RISK-INFORMED OPTIMIZATION OF SURVEILLANCE TEST INTERVALS

Sami Sirén[1], Kalle Jänkälä[2]

[1] *Fortum Power and Heat Oy, P.O. Box 100, 00048 FORTUM, Finland, sami.siren@fortum.com*
[2] *Fortum Power and Heat Oy, P.O. Box 100, 00048 FORTUM, Finland, kalle.jankala@fortum.com*

A risk-informed review and optimization of surveillance test intervals (STIs) has been performed for Loviisa nuclear power plant as a part of the risk-informed inspection of Technical Specifications. The motivation was, in addition to meeting regulatory requirements, to balance the testing schedule by relaxing the testing requirements for non-risk significant tests and to identify needs for more frequent testing for risk-significant systems. A maximum limit of 1 % was set for the computational increase in core damage frequency (CDF) and large release frequency (LRF). A prerequisite for the review to produce reliable results is a comprehensive PRA model for levels 1 and 2. Surveillance testing procedures were examined to assess which basic events in the PRA model are affected by a particular STI, and how a change in an STI affects each type of basic event in the PRA model. Plant specific failure history was used to estimate the fraction of failures detected by surveillance testing. Fussell-Vesely risk importance measures were then used to estimate how the changes in basic event probabilities affect CDF and LRF. As a result 27 STIs qualified for an extension, generally from 4 weeks to 12 weeks. Consideration for shortening two of the STIs was recommended.

I. INTRODUCTION

Surveillance testing is the main way to ensure high availability for safety systems at nuclear power plants (NPPs). More frequent testing means higher availability, as long as the test itself does not have adverse effects. Originally, the surveillance test intervals (STIs), like all requirements in Technical Specifications (TS), have been based on deterministic criteria, such as safety class and success criteria in a set of representative initiating events.

The PRA model for Loviisa NPP has reached full scope, i.e. it includes all initiating event categories for both power operation and shutdown states, and for both PRA levels 1 (core damage frequency, CDF) and 2 (large release frequency, LRF). This achievement, as well as conscious efforts to remove any excess conservatism, enables using probabilistic methodology with confidence in the results. In many countries, regulatory requirements related to using risk information have increased accordingly. As with most other PRA applications, due to differences in PRA models and their use, there is no universally accepted way of performing a risk-informed optimization of STIs. Using the living and fairly detailed PRA model of Loviisa NPP, as well as the plant-specific failure event database, a methodology was developed and used for a thorough inspection that takes into account all the major - sometimes conflicting - effects of changing STIs.

This paper presents the methodology and overall results of the risk-informed inspection of STIs that was performed for Loviisa NPP. The mathematical methods are presented in Chapter II, and a summary of the inspection scope and results in Chapter III.

II. RISK SIGNIFICANCE OF SURVEILLANCE TESTING

II.A. Overview

Surveillance testing has multiple effects on NPP safety. Its main purpose is to expose latent failures and minimize unavailability of safety related equipment. Tests may also prevent some failures like sticking of valves from developing into critical ones. However, tests may also cause unavailability by requiring temporary process configurations, causing wear, or they can be sources of human errors or even initiating events. To have confidence in a risk-informed optimization method, it is important to identify all these aspects. To be able to take them into account, a full-scope and detailed PRA model is needed. The overall risk significance of changing a test interval, or even whether it is increasing or decreasing the overall risk, is not always self-evident.

The steps for estimating the risk significance of a surveillance test are:

1. Choose the STI(s) to be changed
2. Identify all basic events and initiating events that depend on the STI
3. Estimate the change in each event probability or frequency as a function of the STI
4. Estimate the change in CDF and LRF

The first step, while seemingly trivial, can be a process in itself. Sometimes changing one STI can lead to unacceptable risk increase, while combining multiple changes keeps the total effect on risk more neutral. If only one STI is studied, these trade-off possibilities are not found. In most cases, the choice of scope is guided by the motivation to do the analysis. The need may arise, for example, from regulatory requirements or problematic issues identified with the current situation. For Loviisa NPP, an earlier study[1] only focused on diesel generator STIs, as their original 2-week STIs were found problematic and the increase to 4 weeks could be justified without considering other tests. Later, as the PRA model was reaching full scope, a comprehensive optimization was planned, even if the final push to perform it came from the regulatory body.

