Risk-Informed Methodology for decision-making on Technical Specifications Allowed Outage Times

Stefan Authén[a*], Erik Cederhorn[a]
[a]Risk Pilot AB, Stockholm, Sweden

Abstract: This paper presents a methodology for risk-informed decision making on Allowed Outage Times (AOT:s) within a utility's Technical Specifications (TS). The developed approach combines traditional quantitative PSA-based approaches, e.g. based on NRC Regulatory Guide 1.177, [1], for evaluation of AOT:s with a qualitative risk analysis developed to ensures that the suggested AOT:s meets the licensing basis and fulfils deterministic requirements of the Safety Analysis Reports.
Keywords: Risk Informed Decision Making, Technical Specifications, Allowed Outage Times, PSA Applications.

1. INTRODUCTION

This paper presents a methodology for risk-informed decision making on Allowed Outage Times (AOT:s) within a utility's Technical Specifications (TS). The developed approach combines traditional quantitative PSA-based approaches, e.g. based on [1] and [2], for evaluation of AOT:s with an additional qualitative risk analysis.

The final AOT is decided by an expert panel evaluation, considering the results from quantitative and qualitative analysis together with any additional conditions and requirements, e.g. maintenance and repair aspects. Finally, an overall assessment of the total impact of the Technical Specifications (TS) changes on reactor safety is made. The complete process is shown in a simplified manner in Figure 1.

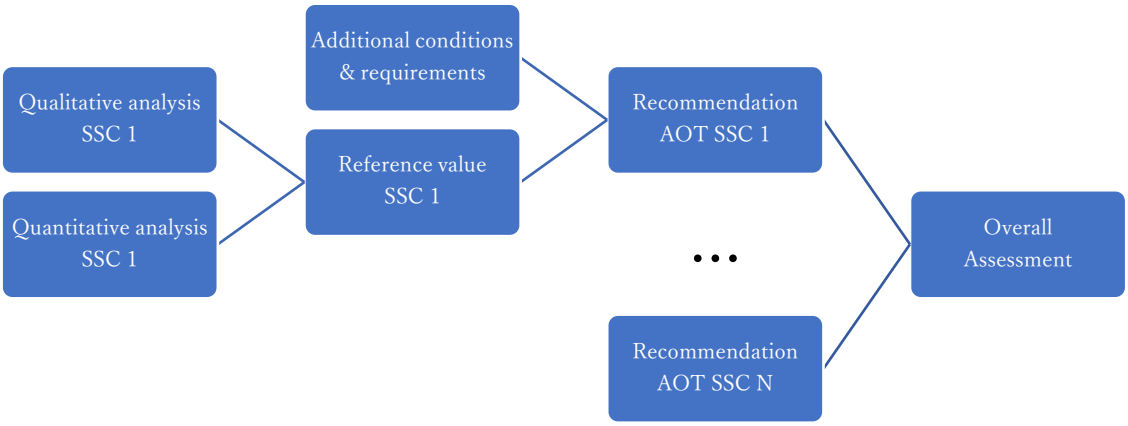

Figure 1. Complete process for the AOT risk-informed methodology

2. BASIC RISK INFORMED PRINCIPLE

The methodology is built based on two keywords: Systematics and Justification. With Systematics is meant that there shall be:

- Consistent rules for assessments
- comprehensive assessment rules,
- transparent decision logic (the reasoning),
- well-defined concepts and terms.

With Justification is meant that:

- The safety impact of the analyzed cases must be described in an understandable way, and
- every assessment must be justified.

The requirements in the TS are in general based on the principle that the fundamental barrier protections of the plant shall be available, i.e.:

- The barriers against core damage (CD barrier),
- The barriers against releases to the environment.

The TS additionally contains requirements to control events that leads to an increased risk for operational disturbances, i.e. initiating events.

