RISK - INFORMED DECISION MAKING AT LOVIISA NPP

J. K. Vaurio
Fortum Power and Heat Oy
P.O. Box 23, 07901 Loviisa, Finland

1. INTRODUCTION

Loviisa nuclear power station is a two-unit plant with VVER-440 type reactors (model 213 PWR) in operation since 1977 and 1980, respectively. The plant is a hybrid of Western and Eastern technologies. The first Level 1 probabilistic safety assessment (PSA) was completed in 1989 for internal initiators at full power. Since then the scope has been extended to external events, and the work continues with focus on shutdown modes and level 2 studies.

PSA has been used continuously to identify dominating accident sequences and to develop plant modifications for safety improvement. Consequently, it has been necessary to update PSA annually and also merge new results from the expanded scope. PSA has also been used in many other ways for risk-informed decision making, as will be described.

The main focus over the period 1989-1999 was to identify risk-based plant modifications to reduce the core damage frequency (CDF) down to the level of an unofficial goal 10^{-4} /yr. These efforts are described in Section 2.

When the total risk is sufficiently reduced, one enters the region of diminishing return. It becomes more and more important to compare the costs and benefits of alternative decisions. The economic criteria developed at Loviisa plant are described in Section 3.

The same criteria apply to back-fitting decisions as well as to other applications concerning test intervals, temporary configurations, allowed outage times etc. Such applications are described in Section 4.

Ageing of nuclear power plants is an issue gaining more and more attention. Risk measures and reliability engineering techniques can be used in making ageing-related decisions, as described in Section 5.

2. PLANT BETTERMENT

Since 1989 the main objective of the PSA effort at Loviisa plant has been to identify dominating accident sequences and plant modifications to reduce the core damage frequency (CDF) down to the level of an unofficial goal 10^{-4} /yr. Fig. 1 indicates that this has been nearly accomplished by 1998.

Fig. 1 gives CDF-values at full power operation for internal initiators, floods, fires and severe weather phenomena, and the annual risk due to a refuelling outage (shutdown) for internal initiating events. Some of the values were estimated backwards in time from the years when partial PSA-studies were completed. The current risk values and the major plant modifications are listed below in Sections 2.1 through 2.5.

The following conclusions can be drawn from these back-fitting efforts:

- Dominating accident sequences and phenomena were quite plant-specific, with little possibility to learn from other plants (even with the same reactor type)
- Possible plant modifications were rather unique and often self-evident (few or no reasonable alternatives)
- New generic phenomena (ageing mineral wool insulation & boron dilution risk) caused major updating
- The driving force was the goal (CDF $\leq 10^{-4}$/yr) rather than balancing the risk-impact and the cost of a modification; nevertheless, cost-effective modifications such as changes in procedures or valve positions were often feasible.

2.1 PSA for Internal Initiating Events (IIE)

Fifteen plant modifications and several new or modified emergency operating procedures have been completed during 1989-1998 to reduce IIE-CDF from over 10^{-3}/yr to $1.5 \cdot 10^{-5}$/yr. The most important modifications were

- Improved air cooling system for instrumentation rooms, to reduce probability of spurious signals causing LOCA (1990)
- New sump strainers and a back-flushing system to prevent blockage of the ECCS sump by aged mineral wool insulation potentially released by LOCA (1993)
- Improved detection of primary coolant leakage outside of the containment via the coolant purification system (CVCS), and automated isolation of such leakage (1994)
- Reduction of risk due to steam generator (SG) leakage: automated isolation of a leaking SG, improved N^{16} detection, an additional pressurizer spray system and an additional emergency core coolant (ECC) tank (1994-1996)
- Modifications of the ECC system minimum flow lines to prevent alternating suction of the ECC between ECC tank and the sump (1996-7).

2.2 Flood PSA

Several modifications have been made to reduce CDF due to internal floods from $3 \cdot 10^{-4}$/yr (1994) below 10^{-5}/yr (1998). The main modifications were

- New wall (dam) to prevent turbine building floods from expanding to the reactor building basement through cable tunnels (threatening PCP seal cooling pumps and ECCS)
- Protecting feedwater system pipelines above the control building to reduce flood risk in the control and instrumentation rooms
- Improving drainage above the control and instrumentation rooms
- Re-routing service water and hydrant pipes to avoid floods in control and instrumentation rooms
- Moving up seawater system valve actuators and service water system pressure transmitters (in turbine building).

