ACTIVITIES RELATING TO PSA IN THE REGULATORY PROCESS

J F Campbell & G C Grint.
Prepared for the IAEA Specialist Meeting on
"Use of PSA in the Regulatory Process"
Vienna 5-8 December 1994

1. Introduction

In addition to the IAEA activities concerning the use of PSA in the regulatory process there are two other international initiatives in this area by the European Commision and the OECD's Committee for Nuclear Regulatory Authorities (CRNA). This paper gives a brief outline of these activities as well as introducing an update on the regualory use of PSA in the UK.

2. European Commission

The Nuclear Regulators Working Group (NRWG) operate under the auspices of CEC DGXII as a regular forum for nuclear regulators in the European Union (EU) to discuss matters of common interest. Each country has developed its own approach to the use of PSA in regulation and, while there was information available on each of these, NRWG wanted a clearer idea of the degree of concensus and of the main differences between the various approaches. Accordingly NRWG set up a Task Force to consider the topic of "Regulatory Actions Related to Probabilistic Safety Assessment". Regulators from eight European countries participated in the work of this Task Force: Belgium, France, Germany, Italy, the Netherlands, Spain, Sweden and the United Kingdom.

The work is essentially complete and it is expected to publish the report *"Regulatory action related to PSA studies" (EUR 15720)* before the end of 1994. The report represents only a snapshot in time and the position in a number of the countries represented on the Task Force may well now be different. Indeed during the writing of the report changes were made to reflect developments in a number of countries.

The aims and objectives of the Task Force were:

a) Assessment of how regulatory bodies currently estimate the value of PSA results, including the understanding of benefits and limitations with regard to methods and approaches.

b) To show the current use of the PSA tool at the regulatory level, and to establish differences in the approach in various countries, for example whether PSA is part of the licensing process or is used outside the licensing process as a supplementary tool by the utility.

c) Specific requirements in PSA methodology and guides by regulatory bodies on PSA procedures. Also guidelines on how to review a PSA once it has been submitted by the licensee.

d) Contributions made by the regulatory body in PSA with regard to review of the PSA and the evaluation of the numerical values in the PSA.

An overview of the findings of the EU work was given in a paper entitled "The CEC NRWG Task Force on Regulatory Actions Related to PSA" presented at the IAEA meeting on the regulatory use of PSA held in April 1993 and a summary the information is given in tables 1 to 3 of this paper.

3. OECD.

The OECD's CRNA are also interested in regulatory approaches to PSA and have initiated their own study. The objectives of the OECD work are :

a) to collect from OECD countries the technical information required for a state of the art presentation to the CRNA, and

b) to produce a report which includes the technical information as well as any conclusions on regulatory implications

To get the information, OECD have developed a questionnaire which is divided in to 2 basic sections, with a total of 5 general questions, namely:

I. Regulatory Environment

- Background and regulatory environment

II Role of PSA in Safety Regulation

- General description of national PSA programmes
- Regulatory Authorities Role
- Current PSA applications
- Future PSA applications.

The OECD anticipate produing a draft report by June 95 and hope to approve a final report by November 95.

4. UK Position.

PSA is one of the tools used for the assessment of safety in the regulation of nuclear power in the UK and is an important part of the safety case required for a nuclear installation. The PSA needs to demonstrate that the risks associated with accidental releases are sufficiently low. As far as NII is concerned, the main value of PSA, and the most robust use, lies in the identification of weaknesses in the design or operation of the plant and enabling the various contributions to the risk to be seen relative to one another in a consistent overall framework.

A paper on the use of PSA in the regulatory process in the UK was presented at the IAEA meeting on the regulatory use of PSA held in April 1993. An updated version of this paper is included as appendix 1.