In modern NPP designs these principles often are clearly linked to the different levels of Defense in Depth (DiD) and Safety Classification of the SSC:s and the system functions, while this seldom is the case for older NPP designs. To cover for the latter case, these principles can be illustrated by the simplified risk model of Figure 2. The risk model is developed for a Gen. II reactor design and has three main elements, where each element can be connected to plant condition categories, Defense in Depth levels and levels in the PSA. If there exists a safety classification of the system functions of the plant, the risk model should be adjusted according to that.

Figure 2. Simplified Risk Model.[1]

The developed methodology is based on principal Operational Readiness Requirements:

1. If a barrier protection is found to be completely missing, continued operation is not permitted.
2. If a barrier protection is found to be partially degraded, operation can continue for a certain period of time (repair criterion) depending on the degree of risk of the degradation.
3. If an increased risk of operational disturbances is detected, operation can continue for a certain time (repair criterion) depending on the significance of the risk of the disturbance and the frequency increase of the disturbance.

The first requirement is self-evident and is not addressed further in the paper. However, the developed qualitative and quantitative methods provide guidance on how requirements 2 and 3 should be interpreted in a consistent and systematic way. The defined limiting conditions in the TS are interpreted as rules to be applied when a SSC failure occurs which, directly or indirectly, affects one or more of the three elements of the risk model.

The methodology aims to provide balance between the AOT:s of the SSC:s covered in the TS, and realistically reflect the SSC:s risk significance and thereby improve general plant safety. The methodology is approved by the Swedish Radiation Authority and has been used to revise and implement new, balanced, AOTs for the complete TS of a Swedish BWR.

3. METHODOLOGY FOR QUANTITATIVE ANALYSIS

The methodology for quantitative evaluation is based on traditional methods using the PSA model to search for the “optimal” AOT given certain conditions and will hence only be briefly described in this paper.

[1] AOO: Anticipated Operational Occurrence, DBA: Design Basis Accident, DEC: Design Extension Condition

The developed method for calculating AOTs is mainly based on [1], which compares the risk of performing on-line repair with the risk of shutting down the plant and instead performing the repair at cold shutdown. The methodology is fairly straight-forward and uses the PSA model to calculate the risk contributions for the different plant states (power operation and cold shutdown). The different risk contributions is illustrated by Figure 3, [3].

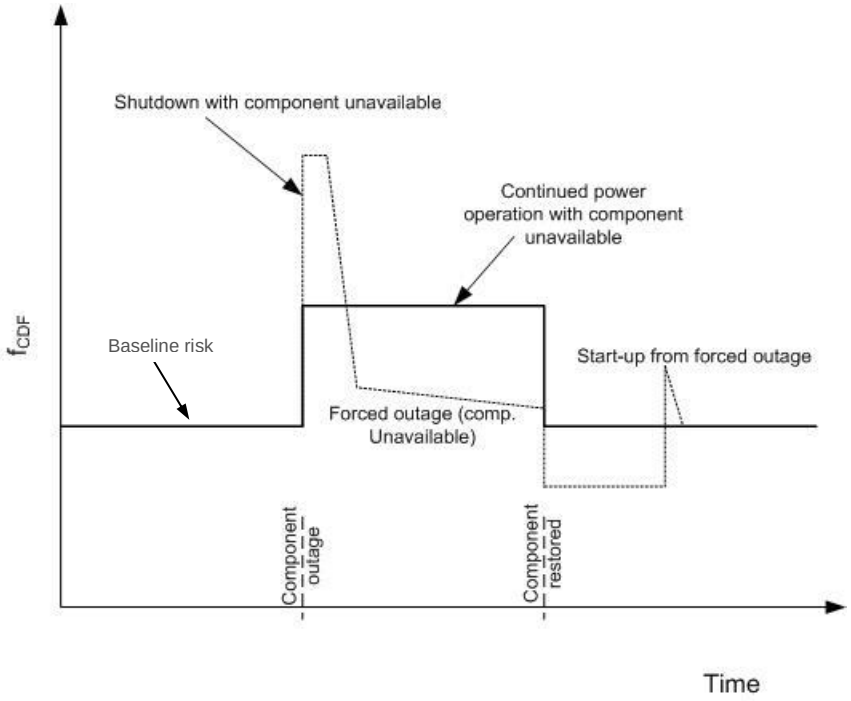

Figure 3. Example of two different risk curves: One represents the case of on-line repair and the other the case of forced shutdown and repair during cold shutdown (dashed line).