2.3 Severe Weather PSA

Several modifications have been made to reduce CDF due to severe weather such as high sea level, snow, storms, sea vegetation, frazil ice, extreme air & water temperatures, lightning (and combinations) from $4 \cdot 10^{-4}$/yr (1993) to $4 \cdot 10^{-5}$/yr (1998). The main modifications included

- Increased height of a temporary dam during refueling outages (high sea level risk)
- Improved detection and automated flow reduction in case of accumulating sea vegetation (blockage of sea- & service water flow)
- Redundant air-intake in the emergency diesel generator building (against blockage by snow or freezing rain)
- New procedures to remove the main condenser purification balls and ensure alternate intake of warmer seawater from the outlet side, in case of threatening icy, sub-cooled sea conditions.

2.4 Fire PSA

More than twenty protecting measures have been completed over the years 1989-1998 to reduce the fire risk from $7 \cdot 10^{-4}$/yr to $3 \cdot 10^{-5}$/yr.[3] Some changes were based on deterministic regulations, some on the estimated risk significance. Major changes included

- A new auxiliary emergency feed water system outside of the turbine building (the main FW and normal AFW system were vulnerable to turbine building fires in the original design)
- Separating the control building (and FW areas) from the turbine building by fire-walls
- Protecting high pressure hydraulic oil pipelines (to prevent oil jet fires)
- Protecting and re-routing critical cables
- Extension of the sprinkler system to cable areas and transformers

At present the control building contributes about 45% of the fire risk while the turbine building contributes 28%. In terms of room types, 32% is due to fires in cable areas or tunnels, and 17% is due to fires in process rooms. The risk is rather evenly spread around the plant.

In terms of accident sequences, about 44% of the fire risk is due to the primary coolant pump seal LOCA caused by loss of flow or cooling of the component cooling or service water. About 20 % is due to total loss of feedwater sequences.

2.5 Other PSA-related activities

A seismic PSA was completed in 1992 with conservative assumptions. Due to low seismicity the mean CDF was $3 \cdot 10^{-6}$/yr . No back-fitting was necessary.

A shutdown-state PSA for internal initiators during a normal refueling outage resulted[4] in CDF equal to $2{,}8 \cdot 10^{-5}$/yr. Half of this estimate is due to hoisting and transfer of heavy loads (pressure vessel lid and internals) inside of the containment building. Only limited possibilities have been identified so far for reducing the outage risk.

So far, level 2 PSA has been carried out for internal initiators and floods during full power operation. However, these are only predictions beyond year 2001 when a number of severe accident management backfittings will be completed. These include an ex-vessel system for cooling the core debris inside of the pressure vessel, installation of hydrogen recombiners and burners, and assuring timely operation of the ice-condenser doors. Means for primary pressure reduction and outside containment cooling have been installed. Some efforts are still needed to reduce the probabilities of containment bypass sequences.

Plans to reduce CDF even further include a separate residual heat removal system, and modifications to provide a redundant supply of the primary pump seal coolant. These are expected to reduce especially the fire and severe weather risks significantly, even beyond 24 hr mission times (cold shutdown).

3. COST/RISK CRITERIA

Economic criteria have been developed for tentative use at Loviisa NPP to decide which plant modifications can be justified on the basis of risk reduction vs. the cost of backfitting, and how to select an optimal combination from a set of possible modifications. Two risk-measures are used for a backfit or modification:

ÄCDF = change (reduction) of the core damage frequency (per year)
ÄLERF = change (reduction) of the large early release frequency (I, Cs ; per year)

The "expected benefit" of plant modification i can be presented as

$$R_i = \alpha\ \text{Ä}CDF_i + \beta\ \text{Ä}LERF_i, \qquad (1)$$

where α and β depend on the expected cost of an accident (including lost production), the remaining lifetime (n, years) and the interest rate (p). A proposed plant modification is justifiable if the cost C_i (investment and present value of future costs) is smaller that the expected benefit, i.e. $C_i < R_i$. In case of multiple choices for back-fitting measures, one should select the one with largest $R_i - C_i$:

$$R_i - C_i = \max! \qquad (2)$$

(Please observe that with k individual back-fitting options there are actually 2^k possible combinations of plant modifications to be compared, i.e. i = 1,2,... 2^k).[2]