Over the last couple of years NII has been applying the revised Safety Asssessment Principles (SAPs)[1] to safety cases and has published a paper[2] giving further deatails on the probabilistic principles. The main points from this paper are:

1. PSA is now an established feature of safety analysis of nuclear plants in the UK.

2. A plant specific PSA forms an integral part of a safety case and is not an isolated study.

3. PSAs have mostly been performed to Level 1, but a Level 2 PSA is expected for future applications.

4. HSE's general approach to the assessment of risk has been established in its Tolerability of Risk (TOR) document[3]. TOR describes a framework of ALARP with an upper limit of tolerability and a lower broadly acceptable level, discusses individual risk to workers and members of the public, and societal risk, and sets numerical values for individual risk.

5. NII's revised Safety Assessment Principles (SAPs) are linked to the high level guidance in TOR, take account of experience with the previous version of the SAPs and of international developments, and cover all types of nuclear plants.

6. The revised SAPs related to PSA include numerical principles addressing the three types of risk discussed in TOR. They also include principles on the frequency of plant damage and of accidental criticality, to reinforce the concept of defence-in-depth.

7. A PSA should aim for completeness, should preferably be best-estimate and should be kept up to date, as part of the safety case.

References

1. HSE, Safety assessment principles for nuclear plants, HMSO, London, 1992.

2. Campbell, J.F. The NII's revised Safety Assessment Principles Related to PSA. PSA/PRA for the Nuclear Industry. IBCTechnical Services Ltd..London Nov. 1993

3. HEALTH AND SAFETY EXECUTIVE (HSE), The Tolerability of risk from nuclear power stations, HMSO, London [(ISBN 0 11 883982 9) 1988 and (ISBN 0 11 886368 1) 1992.]

Table 1. Scope, Practice and status of PSAs (1 of 2)

	Belgium	Finland	France	Germany	Italy	Netherlands	Spain	Sweden	UK
Scope of PSAs	internal events, all plant states	internal and external events, CCI[1] events. all plant states	internal events, all plant states	internal, external, CCI -events, power generation, other states in future	internal, external, CCI- events, all plant states	internal, external, CCI- events, power generation & non-power states	internal, some external, CCI- events, power generation	internal, some CCI- events, power generation, shut-down transients	all initiating events, internal & external hazards. all plant states for recent & current PSAs
Undesired end states	core damage, PDS[2]	core damage, PDS	core damage	plant hazard states (PHS), core damage, PDS	core damage and accident classes	core damage	core damage	core damge, RPV-over-pressure	core damage, 5 levels of offsite dose to person at greatest risk
Success criteria for end states	FRCT[3]	FRCT, pressure in PCS[4], pressure in containment	core uncovery, pressure in PCS, FRCT	PHS: SG-level, RPV-level, core damage: RPV-level, FRCT	FRCT, pressure in PCS	FRCT, Zr-oxidation of FR, long term RHR	FRCT, pressure in RCS	FRCT, pressure in RCS, pressure in containment	FRCT for core damage, Dose Freq. mSv /yr 0.1-1 $<10^{-2}$ 1-10 $<10^{-3}$ $10-10^{2}$ $<10^{-4}$ $10^{2}-10^{3}$ $<10^{-5}$ $>10^{3}$ $<10^{-6}$
Considered accident management, level 1	PBF[5]	Cross-tie of emergency DGs to other units	PBF, Back-up of SGF[6], SI[7]	PBF, SBF[8]	PBF	PBF	PBF	PBF, restoration of SGF, RHR from containment by mobile equipment	PBF, SGF
Review of PSA by	Regulator	Regulator	Cross review by EdF, IPSN	GRS, TÜV on behalf of regulator	Regulator	Regulator, IAEA, utilities, utilities research institute	Utilities, regulator	Regulator	Utilities, Regulator (supported by consultants in some cases)

Table 1. Scope, Practice and status of PSAs (2 of 2)

