nks

Nordisk kernesikkerhedsforskning
Norrænar kjarnöryggisrannsóknir
Pohjoismainen ydinturvallisuustutkimus
Nordisk kjernesikkerhetsforskning
Nordisk kärnsäkerhetsforskning
Nordic nuclear safety research

NKS-72
ISBN 87-7893-128-2

A risk informed safety classification for a Nordic NPP

Kalle Jänkälä
Fortum Nuclear Services Ltd, Finland

January 2002

Abstract

The report describes a study to develop a safety classification proposal or classification recommendations based on risks for selected equipment of a nuclear power plant. The application plant in this work is Loviisa NPP unit 1. The safety classification proposals are to be considered as an exercise in this pilot study and do not necessarily represent final proposals in a real situation. Comparisons to original safety classifications and technical specifications were made. The study concludes that it is possible to change safety classes or safety significances as considered in technical specifications and in in-service-inspections into both directions without endangering the safety or even by improving the safety.

Key words

Safety classification, importance measures, PSA

NKS-72
ISBN 87-7893-128-2

Pitney Bowes Management Services Denmark A/S, 2002

The report can be obtained from
NKS Secretariat
P.O. Box 30
DK – 4000 Roskilde
Denmark

Phone +45 4677 4045
Fax +45 4677 4046
www.nks.org
e-mail nks@catscience.dk

A RISK INFORMED SAFETY CLASSIFICATION FOR A NORDIC NPP

Kalle Jänkälä
Fortum Nuclear Services Ltd

January 2002

Contents

Acknowledgements

The work has been funded by Nordic Nuclear Safety Research (NKS) SOS-2 project, Fortum Nuclear Services and Fortum Power and Heat. The author is grateful to colleagues in Fortum for discussions and comments and especially to Dr. J.K. Vaurio, Loviisa NPP, for his valuable review and comments, and who as an initiator suggested this topic for NKS research program.

The views expressed and conclusions made are those of the author or the initiator and do not necessarily reflect those of Fortum Oyj or the funding organisations.

Abbreviations

AOT	Allowed outage time
CCDP	Conditional core damage probability
CCF	Common cause failure
CCW	Component cooling water (TF system in Loviisa NPP)
CDF	Core damage frequency
EYT	Classified non-nuclear
FV	Fussell-Vesely importance measure
HPSI	High pressure safety injection (TJ system in Loviisa NPP)
LERF	Large early release frequency
LLOCA	Large loss of coolant accident
LOCA	Loss of coolant accident
MCS	Minimal cut set
MLOCA	Medium loss of coolant accident
NPP	Nuclear power plant
PCP	Primary coolant pump
PSA	Probabilistic safety assessment
RDF	Risk decrease factor
RIF	Risk increase factor (= risk achievement worth)
SC	Safety class
SLOCA	Small loss of coolant accident
STUK	The Radiation and Nuclear Safety Authority in Finland
Tech Spec	Technical specifications

1 Introduction

The objective of this study is to develop a safety classification proposal or classification recommendations based on risks for selected equipment of a nuclear power plant. The application plant in this work is Loviisa NPP unit 1. These safety classification proposals are to be considered as an exercise in this pilot study and do not necessarily represent final proposals in a real situation. Comparisons to original safety classifications and technical specifications will be made.

The work described in this report comprises the following tasks:

1. Application systems and equipment are selected so that all the different safety classes and a wide range of safety importances are covered.
2. Probabilistic Safety Assessment (PSA) importance measures are quantified for the selected components and groups of components as needed.
3. PSA importance measures are compared to the safety classes and to the safety importance as considered in technical specifications and reasons for possible differences are studied.
4. PSA importance measures that are best applicable to different purposes in a safety classification are selected.
5. Pilot safety classifications based on risk estimates and/or importance measures are developed.
6. Other comments and recommendations on safety classifications.

The risk estimates cover at least internal initiating events and relevant part of external initiators.

2 Safety classes

2.1 Definition of safety classes

The Radiation and Nuclear Safety Authority STUK issues the safety regulations of the Finnish nuclear power plants in the YVL guides. The present guides are literally intended for new nuclear power plants. Nevertheless, serious efforts are made to apply the same to old plants as well, or to prove that acceptable level of safety can be accomplished by other means. The principles of safety classification are presented in the YVL Guide 2.1: Nuclear plant systems, structures and components and their safety classification. In accordance with the Council of State Decision on the safety of nuclear power plants /1/:

The functions important to the safety of the systems, structures and components of a nuclear power plant shall be defined and the systems, structures and components classified according to their safety significance.

The systems, structures and components important to safety shall be designed, manufactured, installed and operated so that their quality level and the inspections and tests required to verify their quality level are adequate considering any item's safety significance.

According to the new YVL Guide 2.1 that was issued in the beginning of 2001: To comply with the above principles, the systems, structures and components of the nuclear power plant are grouped into Safety Classes 1, 2, 3, 4 and Class EYT (classified non-nuclear). The items with the highest safety significance belong to Safety Class 1.

A safety class of a system, structure and component of a nuclear power plant has to be specified and it is determined by its safety significance.

2.2 Effect of safety classes

The effect of the safety class on the systems and components is substantial starting from the design, manufacturing and construction and their quality assurance and extending to technical specifications, inspections and tests during operation. According to the YVL guides for example

- In Safety Class 1, the basic dimensioning of valves shall be in accordance with ASME Boiler and Pressure Vessel Code and a stress and fatique analysis in accordance with ASME Code.
- Components in Safety Classes 1 and 2 shall as a rule be subjected to component-specific functional tests in connection with their manufacture.
- The applicability of the manufacturing instructions shall be checked by means of work and procedure tests as regards Safety Classes 1 and 2.
- The welding procedure or work tests associated with manufacture or repair shall be performed on the pressure-retaining components of Safety Class 1 and 2 valves. The tests shall be performed on other valves if so required in the design bases.
- The pressure and tightness tests shall be performed in accordance with the design basis standard. If not so required in the design bases, a separate pressure and leak-tightness test plan shall be presented for Safety Class 1 valves.
- Safety Class 2 and 3 valves shall, in addition to internal pressure, be dimensioned against the greatest possible force exerted by piping. If a valve is subjected to a load causing significant fatique, the valve shall undergo fatique analysis in accordance with Standard ASME Code, Section III, NB-3500.
- The durability of a valve's seat and disc surfaces in Safety Classes 1 and 2 shall be demonstrated by means of one of the following clarifications:
    - surface pressure calculations,
    - impact velocity,
    - experimental investigations and operating experience.
- The construction inspection of Safety Class 1, 2 and 3 valves is aimed to be performed at the manufacturing plant.
- STUK controls the manufacture of Safety Class 1 and 2 valves and their actuators by audits to the manufacturing plant.

- STUK conducts the construction inspection of Safety Class 1 and 2 valves with the valve assembled and disassembled.
- A construction inspection pertaining to installation is performed on all Safety Class 1, 2 and 3 valves and their actuators after completion of installation. Class EYT/A valves may be structurally inspected in conjunction with the construction inspection pertaining to installation.
- Classified valves and actuators shall undergo periodic tests to verify operability and condition of the valves. For this purpose, the operator of the plant shall have a programme presenting the testing times for each component and the instructions to be followed in testing.
- In-service inspections of piping are much more frequent and extensive for Safety Class 1 piping than for Class 2 piping.
- Safety Class 1 and 2 systems have to fulfil the single failure criterion as a rule. This criterion is usually fulfilled by systems designed to perform a safety function but not by such systems or equipment like the pressure vessel and the primary pressure boundary in general the failure of which leads to an initiating event.

The amount of documentation and costs linked to the equipment increases dramatically as the safety class is raised. The aim of "correct" classification is to ensure that resources are used where needed or useful, and not wasted in less important systems or components. The above list indicates that the rules are not truly distinct to uniquely separate classes 1, 2 and 3 from each other.

Most of the above criteria address the QA requirements under design, manufacturing and installation (including spare-parts). A few concern actions during plant operation like inspection and test intervals as well as Allowed Outage Times (AOT). This study will show that there may be good reason to evaluate separate safety significances for these two areas,

- one close to the traditional QA-purposes defining Safety Classes and
- the other one for technical specifications and in-service inspections.

Different risk-importance measures apply to different areas. The choice of the measure depends on what one wants to influence. The safety classification of the systems and equipment is defined on the basis of the first area. The other area is taken into account in defining in-service inspections and inside technical specifications defining e.g. test intervals and allowed outage times.

One should also keep in mind two subsets, passive structures and active components. Initial QA is rather similar to both and depends on certain risk-importance measure(s), although active components (including electronics) may be subject also to long series of tests or field-use to demonstrate some degree of reliability (failure rate).

During plant operation passive structures rely on periodic inspections or monitoring. The quality of components and structures that can cause initiating events is assured with methods similar to those listed above for initial QA, and inspections or preventive maintenance during operation.

When Safety Class is raised the extent and frequency of in-service inspections and testing is increased in general. However, small diameter piping may have less requirements than larger diameter piping of a lower safety class.

Considering piping it is acknowledged that the higher class piping components should have in general smaller break probabilities than the lower class piping components. This is especially true if the Leak Before Break principle is applied. LBB implies that a piping system is not susceptible to any damage mechanisms and that it is under in-service-inspection and leak monitoring as means to prevent major piping failure.

Sufficient availability of active components in standby systems is obtained by periodic activations (tests) and prompt repairs (AOT, which however should be in reasonable relation to the test interval T, because T/2 is an "accepted" average outage anyway). Components with revealed failures rely on prompt repair (AOT) if they do not cause initiating events.