In terms of c = annual cost of replacement power, taking into account that an accident can happen any year, one can calculate at least an approximate value $\alpha = b \cdot c$, where

$$b = \frac{1}{1+p} + \frac{2}{(1+p)^2} + \ldots + \frac{n}{(1+p)^n} = \frac{1-[(n+1)p+1](1+p)^{-n}}{p^2} . \qquad (3)$$

In case of Loviisa, assuming the remaining lifetime n = 20, interest rate p = 0.05 and the cost of replacement power 2.5 c/kWh yields $\alpha = 10^{10}$ \$. The same value can be obtained if one assumes the mean accident cost C_A equal to one billion dollars and $\alpha = aC_A$, where a is the discount factor $a = [1-(1+p)^{-n}]/p$. Typical values for the ratio β/α are 10...100.

Even if some of the parameters and assumptions in this formalism are uncertain, it provides a consistent way to rank alternatives. Usually the result is so clear that changing uncertain parameters somewhat would not change the conclusions. This was the case with virtually all backfitting measures mentioned in Section 2.

4. RISK-INFORMED APPLICATIONS

4.1 Limiting Backfitting of Motor Operated Valves

Opening and closing of a motor operated valve (MOV) is normally stopped by a limit signal and/or a torque limit switch. If the limit system fails, there is a danger that the valve jams or is damaged, causing internal or external leakage, especially if the valve is equipped with an oversized actuator. Loviisa plant has about 500 valve/motor combinations such that the maximum torque exceeds the

nominal strength of the valve structure in case the limits fail. Replacing all such valves or motors would cost several millions of dollars.

Detailed assessment of the reliabilities of the limit/switch systems, the ratios maximum torque/nominal strength, and the risk-significance of each valve, led to a significant reduction of the number of valve/motor combinations that needed to be changed. About 10 % of the valves contributed to more than 90 % of the risk, limiting the scope of modifications considerably.

4.2 Limiting Testing of Containment Isolation Valves

The containment isolation valves were originally tested for leak tightness once per year, and after any maintenance works. A task was given to the PSA project to identify groups of valves that could be leak-tested every other year instead of annually.

First, 52 valves (at each unit) were identified such that the maximum leakage in six latest tightness tests was no more than 20 % of the alarm limit. These were candidates for the extended test interval (ETI), and a reliability study was carried out to assess the additional risk due to ETI. The work was based on plant-specific failure histories. Based on the study of the failure causes, it was considered a good assumption that the tightness unavailability would double when doubling the test interval.

The acceptability of the test interval extension was studied line by line. The potential leak routes and leak sizes were evaluated (e.g. via closed or open systems). Based on the study, the extended test interval was approved for most of the 52 valves. Even if level 2 PSA has not yet been completed for this change, one can conclude that the relative risk-impact of the ETI is small.

4.3 Accepting Temporary Configurations

PSA has been used in several cases as a basis for accepting temporary configurations and other exceptions from Technical Specifications (TS), such as exceeding allowed outage times (AOT). Some examples:

- A check valve in the Chemical and Volume Control System was leaking slightly in excess of the leak rate limit specified in TS. Even under the conservative assumption that the valve would break in case of a certain medium LOCA initiator, the CD-risk increase until the next refueling outage would be less than $2 \cdot 10^{-7}$. Thus, plant operation was allowed without repair until the next refueling outage.

- A motor operated valve of the line used for warming up the ECC water was found to be failed. The valve could only be repaired during a long outage when the ECC tank is empty. A temporary rule of operation was issued, instructing the control valve in the same line to be kept normally closed. Conservatively estimated risk increase was $6 \cdot 10^{-7}$ /a. This additional risk was accepted until the next refueling outage.

- Certain pipe sections of the service water (SW) system were to be re-routed and replaced by a more durable material in order to reduce flood risks. The work was to be performed during power operation. It required certain parts of SW redundancies to be switched off consecutively for 5 days, preventing the air cooling of the emergency feed water pump rooms. Furthermore, one cooling unit of the instrumentation room ventilation could not be cooled for 5 hours. The additional risk was estimated to be as small as $8 \cdot 10^{-9}$ and the highest increase of CDF was about $7 \cdot 10^{-6}$ /a during those 5 hours, justifying the work.