	Belgium	Finland	France	Germany	Italy	Netherlands	Spain	Sweden	UK
Use of Living PSA (LPSA)	considered	LPSA in use	-	LPSA system under development	LPSA implemented (workstation)	LPSA implemented (NUPRA & CAFTA)	-	LPSA system under development	RISK monitor implemented at 1 plant, other uses considered. LPSA being developed for Sizewell B.
Number of NPPs in operation	7	4	54	20	3, operation suspended	2	9	12	35
Number of NPPs with PSA	2	2	54	8 3 under way	3	2	7	12	36 (inc Sizewell B)
Level, type of PSAs	2 level 1 +, plant specific	2 level 1 +, plant specific	2 level 1, plant type specific	6 level 1+, 1 level 2-, plant specific, 1 level 3, generic, 3 level 1+ under way	2 level 1, 1 level 2, plant specific	2 level 2-, plant specific	5 level 1, 2 level 2, plant specific	12 level 1, plant specific	2 level 3, rest level 1, but some of limited scope which will be extended in due course
Future applications for existing NPPs	level 1+ for all NPPs	level 2 for all NPPs	Level 2	level 1+ for all NPPs	-	level 3 for all NPPs	level 2 for all NPPs	level 2 for all NPPs in ASAR 90	at least level 1 for all NPPs
Who carries out the PSA studies	Tractebel (Contractor)	Utilities	IPSN, EDf	GRS, TÜV, Utilities	ENEL and Contractors	SAIC, NUS, Siemens	Utilities	Utilities	Utilities, Contractors

1) CCI: Common cause initiators, 2) PDS: Plant damage states, 3) FRCT: Fuel rod cladding temperature, 4) PCS: Primary coolant system, 5) PBF: Primary side bleed and feed, , 6) SGF: Steam generator feed, 7) SI: Safety injection, 8) SBF: Secondary side bleed and feed 9) FCV: Filtered containment venting, 10) PB: Primary side bleed for prevention of high pressure melt ejection

Table 2. Safety Benefits from PSA. (1 of 2)

	Belgium	Finland	France	Germany	Italy	Netherlands	Spain	Sweden	UK
Evaluation of Incidents	planned	carried out for TVO, Fire, and Loviisa, FW pipe rupture	carried out	carried out for some plants	carried out	planned	planned	carried out for 3 plants	planned
Maintenance planning	-	Implemented for evaluation of LCO's** and test intervals	-	implemented for determining test intervals	-	planned	tentative for some plants	planned	implemented at some plants
Support for decisions and development for new reactors	-	Support for several regulatory decisions on plant changes, backfits and operational incidents	support of the design of the N4 and EPR*	support of the design of EPR	support of the design of the AP600, PIUS, SBWR	-	-	support of the design of the next generation BWR	expected for any new reactors

Table 2. Safety Benefits from PSA. (2 of 2)

	Belgium	Finland	France	Germany	Italy	Netherlands	Spain	Sweden	UK
Backfitting measures to overcome identified vulnerabilities	several detailed modifications-	PWR: improvements of service water system, primary coolant pump seal system, ECC system, cooling of electrical and control instrumentation rooms	reduction of vulnerabilities to boron dilution, loss of cooling in mid loop operation	PWRs : provision of diverse feed water supply, improvement of the control logic of secondary side steam relief valves, improved control logic for dealing with STGR all BWRs: diverse main relief valves BWRs, series 72: provision of diverse RHR,	-	Installation of mini flow lines for HPI pumps, improvement of check valves	General improvement of design and procedures	improved defence against CCF, improved actuation logic of protection systems, provision of backflush operation in case of clogging of strainers in BWRs	Magnox reactors : provision of diverse second. guardlines, automation and extension of the secondary shut down system, improvement to the emergency boiler feed system. AGR reactors : improvement to refueling, provision of back-up feedwater supplies

* EPR : European PWR, **LCO : Limited condition of operation

Table 3. Requirements, Guidelines, Targets and Preconditions.(1 of 3)