The effect of Safety Class on the reliability of a component is not clear in all respects. The qualification of a component to the operating conditions has to be shown by tests for classified components. Therefore it is known that the classified, and qualified, components will operate in the accident conditions as designed. On the other hand non-classified components are not known to be operable in accident conditions if the conditions deviate from their design conditions or normal environment in which there is experience or tests. In the sense of reliability and risk analysis we know that we can usually apply the reliability parameters obtained in normal conditions for the qualified components. We can use the testing experiences of the qualified components for estimating their reliability parameters. We do not know if non-classified components operate in accident and harsh environmental conditions and therefore we cannot straightly apply the reliability parameters of normal conditions if the accident conditions deviate from normal. However, there are plenty of safety related components that even in case of an accident need to function only in similar conditions as normally, and for those testing and reliability parameters under normal conditions are valid.

Table 1 illustrates the testing demands of active equipment of the different safety classes for accident conditions when they differ from the normal conditions. Safety Class 1, 2 and 3 components should always be designed for accident conditions. Safety Class 1 and 2 equipment is qualified by extensive type tests for accident conditions. Safety Class 3 equipment is not usually type tested but it can be qualified as needed. Then the qualification tests are not as extensive. Sometimes non-classified components may need a qualification as well. Long series of tests that demonstrate the reliability of Safety Class 1 equipment are needed, like for example for primary safety valves. Reliability tests are also demanded for some Safety Class 2 equipment, like for example for automation equipment.

Table 1. Testing demands in accident conditions.

Safety Class	Designed for accident conditions	Type test	Reliability test
1	Yes	Yes	Yes
2	Yes	Yes	Yes / No
3	Yes	No / Yes	No
EYT	No	No	No

In many cases the environment is not different under accident conditions, at least not when the equipment has to operate. In such cases the conventional components out of large batches and with extensive operating experiences can be more reliable than components of a small batch of qualified components. This fact may be taken into account in the safety classification of components. Current classification system or licensing practice does not seem to very well recognise the possibility to prove a certain reliability for any EYT component by testing or field experience, when accident conditions for it do not deviate essentially from normal.

We must qualify equipment for accident conditions if that equipment is needed in the mitigation. If we do not have equipment qualified for the conditions where it is needed it is hard to specify in PSA analyses a value better than 0.5 for such a component, expressing a total ignorance. The safety classification of equipment must be defined in such a way that the operability is quaranteed in all kinds of conditions in which the equipment is needed.

Basically the same preventive maintenance actions are performed for both the classified and non-classified components. However, only specified and qualified spare parts can be used for classified components. The quality control for classified components is much more detailed and their testing is more careful. This leads to the assumption that the failure probability due to design, installation, maintenance and aging problems should be lower for classified components. This means also that the possibility of common cause failures should be smaller for classified components.

The problem is that no convincing empirical studies exist to demonstrate how much the failure probabilities of different safety class components differ. We do not know how much the failure rate of a component or here actually a process position changes when its safety class is changed. We can only assume that the failure rate of a higher class component is smaller than that of a lower class component or we can be more confident with the failure rate of a higher class component. But we do not know if the difference is significant or negligible. Sometimes non-classified components manufactured and used in large quantities have better reliability than a small number of classified components with limited experience.

If there is a rule that the test interval of a component must be shorter than some value in a certain safety class or with certain safety significance (or Tech Spec class, if such is defined), we know approximately the effect on the unavailability *u* of the component. There exists evidence that most component failures tend to be more time related than demand related, according to the well known formula in approximative form

$$u = q + \lambda\tau + \lambda T / 2\,, \tag{1}$$

where q = failure probability per demand,

λ = failure rate,

τ = repair time and

T = test interval.

The time dependent behaviour dominates with long test intervals. However, the test intervals of differently classified components are often the same, due to practical reasons related to the operation of the plant. On the other hand, if safety classification truly reduces the failure rate, this has a double impact in Eq. 1.

We know that design, installation, maintenance and aging problems contribute significantly to the common cause failure probabilities. Therefore we can conclude at least for this pilot study that common cause failure rates are lower for higher class components. The test interval effect should be quite clear, too: the longer the test interval the higher the CCF unavailability. Testing schemes affect also the CCF probabilities but they are not administratively or by regulatory guides dictated by the safety class.

So, different risk measures and safety significances may be justified for different purposes and systems.

3 Safety significance and importance measures

3.1 Safety significance

A safety class of a system, structure and component is to be determined according to its safety significance. How to assess a safety significance of a system, structure and component? YVL Guide 2.1 does not present guidance to assess safety significance but it presents guidance to assigning systems to the safety classes and the requirements of the classification document, in which the applicant for the operating licence shall describe the classification of the nuclear power plant's systems, structures and components. The classification practices and rules are not presented here because probabilistic risk estimates are the basis in this report.

Importance measures that are usually calculated in the PSA's today can be used for estimating the safety significance of a component or a system. PSA tools include usually several risk importance measures that are quantified with simple mathematics. These importance measures are easily quantified for all basic events and initiating events of a PSA model.

3.2 Importance measures

Several different importance measures have been developed to quantify a safety significance of an item based on the PSA. Here we consider only those importance measures that are available in the codes used for PSA modelling and quantification, like Risk Spectrum /2/.

The Fussell-Vesely importance of an item i is the share of the probabilities of those minimal cut sets (MCS) that include i. FV importance is the probability of the MCSs including item i divided by the system failure probability Q_{TOP}:

$$FV_i = \frac{Q_{TOP}(MCSs\_including\_i)}{Q_{TOP}} \approx \frac{Q_{TOP} - Q_{TOP}(Q_i = 0)}{Q_{TOP}} \tag{2}$$

The right hand version of Equation 2 is also calculated by Risk Spectrum and called as the Fractional Contribution. FV gives the relative risk reduction when the probability of item i is decreased to zero. It gives also the relative risk increase when the probability of item i is doubled.

The Risk Reduction Worth or Risk Decrease Factor is a measure of the risk that would be reduced by reducing the probability of item i to zero:

$$RDF_i = \frac{Q_{TOP}}{Q_{TOP}(Q_i = 0)} \tag{3}$$

RDF_i gives the maximum achievable risk decrease in trying to improve the reliability of a component. [Note that FV and RDF uniquely determine each other, i.e. they measure the same thing]. Thus, if RDF_i is large and there is a need to reduce risk, it is worth while to consider raising the Safety Class of a component. A special feature of RDF_i is that it can give equal importances for two lines of a redundant system (e.g. if they appear in the same minimal cut sets) even if the other line were much more reliable. Between such components or lines, if there is need to reduce risk, one has to consider improving the item that has technically and/or economically better potential for improvement. If a higher safety classification has an effect as a relative multiplier on failure rates, it does not really matter which one is improved.

The Risk Achievement Worth or Risk Increase Factor is the factor by which the risk increases when item i is not available:

$$RIF_i = \frac{Q_{TOP}(Q_i = 1)}{Q_{TOP}} \tag{4}$$

RIF_i gives the risk increase when a component is taken out of use. If RIF_i is small then maybe the safety class can be lowered. A problem with RIF_i is that in a redundant system it can give a higher importance for a more reliable component, which is not reasonable when we consider changing the safety class. However, since RIF is a measure of the importance of a failed state, it might be a good measure for prioritisation of repairs, if several components are failed. Furthermore, as it reflects the importance of detecting and repairing a failed component, it might be a good indicator for technical specification classification in determining allowed outage times.

Combinations of these risk importances have also been used to measure a safety significance of a component. An example of measuring a risk importance of a component has been presented in a report on risk-informed in-service inspection and in-service testing /3/

Risk Category	Criterion
High	FV > 0.001 (or > 0.005)
Potentially high	FV < 0.001 (or < 0.005) and RIF > 2
Low	FV < 0.001 (or < 0.005) and RIF < 2

Several other importance measures have been developed and applied but the ones presented above are the most frequently used and automatically quantified by PSA programs. Other interesting measures for this study are the conditional Core Damage Probability (CCDP) estimates, which have been used for example for measuring the risk significance of piping segments in EPRI's in-service-inspection program, which gives an example of measuring the consequence importances

CCDP	Consequence class
$< 10^{-6}$	Low
$10^{-6}\ldots10^{-4}$	Medium
$> 10^{-4}$	High

These can be utilised for estimating the safety significance of piping segments and maybe of other components the failures of which lead to initiating events.

The above measures of safety significance are usually defined in terms of annual core damage frequency (CDF). If the level 2 PSA has been performed it is worth while to study the importance measures in terms of large early release frequency (LERF), too, because some components may be important in for example maintaining the integrity of containment even though not important in terms of CDF.

3.3 Group importances

The above measures of safety significance are defined for basic events or initiating events. Group importances are calculated in the same way as presented above for individual basic events. When quantifying RIF or RDF the unavailabilities are set to 1 or to 0 for all the basic events that belong to the group. This group can include for example different failure modes of a component. In a group of components, say a part of a system, which performs the same safety function, the system-specific RIF is equal to the corresponding importance of a basic event, for example a CCF that fails the system. The group of redundant identical components has the same RIF-importance as the complete CCF of these components.

FV importance of a group of components is obtained by quantifying Eq. 2 taking into account all MCSs that include one or more items i that belong to the group. It is easier to quantify the right hand side of Eq. 2 by setting to 0 all the basic events that belong to the group. Risk Spectrum calculates this Fractional Contribution for a group of components. If the group of components is a system or a subsystem this importance measure takes into account not only the complete failures of the system but also partial ones. Another way to quantify FV importance of a system would be to take into account only those MCSs that include such failure combinations of the components of that system that fail the system. Considering initiating events FV measures can be summed up. The same is usually true for different failure modes of a component.