- A containment internal spray system check valve under the ECC tank was found to be leaking. However, the CDF risk was estimated to be low, and repair was postponed until the next extended refueling outage.

- A crack was found in 1994 in a pressurizer spray system valve that is used for pressure reduction when the plant is shut down. This spray line has to be used when there is a need for rapid pressure reduction. Based on the assumption of a valve break in these situations the additional CDF was estimated to be almost $2 \cdot 10^{-4}$ /a, if the plant operation would be continued. The plant was shut down to replace this valve.

- Technical Specifications originally required in hot standby status that failure of any pump in emergency cooling (LPSI), containment spray, component cooling or service water systems has to lead immediately (in 8 hours) to cold shutdown of the plant.
  Assuming an AOT of 72 hours in hot standby (rather than cold shutdown) is equivalent to core damage probability of about 10^{-6}. Since this kind of situation is not expected to occur more frequently than once a year, the extended AOT is quite acceptable.

- The emergency power supply system of the plant includes four dedicated diesel generators (per unit). In addition, there is a power line to a nearby hydropower station, and two gas turbine power units on site.[5] The risk (CDF) due to a loss of offsite power event would be $3.6 \cdot 10^{-6}$/yr higher if the gas turbines were not available at all. Based on this and the cost criterion (Section 3) the gas turbines were sold to the national grid operator. Nevertheless, the gas turbines are still on site and available most of the time, if needed.

- A question was raised by safety authorities about the need to back-up the electric power supply to the auxiliary oil pumps lubricating the bearings of the motors of the primary coolant pumps. A detailed analysis pointed out that the risk reduction (CDF) would be only $2 \cdot 10^{-8}$/yr if the power supply were assured by DC batteries. This result satisfied the authorities and the question was dismissed. The economic criterion of Section 3 indicates that this kind of improvement is not justified if it costs more than $1000.

  About half a dozen other similar risk-informed decisions have been made in recent years.

Considering the goal 10^{-4}/yr for CDF, it is reasonable to approve temporary configurations and AOT until the next regular maintenance outage whenever the risk increase due to the temporary situation is less than $5 \cdot 10^{-6}$ /yr. Approval of delays up to one month are reasonable if the risk increment is between $5 \cdot 10^{-6}$ /yr and $5 \cdot 10^{-5}$ /yr, unless there is a serious threat to containment integrity (LERF) at the same time.

4.4 Risk-Informed Operator Training

Most of the plant modifications (mentioned in Section 2) required some changes in emergency operating procedures, and those had to be trained to the operators by simulator exercises. Besides this, PSA has been used to restructure and prioritise the whole simulator training program.

The risk-importance of human errors in post-initiator actions of the operators has been used for planning and prioritisation of transient types for simulator exercises in operator training. The higher the risk reduction worth of the operator error (diagnosis, decision and response), and the more complex the situation and actions, the more frequently the transient type is repeated in simulator exercises. The most important transients are repeated every one to two years, the second category every three to four years, and so on. Of course, the priorities change whenever plant modifications are made.

There has been significant feedback also from the simulator trainers to improve procedures and find new ways to deal with exceptional situations such as sub-cooled seawater or vegetation.

4.5 Risk Follow-up

In several cases after an operational event (an initiating event or some degree of loss of a safety function or barrier) the safety authorities have asked the utility to a estimate afterwards what the risk – significance of the event was. Supposedly, such an estimate could be used to assess the INES severity class of an event. However, if no core damage occurred, the true risk is known for sure to be (and have been) zero. This poses some philosophical problems as to what part of the now available a posteriori - information should or should not be taken into account in such follow-up assessments, and what conclusions or requirements should be made. Because the states of components are random variables (risk assessment indicating the time-average level), most of the time hidden states for standby safety components, it is difficult to justify strong conclusions based on few selected moments or cases on which information is gathered afterwards. At least one should not be biased by taking into account known failures with probability one while ignoring successful components (now known to have failed with probability zero).

5. RISK-INFORMED DECISIONS ON AGING

Particular attention has been paid on the following areas of plant ageing.