	Belgium	Finland	France	Germany	Italy	Netherlands	Spain	Sweden	UK
Requirements and Guidelines									
Requirement by regulator for PSA	yes	yes	no	yes	yes	yes	yes	yes	yes
Will a PSA be required for continued licensing of existing NPPs?	level 1+ required for the periodic safety reviews	yes, level 2	-	yes, level 1+, within the dicennial safety review	no	yes, level 3	yes, level 2	yes, level 2	yes, at least level 1
Will a PSA be required for licensing of reactors of new design	yes, level 2	yes, level 2	no, but at least level 1 expected	yes, at least level 1+	-	yes, level 3	yes, level 3	yes, level 2	yes, level 2
Guidelines on PSA procedures	based on NUREG 2728, 2300, 2815	NUREG 2300, 2728, 2815 and plant ones by utilities	-	PSA Leitfaden (Guidelines)	NUREG 2300	based on NUREG 2300, 2815. Future: Dutch PSA Guide based on IAEA Guide	-	informal guide evolved from PSAs	NII Safety Assessment Principles, draft PSA assessment guide. IAEA Guide referred to
Sensitivity analysis required	yes	yes	no	yes	yes	no	yes	no	yes
Uncertainty analysis required	no	yes	no	yes	no	yes	yes	no	no

Table 3. Requirements, Guidelines, Targets and Preconditions.(2 of 3)

	Belgium	Finland	France	Germany	Italy	Netherlands	Spain	Sweden	UK
Targets and Preconditions for PSA									
Targets for core melt or plant damage frequency, level 1	not explicit	-	--	not explicit, in practice: CDF[1] > 10^{-4} resp. 10^{-5}: Backfitting is required immed., resp. in due time	not explicit, CDF < 10^{-5} is desired	not explicit, CDF < 10^{-4} is desired	not explicit	not explicit	Basic safety objective of less than 10^{-5} /yr.
Targets for level 2	-	-	-	-	conditional probabillity of severe containment failure < 0,1 (not mandatory)	-	-	-	Large release limit 10^{-5}, objective 10^{-7} /yr
Targets for off-site consequences, level 3	-	-	-	-	-	indiv. risk < 10^{-6}, societal risk must comply with CCDF	-	-	Individual risk < 10^{-6} /yr
CCF limits	-	-		-	lower bound	realistic lower bound, > 10^{-4}/d	-	-	generally a lower bound 10^{-5}/d
Minimum time scale for claimed operator actions	according to failure probability vs time curves	-		at least 30 min for diagnosis and action	-	realistic time scale required	-	-	30 min in deterministic success criteria - less if justified.
procedures for claimed operator actions	written, exc: STG[2] feed	-		written	written, exc. permitted if supported by analysis	written procedures for recovery actions	-	written	written

Table 3. Requirements, Guidelines, Targets and Preconditions.(3 of 3)

	Belgium	Finland	France	Germany	Italy	Netherlands	Spain	Sweden	UK
Credit for claimed equipment	safety grade, non-safety grade for specific scenarios	-		safety grade, non-safety grade if supported by analysis	safety grade, some non-safety grade	no specific conditions	-	-	safety grade, also non-safety grade, if supported by analysis
Choice of data	no specific requirement	plant specific	-	plant specific, to be collected according to PSA guidelines	plant specific and generic data	plant specific	-	plant specific	plant specific, generic if plant specific data are insufficient
Mission time to be considered	72 h, in some cases also longer	24h	-	until stable conditions are reached	24 h, in some cases also longer	until stable conditions are reached - mostly 24 h	-	24 h, in some cases also longer	24 h for transients, longer for LOCAs. All mission times should be justified.
Human intervention model	no specific requirement, but the model must be justified	no specific requirement, models used reviewed by regulator in advance	-	ASEP for screening, THERP, but with error factor = 5	SHARP, THERP, HCR	SHARP framework, no specific requirement, but errors of commission should be considered	-	THERP, HCR	no specific requirement, but the model must be justified

1) CET: Containment Event Tree, 2) STG: Steam Generator

APPENDIX 1.

USE OF PSA IN THE REGULATORY PROCESS IN THE UK

J F Campbell & G C Grint.
Prepared for the IAEA Specialist Meeting on
"Use of PSA in the Regulatory Process"
Vienna 26-29 April 1993

(Amended 17 November 1994)

1. Introduction

PSA is one of the tools used for the assessment of safety in the regulation of nuclear power in the UK. This paper describes the approach to licensing and the role played by PSA, discusses the scope of the PSAs carried out, the use made of PSA and the criteria against which the results of PSAs are assessed.