The second step is probably the most laborious part of the process, depending on what kind of information is already available in the PRA documentation. As surveillance testing may also reveal failures that are not evident from the testing procedures, e.g. erroneous valve positions or pipe blockages, a systematic study should be performed to document all the basic events in the PRA model that are somehow involved in the surveillance test. On the other hand, for many basic events involved in any one surveillance test, there are other tests and checks that affect them. It is important to get a complete picture, so even if a change of only one STI is to be considered, the study must be extended to others as well. Normally only the shortest relevant STI is taken into account when estimating the probability of a basic event.

The third step is discussed in Chapters II.B and II.C. The fourth step is discussed in Chapter II.D.

II.B. Importance of Surveillance Testing in Detection of Failures

Although surveillance testing is usually the main method of detecting failures, not all failures are detected by tests. Many failures are detected either by surveillance other than testing (e.g. control room alarms or shift walk downs.), when the equipment is operated, or simply by accident. In this paper, the fraction of failures detected by other means than surveillance testing is denoted by r. Assuming that surveillance testing is responsible of detecting of all failures (i.e. $r = 0$) would lead to overestimation of its importance and misguided decision-making.

To determine the values of r for various safety related equipment, the failure history of Loviisa NPP safety related systems was studied[2]. The data was pooled in various ways to take into account the factors identified as the most important to the value of r:

- system the component belongs to,
- type of the component, and
- mode of operation for the component (running, alternating, stand-by).

The results of the study are summarized in Table I. At first, all the failure data was pooled to get a generic value $r = 0.32$. Smaller subsets were then studied to determine the dominating factors. The study revealed that differences between valves, pumps and diesel generators were quite small in general, while differences between systems were extremely significant. This is partly explained by the differences in operation. Failures in running systems are mostly detected immediately, while failures in stand-by systems are mainly detected by surveillance testing. There is a significant difference between the estimates for all pumps and stand-by pumps. Therefore, for stand-by pumps, the value $r = 0.12$ is used. The values estimated for individual systems are used for other pumps, valves and diesel generators.

The values for measurement transmitters differ greatly from other types of components. Most failures are immediately detected from various alarms, so the importance of surveillance testing is small. Since there is no significant difference between the different types of measurements, the value $r = 0.94$ is used for all of them. The value $r = 0.50$ is used for thermostats.

TABLE I. Estimated values for *r* using plant data from Loviisa NPP.

Component Group	***r***
All	0.32
Valves	0.41
Pumps (All)	0.29
Pumps (Stand-by)	0.12
Diesel Generators	0.31
Measurements (All)	0.94
Measurements (Pressure)	0.93
Measurements (Level)	0.95
Measurements (Temperature)	1.00
Thermostats	0.50
Pumps & Valves of Individual Systems	0.04…0.71*

*Only systems with at least 10 failures are included in the range.

II.C. Effect of Test Interval on Basic Events

Changes in STIs affect basic events in different ways, depending on the type of the basic event. Usually increasing the STI also increases the unavailability, but in some cases the effect is negligible or the unavailability is even decreased. In the general case, the relative change in the probability or frequency of event A, is stated as:

$$R_A = \frac{u_{new}}{u_{old}} = r + (1-r) \cdot \frac{T_{new}}{T_{old}}, \quad (1)$$

where $u_{new/old}$ is the event probability or frequency after/before the STI change, $T_{new/old}$ is the new/old STI. Thus, any change in the STI only affects the contribution of those failures that are detected by surveillance testing.