3.4 Selection of importance measures

The safety significance of a system is important to define and measure when we are setting a safety class (or classes) for a system. Traditionally we are interested in what safety functions the system performs. One good measure of the system is obtained when we quantify the risk increase when the system is taken out of use. For that purpose the RIF is a relevant measure. The same concerns a group of redundant identical components. Therefore RIF might be a good measure to define safety significance for traditional QA-related safety classification purposes.

As concluded at a component level RIF measures the importance of prompt repairs, or plant shutdown in extreme cases, as may be reflected in Tech Spech. Therefore RIF can be used in defining allowed outage times.

If the failures of the system can lead to initiating events then RIF cannot be used. For that purpose CCDP is a relevant measure of the safety significance.

RIF and CCDP are not dependent on the reliability estimate of the item that we consider. In that sense they are good measures for QA-related safety classification purposes. However, they pose the following problems

- they do not depend on the properties of the item but only on the properties of all other items,
- RIF measures the importance of downtime (relevant Tech Spech measure) but it does not take into account natural detection and repair opportunities (duration of states $Q_i = 1$), even if they can be quite different for units of the same RIF value,
- CCDP can give the same importance for different initiators that have very different frequencies, and therefore different true risk significance.
- RIF can be rather independent of the number of redundant trains or the degree of separation between the trains (minimisation of CCF vulnerabilities).

FV has some features better, but it can be used for a specific new system only after the system is designed or when a definite reliability target has been set for it. Given that a PSA is available in this pre-design phase one can apply RIF and CCDP to define QA-related Safety Class as well as availability targets and initiating event rate targets for guiding individual new system design. (If a PSA is not available, none of the importance measures can be applied for design guidance.) Redundancy, diversity and safety classification can be used to accomplish the reliability target, given that safety classification is relevant for assuring the reliability. Safety classification alone does not define redundancy adequately. When the system has been designed, FV can be quantified by using relevant generic reliability data or relevant other experience. In this phase FV can give guidance in modifying the safety class and in setting test intervals for the active components and in defining the in-service-inspection program.

It is assumed here, that PSA is used as a design aid, as required or implied by YVL 2.8. It means that reliability and risk assessments are carried already at the conceptual level of design, and at least generic data is available for quantification. Thus FV and other importance measures can be used in the design process. It turns out that it is better to consider the pairs (RIF, FV) and (CCDP, FV) together rather than single measures.

Let us consider smaller entities like individual valves or pumps or pump lines. We found earlier in Ch. 3.2 that RIF does not always give reasonable values and therefore is not a reliable measure of safety significance for this purpose. In this case FV can be used and it is applicable for both initiating events and basic events.

FV takes into account the reliability estimate of the item that we are looking at. The more reliable item the smaller its importance is. Therefore FV is not an absolute measure of a safety significance of an item. If we raise the Safety Class the reliability may get better and the FV gets lower, which truly is the objective. After that change is made, the measure shows, probably, that further change is not needed.

If a component is replaced by a component with a higher failure rate FV is increased and if all redundant components are replaced FV could be increased to the power of that redundancy. For example if the failure rate of all the four redundant components is doubled FV could get $2^4 = 16$ times higher. Taking into account common cause failures this effect is not as drastic. One could question if this is correct behaviour of the risk importance used for the selection of a safety class. This means that we should determine the safety class of a system with high redundancy into a higher class than a system with lower redundancy *given the same importance* and need for improvement, and a system with bad components into a higher class than a system with better components. If the higher safety class then improves the components of that system FV would get lower and we can say that the safety classification has affected ideally. A conclusion in this kind of situation is that FV can be used as a basis for safety classification.

The problem in the previous two cases is that we do not know the effect of the safety class on the failure rate. On the other hand we know the effect of the test interval and therefore FV can be used in adjusting the test intervals. FV can also be utilised in selecting between two components if we know their reliabilities and in determining the redundancy level to achieve the needed safety targets. Thus, FV can be used in defining test intervals and in balancing plant safety based on known component reliabilities and system structures.

Let us consider a situation where we have a system with low FV importance. Given that the total risk is also already low, can we set a low safety classification for it? Lowering the classification could mean higher failure rates of the components and therefore higher FV. If the obtained FV is still low enough we can be satisfied with it. However, if FV gets too high lowering the classification is not correct.

As a conclusion RIF may be a good importance measure in assessing the initial safety significance of a system for traditional QA-related safety classification. Conditional Core Damage Probability can be used initially for comparing the safety significances of initiating events. However, it is advisable to use both pairs (RIF, FV) and (CCDP, FV) in the design and licensing process, when they can be defined.

When components of an existing system are being requalified FV importance can give reasoning for upward or downward qualification. It can be used for initiator type events like pipe breaks as well as for unavailabilities. Both RIF and FV can be used for measuring safety significances for technical specifications. RIF is useful in defining allowed outage times and FV useful in defining test intervals. All these three measures are useful and actually have been used in defining in-service-inspection programs. All these measures can be quantified for both CDF and LERF and it is recommended to consider both points.

4 Application systems and components

Application systems and equipment are selected so that all the different safety classes and a wide range of safety importances are covered. Therefore the application systems are selected Class by Class taking into account their safety importance.

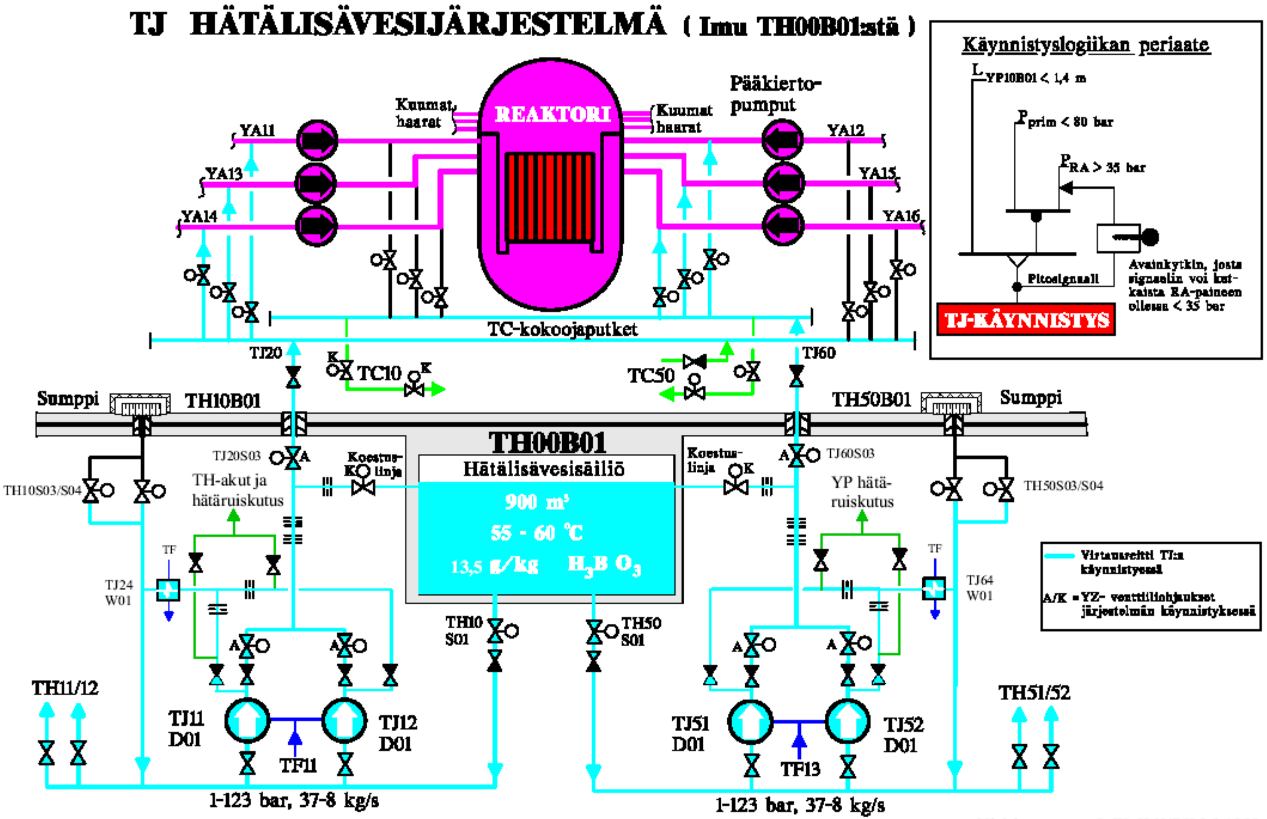
4.1 Safety Class 1

According to the YVL Guide 2.1 Safety Class 1 includes primary circuit components whose rupture would result in a leakage of such magnitude that it could not be compensated for by the make-up water systems of the nuclear power plant. In conformity with this principle, the following primary circuit components remain outside Safety Class 1:

- small-diameter pipes (inner diameter not more than 20 mm, in case of Loviisa much less)
- components connected to the reactor coolant system through a passive flow-limiting device and which, if ruptured, do not cause a leak larger than that caused by the rupture of a 20 mm pipe, as well as
- components which, in the event of their failure, can be isolated from the reactor coolant system by two successive, automatically closing valves whose closing time is short enough to allow for normal reactor shutdown and cooldown.

All these systems have the potential to cause a Loss of Coolant Accident (LOCA) when the pressure boundary is broken. Thus, by quantifying their importance measures we get a range of values to which we can compare the importance measures of components from other safety classes.