2. Background - Licensing in the UK

A site may only be used for the installation or operation of a commercial nuclear facility if a licence has been granted by NII on behalf of the Health and Safety Executive.

Conditions are attached to the site licence which are required in the interests of safety. These may be amended, added to or revoked at any time by NII. Furthermore the licence allows direct action by NII in the form of Consent, Approval and Direction, providing a very flexible but rigorous regime of regulatory control over, amongst other things, construction of, and modification to, the plant.

Any application for a licence must be supported by a safety report of which PSA is a significant part. This safety case is assessed by NII using their Safety Assessment Principles (SAPs)[1,2] which contain numerical criteria for accident frequency and consequence.

The Health and Safety Executive (HSE) has recently published a revision to its paper on The Tolerability of Risk From Nuclear Power stations (TOR)[3]. This paper is used by NII assessors as additional guidance for the assessment of safety submissions, although it has no formal regulatory status. The numerical criteria in the SAPs[2] are broadly equivalent to the risk criteria in TOR.

3. Regulatory Requirement for PSA

Level 1 PSAs were provided by the licensees as part of the pre-construction and pre-operational safety reports (PCSR & POSR) for Heysham 2 and Torness AGRs. A level 1 PSA was required for Sizewell B, although a level 3 was done as part of the POSR (and

formed part of the PCSR). Level 1 PSAs are also required as part of the periodic reviews (called Long Term Safety Reviews in the UK) of Magnox reactors and will be a feature of the periodic reviews of the AGRs. Level 1 PSAs were required for the licensing of AEA reactors although AEA, in fact, submitted level 3 PSAs. In the future a level 2 PSA will be required for new plant, although it is anticipated that a level 3 PSA will be provided voluntarily by licensees for major new plant.

PSAs in the UK are carried out by the licensee or his contractor, with the timing dependent on the reason for doing it:

New plant: to support application for license and consent to operate.

Older plant: as part of periodic review. Timing here is based on the age of the plant and agreed between NII and the licensee.

Modifications: in support of plant modifications. Plant modifications are often supported by level 0 PSAs with the system requirement being derived from high level criteria, such as the SAPs.

3.1 Criteria.

NII's safety assessment principles (SAPs) contain numerical criteria for fault conditions. In the 1979 (rev 1988) SAPs, accidents which could give rise to a large uncontrolled release (leading to a maximum offsite dose >100 mSv) had a summated frequency target of 10^{-6}/yr, with no single fault group contributing more than 10% of this. Criteria were also given for smaller releases.

The Tolerability of Risk From Nuclear Power stations (TOR) proposes maximum tolerable level of risk of death to any member of the public of 10^{-4}/yr. In accordance with the findings of the public inquiry for Hinkley Point C, a risk of 10^{-5}/yr is proposed as the benchmark for new nuclear power stations in the UK. TOR also proposes broadly acceptable levels of individual risk of death (prompt and delayed) to a member of the public of 10^{-6}/yr.

A new version of the SAPs was published in 1992 and now the criteria are in the form of Basic Safety Limits (BSLs) and Basic Safety Objectives (BSOs) which are broadly consistent with TOR. The BSLs represent the limit of tolerability and a proposed plant must satisfy these limits in order to be considered for licensing. Under UK law it is not enough to just satisfy numerical risk criteria, the risk must be shown to be As Low As Reasonably Practicable (ALARP). Legal precedent within the UK defines ALARP in terms of a balance in which the "costs" in money, time, trouble and effort involved in reducing the risk must be grossly disproportionate (ie very much greater) than the "benefits" in terms of increased safety, before the risk be considered ALARP.

The ALARP principle tends to drive the risks from the plant even lower than the BSLs. However, there comes a point at which further consideration of the case would be more costly in NII resources than the benefit from applying that effort to other tasks. The BSLs are therefore complemented by BSOs which define the point beyond which NII need not seek further improvements on grounds of ALARP; instead NII effort can be confined to checking the validity of the licensee's case.