1. **Pressure vessel embrittlement.**
   Gradual embrittlement of the pressure vessel under neutron flux causes a increasing risk that a thermal shock (injection of cold water) under high pressure could fail the pressure vessel. Based on sample measurements of the pressure vessel properties, the critical transient temperature as a function of time(age) has been determined and the risk due to pressurised thermal shock (PTS) has been estimated. These led to annealing of the Loviisa 1 pressure vessel in 1996. This was done well before the risk would increase to a significant level.

2. **Ageing of active components.**
   Ageing of active components (pumps, valves, relays, breakers) may lead to an increasing failure intensity if repairs are imperfect or if preventive maintenance is ineffective. This can be detected by monitoring the numbers of failures in the failure history (a computerised system developed as a side-product of PSA), and performing statistical testing to confirm the significance. Both increasing and decreasing trends have been observed, even among nominally identical or rather similar components.[1] Because failure statistics are regularly reviewed by maintenance engineers, significant upward trends (if any) are nowadays normally detected without formal statistical tests.

3. **Ageing of electrical equipment, cables & instrumentation.**
   Recent measurements in the containment building indicate that in several locations the temperature exceeds 50 °C, the design temperature of the electrical equipment, instrumentation and cables. Because of this, increased failure rates were assessed for a number of valve actuators, seals, limit switches, protection instrumentation and associated cables. As a consequence the risk increased due to increased initiating event frequencies (due to increased probability of false signals or failing protection/limits) as well as increased

unavailabilities of safety system components expected to response to the events. A special complicating aspect was that some valves have oversize actuators so that the valves likely fail if the limit control or torque limit switches fail, and these limit systems also have higher failure rates due to the elevated temperatures. It turned out that the risk increase was dominated by the condition of two valves in the chemical and volume control system. Failure to close one of the valves in case of a certain medium size LOCA would eliminate HPSI and lead to core damage. Keeping one of the valves continuously closed turned out to be possible, virtually eliminating the risk increase without any cost or loss of production. With risk assessment a long shutdown outage and expensive renewals of cables and/or equipment were avoided.

4. **Ageing of secondary circuit pipes and components.**
Virtually no steam generator tube leakages have been experienced at Loviisa plant. However, significant erosion-corrosion ageing has taken place in other secondary pipes. This even caused two main feedwater pipe breaks, in 1990 and 1992. Extensive secondary pipe replacements have taken place since then, including the feedwater distribution lines in steam generators. The main condensers have been replaced with new ones made of stainless steel and titanium. The structural work on the secondary circuit is motivated by economy and production rather than risk or safety concerns, except for the feedwater pipelines.

5. **In-Service Inspections.**
A pilot project has been started in co-operation with safety authorities to prioritise in-service inspections (ultrasonic etc.) of primary and safety system pipes, based on the risk-significance of leakages. It is anticipated that this leads to a reduction in the total rate of inspections, while enhanced inspections could be needed in a limited set of pipe segments and welds.

6. SUMMARY

PSA has been used in many ways for risk-informed decision making at Loviisa power station. The most fruitful areas so far include:

* Identification of dominating risk contributors and possible means for reducing risk by plant modifications and improved procedures
* Providing risk perspective and economic criteria for assessing backfitting proposals
* Assessing the significance of ageing and needs for renewals
* Limiting, prioritising and optimising plant modifications
* Reducing testing requirements
* Justification of temporary as well as permanent configurations and extended outage times
* Planning and prioritisation of training programs.

REFERENCES

1. Jänkälä, K. E. & J. K. Vaurio: Component ageing and reliability trends in Loviisa nuclear power plant. Proc. PSA'89, ANS/ENS Topical Mtg., April 2 – 7, 1989, Pittsburgh, USA.
2. Vaurio, J.K.: Safety-related decision making at a nuclear power plant. Nuclear Engineering and Design 185(1998)335-346.

3. Lehto, M. et al.: Fire risk analysis for Loviisa 1 during power operation. Proc. PSA'96, Sept. 29 – Oct. 3, 1996, Park City, Utah, USA. American Nuclear Society.
4. Jänkälä, K.E., Mohsen, B. & J.K. Vaurio: PSA for shutdown modes of Loviisa NPP. Proc. PSAM 4 Conf., Sept. 13 – 18, 1998, New York, USA.
5. Vaurio, J.K. & P. Tammi: Modeling the Loss and Recovery of Electric Power. Nuclear Engineering and Design 157(1995)281-293.