We select the primary piping and a relevant part of the High Pressure Safety Injection (HPSI) system TJ as an example of Safety Class 1 systems. TJ system (Fig. 1) includes 4 pumps that are connected to two redundant main lines, two pumps in both lines. One pump is needed to provide water into the reactor and for cooling of the reactor in primary and steam piping breaks and equipment failures. Only the part from the containment isolation valve TJ20/60S003 towards the reactor belongs to Safety Class 1. TJ system is interesting because a part of it belongs to Safety Class 2, too, and a corresponding system is likely to be important for all PWR plants.



Yleiskuvaus, osa5, TJ, ILK/RII 9.9.1998

Figure 1. High pressure safety injection system TJ.

4.2 Safety Class 2

The following is an example list of systems that belong to Safety Class 2 according to YVL 2.1:

- Primary circuit components not assigned to Safety Class 1.
- Systems and components required for a reactor trip.
- Emergency core cooling systems intended for loss-of-coolant accidents.
- The boron supply system required to shut down the reactor or to maintain it in a sub-critical condition during a postulated accident.
- At a PWR plant, the part of the make-up water system which is bounded by make-up water pumps and the primary circuit.
- The following parts of the steam and feed water systems:

    - at a PWR plant, the part inside the reactor containment that is bounded by the outermost isolation valves,
    - at a PWR plant, the part of the emergency feed water system of the steam generators that is bounded by the emergency feed water pumps and steam generators, and
    - at a BWR plant, those parts of the steam system outside the reactor containment that are bounded by the isolation valves and the subsequent shut-off valves.
- A protective instrumentation and automation system for starting a reactor trip, reactor emergency cooling, isolation of reactor containment or other safety function necessary in a postulated accident.
- Electrical components and distribution systems necessary for the accomplishment of safety functions of systems in Safety Class 1 and 2.
- Electrical power supply equipment ensuring electricity supply to Safety Class 2 components upon loss of both offsite power and power supplied by the main generators.

We select the small primary piping and a relevant part of the high pressure safety injection system TJ (Fig. 1) as an example of Class 2 systems. See the presentation of the TJ system in the previous Chapter 4.1.

4.3 Safety Class 3

The following is an example list of systems that belong to Safety Class 3 according to YVL 2.1:

- The boron supply system bounded by the borated water storage tank in so far as the system or parts thereof are not classified to a higher safety class.
- At a PWR plant, those parts of the reactor volume control system that are not assigned to a higher safety class.
- At a PWR plant, those parts of the emergency feed water system that are not assigned to Safety Class 2.
- Systems needed for the cooling and pressure relief of the primary circuit, if they are not classified to a higher safety class.
- Cooling systems, including their cooling water channels and tunnels, essential for the removal of
    - reactor decay heat,
    - decay heat from spent fuel stored outside the reactor ,
    - heat generated by Safety Class 2 components,
    - heat generated by the above-mentioned systems themselves

  into the ultimate heat sink, and which do not belong to a higher safety class.

- Parts of the sealing water, pressurised air, lubricating, fuel etc. systems necessary for the start-up or operation of systems in Safety Classes 2 and 3.
- Electrical components and electric power distribution systems required to accomplish the safety functions of Safety Class 3 systems.

We select the Component Cooling Water (CCW) system TF as an example of Class 3 systems. TF consists of 4·100 % pumps, 5·50% heat exchangers and redundant pipelines TF11 and TF13 (Fig. 2) to the objects that need cooling (Fig. 3). One pump and two heat exchangers are needed in LOCA situations to transfer the heat from the emergency cooling systems to the service water system and eventually to the ultimate heat sink. TF system is a support system for example of the previously presented TJ system providing cooling water for the TJ pump motors and sealing water for the TJ pumps. Normally two pumps and four heat exchangers are in operation.

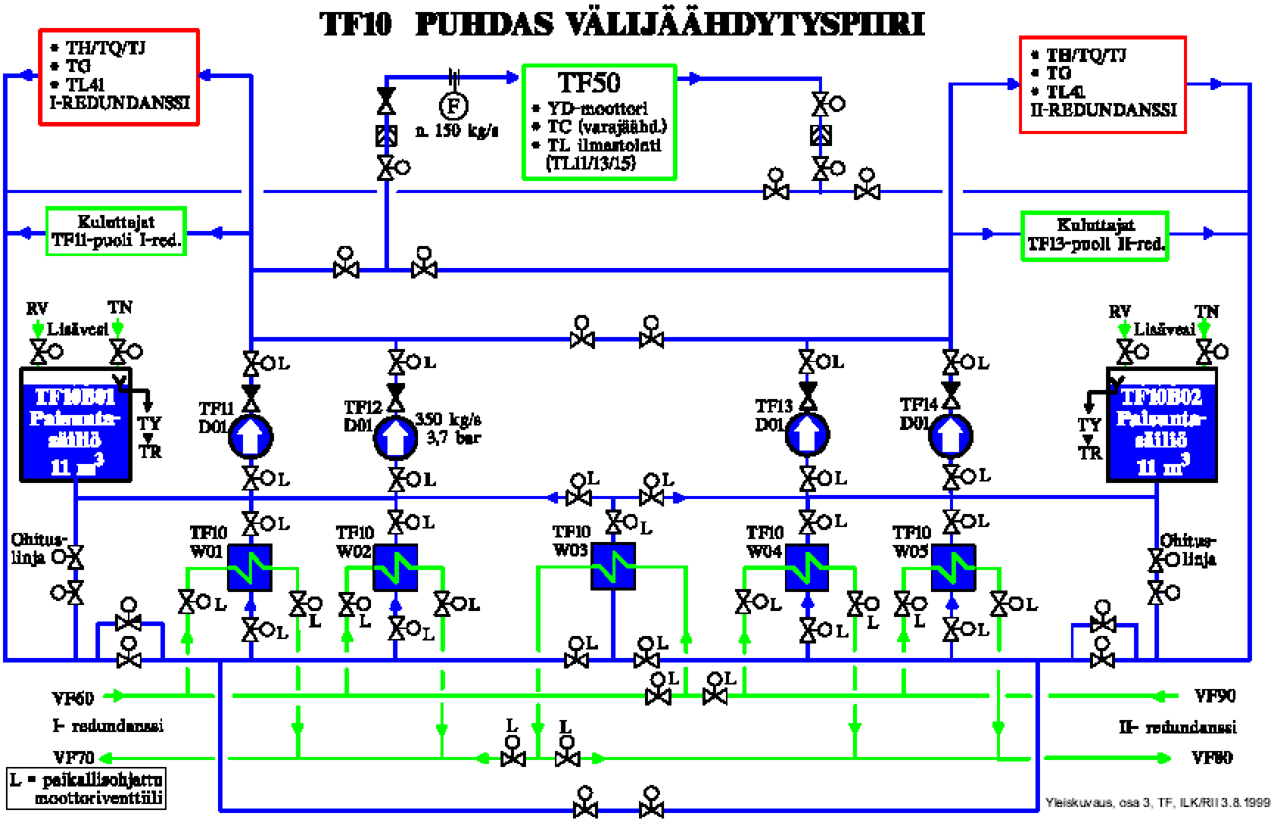


Figure 2. Component cooling water system TF (subsystem TF10).

Parts of TF system belong to Safety Class 2 like containment isolation valves and some valve actuators that are controlled by the plant protection system. Some valve actuators are non-classified.

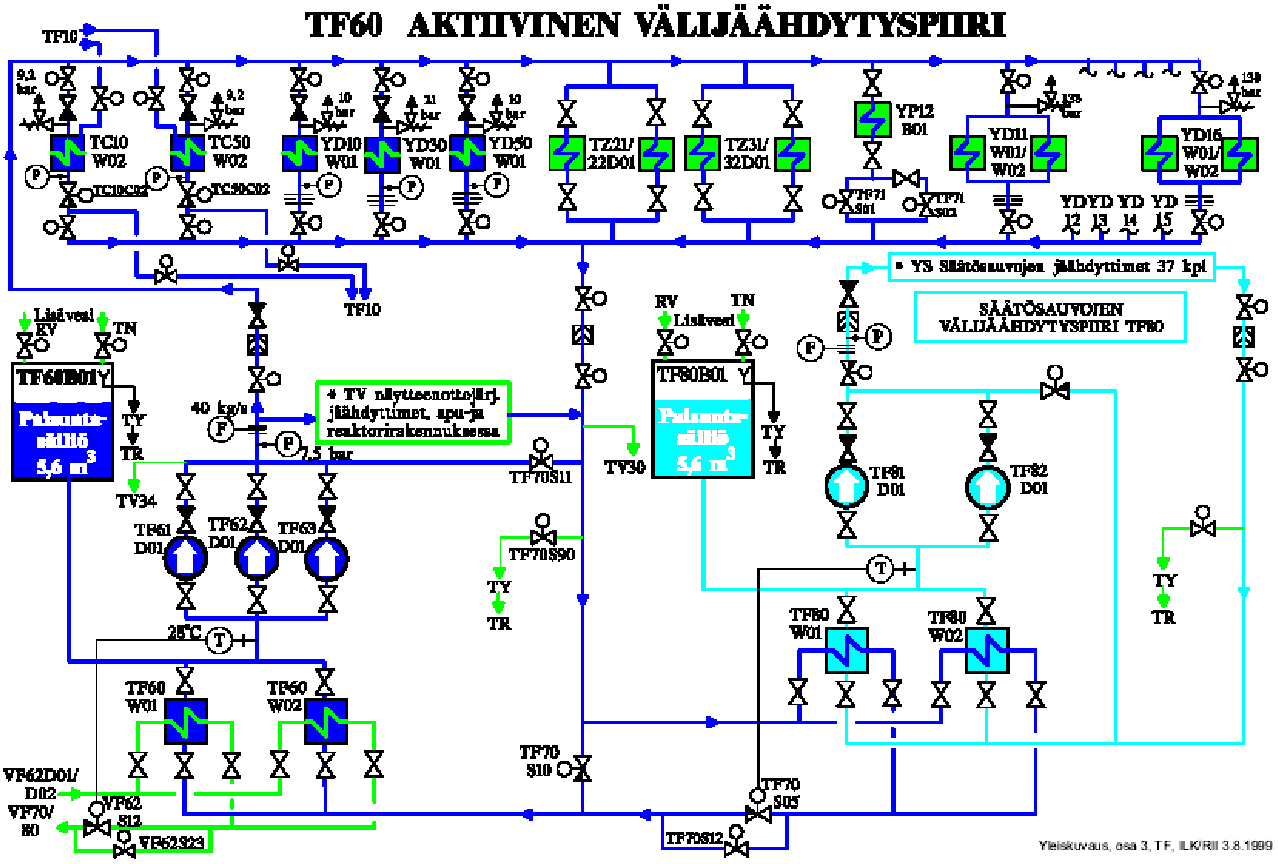


Figure 3. Component cooling water system TF (subsystem TF60).