The BSLs and BSOs for accident conditions are:

Max. Effective dose to Public mSv	**Total Predicted Frequency, per year**	
	BSL	**BSO**
0.1-1	1	10^{-2}
1-10	10^{-1}	10^{-3}
10-100	10^{-2}	10^{-4}
100-1000	10^{-3}	10^{-5}
>1000	10^{-4}	10^{-6}

The above BSLs and BSOs are surrogate measures for individual risk and also, to some extent, the societal effects of accidents. As in the earlier SAPs, no single fault group should contribute more than 10%. Societal risk is also dealt with by a surrogate measure defined as a large release - >10000 TBq of Iodine 131 or 200 TBq Caesium 137 or any other isotope, or mixture of isotopes, which would lead to similar consequences. The BSL is 10^{-5}/yr and the BSO is 10^{-7}/yr

The BSL for plant damage (degraded core for a reactor) is 10^{-4}/yr and the BSO is 10^{-5}/yr.

The total predicted individual risk of death to any worker on the plant attributable to radiation doses from accidents has a BSL of 10^{-4}/yr and a BSO of 10^{-6}/yr.

3.1.1 Licensee's Criteria.

The major nuclear licensees in the UK are Nuclear Electric (NE), Scottish Nuclear Ltd (SNL), BNFL and UKAEA. NE and SNL have their own design safety criteria which are similar to the BSOs in the SAPs. BNFL and UKAEA have mainly used individual risk criteria which are nominally the same as the broadly acceptable level proposed in TOR.

3.2 Scope of PSAs.

The scope of PSAs vary in that NII expects the same range of faults to be covered but for older plant the depth of coverage can be less.

Completeness of a PSA is considered to be of fundamental importance. One of the driving forces for this is the need to consider high level risk criteria (eg TOR) and the PSA should aim to account for all identified contributors, even if this means that some can only be quantified by judgement. The fault schedule is compiled as part of the PSA, often using the fault schedule from a similar reactor as a starting point to be amplified by plant reviews, operational experience, etc. FMEA can be used to try and ensure completeness.

For Sizewell B the PSA covers all reactor states and includes non-core sources of radioactivity and internal and external hazards. For the older, magnox reactors a more limited PSA was undertaken in which these items were largely excluded. The licensees of these older reactors are now extending their PSAs to give these items greater coverage although NII does not expect the same level of detail as that for Sizewell B, particularly for faults which give a small contribution to the summated accident frequency.

Sensitivity studies are performed although in practice they are not always extensive enough and fail to address all of the assumptions made in the PSA. The results of sensitivity studies are used by NII as a check that the calculated risk is not unduly influenced by assumptions made in the PSA or, where only poor quality data is available, it is not a critical factor.

Importance factors are usually calculated as they form part of the output of most fault tree programs. These factors are useful for identifying items for consideration in sensitivity studies. This has been done in PSAs submitted to NII, although licensees have been asked to go further down the list of items.

Uncertainty analysis is not a currently a requirement for PSAs in the UK.

In the past PSAs did not generally take credit for accident management in beyond design basis conditions. More recent PSAs (AGR and Magnox) do, however, take credit for Symptom Based Emergency Response Guidelines and the Sizewell B PSA takes credit for a number of the more important recovery actions. In any PSA which contains claims for accident management, NII would wish to see the analysis carried out on a best estimate basis and also see the effect on the results of exclusion of the accident management claims. NII would be concerned if accident management measures were needed to meet the Basic Safety Levels in the SAPs.

3.4 Guidance to Licensees.

Some high level guidance is given in the SAPs. In addition NII does give informal guidance at meetings with the licensee as well as supporting the use of the IAEA PSA guide. The emphasis at meetings is usually on the scope and completeness of the PSA although for Sizewell B, a lot of time has been spent discussing specific methodologies. NII has a draft internal PSA assessment guide (AG) and parts of this have been made available to licensees. The AG is currently under revision to make it compatible with the revised SAPs.

As far as possible, NII prefers best estimate methods and data to be used in PSAs, provided there is a reasonable basis for the estimate or judgement. In practice, however, the conservative design basis analysis is often used.