In addition to [1] the methodology takes into account the recommendations of [4] to calculate the AOT by using two different equations which reflects different aspects of AOTs. With this approach a reference range is given by the two equations, which can be considered as an upper and lower limit for the AOT. Both equations are based on the position that a reasonable AOT is achieved when the risk of on-line repair is equal to the risk of taking the reactor to a cold shutdown state and then perform the repair. The difference lies in the consideration of repair during power operation:

1. The lower limit of the AOT is calculated on the assumption that the AOT will always be fully utilized and if the repair action takes longer than the AOT, the plant will be taken to a cold shutdown state to complete the repair.
2. The upper limit is calculated on the assumption of perfect information on the required repair time, i.e. it is always known initially whether it will be possible to completed the repair within a given AOT or not. Optimal decision is hence always taken whether to repair on-line or at cold shutdown.

The range between the two approaches can be broad but is sufficient to detect anomalies in the TS.

Finally, the method accounts for safety improvements at a plant by introducing a parameter for acceptable risk increase, ΔP. The parameter is calculated as a percentage of the plants CDF safety goal, e.g. 1% of a safety goal of 1E-05/year. Provided that the actual plant CDF is lower than the plants safety goal, this risk increase is always considered as acceptable when performing on-line repairs.

3.1. Theoretical basis

The AOT lower limit is calculated by minimizing τ in the following equation:

$$\Delta P(x,\tau) = \Delta f(PO|x) \bullet \tau + (1 - G(x,\tau)) \bullet P(SD|x) \quad (1)$$

$$P(SD|x) = P(SDN|x) + f(SDA|x) \bullet t(x) + P(SDU|BAS) \quad (2)$$

Under the assumption of exponentially distributed repair time t(x) and a mean time to repair MTTRx the optimal AOT can be calculated as:

$$\tau\,(x) = \max \text{ w.r.t.x } \{-\ln(\Delta f(PO|x) \bullet MTTRx / P(SD|x)) \bullet MTTRx,\ \Delta P/\Delta f(PO|x)) \quad (3)$$

The AOT upper limit is simply calculated as:

$$\tau\,(x) = (\Delta P + P(SD|x)) / \Delta f(PO|x) \quad (4)$$

where:

$\Delta P(x,\tau)$ = Acceptable risk increase.
$\Delta f(PO|x)$ = Risk increase per time unit at on-line repair of SSC x.
$G(x,\tau)$ = Cumulative probability distribution for repair time $\tau(x)$.
$P(SD|x)$ = Risk due to forced shutdown, repair at cold shutdown and start-up given configuration x.
$P(SDN|x)$ = Risk due to forced shutdown with SSC x unavailable
$f(SDA|x)$ = Risk increase per time unit at repair during cold shutdown.
$P(SDU|BAS)$ = Risk due to start-up.

Note 1: If the risk per time unit at configuration x is larger at cold shutdown than at power operation it will always be optimal to perform on-line repair and the upper limit will be "infinite". In these cases formula (4) will underestimate the AOT.

Note 2: It is of high importance that all parts of the PSA model have a high, and similar, degree of realism, and that at unavailable SSCs no parameter, model or completeness uncertainties have unacceptable impact on calculated risk measures. All existing conservatisms and uncertainties in the PSA model shall be known and where necessary evaluated by sensitivity and uncertainty analyses. This is however not further addressed in this paper.

3.2. Analysis Steps

The following analysis steps are applied in the quantitative AOT methodology:

Step 1: Identify the analysis conditions, e.g. scope, PSA model and/or method adjustments needed in order to achieve realistic results, i.e. treatment of unacceptable conservatisms and uncertainties, SSC configuration aspects, e.g. equipment in operation vs. standby, treatment of correlation between the different operational modes, etc.