4.4 Safety Class 4

The following is an example list of systems that belong to Safety Class 4 according to YVL 2.1:

- Fire protection systems:
  - fire alarm systems and
  - fire extinguisher systems.
- Of systems and components connected to turbine and generator, those that could significantly contribute to their failure, for example:
  - bearings,
  - rotor,
  - turbine and generator protection systems,
  - turbine trip valves,

  - oil systems,
  - generator hydrogen cooling system,
  - vibration monitoring system,
  - generator circuit-breaker and field breaker.
- The below I&C and computer systems:
  - PWR secondary side main controls,
  - monitoring of secondary circuit water chemistry,
  - monitoring for radioactivity in laboratories,
  - I & C and computer systems contributing to safe plant control and operation,
  - safety-significant information management systems relating to plant operation and maintenance.
- Plant communication systems to assure normal operation and for use in accident management.
- Environmental radiation monitoring and meteorological measurements.
- Systems for monitoring external threats, for example:
  - a flood monitoring system,
  - a system for monitoring the ultimate heat sink (i.e. the sea),
  - a frazil ice monitoring system.
- The main electrical power systems.

Currently no components belong to Safety Class 4 at Loviisa NPP, because this safety class has been defined in the latest version of the YVL Guide 2.1 that was published in the beginning of 2001. Therefore no systems were selected from this group to this study. It can be seen from the examples above that some Safety Class 4 systems may be important for safety like systems for monitoring external threats.

4.5 Class EYT

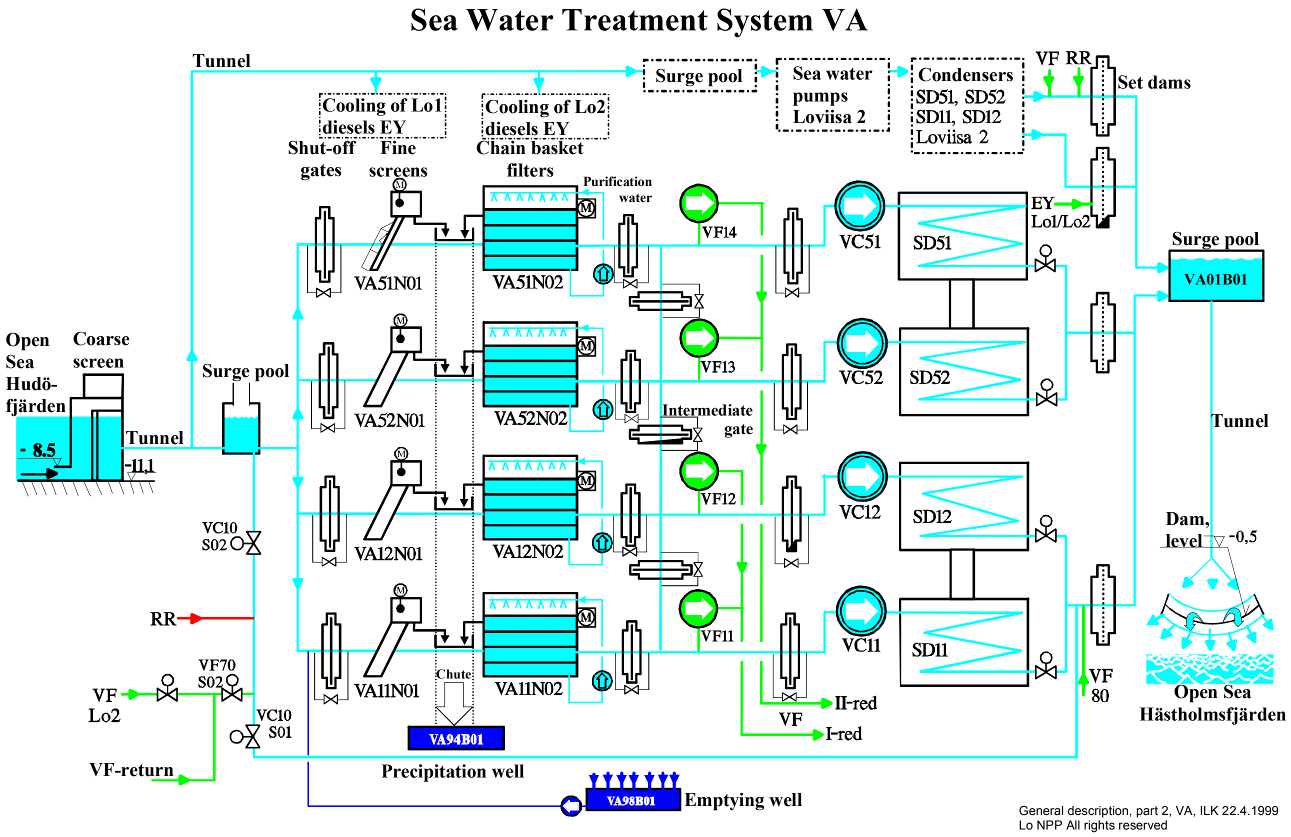
Safety Class EYT includes all systems, structures and components not assigned to Safety Classes 1, 2, 3 or 4.

Several EYT systems are not safety significant and are not interesting in this study. We select sea water treatment system VA (Fig. 4) as an application system because it is safety significant in many plants, not only in Loviisa. The cooling water for Loviisa NPP is taken from the sea via a 67 m^2 tunnel that is branched into both units. Both tunnels end up in a pond in front of the sea water pumping stations, which are divided into four channels. Every channel is equipped with a cleaning device, a service water pump VF11…VF14D001 (0.5 m^3/s) and a main sea water pump VC11, 12, 51, 52D001 (6.4 m^3/s). The service water pumps provide component cooling water and the main sea water pumps feed the main condensers. The cleaning device consists of

- three coarse bar sreens in the main tunnel intake (clear opening 80 mm),
- a fine bar screen in all four channels (clear opening 16 mm) and
- a chain basket filter in all four channels (netting density 1 mm^2).

The chain basket filters operate normally with an interval of six hours. In addition to this they start automatically if the level difference accross them gets over 7 cm. If the automatic start-up takes place four times per hour the filters are taken into continuous operation. The largest allowed level difference is 50 cm.

There are four service water pumps of which two operate normally. One pump is enough for safety systems in accident situations and one operating chain basket filter is judged to be enough for service water pumps. There are four CCW heat exchangers (TF) normally in operation and one is standby (see Ch. 4.3). If a plant unit has problems in getting cooling water it is possible to connect the service water from the other unit to provide cooling water for CCW heat exchangers.


Sea Water Treatment System VA

General description, part 2, VA, ILK 22.4.1999
Lo NPP All rights reserved

Figure 4. Sea water treatment system VA.

5 Importance measures and safety classes

The importance measures in this report are calculated for the PSA model at power operation taking into account internal and external initiators according to the Loviisa NPP PSA of year 2001 before the annual refuelling outage. The external initiators cover floods and severe weather phenomena but not fires. Fires are not taken into account because the fire model is currently being integrated with the other model. Seismic risks are low due to low seismicity. Some backfittings of the primary coolant pump (PCP) seal cooling system were implemented in the year 2001 refuelling outage decreasing considerably the risks due to both internal and external initiators from the values of this report.

5.1 Safety class 1

5.1.1 Safety Class 1 Primary Piping Importance Measures

Safety Class 1 consists of primary circuit components whose rupture would result in a leakage of such magnitude that it could not be compensated for by the make-up water systems of the nuclear power plant. Even smaller piping can have risk importance but such pipe breaks are not considered here. The CCDP values are the following:

- 0.004 if the rupture can lead to SLOCA, MLOCA or LLOCA,
- 0.012 if the rupture can lead to SLOCA or MLOCA and simultaneously a potential loss of the other HPSI redundancy,
- 0.0014 if the rupture can lead to SLOCA or MLOCA and
- $5.9 \cdot 10^{-4}$ if the rupture can lead to SLOCA.

These values indicate clearly the importance of such piping. They indicate the high safety significance potential of such piping sections, but they do not indicate the importances of the individual piping sections taking into account their weak and strong points. FV importance measure is needed for such purposes.