I.C.1. Failures to Function per demand

The most common type of basic event in PRA is failure to function per demand. For a pump it translates to 'fails to start' and for a valve or a circuit breaker to 'fails to open' or 'fails to close'. The unavailability *u* for these failure events can be expressed as:

$$u = q + \lambda \cdot (\frac{T}{2} + \tau), \quad (2)$$

where q is the probability of failure on demand, λ is the failure rate, T is the STI and τ is the mean time to repair. As Eq. 1 equates the fractions of failures with their corresponding contribution to unavailability, it is most accurate with small values of *r*, or when the average unavailability time does not vary much between the most relevant detection methods. Normally q and τ are relatively small, so Eq. 1 can be used with values for *r* determined in Chapter II.B. Measurements mostly operate continuously, so their *r* is very large and most failures are detected immediately. In these cases there is a mismatch between the fraction of failures detected by surveillance testing and their contribution to the unavailability, so the method does not work as well as for other types of components. However, it would be more conservative to treat all measurement failures as failures during operation (i.e. assume $r = 1$). Their relatively small risk significance mitigates the impact on the optimization results.

I.C.2. Failures During Operation

Failures during operation include 'fails to run' events for pumps and 'spurious opening/closing' for valves. Such events are assumed to be independent of STIs, so value $r = 1$ is used in Eq. 1.

I.C.3. Incipient Failures

Incipient failures do not cause unavailability themselves, but indirectly through the time taken to repair such failures. If the STI is lengthened, fewer of these failures are detected during the power operation, and the unavailability due to repairs is decreased. However, some of the incipient failures may then develop into critical failures, again causing unavailability until detected and repaired. It is therefore difficult to assess whether increasing an STI increases or decreases the risk due to these failures. The overall effect is assumed to be small and therefore incipient failures are not assessed quantitatively.

I.C.4. Human Errors

Of the three types of human errors (before/leading to/after an initiating event), only the first type (errors before an initiating event) is considered here. The second type (errors leading to initiating events) is included in Chapter I.C.7. Valves can be in an erroneous position and measurement transmitters can be erroneously calibrated. Some of these are affected by the STI.

For the valves that are operated only during shutdown, surveillance testing is only used to verify the correct position. Unavailability is then only possible before the first test is performed after the start-up. For these valves Eq. 1 with $r = 0$ is used.

For the valves that are operated in the surveillance test, the error can be both detected and made during the test, so the STI is assumed to have no effect on the probability. Similarly, the probability of erroneous calibration of a measurement transmitter is assumed to be independent of the STI.

If the erroneous position of a valve triggers an alarm in the main control room, the effect of the STI on the error probability is assumed to be negligible.

I.C.5. Unavailability due to Testing

Some surveillance tests require temporary process configurations, e.g. closing of main pump lines and opening of test lines to avoid disturbing the main plant processes. While these tests are important to reveal any latent equipment failures, they can also cause unavailability during the test itself. The unavailability due to testing is defined as:

$$u = \frac{T_E}{T}, \tag{3}$$

where T_E is the unavailability time per test and T is the test interval. Since T_E is constant, the unavailability decreases as T increases and the Eq. 1 is replaced by:

$$R_A = \frac{u_{new}}{u_{old}} = \frac{T_{old}}{T_{new}}. \tag{4}$$

I.C.6. Common Cause Failures

The fractions of different detection methods for common cause failures in the international common cause failure database (ICDE) are roughly similar to the fractions derived from the failure data of Loviisa NPP[3]. Therefore the same values for r are used for common cause failures as for single failures.

I.C.7. Initiating Events

Some surveillance tests may cause initiating events, either by design or (e.g. stopping of fuel pool cooling to test containment isolation valves) or if carried out erroneously. Eq. (4) can be used for such cases.

II.D. Effect of Test Interval on Plant Risk

II.D.1. Generic Case

The effect of a change in a single basic event probability or frequency on the plant risk can be estimated using risk importance measures. The Fussell-Vesely (*FV*) importance of basic event *A* is the fraction of all minimal cut sets (MCSs) that contain *A*:

$$FV_A = \frac{Q(MCS\ including\ A)}{Q(All\ MCS)}. \quad (5)$$

Surveillance tests normally affect multiple basic events in the PRA model. From (5) it follows that the FV importance of two basic events can be added together if the fraction of MCSs containing both events are subtracted from the sum. Generally, however, this fraction is small so we can approximate:

$$FV_{AB} = FV_A + FV_B - FV_{AB} \approx FV_A + FV_B. \quad (6)$$

The relative change on the plant risk due to a change in one basic event can be estimated as:

$$\frac{Q_{new}}{Q_{old}} = 1 + FV_A \cdot (R_A - 1). \quad (7)$$

Using Eqs. 6 and 7 we can then estimate the relative change on the plant risk for multiple basic events:

$$\frac{Q_{new}}{Q_{old}} \approx 1 + FV_A \cdot (R_A - 1) + FV_B \cdot (R_B - 1) + \ldots \quad (8)$$