Step 2: Quantification of risk measures, e.g. $\Delta f(PO|x)$, $P(SDN|x)$, $f(SDA|x)$ and $P(SDU|BAS)$.

Step 3: Review the results (cut-sets and importance measures) and verify that no unacceptable conservatisms/non-conservatisms exists. If such exists, address them if possible and repeat step 2 until an acceptable degree of realism is achieved. If a significantly contributing conservatism/uncertainty (e.g. Fussel-Vesely> 1%) cannot be corrected then it should be evaluated in a sensitivity or uncertainty analysis (step 6).

Step 4: Calculate MTTR based on operational experience.

Step 5: Calculate lower and upper limit in accordance with equations (3) and (4).

Step 6: Perform necessary sensitivity and uncertainty analyses for identified uncertainties.

Step 7: Report the calculated lower and upper limit together with findings and conclusions from step 6.

4. METHODOLOGY FOR QUALITATIVE ANALYSIS

As the TS shall ensure that the facility is operated within the framework of the Safety Analyses Report the methodology is based on the safety functions and their success criteria given by the deterministic safety analysis. However, it should be noted that the methodology itself does not rest on deterministic grounds but on a qualitative and realistic assessment of the safety impact obtained when applying an AOT. There are several reasons to include a qualitative component into a methodology for evaluation of AOT:s:

1. To ensure that the suggested AOT:s meets the licensing basis and fulfils deterministic requirements of the Safety Analysis Reports.
2. To evaluate SSCs covered by the TS but not included in the PSA.
3. To complement the quantitative analysis with robustness and qualitative insights either by supporting the quantitative results or questioning them.

Qualitative assessments also provide an opportunity to provide comprehensible interpretations of the safety impact of various events, which safety function is affected and how important the impact is to reactor safety. Since many events can still be evaluated with PSA, an interpretable scale for qualitative assessments is achieved.

The developed methodology for qualitative assessment of AOT:s is based on similar methodologies for probabilistic/deterministic analysis, e.g. for safety classification of SSC:s [5]. The complete logic of the methodology is described in Figure 4. For a given SSC[2] a preliminary classification is made based on the main functional impact of the failure event (failed SSC). Decisive is if there are direct or indirect impact on system redundancies in the barrier protections or on the frequency of initial events. The classification can then be adjusted towards a shorter time limit if the event has a multiple impact on the three risk elements (see Figure 2) or towards a longer time limit if there are extenuating factors.