FV importance measures of such LOCA initiators depend on the rupture frequency of that component compared to the overall LOCA initiator frequency. The following FV importance measures are obtained for primary piping components (pipe sections) altogether

- $8 \cdot 10^{-3}$ if the rupture can lead to SLOCA, MLOCA or LLOCA,
- $9 \cdot 10^{-3}$ if the rupture can lead to SLOCA or MLOCA and simultaneously a potential loss of the other HPSI redundancy,
- $5 \cdot 10^{-3}$ if the rupture can lead to SLOCA or MLOCA and
- $4 \cdot 10^{-3}$ if the rupture can lead to SLOCA.

The rupture of a large pipe can lead to all LOCA categories whereas the rupture of a small pipe can lead only to a SLOCA. These values indicate the maximum possible risk importance of each kind of Safety Class 1 piping.

Let us assume that such primary leak frequencies in each category come from 100 components that have equal rupture frequencies. In that case the above values must be divided by 100. However, in the second category with the potential loss of the other HPSI redundancy the number of piping sections is limited so that the value can be divided by 10 at most. If the leak frequencies are dominated by e.g. 10 components then the above FV values must be divided by 10 to obtain their FV values.

The in-service inspection and testing program follows ASME Code, Section XI. Small diameter piping, < DN25 in Safety Class 1 and < DN100 in Safety Class 2, is not inspected. The SLOCA frequency comes probably mostly from the not inspected Safety Class 1 and Safety Class 2 piping. If we assume that 1/10 of the SLOCA frequency comes from the inspected Safety Class 1 piping and the leak frequencies are dominated by 10 components then the above values would be the following for these components

- $4 \cdot 10^{-4}$ if the rupture can lead to SLOCA, MLOCA or LLOCA,
- $9 \cdot 10^{-4}$ if the rupture can lead to SLOCA or MLOCA and simultaneously a potential loss of the other emergency core cooling redundancy,
- $1.4 \cdot 10^{-4}$ if the rupture can lead to SLOCA or MLOCA and
- $4 \cdot 10^{-5}$ if the rupture can lead to SLOCA.

This indicates the difficulty in applying FV importance measure for pipes as it depends on the partitioning of the piping and the scope included in estimated values of the item that is being studied, and the estimated values may depend on the safety class that is set to the components. But one can also argue that this is exactly how it should be, when using generic data (for some class/classes) at plant commissioning and more plant-specific data later on.

This indicates also that there are large differences between the component FV importances within the Safety Class 1 piping components. Some of them might have negligible importance measures and some as high as $1 \cdot 10^{-3}$. There is evidently a potential to reduce the risks by reallocating the in-service-inspection resources. Small diameter piping can be as important as larger piping and even more important. Thus, as much attention has to be paid on them as to the larger piping.

Considering the potential effect of a change in the safety classification one has to face the question: If the safety classes of such components are changed into a lower class are the rupture frequencies increased due to lower quality requirements and less inspection and control? At least we tend to believe that the effect is such. Piping failure data collection systems hopefully can help answering such questions in the future. The risk-informed in-service-inspection programs are also promising.

The Leak Before Break concept has been shown to lead to very low pipe rupture frequencies according to the probabilistic fracture mechanics analyses. LBB is usually applied to the large Safety Class 1 piping. It is not applied for Loviisa piping, which is the reason why we have not assessed lower LOCA initiating event frequencies.

5.1.2 Safety Class 1 HPSI System Importance Measures and Comparison to Technical Specifications

The following FV importance measures are obtained for High Pressure Safety Injection (HPSI) system components that belong to Safety Class 1:

- $2.9 \cdot 10^{-4}$ and $1.5 \cdot 10^{-3}$ for a rupture of each of the two HPSI lines outside containment,
- $1.2 \cdot 10^{-3}$ for the common outlet line components (TJ20S003 and S004 that is the check valve inside the containment) of the two HPSI pumps (the HPSI system consists of two redundancies and one redundancy includes two pumps),
- $1.2 \cdot 10^{-3}$ for the CCF of HPSI Safety Class 1 components (the check valves) and
- $4.2 \cdot 10^{-3}$ for the HPSI system Safety Class 1 components altogether.

Notice that the first example above for the HPSI system is an initiating event quantified with a frequency and the second one consists of basic events having unavailabilities. The system importance for Safety Class 1 components altogether includes also the above mentioned initiating events.

It should also be noticed that the active components presented above belong functionally to Safety Class 2. Therefore such failure modes could have been dealt with Safety Class 2 components. However, in this study all the failure modes of these components are taken into account under the comparison of Safety Class 1 importances.

The CCDP value for a pipe rupture of a HPSI line outside containment is as high as 0.9, because that can lead to a loss of the emergency core cooling. Therefore special attention should be given to the in-service-inspection of those pipe sections.

If we defined FV importance measures so that we take into account only those MCSs that include such failure combinations of the components of that system that fail the system the FV importance would be

- between $4.2 \cdot 10^{-3}$ and $1.2 \cdot 10^{-3}$ for the HPSI system Safety Class 1 components altogether.

The corresponding RIF measures of the basic events (not initiating events) are

- 2.5 for the the common outlet line components,
- 34.5 for the CCF of HPSI Safety Class 1 components (check valves) and
- 34.5 for the HPSI system Safety Class 1 components altogether.

The technical specifications of the HPSI system define the Allowed Outage Times so that as a rule one component failure has the AOT = 3 days. Failures that cause the failure of the other redundancy lead to the immediate shutdown of the plant. Consequently

- an immediate shutdown is demanded in case of the failure to open of the check valve TJ20S004 and also of the motor operated valve TJ20S003, but the AOT = 3 days in case of the failure to close of TJ20S003, because that failure mode affects only the containment integrity. TJ20S003 is normally open and it is closed when a pump is tested.

The FV importance measures of TJ system Safety Class 1 components are in the same range as those of the primary piping components. The system importance according to the RIF is very high 34.5. One reason for this importance is that the TJ system is necessary for coping with the PCP seal LOCA that is the most important risk contributor in Loviisa NPP.

The importances in the Tech Spec of this system are well in accordance with the PSA importance measures.

5.1.3 Comparison of Safety Class 1 Importance Measures

The different importance measures of Safety Class 1 components are compared in Table 2. Pipe rupture events have been quantified assuming that ten components determine the rupture frequencies. In case of the HPSI line outside containment an average value has been quantified for the two lines. All these values can be considered to be high and the components are considered to have a high safety importance. However, a part of the piping components that have little influence on the rupture frequencies and therefore their FV values are low can be considered to have lower importance. The extent of their in-service-inspection can be reconsidered.

Even if CCDP and RIF values in Table 2 are high, reasonably low FV-values indicate that current classification and practices have kept the risk under control. Special attention has to be given to the in-service-inspection of the piping sections that have a high CCDP, because of the potential uncertainties in assessing the rupture frequencies.

Table 2. Comparison of Safety Class (SC) 1 importances.

Event / equipment	FV	CCDP	RIF
SC 1 Piping with the possibility of SLOCA, MLOCA or LLOCA	$8\cdot10^{-4}$	0.004	
SC 1 Piping with the possibility of SLOCA or MLOCA and simultaneously a loss of the other HPSI redundancy	$9\cdot10^{-4}$	0.012	
SC 1 Piping with the possibility of SLOCA or MLOCA	$5\cdot10^{-4}$	0.0014	
SC 1 Piping with the possibility of SLOCA	$4\cdot10^{-4}$	$5.9\cdot10^{-4}$	
SC 1 HPSI line outside containment	$9\cdot10^{-4}$	0.9	
TJ20S003 and TJ20S004 together	$1.2\cdot10^{-3}$		2.5
CCF of the check valves	$1.2\cdot10^{-3}$		34.5
SC 1 components of the HPSI system altogether	$4.2\cdot10^{-3}$		34.5

5.2 Safety Class 2

5.2.1 Safety Class 2 Primary Piping Importance Measures

Safety Class 2 primary piping has a potential to cause a LOCA when the pressure boundary is broken. The importance measures are

- CCDP = $5.9 \cdot 10^{-4}$ and
- FV = $4 \cdot 10^{-3}$

if the rupture can lead to a SLOCA. The FV importance measures of such components assuming 100 dominating pipe sections with equal rupture rates are $4 \cdot 10^{-5}$. PCP seal water system pipelines (20…50 mm inside diameter) outside containment are important risk contributors because their rupture can lead to containment outside leakages, loss of PCP seal integrity and a potential loss of emergency core cooling. The importance measures are

- CCDP = 0.02 and
- FV = 0.18.

PCP seal water cooling heat exchangers (13 mm tube diameter) are important risk contributors because their rupture can lead to containment outside leakages via the CCW system, loss of PCP seal integrity and a potential loss of emergency core cooling. The importance measures are

- CCDP = 0.07 and FV = $7 \cdot 10^{-4}$ for YD11…16W001,
- CCDP = 0.7 and FV = $7 \cdot 10^{-3}$ for YD11…16W002.

Other component cooling water heat exchangers have also high importance values due to basically similar reasons as above.

The importance measures of Safety Class 2 piping are compared in Table 3 with the importance measures of Safety Class 1 piping. Ten dominating components are assumed in the quantification of FV importances. Reconsideration of in-service-inspection and safety classes is evidently needed. Especially in one case high FV (0.18) indicates that classification may not be satisfactory. In cases of high CCDP and relatively low FV-values classification is considered adequate, but in-service-inspection should be reconsidered. In the cases of the lowest CCDP values and low FV-values lowering SC1 to SC2 may be justified. Notice that there may be long sections of piping that have very low FV-values.

Sometimes plant modifications can give better results. An improvement to be implemented in Loviisa in the year 2002 refuelling outage ensures a reliable isolation of small primary leakages via certain parts of Safety Class 2 and 3 piping. This change will affect considerably the values presented above and in Table 3.