Eq. 8 can then be used separately for PRA levels 1 and 2 (CDF and LRF). As can be anticipated from the equations, the overall plant risk generally increases almost linearly as the STI is extended. Also, the relative change in risk is somewhat overestimated because of the approximation used. Therefore, in the usual case of extending the STIs, the estimated effect on plant risk is generally conservative.

II.D.2. Risk Optimum

In some cases, where testing may cause unavailability or initiating events, a risk optimum may exist. In Fig. 1 below is presented the estimated effect of changing the STIs for three safety systems that are tested as a group. To be able to carry out the tests during power operation, test lines back to the emergency core cooling water tank are opened, and the containment isolation valves are closed. Should a need for these systems arise during the test, the safety automation system would send a signal to close the test lines and open the containment isolation valves. A failure of a single valve to open or close in such a situation would lead to loss of two safety trains in the corresponding system. Therefore, the unavailability caused by the surveillance testing is a significant risk contributor.

The current interval for these surveillance tests is 4 weeks. If the STI was halved to 2 weeks, the risk due to the unavailability during the test would outweigh any benefits gained from the shorter latent unavailability of any component failures. Extending the STI to 8 or 12 weeks increases the estimated risk somewhat, but the change is still tolerable and within the margin of error. With an extension longer than that, the significance of test-induced unavailability is diminished and the risk increases linearly.

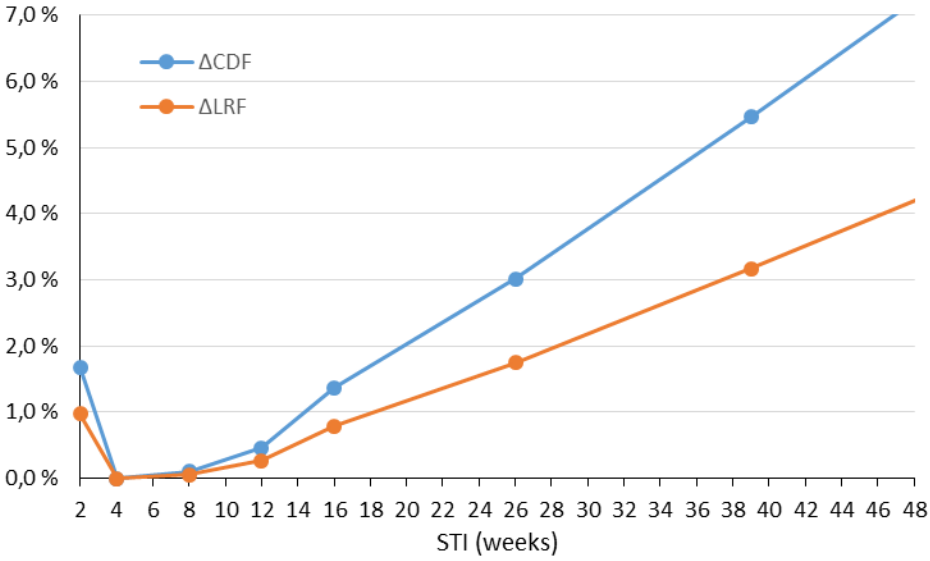

Fig. 1. The estimated risk effect of changing the interval for selected surveillance tests.