There are a number of PSA features in which NII effectively sets pre-conditions or limits to claims which can be made in the PSA, including:

Common Cause Failure. A lower limit of 10^{-5} f/d is to be used for non-diverse standby systems. In practice many such systems do not merit such a low figure.

Human Factors. A 30 minute rule exists for deterministic analysis but, for PSA, NII has no fundamental objection to claims for operator action within this period. NII do not impose any preconditions on the human reliability model used. The probabilities used in the PSA do, however, need to reflect the complexity of the task, take account of the aids provided for diagnosis and of factors such as stress, time available, training etc.

FMEA. FMEA is being increasingly used as an input to PSA. For Sizewell B it was an NII requirement to use FMEA for each safety system as an aid to ensuring completeness in the structure of the system fault trees (following the first CEC Reliability Benchmark Exercise). In addition FMEAs are being done as part of the Magnox life-extension program (post LTSR), although here the main reason is to help demonstrate the completeness of the fault schedule.

Data. NII prefers that data from all available sources is considered. In assigning data for use in PSA, plant specific data, supported by other sources is preferred. In the absence of plant specific data, data from similar plant supported by generic data should be used. In the absence of specific or similar plant data NII accepts the use of generic data sources. For Magnox LTSR (periodic review) licensees are required to produce a systematic programme for the examination and monitoring of plant and components for the effects of ageing.

Mission time. NII requires that mission times to be fully justified. For Sizewell B, NII generally accepts a mission time of 24 hours on the basis that after this period, operators would have plenty of time to cope with any contingencies. Longer mission times were to be used for LOCAs, by defining an additional operating state - post LOCA recirculation.

4. Use and Review of PSA

Before submission to NII, the licensee normally arranges for a review of the PSA to be carried out by a separate part of the organisation which is notionally independent of those carrying out the PSA. The report on this review is not normally submitted to NII. NII assessors then review the submitted PSA, to the depth necessary to satisfy themselves of its adequacy for its particular purpose. NII may use consultants to assist them in parts of their review, for example a peer review of the Sizewell B PSA methodology has been carried out by a US consultancy on behalf of NII.

4.1 NII Assessment.

In an effort to make best use of a PSA NII follows a systematic assessment process:

a. Check that the PSA is satisfactory, eg that the scope is suitable, that appropriate allowance has been made for CCF and human error. Any particularly low probability sequences are given additional scrutiny to ensure they do not contain excessive claims for independence between equipment or operators. If NII was not satisfied the matter would be discussed with the licensee who may be asked to revise that part of the PSA.

b. The dominant sequences are identified and examined, their frequencies being compared both relatively and against the target for a single accident. If the targets are met assessment effort is directed at checking the validity of the PSA. If not effort is also given to establishing the specific limitations (features of the PSA or of the plant) which lead to higher than target risks.

c. Assuming that some sequences give relatively high contributions to the risk, this is taken as an indication that there may be weaknesses in the plant. It is important to establish that the PSA result in question does actually reflect the weakness of the engineering or operation of the plant and is not merely a function of the way the PSA has been done. If the result is believed to be overly pessimistic then the licensee would be asked to repeat the analysis on a more realistic basis.

d. Where a weakness is real, the licensee has to identify measures (design and/or operation) to reduce the risk as far as reasonably practicable and include the effects of these measures in a revised PSA.

e. Finally attention is given to the summated frequency criteria (eg 10^{-6}/yr for large uncontrolled release). Judgement here is more difficult and needs to take account of optimisms and pessimisms in the PSA. For example the PSA may not have quantified all initiating events (eg RPV failure) nor taken account of management influences. Sensitivity studies are a useful aid here.

4.2 Precursor studies.

Currently NII do not undertake accident precursor studies but it is anticipated that such work will become part of NII's activities in the future.

4.3 Emergency Planning.

On existing reactors PSA is seldom used for emergency planning. In the future it is expected that the results of level 3 PSAs will be taken into account in offsite emergency plans. Limited

PSAs carried out as part of AGR and Magnox beyond design basis studies are having an input into symptom based emergency procedures.