Table 3. Comparison of the importance of Safety Class (SC) 1 and 2 piping.

Event / equipment	FV	CCDP
SC 1 Piping with the possibility of SLOCA, MLOCA or LLOCA	$8 \cdot 10^{-4}$	0.004
SC 1 Piping with the possibility of SLOCA or MLOCA and simultaneously a loss of the other HPSI redundancy	$9 \cdot 10^{-4}$	0.012
SC 1 Piping with the possibility of SLOCA or MLOCA	$5 \cdot 10^{-4}$	0.0014
SC 1 Piping with the possibility of SLOCA	$4 \cdot 10^{-4}$	$5.9 \cdot 10^{-4}$
SC 1 HPSI line outside containment	$9 \cdot 10^{-4}$	0.9
SC 2 Piping with the possibility of SLOCA	$4 \cdot 10^{-4}$	$5.9 \cdot 10^{-4}$
SC 2 PCP seal cooling lines outside containment	0.18	0.02
SC 2 PCP seal cooling heat exchangers YD11…16W001	$7 \cdot 10^{-4}$	0.07
SC 2 PCP seal cooling heat exchangers YD11…16W002	$7 \cdot 10^{-3}$	0.7

5.2.2 Safety Class 2 HPSI System Importance Measures and Comparison to Technical Specifications

The FV importance measures of the most important HPSI system parts or components are

- $3.1 \cdot 10^{-5} \ldots 3.5 \cdot 10^{-4}$ for a HPSI pump
- $7 \cdot 10^{-5} \ldots 5.5 \cdot 10^{-4}$ for a HPSI pump line including the pump and the valves
- $5.3 \cdot 10^{-4}$ for the common cause failures of the HPSI pumps
- $1 \cdot 10^{-3}$ roughly for the HPSI system Safety Class 2 components altogether.

These values are a few times smaller than the corresponding values of the Safety Class 1 components of the same system, as expected. The other components of the HPSI system have much smaller importance measures than those presented above. The FV importances of the pump line components are shared according to their failure probabilities.

The corresponding RIF measures of the basic events are

- 1.01…1.08 for a HPSI pump
- 1.01…1.08 for a HPSI pump line including the pump and the valves
- 34.5 for the common cause failures of the HPSI pumps
- 34.5 for the HPSI system Safety Class 2 components altogether.

The pump line components have the same RIF values. The other components of the HPSI system have smaller importance measures than those presented above.

The importance measures of the HPSI system components of Safety Class 1 and 2 are compared in Table 4. The values of the individual components of Safety Class 2 are smaller than those of the Safety Class 1 components of the same system. However, the system specific RIF value is the same, because the same emergency cooling function is lost. Even these high RIF-values do not point to a need to change classification, as the FV-values are relatively low.

Table 4. Comparison of Safety Class (SC) 1 and 2 importances.

Event / equipment	FV	RIF
SC 1 TJ20S003 and TJ20S004 together	$1.2 \cdot 10^{-3}$	2.5
SC 1 CCF of the check valves	$1.2 \cdot 10^{-3}$	34.5
SC 1 components of the HPSI system altogether	$4.2 \cdot 10^{-3}$	34.5
SC 2 HPSI pump	$3.1 \cdot 10^{-5}$.. $3.5 \cdot 10^{-4}$	1.01.. 1.08
SC 2 HPSI pump line including the pump and the valves	$7.0 \cdot 10^{-5}$.. $5.5 \cdot 10^{-4}$	1.01.. 1.08
SC 2 CCF of the HPSI pumps	$5.3 \cdot 10^{-4}$	34.5
SC 2 components of the HPSI system altogether	$1 \cdot 10^{-3}$	34.5

The technical specifications of the HPSI system define the Allowed Outage Times so that as a rule one component failure has the AOT = 3 days. Failures that cause the failure of the other redundancy lead to the immediate shutdown of the plant. Consequently

- An immediate shutdown is demanded in case both pumps have failed or neither pump line motor operated valve does not open in the same redundancy, but the AOT = 3 days in case of one pump failure or one valve failure.

The pump lines are tested with 4 weeks test interval. It means in this kind of system that some components, which are needed in both tests of the same redundancy, are tested with two weeks test interval.

The importances of the Tech Spec seem to be in line with the PSA importance measures. The RIF shows most clearly the importance of the system and makes no difference between the safety classes when we consider a subsystem or a group of components. However, individual Safety Class 1 components have even RIF larger than 2.

5.3 Safety Class 3

5.3.1 Safety Class 3 importance measures

The intermediate Component cooling water CCW system has a wide range of component importances. FV and RIF values are presented in Table 5 for the CCW components indicating risk measures both for individual components and for groups of components. Some interesting FV-values are

- 0.01…0.04 for CCW heat exchangers (clogging failure due to algae)
- 0.008 for CCW pumps switchover automatics
- 0.0013…0.0014 for the PCP seal water cooling heat exchanger isolation motor operated valves TF74S001…12

- $2\cdot10^{-5}$…$1.4\cdot10^{-4}$ for the HPSI pump cooling line valves TF35S023, -24, TF45S023, -24
- $1.28\cdot10^{-5}$…$2.66\cdot10^{-4}$ for the TF11-14 pumps
- $1.84\cdot10^{-3}$ for TF11-line including the valves

The range of FV-values is large from negligible to 0.04. The largest values come from the clogging failures of the CCW heat exchangers. Would a safety classification affect this probability? Would the cleaning device or the cooling water system have been designed differently if the safety class would have been higher? Notice that the cleaning device that affect the clogging probability do not belong to this intermediate CCW system but to the main sea water system.

The second largest FV values come from the CCW pumps switchover automatics and restarting automatics.

In general the component-specific RIF values are small: 1.00…1.1. The largest ones are

- 35.6 for the CCF of the TF11…TF14 pumps
- 3.2 for TF11-line including the valves
- 2.1 for CCW pumps restarting automatics (after loss of off-site power)
- 1.7 for CCW heat exchangers (clogging failure due to algae)
- 1.6 for CCW pumps switchover automatics
- 1.00 for the PCP seal water cooling heat exchanger isolation motor operated valves TF74S001…12
- 1.01…1.08 for the HPSI pump cooling line valves TF35S023, -24, TF45S023, -24
- 1.01…1.06 for the TF11-14 pumps

The system-specific RIF importance 35.6 is a bit higher than for the TJ system, because TF is a necessary support system for TJ and some other systems, too. The FV importance is higher than for the TJ system. Therefore a preassumption would be that these systems would have the same safety classes.

The containment isolation valves TF70S001…4 belong to Safety Class 2 but their importance measures in level 1 PSA are negligible. TF70S001 has AOT = 3 days and the other valves have AOT = 24 hours. They are annually tested during shutdown.

Very small FV and RIF < 1.1 indicate that there may be justification to declassify some components. Few cases of high FV > $1\cdot10^{-3}$ and RIF > 1.5 might indicate need to upgrade SC3 to SC2. Remaining low FV even with higher RIF points to no need for upgrading the classification.

Table 5. The importances of TF system components and component groups.

Event / equipment	FV	RIF
CCW heat exchangers (clogging failure due to algae)	0.01…0.04	1.7
CCW pumps switchover automatics	0.008	1.6
CCW pumps restarting automatics (after loss of off-site power)	$4.5\cdot10^{-4}$	2.1
PCP seal water cooling heat exchanger isolation motor operated valves TF74S001…12	0.0013…0.0014	1.0
HPSI pump cooling line valves TF35S023, -24, TF45S023, -24	$2\cdot10^{-5}$…$1.4\cdot10^{-4}$	1.01…1.08
TF11…14 pump fails to start or run	$1.3\cdot10^{-5}$…$2.7\cdot10^{-4}$	1.01…1.06
Pumps TF11,12,13,14D01 fail to run CCF	$5.9\cdot10^{-5}$	35.6
TF11-line including the valves	$1.8\cdot10^{-3}$	3.16
Motor operated valve TF11S006	$2.3\cdot10^{-5}$	1.01
TF13-line including the valves	$7.9\cdot10^{-4}$	1.93
Motor operated valve TF13S006	$2.1\cdot10^{-5}$	1.007
Motor operated valves TF33S002, 3	$2.8\cdot10^{-5}$…$5.7\cdot10^{-5}$	1.04
Cooling of TL41 through TF34 (S001, 4, 5 together)	$8.45\cdot10^{-5}$	1.09
Cooling of TL41 through TF34 (S002, 3, 6 together)	$3\cdot10^{-4}$	1.08
Motor operated valve TF43S002 and 3	$1.8\cdot10^{-6}$	1.003
Cooling of TL41 through TF44 (S001, 4, 5 together)	$2.84\cdot10^{-5}$	1.013
Cooling of TL41 through TF44 (S002, 3, 6 together)	$1.47\cdot10^{-5}$	1.015
Cooling of PCP seal coolers	$9.36\cdot10^{-4}$	1.069
Pump TF61D001	$2.75\cdot10^{-5}$	1.009
Pump TF62D001	$3.78\cdot10^{-6}$	1.001
Motor operated valve TF10S006 FAILS TO OPEN	$2.91\cdot10^{-4}$	1.09
Motor operated valves TF10S011…15	$5.2\cdot10^{-10}$... $4.0\cdot10^{-7}$	1.00
Motor operated valve TF10S021, 22	$2.1\cdot10^{-5}$...$2.3\cdot10^{-5}$	1.00
Motor operated valve TF10S031…34 fails to close	$6.4\cdot10^{-9}$...$1.6\cdot10^{-8}$	1.00
Motor operated valve TF24S001, 3	$4.2\cdot10^{-6}$…$5.0\cdot10^{-6}$	1.06
Motor operated valve TF24S04, TF24S006, TF25S01, TF25S08, TF25S011 or TF25S018 (each)	$5.6\cdot10^{-7}$	1.01
Motor operated valve TF25S030 or TF25S040 (each)	$1.56\cdot10^{-8}$	1.00
TF28 and TF 29 manual cooling valves	$1.4\cdot10^{-7}$…$2.1\cdot10^{-8}$	1.00
Control valves TF28S011 and TF29S011	$1.1\cdot10^{-7}$…$6\cdot10^{-7}$	1.00
Manual valve TF32S011 or 12 (each)	$3.14\cdot10^{-4}$	2.49
Manual valve TF33S001	$6.95\cdot10^{-4}$	1.82
Manual valve TF42S011 or 12 (each)	$7.91\cdot10^{-5}$	1.38
Manual valve TF43S001	$3.36\cdot10^{-4}$	1.40
Motor operated valve TF50S011 or 14 (each)	$4.00\cdot10^{-7}$	1.00