III. OPTIMIZATION

III.A. Scope and Principles

The study was focused primarily on the STIs defined in the Technical Specifications (TS) of Loviisa NPP. All tests that are performed during power operation were included. Tests that are only performed during shutdown modes were excluded, except for a few that were specifically selected for the inspection, as they were considered unnecessarily frequent. To get a more complete picture of the surveillance testing, tests outside of TS scope were included if they were assumed to have some risk importance. Identical tests for redundant trains were considered as one test in the study, as no advantage was seen in assigning them different STIs. The final number of STIs studied was 57 and their distribution is summarized in Table II. Most of the STIs of 52 or 104 weeks are for tests that are carried out during the annual refueling outage.

TABLE II. The distribution of STIs in the study.

STI (weeks)	Count
1	1
2	1
4	31
6	1
8	1
12	9
13	3
16	1
32	1
52	6
104	2
Total	***57***

The annual maintenance and refueling outage at Loviisa NPP takes roughly 4 weeks, which leaves 48 weeks for the power operation. Most safety systems have an STI of 4 weeks, so each train is tested 12 times during a power operation cycle. With staggered testing, this means that one train is tested every week. For practical reasons, it is desirable to keep the number of alternatives for STIs limited, and also to keep the 'divisible by four' principle. Therefore, it was decided to choose the STIs for tests carried out during power operation from a set of 4 weeks, 12 weeks and 52 weeks.

There is – generally – no 'optimal' value for any STI from the risk point of view. Also, the PRA model cannot take into account all the perspectives when it comes to surveillance testing. Therefore, other sources of information are needed to be able to make meaningful decisions on which STIs should be extended and which could be shortened. Plant personnel responsible for operation, testing and maintenance, as well as other experts were interviewed to come up with a list of desired changes. Non-quantified issues to consider can be, for example, savings in man-hours and radiation dosage, and test-induced wear and transients. An earlier study at Loviisa NPP on leak-tightness testing intervals for containment isolation valves allowed big savings in man-hours without increase in risk.

As a basic principle, no plant or procedure modification that increases risk is allowed. In this study it was recognized that most of the adverse effects of testing are not quantified. Thus it is preferable to set the STIs to be long enough to minimize the adverse effects but short enough to keep the quantified risk increase tolerable. A limit of '1 %' was set for the quantified risk increase for both CDF and LRF.

III.B. Results

III.B.1. Unchanged STIs

As an overall result, 30 STIs out of the 57 that were studied were left unchanged. For 12 STIs this was because the risk significance of extending the STI would be unacceptable. For 15, the current STI was at least 12 weeks, and no benefit was seen to be gained by extending it. For some of these, an extension would mean that all redundant trains would only be tested simultaneously during the refueling outage, greatly increasing the risk of common cause failures, compared to current staggered testing strategy. Finally, 3 STIs related to turbine systems were considered important to ensure the availability of the plant, even if they had no effect on core damage risk.

III.B.2. Extended STIs

Of the 57 STIs studied, an extension was recommended for 27. To qualify for extension, the effect on risk had to be small enough so that the cumulative effect of all the changes did not breach the accepted limit of 1 %. In addition, there had to be an understanding that the extension would not cause any adverse effects due to non-quantified factors. The results are summarized in Table III.

The most common extension was from 4 to 12 weeks (19 STIs). One of these extensions would even decrease the risk (-0.09 % for CDF and -0.25 % for LRF). This is because the testing of containment isolation valves requires to stop and restart the fuel pool cooling system. Another STI was to be extended from 4 to 52 weeks, justified by the low risk significance and a reduction of system transients. Overall, two thirds of the studied 4-week STIs qualified for extension.

Five unnecessarily short STIs could be extended from 12, 13 or 32 weeks to 52 weeks, with negligible effect on risk. One STI related to ventilation systems was doubled from 2 to 4 weeks. The extension from 2 to 8 years for check valves of emergency core cooling water accumulators was included, even if the risk increase is non-negligible With the extension the surveillance testing can be synchronized with the longer maintenance outages where the reactor is drained and the possible failures of the check valves can be repaired. The combined effect of all the changes is below the set 1 % limit.

TABLE III. The counts of STIs qualified for extension and their effect on plant risk.