4.4 Plant Improvements.

PSA has had a significant influence on improvements to the Magnox reactors following the LTSRs (periodic reviews). Specific examples include provision of diverse secondary guardlines, automation and extension of the secondary shutdown system, improvement to and augmentation of the emergency boiler feed system. Improvement of the emergency boiler feed system, and automation of the secondary shutdown system were NII requirements. The others were on the licensees' initiative but the extent of fault coverage on the secondary guardline was enhanced as a result of NII concern. Similarly PSA has been used to identify improvements to AGR refuelling and has also led to incorporation of back-up, diverse feedwater supplies for AGRs.

4.5 Maintenance Planning.

PSA is increasingly important in maintenance planning. On their own initiative the licensees of Heysham 2 and Torness AGRs, use PSA as the basis of all planned outages of equipment required for post trip cooling. Sizewell B will be expected to plan maintenance with due regard to its impact on the risk and the living PSA (see 4.7) will be important in this respect. For Magnox plant, maintenance outages have traditionally been based on deterministic considerations but as PSAs become available for these plants the operating rules which govern maintenance outage will be reviewed at NII's request.

4.6 Identification of Research needs.

PSA was used to a limited extent in the Beyond Design Basis (BDB) research work undertaken by NE for gas cooled reactors, and to a large extent to determine requirements for research in support of the level 2 PSA for Sizewell B.

4.7 Living PSA.

Living PSAs are not mandatory in the UK, although NII supports their development. A living PSA is one which is used continuously, or regularly, as part of the decision making process on the station and is maintained in an up to date condition in terms of the plant design, operation, state of maintenance and the component reliability data. A living PSA therefore provides current best estimates of the risk (eg of core damage frequency).

The only example of a living PSA approach in use in the UK is the Essential Systems Safety Monitor (ESSM) at Heysham 2 AGR. The ESSM provides an on-line operator aid which the operator can input actual or planned outages and get advice on the actions to be taken. The ESSM is updated annually with data from the plant and modifications can be coded into the

PSA model. At Torness the allowable combinations of outages have been determined by multiple runs of the PSA. The results of these runs are tabulated within a computer based system which is used interactively by the operator. Nuclear Electric are developing a Living PSA for Sizewell B for off-line operational support. It is NII's intention that all of the PSAs, for all reactors, should be regularly updated and used to enhance the safe operation of the plants to which they relate but, as stated above, this is not yet a mandatory requirement.

4.8. Cost Benefit Analysis (CBA).

NII does not use CBA itself but does consider licensees cases containing CBA. Up to now such cases have not often been made in connection with PSA and, when made, are not often persuasive in themselves. However, it is likely that CBA will be used more in the future. Clearly CBA can only be a factor in an ALARP argument when the risk is below the tolerable level. NII would require that any CBA which seeks to justify not improving the plant should take account of all the potential health and safety costs of an accident.

5. Limitations of PSA

The limitations of PSA include (order not significant):

Quality of data
Quantification of human error and CCF
No account taken of management/safety culture aspects
Quantification of engineering judgements
Difficulty in ensuring completeness
No account taken of construction errors, other than appears in experience data.
Difficulty in quantifying cognitive human errors

Because of these limitations, NII views the results of PSA cautiously and, in an effort to identify weaknesses, takes account of relative contributions to the summated frequency as well as comparisons with target values.

6. Conclusions.

PSA is an important part of the safety case required for a nuclear installation in the UK. The PSA needs to demonstrate that the risks associated with accidental releases are sufficiently low.

In NII's view the main value of PSA, and the most robust use, lies in the identification of weaknesses in the design or operation of the plant and enabling the various contributions to the risk to be seen relative to one another in a consistent overall framework.

7. References.

(1) HSE Safety Assessment Principles for Nuclear Power Reactors HMSO 1979 (amended 1988).

(2) HSE Safety Assessment Principles for Nuclear Plants. HMSO 1992

(3) HSE The Tolerability of Risk from Nuclear Power Stations. HMSO 1992.