5.3.2 Comparison of Safety Class 3 importances to technical specifications

The technical specifications of this system indicate the same level of safety significance as the TJ system. They define the Allowed Outage Times so that as a rule one component failure has the AOT = 3 days. Failures that cause the failure of one redundancy lead to the immediate shutdown of the plant. Consequently

- An immediate shutdown is demanded in case both pumps have failed or heat exchanger does not function or a valve in a heat exchanger line TF10S001…4 or TF10S007…10 does not open or in case of some valve failure combinations, but the AOT = 3 days in case of one pump failure or one valve failure.

An example of valve failure combinations leading to immediate shutdown is TF10S017 and S018 do not close, because these valves are used for isolating the line that connects the two redundancies.

Two pumps are running normally. The running time is 2 weeks and the dormant time is also 2 weeks and the pumps are tested with 2 weeks test interval.

As we can see the PSA importance measures and the technical specifications assess this system or parts of it as an important one. If the systems are to be classified according to their safety significance then clearly the classification of this system or parts of it are not consistent with the classification of the HPSI system.

5.4 Safety Class EYT

Sea water treatment system includes some important components. Their importance measures are presented in Table 6. The RIF values of the common cause failures are large indicating a large RIF of the system. The corresponding FV values are also large indicating that the initial QA-safety classification probably should have been higher. The RIF values of the individual components are rather small, but the FV values are comparable to those of the important Safety Class 1 and 2 components. RIF indicates that AOT has to be short for common cause or multiple failures. Clearly the safety classification does not reflect the safety significance of this system.

FV and RIF are rather clearly correlated in this case. As shown earlier, high RIF alone does not necessarily point to higher classification, but association with high FV points to a need for upgrading.

Table 6. The importances of the sea water treatment system components and component groups.

Basic Event / Equipment	FV	RIF
Coarse bar screens	$1.3 \cdot 10^{-3}$	1.03
Water Spray Pump VA11D001	$4 \cdot 10^{-3}$	1.2
Fine Bar Screen VA11N001	$5 \cdot 10^{-4}$	1.2
Chain Basket Filter VA11N002	$1.5 \cdot 10^{-3}$	1.2
Water Spray Pumps CCF	0.019	26
Chain Basket Filters CCF	0.02	26
Fine Bar Screens CCF	0.02	26

This is an exceptional example of the Safety Class EYT systems indicating that there are non-classified systems or equipment that are safety significant. Most of the EYT systems are insignificant to the safety of the plant and they are not modelled in the PSA. But this and earlier examples also indicate the need for the evaluation of safety significance for different purposes, each with its own numerical criterion. Notice also that the backfittings of the primary coolant pump seal cooling system decreased these importance values.

6 Pilot safety classification and conclusions

The original Safety Classification guides the design, manufacturing and installation and especially the QA process in them. It has also affected technical specifications and in-service inspection and testing. Based on the results of this study it is recommended that Safety Classification is limited to the QA-related issues and other points of view of safety significances are considered separately in technical specifications and in in-service inspection and testing.

According to the PSA importances the safety significances of many small diameter piping sections in Safety Class 2 are as high or even higher than those of larger diameter piping sections in Safety Class 1. This indicates that there is a need to reconsider the classifications or actually the in-service inspection programs. Nowadays very important piping sections are hardly ever inspected and on the other hand inspections are performed for piping sections that have minor risk importance. This fact has already been noticed in the pilot risk-informed in-service inspection studies.

The incompatibility concerning the piping classifications extends to the other components of the safety systems as well. Concerning the systems that were studied in this report we found out that the high pressure safety injection system classifications into Safety Classes 1 and 2 were in line with the PSA importance measures and also with the importances assigned to this system in the technical specifications. But the classifications of the component cooling water (CCW) system TF into Safety Classes 2 and 3 were inconsistent with the safety significances according to the PSA. The same inconsistency was found out from the sea water treatment system.

The reclassification of the CCW system would mean that some components should be raised into a higher Safety Class and some of them could be lowered. If such reclassification is made the support systems like the instrumentation and control systems have to be reconsidered, too. Other issues of the original deterministic reasoning have to be taken into account. Changing the classification of one system would mean a consideration or at least the reasoning of the support system classifications.

In order to achieve a balanced safety classification all relevant issues have to be taken into account and the classification cannot be limited into one system classification only, because the reasoning behind the support system classifications is often dependent on the main system classification. It is possible that this problem can be evaded and new classifications can be assigned to a system of an old plant if needed. It should be easier to define new inspection and testing programs as well as technical specifications for such systems. But difficulties might be encountered in this case, too, because of many interconnections. Therefore even a pilot reclassification is not tried in this study.

PSA importances can be used to valuate a safety significance of a system for safety classification. Risk Increase Factor (RIF) known also as Risk Achievement Factor is a good importance measure for setting reliability targets and possibly useful in initially classifying new systems or groups of redundant identical components. Conditional Core Damage Probability is useful for in-service-inspection purposes and for setting frequency targets for initiating events and comparing the safety significances of initiating events. When components of a system are being requalified Fussell-Vesely (FV) importance can give reasoning for upward or downward qualification. FV importance is well suited for consideration of modifications. It can be used for initiator type events like pipe breaks as well as for unavailabilities. However, it is useful to consider pairs of risk measures (RIF, FV) and (CCDP, FV) for requalification purposes in an NPP design phase or for an operating plant. Both RIF and FV can be used for measuring safety significances for technical specifications. RIF is useful in defining allowed outage times and FV useful in defining test intervals. All these measures can be quantified for both Core Damage Frequency (CDF) and Large Early Release Frequency (LERF) and it is recommended to consider both points.

Some other important issues that need to be considered in the classification are

- Operability of the equipment must be ensured with sufficient safety classification. If the equipment is needed in accident conditions essentially different from normal conditions it has to be qualified for those conditions.
- Equipment can have a high safety significance even if their operability does not need any qualification and therefore a high safety class. We need to specify a high safety class for them in cases in which the classification affects Common Cause Failure possibility and the system failure has a high importance.
- In many cases the environment is not different under accident conditions, at least not when the equipment has to operate. In such cases the conventional components out of large batches and with extensive operating experiences can be more reliable than components of a small batch of qualified components. This fact should be taken into account in the safety classification of components or in the definitions of what is considered as "adequate qualification".
- Instead of changing a safety classification other measures like
    - new test and inspection programs,
    - different Allowed Outage Times and
    - plant modifications

  could have better effects on the safety of the plants and on the allocation of the resources. An improvement in Loviisa will ensure a reliable isolation of small primary leakages via certain parts of Safety Class 2 and 3 piping and thereby it will decrease the safety significance of those piping sections.

As a conclusion we can say that it is possible to change safety classes or safety significances as considered in technical specifications and in in-service-inspections into both directions without endangering the safety or even by improving the safety. It is good to start such exercise from the most extreme importances, aiming at allocating the limited resources to points where they are most needed or useful, and not wasted in less important systems or components. It is also worth while to apply this when modifications and new systems are designed.

7 References

1. Decision of the Council of State (395/1991) on the General Regulations for the Safety of Nuclear Power Plants, 14 February 1991.
2. Risk Spectrum Theory Manual. Relcon Ab, 1998.
3. European Commission. Nuclear Safety and the Environment. Report on risk-informed in-service inspection and in-service testing. Final report - June 1999. EUR 19153 EN.

Title	A risk informed safety classification for a Nordic NPP
Author(s)	Kalle Jänkälä
Affiliation(s)	Fortum Nuclear Services Ltd, Finland
ISBN	87-7893-128-2
Date	January 2002
Project	NKS/SOS-2.1
No. of pages	33
No. of tables	6
No. of illustrations	4
No. of references	3

Abstract

The report describes a study to develop a safety classification proposal or classification recommendations based on risks for selected equipment of a nuclear power plant. The application plant in this work is Loviisa NPP unit 1. The safety classification proposals are to be considered as an exercise in this pilot study and do not necessarily represent final proposals in a real situation. Comparisons to original safety classifications and technical specifications were made. The study concludes that it is possible to change safety classes or safety significances as considered in technical specifications and in in-service-inspections into both directions without endangering the safety or even by improving the safety.

Key words Safety classification, importance measures, PSA

Available on request from the NKS Secretariat, P.O.Box 30, DK-4000 Roskilde, Denmark.
Phone (+45) 4677 4045, fax (+45) 4677 4046, e-mail nks@catscience.dk, www.nks.org.