Original STI (weeks)	New STI (weeks)	Count	ΔCDF	ΔLRF
2	4	1	0.03 %	0.00 %
4	12	19	0.73 %	0.17 %
4	52	1	0.08 %	0.09 %
12	52	3	0.00 %	0.00 %
13	52	1	0.00 %	0.00 %
32	52	1	0.00 %	0.00 %
104	416	1	0.08 %	0.18 %
Total		***27***	***0.91 %***	***0.45 %***

III.B.3. Shortened STIs

Two STIs were identified as giving a potentially significant risk reduction, if they were to be shortened. One of them was the test for the additional emergency feed water pump system. Halving the STI from 4 to 2 weeks would decrease the CDF by 0.26 % and LRF by 0.05 %. However, since the new STI would be very short, the quantified risk decrease was not considered a good enough compensation for the increased wear the frequent testing would expose the components to.

Another possibility for a significant risk decrease was found in shortening the STI for an additional emergency diesel generator. This generator and its surveillance testing are not in the scope of TS, and it is not a safety classified system. However, if the STI was changed from 6 weeks to 4 weeks, the quantified risk decrease would be 0.34 % for the CDF and 0.68 % for the LRF. Any modification with such a potential for risk decrease for such a small cost would generally be implemented. However, the diesel system is fairly new and there have been lots of failures. It is assumed that the quantified effect of changing the STI will decrease dramatically as the infant failures are eliminated.

One idea for risk reduction to consider could be shortening the STI for just the most important single components. The basic event contributions to the total risk increase are easily obtained from the study so possibilities for risk reduction could be found with minimal effort. It is, however, very case-specific whether testing single components instead of the whole system is worth it. Functional tests of valves could be such a case, if the whole system test would require temporary configurations.

III.C. Implementation

One of the potential problems with implementing risk-informed TS is that the PRA model and even the plant are changing. It is not desirable to have STIs that are changed every year when new risk information is available from the updated PRA. Another challenge is the frequent mismatch between safety classification and risk importance, as some non-safety systems may have a bigger risk significance than some safety classified systems.

The original plan for Loviisa NPP was to perform a risk-informed optimization of Technical Specifications when all the major plant modifications relevant to safety were completed. Long delays in the automation renewal project lead to performing a somewhat 'premature' risk-informed inspection mainly due to regulatory requirements. The results of that inspection are reported in this paper, but the majority of proposed STI changes have not yet been implemented. Only some of the changes with negligible risk effect have been implemented, but some independent assessments using the methodology have been made to support various plant operations and modifications. A thorough risk-informed optimization is still in plans, and after optimizing the STIs, it will be followed by risk-informed optimization of allowed outage times[4].

IV. CONCLUSIONS

The thorough risk-informed inspection of STIs revealed that many of the most frequently carried out surveillance tests have little or no effect on the plant risk level, and can thus be extended if there are no arguments against the decision. When the inspection covers simultaneously all the surveillance tests, trade-offs can be found so that the total risk change remains close to zero.

As with any risk-informed application, the optimization of STIs relies heavily on the quality of the PRA model and the available data. With a sufficiently detailed methodology, all the major effects of changing an STI can be taken into account in the quantification. Any method, however, cannot quantify all the effects, so it is important to communicate with experts of various fields to reach a consensus of what is acceptable and practicable.

REFERENCES

1. A. HÄMÄLÄINEN, K. JÄNKÄLÄ and J. VAURIO, "Risk-Informed Testing Program for Emergency Diesel Generators", *PSAM7 – ESREL'04*, Berlin, June 14-18, 2004.
2. R. KLEINBERG, "Turvallisuudelle tärkeiden laitteiden koestusten merkitys vikojen havaitsemisessa", Bachelor's thesis (in Finnish), Aalto University, Espoo 2012, Finland.
3. K. JÄNKÄLÄ, "Estimating Common Cause Failure Probabilities for a PRA Taking into account Different Detection Methods", *PSAM12*, Honolulu, June 22-27. 2014.
4. S. SIRÉN, K. JÄNKÄLÄ, "Risk-Informed Optimization of Allowed Outage Times For Loviisa NPP", *PSA 2008*, Knoxville, September 7-11, 2008.