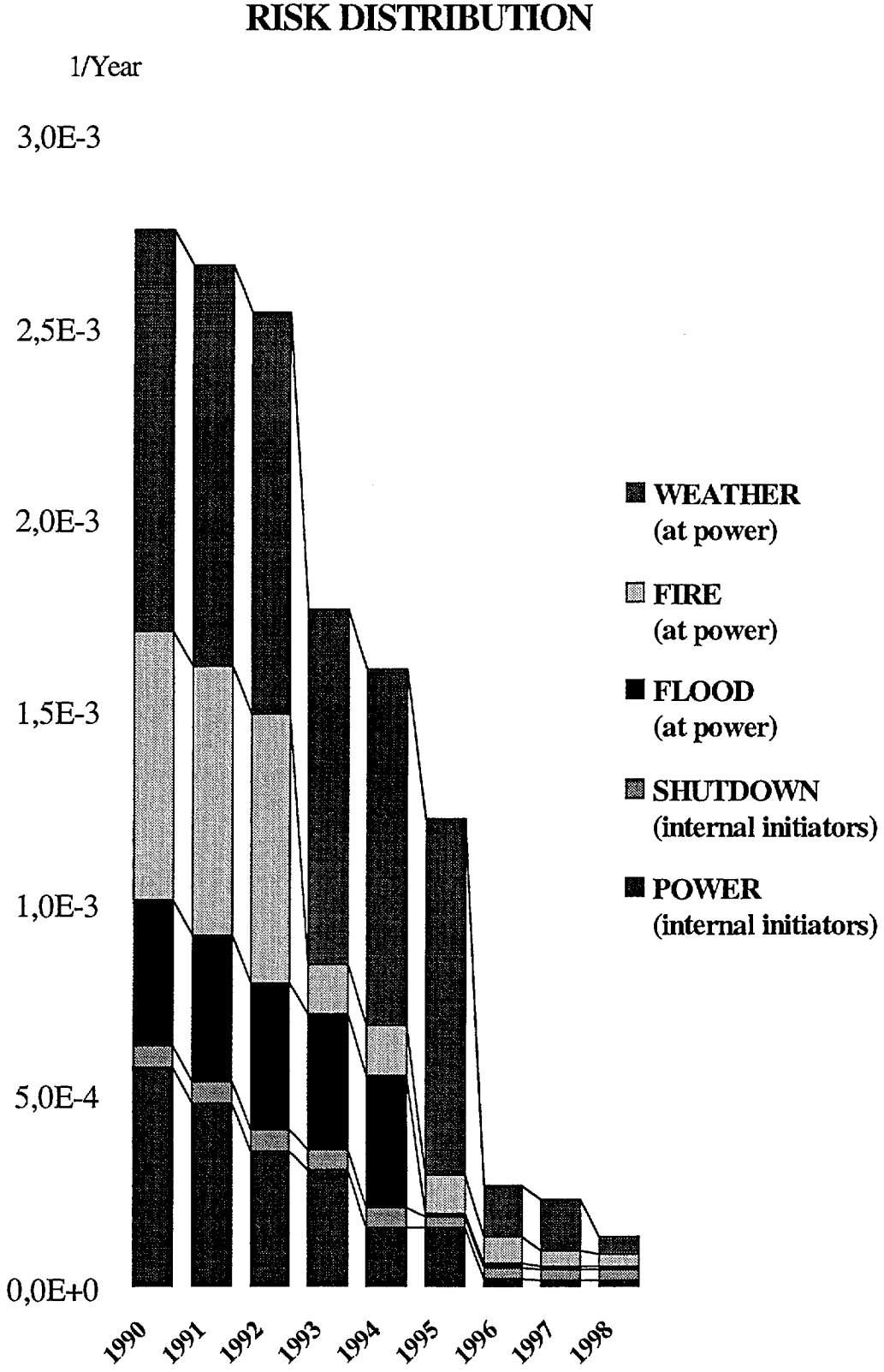

Fig. 1 The effect of plant modifications on the core damage frequency