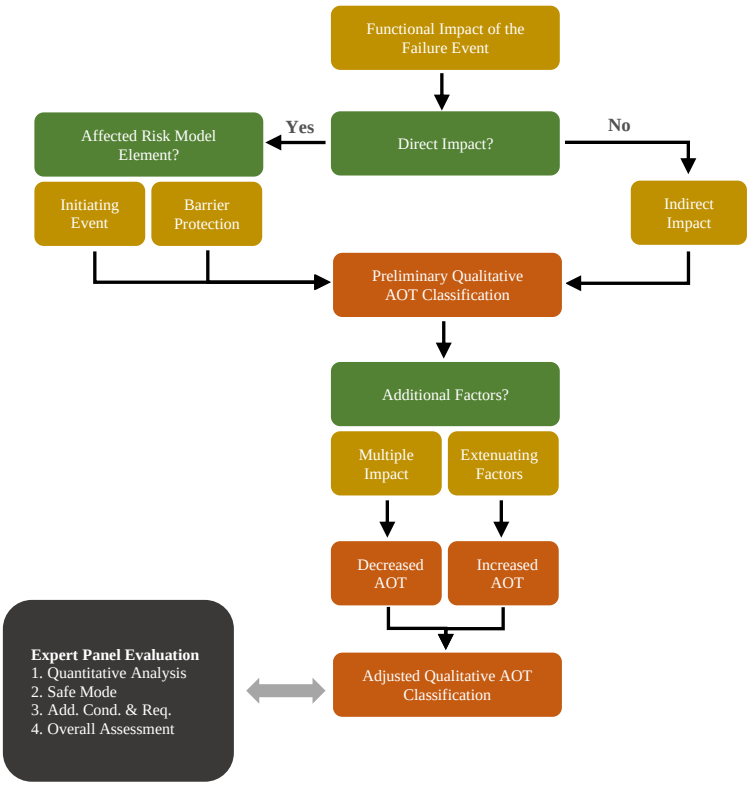

Figure 4. The complete decision logic of the Qualitative Assessment of AOT:s

[2] The SSC:s referred to in this report have Operational Readiness Requirements, or similar, defined in the Technical Specifications with one or several cases of allowed exemptions, for which AOT:s shall be defined.

The methodology uses five different basic classes of AOT:s (time limits) as shown in Table 1. Each class is associated with a qualitative description of the impact of a SSC failure on the plant risk, and an indicative value for an AOT (time limit). Five classes were found to be a reasonable number for the Gen. II reactor used as an example in the methodology development. However, the number of classes should be decided on a case-by-case basis, depending on plant design and risk profile, in such a way that sufficient balance can be achieved between AOT:s for different SSC:s.

Table 1. Basic classes of AOT:s used in the Qualitative Analysis.

AOT Class	SSC impact on plant risk	Indicative AOT value (time limit)	Colour code
1	Negligible	No limit (continuous operation)	
2	Small	Long limit (30 days or more)	
3	Significant	Medium limit (7 to 14 days)	
4	Large	Short limit (max 3 days)	
5	Unacceptable	Shutdown (0-24 hours)	

The analysis steps are further described below.

4.1 Functional impact

The purpose of this analysis step is to assess the functional impact of the failure event on the plants DiD levels, in this case described by the simplified Risk Model in Figure 2. Depending on which element that is affected and on the remaining Safety Margin to the deterministic success criteria for the affected function, a preliminary AOT classification is performed.

Direct impact means that a failure event affects one or more redundancies of a function in a barrier protection or that the failure event increases the frequency of an initial event (i.e. any of DiD levels 2-4). The impact on barrier protections (DiD level 3 to 4) is described by assessing the remaining Safety Margin which is performed by specifying the remaining capacity or number of redundancies calculated as a percentage compared to the identified deterministic success criteria, mainly according to limiting SAR analysis case for the function. From a classification perspective, three main cases can be defined:

- The function does not meet the success criteria. Less than 100% capacity remains.
- The function meets the success criteria but cannot tolerate further failures. E.g. 1 × 100% or 2 × 50% capacity remains.
- The function meets the success criteria and can withstand one additional failure. E.g. 2 × 100% or 3 × 50% remains.

If the system can withstand several additional failures (multiple failures) this is considered as an extenuating factor, and a more generous time limit can be applied for the AOT.

Regarding the impact on the frequency of initial events (DiD level 1 and 2), a simplified scale considering two cases based on the achieved increase of the frequency is applied:

- Low increase in event frequency, by a factor of ~X,
- High increase in event frequency, by a factor of ~Y.

The numerical values X and Y of the increase factor should be defined either by engineering judgement or by quantitative analysis (PSA importance measures) based on plant design and risk profile. There might also be necessary to use more cases than two. The methodology suggests values as X = 2 and Y = 10 in this example.

Indirect impact of a failure event means that there is no direct impact on any of Risk Model Elements, i.e. any lost redundancy or increased initiating event frequency. Examples of indirect impact are:

- Impact on control room indications that are not critical. These may have an impact on operator intervention in accident scenarios.
- Impact on normal operating doses,
- Impact on safety in the long-term (e.g. may accelerate aging of materials or components).

Indirect impact is described qualitatively as:

- "Significant" impact
- "Non-negligible" impact
- "Negligible" impact

Assessment of functional impact must be performed based on realistic considerations, i.e. without consideration of deterministic analysis rules (e.g. postulated concurrent failures). It should be noted that an event may have an impact on more than one risk element and that all impacts should be identified in the analysis. For the preliminary classification of the AOT, the most critical risk element should be selected.

