed risk increase is not needed, so the method can be used in countries where the regulator does not support the idea of allowed risk increase.
- The method considers the possible shutdown and startup risks.
- Based on the risk significance of the components, different risk balance times could be determined. These balance times are independent from the different subjective criteria, it depends purely on the component risk importance in different plant operational states.
- Different end states and alternative shutdown states can be examined (hot or cold shutdown states).
- The multiple unavailabilities can be handled.
- It can be used even in the shutdown state to select the safest plant operational mode in case a random failure occurs.

Critique of the balance time approach:

- According to the Paks NPP investigation the method causes AOT relaxation for all TS regulated safety components; the relaxation of AOT may consequently cause the relaxation of repair works intensity as well. So in order to keep the original repair intensity at the recent level some new measures should be considered.
- The method considers immediate action. In practice, some time is necessary for the diagnosis to evaluate the possible repair time.

### II.C. Integration of the “Balance Time” Method into the Risk Monitor

Risk monitor is a very efficient tool to control the actual risk and support the risk informed decision making in case of unavailability of the component. Most risk monitor softwares support the conventional determination of the AOT. For risk monitoring purpose the Paks NPP applies the RiskWatcher (RW) software tool (Lloyds Register Consulting product). It has been examined how this tool can support the above described risk informed decision making and what kind of additional feature of the software could support such an activity. In the so called “planning mode” the software is capable of evaluating the predefined event sequences in the future time points. The program also supports the evaluation of different alternative event sequences. For the determination of $T_{balance}$ we need the produce the cumulative risk curves of two alternatives (power operation vs. shutdown). At first, in order to produce those cumulative risk curves we have to prepare the CDF curves (see Fig.3). Producing the power operation risk curve is relatively easy. Only the failure of the component should be set and the unavailability as a function of time should be kept. Modelling of the shutdown case is more complex. It consists of 3 phases. The 1st phase is the shutdown transient. For the calculation of this phase the predefined transient shutdown POSs and their durations have to be called. POS times come from plant statistics of the administrative shutdowns. The risk of the 3rd phase “startup after repair” can be evaluated as to be similar to the 1st phase, the only difference is the unavailability/availability of the component considered. The 2nd phase is the safe end state (target POS), when the repair activities are finalized. The CDF of this POS is a function of repair time. The cumulative risk of the 1st and 3rd phases are constant, they do not depend on the time variable. For the interpretation of the cumulative risk function of the shutdown case it is reasonable to reorder these 3 phases and put the 2nd phase to the end. By this maneuver the result is not changed, it is simply the time dependent phase that will be the last one in the order, which helps in the interpretation of $T_{balance}$. Fig. 3 shows the reordered interpretation. Having the CDF curves of the alternative solutions the cumulative risk curves can be generated. This function is provided by the RW software. The intersection of the curves shows the balance of the risks and consequently the balance time can be read (see Fig. 4). This example below shows the failure of the emergency diesel generator. According to the calculations the balance time in this particular case expected as $T_{balance} \approx 5$ days. This means that if the estimated repair time is less than 5 days the repair works should be performed during power operation of the unit, otherwise ($T_{repair} > T_{balance}$) the shutdown of the unit would cause smaller risk increase. This pilot case showed that the risk monitor can potentially support the determination of the risk balance time for the actual, online situation. To make the evaluation more convenient we requested the RW software developers to extend the software with some new features.



D:_munka_\RW\BALANCE-TIME\1.BLOKK\LPSA1.RWH - RiskSpectrum® RiskWatcher

Planning Risk Charts

Risk on 2016.05.10. 01:54 = Not available

Current time display: Entire chart

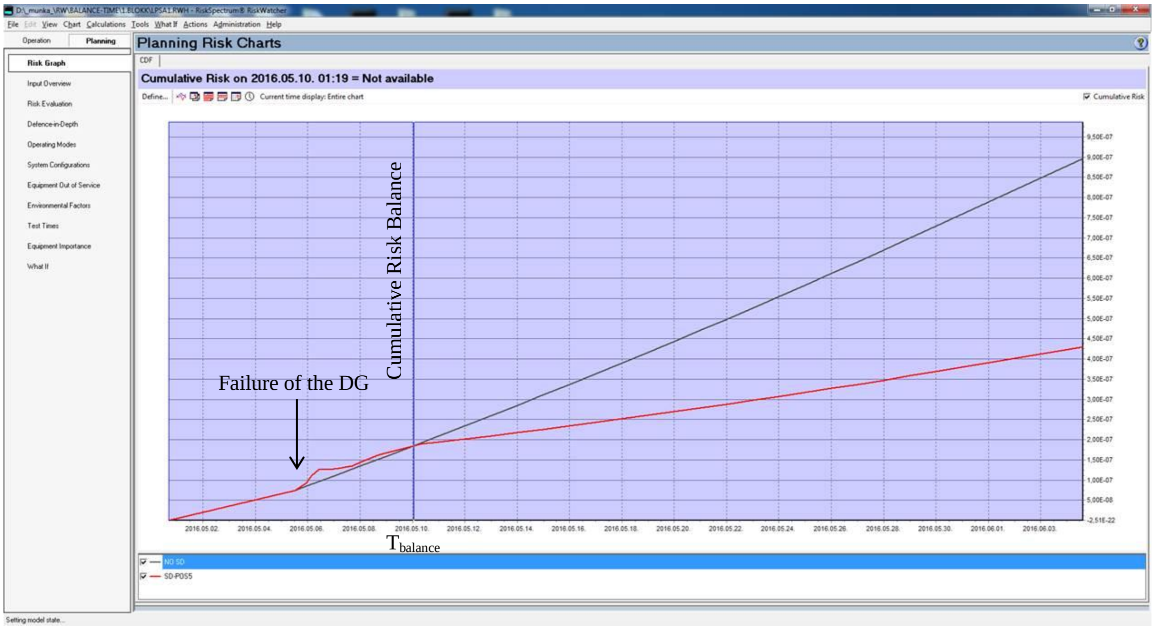
☐ Cumulative Risk

☑ — NO SD

☑ — SD-POS5

Setting model state...

Fig. 3. CDF of the alternative actions



D:_munka_\RW\BALANCE-TIME\1.BLOKK\LPSA1.RWH - RiskSpectrum® RiskWatcher

Planning Risk Charts

Cumulative Risk on 2016.05.10. 01:19 = Not available

Current time display: Entire chart

☑ Cumulative Risk

☑ — NO SD

☑ — SD-POS5

Setting model state...

Fig. 4. Determination of the $T_{balance}$ as an intersection of cumulative risk curves

## III. CONCLUSIONS

The above introduced method was developed to fulfill the Hungarian Nuclear Safety Regulation that requires justification of Allowed Outage Times (AOT) for the safety related systems and components. The main benefit of this approach is that it considers the risk of the potential shutdown and startup over further operation maneuvers, while it does not require any predefined allowed risk increase value. The method fits the ongoing implementation of the risk informed decision making program in Hungary. With some minor feature extensions of the risk monitor software this "balance time" concept could be a powerful tool in the risk informed decision making process.

## REFERENCES

1. Z. Karsa, A. Bareith, T. Javor, "Allowed Outage Time and Surveillance Test Interval Revision", Report No 222-336-00, NUBIKI (2014) (in Hungarian)