4.2 Preliminary Qualitative Classification

The preliminary classification is based on the risk element where the impact is judged to be most critical. The idea is that each failure event may typically have a most critical impact and possibly some other less critical impacts that can be considered in the Adjusted Classification.

The following tables describes examples of classification rules for the different risk model elements and different levels of remaining safety margin at an unavailable SSC (failure event). The tables uses the five basic classes of AOT:s from Table 1. The rules, i.e. which class to assign given a certain impact is based on a qualitative evaluation of the estimated risk importance of key system functions in different levels of DiD, e.g. core cooling (CC) or residual heat removal (RHR) in DiD level 3a, diversified CC or RHR in level 3b and containment spray in DiD level 4.

Table 2 describes an example of classification rules for SSCs in risk model elements Core Damage and Release (Figure 2) for a Gen. II NPP. System functions belonging to Core Damage B have varying degrees of redundancy and safety significance and are not normally credited in plant conditions AOO and DBA. A more generous time limit can therefore be set for system functions belonging to DiD 3b if it is justified by the safety margin.

Table 2. Classification rules for SSC:s within risk model elements Core Damage and Release.

Safety Margin of affected function	**AOT Class**		
	Core Damage A AOO, DBA DiD 3a	**Core Damage B** DEC-A DiD 3b	**Release** DEC-B DiD 4
2 x 100 % capacity or more remains	2	1	1
1 x 100 % capacity or more remains	4	3	3
Less than 100% capacity remains	5	4	4

The classification rules for SSC:s with impact on risk model element Initiating Event should relate to the achieved increase in plant risk (core damage) and insights from the PSA may be used. The methodology example is given in Table 3.

Table 3. Classification rules for SSC:s within risk model element Initiating Event.

Initiating Event Frequency Increase	**AOT Class**
"Low" (factor 2)	2
"High" (factor 10)	4

That a failure event only has an indirect impact on the risk model elements indicates mostly that it also has small impact on the plant risk. In exceptional cases, e.g. cases where the opportunity for the operator to intervene is affected, the impact can be significant. The methodology example is given in Table 4.

Table 4. Classification rules for SSC:s with indirect impact on the risk model elements.

Impact on Risk Model Elements	**AOT Class**			
	Initiating Event	Core Damage A	Core Damage B	Release
"Negligible" impact	1	1	1	1
"Non-negligible" impact	2	2	2	2
"Significant" impact	3	3	3	3

4.3 Adjusted Qualitative Classification

After the preliminary classification, further analysis may be needed to adjust the classification to obtain a more realistic assessment of the risk impact. In cases where an SSC failure event has multiple impacts on the three elements of the risk model, it is reasonable to assume a larger impact on plant risk than if only one element of the risk model is affected, and a tougher, i.e. shorter, AOT should be applied. On the other hand, there may be extenuating factors that may justify a lower class, i.e. a longer AOT.

The methodology applies the following simple rules to adjust the AOT class due to multiple impacts:

- The SSC failure event affects (directly) Initiating Event element and also the Core Damage and/or Release element: one class higher AOT applies.
- The SSC failure event affects (directly) both elements Core Damage and Release: The shortest AOT is applied.

It should be noted that an impact on all three elements of the risk model does not lead to a greater adjustment of the AOT than one class.

Assessment of extenuating factors must take place on realistic grounds, i.e. without taking into account postulates set in the deterministic analysis cases in the Safety Analysis Report. This means that postulated initial events, consequential effects of these, single faults and Common Cause Failures shall not affect the assessment of available extenuating factors. This is done to avoid the AOT being driven by extremely low-frequency events postulated in the deterministic analyses, e.g. CCF in RHR or station black-out.
Credited extenuating factors are:

- The system function meets the success criteria and can withstand additional multiple failures. E.g. 3 × 100% or more capacity remains.
- Existence of functional backup or credible recovery that counteracts or eliminates the consequence of the failed SSC. This option is not valid for safety functions credited in plant conditions AOO or DBA.
- Implementation of safety-enhancing measures, e.g. compensatory action, increased monitoring or more frequent testing in case of ambiguity in the status of the function, control of operational readiness/availability of diversified system functions etc.
- Conservatively estimated functional impact of the failed SSC.

It should be noted that the existence of several extenuating factors does not lead to a greater adjustment of the repair criterion than one class.

If there exist reasons to both increasing and lowering the AOT, they are assumed to offset each other, i.e. an extenuating factor eliminates multiple impacts on the risk model elements.

5. METHODOLOGY FOR EXPERT PANEL EVALUATION

The expert panel evaluation is performed by expertise at both plant level and system level, including maintenance and safety analysis. The expert panel should also include experts from the qualitative and quantitative analysis teams, as well as experts with good knowledge of the Technical Specification. The expert panel evaluation contains four steps where the first three is performed for each individual AOT while the fourth step is performed by considering all AOT:s of the Technical Specification:

1. Review of the results from the qualitative and quantitative analyses with existing AOT (if such exists). In cases where the results from the quantitative and the qualitative analysis strongly deviate from each other, the reasons for this should be investigated and thoroughly explained and the most realistic result should be identified
2. Assessment of safe mode. Cold shutdown is in most cases the safest mode to perform a repair, but in some cases, shutdown may pose a higher risk than continued operation. This is indicated by results from quantitative and/or qualitative analysis, and the safe mode can in these cases be changed/determined to warm shutdown or at-power.
3. Reasonableness of the AOT compared to actual expected repair times. AOT:s as such do not take into account what actual the actual repair times are for the possible failure events of a SSC. It hence needs to be clarified if the AOT is realistic compared to actual repair times, and if not, it should be determined whether the operation and maintenance strategy should be changed or whether the time limit should be extended (if acceptable). If the time limit is significantly longer than the expected repair time, it should be reflected in the operation and maintenance strategy.
4. Overall assessment of the total impact of the proposed AOT changes on plant safety. The purpose is to get an overview of the impact of the changes in safety (risk increase or decrease) and whether the AOT:s in the TS as a whole can be considered balanced. The overall assessment covers a quantitative assessment of the impact of proposed changes on total core damage and large release frequencies using the PSA, together with summaries of proposed AOT:s grouped by impact on safety functions and DiD levels, in order to identify inconsistencies and/or unbalanced AOT:s, while the approach also enabled comparisons between safety functions and DiD levels. The overall assessment is carried out when all AOT:s in the TS have been analysed and reported.

6. CONCLUSIONS

This paper presents a methodology for risk-informed decision making on Allowed Outage Times (AOT:s) within a utility's Technical Specifications (TS). The developed approach combines traditional quantitative PSA-based approaches, e.g. based on NRC Regulatory Guide 1.177, [1], for evaluation of AOT:s with a qualitative risk analysis developed to ensure that the suggested AOT:s meets the licensing basis and fulfils deterministic requirements of the Safety Analysis Reports.

The methodology is approved by the Swedish Radiation Authority and has been used to revise and implement new, balanced, AOTs for the complete TS of a Swedish BWR. The method has in this work proved to provide balance between the AOT:s of the SSC:s covered in the TS, and realistically reflect the SSC:s risk significance and thereby improve general plant safety. The method ensures that consistent and comprehensive rules are applied, and that all AOT:s are justified.

References

[1] An approach for plant-specific, risk-informed decisionmaking: technical specifications. Reg.Guide 1.177, Rev. 1. U.S.NRC, 2011.

[2] Risk based optimization of technical specifications for operation of nuclear power plants, IAEA-TECDOC-729, IAEA, 1993.

[3] Guidance to Risk-Informed Evaluation of Technical Specifications using PSA, Swedish Radiation Authority, SSM 2010:16, 2010.

[4] Homberg J E. Risk informed assessment of Technical Specifications in Olkiluoto 1 and 2, Paper presented at PSA Castle Meeting 2008.

[5] Safety Classification of Structures, Systems and Components in Nuclear Power Plants, Specific Safety Guide No. SSG-30, IAEA, 2014.