# 1. INTRODUCTION TO PSA

## 1.1 Historical Background

Around the middle of this century, up to the 1950s, the main improvements in the reliability and safety of complex technological systems came from the application of quality control and inspection techniques. However, as technology advanced, the techniques for assessing plant safety and reliability had to change. Methods employing probabilistic techniques therefore were started to be developed. The first systems to benefit from these improved analytical techniques, such as fault tree analysis were limited in the main, to those in the aircraft, space and defence industries.

For nuclear power plants, designs traditionally include extensive safety precautions, such as component and system redundancy and diversity within important areas, in order to deduce the possibility of accidents with serious consequences. These precautions are on top of rigid quality assurance and inspection programmes. In the past, the compliance with safety requirements was assessed using deterministic analysis that used pessimistic assumptions in order to ensure the results of the assessments were "on the safe side".

These deterministic techniques however only assessed traditional faults. This method of analysis has the problem that from a probabilistic view point some of the faults analysed may be negligible, or that more importantly some faults not traditionally assessed are overlooked, which may have serious consequences. Justifying further faults to analyse in a traditional deterministic manner, becomes difficult as the inclusion of more and more safety precautions into reactor design has rendered more and more rare, the recording of events of a direct safety significance. However, the lack of operational events does not preclude the existence of underlying safety significant faults. Techniques were therefore required to comprehensively identify and assess these faults.

Gradually since the early 1960's, probabilistic techniques developed, such as the development of Fault Tree Analysis techniques by H.A. Watson in 1961, of the Bell Telephone Company, originally produced as an evaluation of rocket launch control system, and as further developed by the likes of D.F. Haasl, of the Boeing Corporation and W.E. Veseley of the Idaho Nuclear Corporation. With time these techniques were introduced into the nuclear industry, with the benefits of the methods and the results produced becoming very obvious. The culmination of this introduction and the linking together of the various techniques being developed led to the derivation of the concept of Probabilistic Safety Assessment (PSA).

The first comprehensive application of the methods and technique of PSA to nuclear power plant was in 1975, when the USNRC Reactor Safety Study (WASH 1400) was undertaken. This analysis was the first analyses to compare quantitative estimates of risk of nuclear power plant with other non- nuclear risks, this being done for two plants Surry - 1 (PWR) and Peach Bottom - 2 (BWR). Since this landmark study, there has been substantial method development and computer application, and PSA has become a standard tool in the evaluation of the safety of nuclear power plants, with PSAs having been or being undertaken on a large proportion of reactors world wide.

Originally, at the beginning of the application of PSA methods, it was believed that these methods could be used for generating probabilistic acceptance criteria, for the development of nuclear power, for example making comparison with risks which are generally excepted in

life. However, the use of quantitative goals in regulatory requirements turned out to be difficult. The main reasons were the dependence of the results of a PSA upon the PSAs scope, the methodologies adopted, on some of the subjective elements of the analysis, as well as the lack of plant specific data.

However, these first risk analyses provided important insights into the strengths and weaknesses of the design and operation of the plants investigated, as well as pointing out ways to improve plant safety. The many PSAs undertaken to date on existing plant as well as new designs, have continued to confirm the benefit of **PSA** in identifying plant weaknesses, whilst at the same time development in safety goals and technical acceptance criteria continues.

### 1.2 What is PSA?

Probabilistic Safety Assessment (PSA) provides a consistent and integrated model of nuclear power plant safety. It is a conceptual and mathematical tool for deriving numerical estimates of risk for nuclear power plants (and industrial installations in general). Consequently, PSA offers a rigid framework upon which safety related decisions can be made. It allows changes or alterations in different design and engineering areas in a nuclear power plant to be compared to a common basis, in terms of a base line quantitative estimate of risk.

PSA differs from the traditional deterministic analyses as previously mentioned, in that it provides a methodical approach to identifying accident sequences that can result from a broad range of initiating events. It includes the systematic and realistic determination of accident frequencies and consequences, and aims as much as possible to be 'best-estimate'. How true this last statement is depends upon the amount, quality and type of information available for use in the PSA, and in many areas due to lack of information pessimistic assumptions have to be made. The major benefit of PSA is that it provides important safety insights in addition to those provided by any deterministic analysis. These include insights into plant design, performance and operation as well as environmental impact, and the identification of dominant risk contributors.

In summary **PSA** aims to :

i) identify and delineate the combination of events that may lead to a severe accident.

ii) assess the expected probability of occurrence of each combination.

iii) evaluate the consequences.

## 2 OVERVIEW OF PSA

### 2.1 Definition of **PSA**

PSA is a methodical, logical tool for deriving numerical estimates of risk from nuclear power plant (or indeed any plant in general).

PSA methodology integrates information about plant design, operating practices, operating histories, component reliabilities, human behaviour, thermal hydraulic plant response, accident phenomena, and taken to it conclusion potential environmental and health effects.

In practice PSA aims to achieve completeness in defining possible mishaps, deficiencies and plant vulnerabilities, producing a balanced picture of safety significant issues across a broad spectrum.

PSA is one of the most efficient and effective tools to assist in the decision making process for the safety and risk management of nuclear power plants. As such it can have one or more of the following objectives:

- to assess the level of safety of the plant and to identify the most effective areas for improvement ,
- to assess the level of safety and compare it with explicit or implicit standards,
- to assess the level of safety to assist plant operation

The first general objective aims at extending and widening the understanding of the important issues that affect the safety of a nuclear power plant. By doing so, design and operational problems can be identified and areas for improvement or future study can be identified. The second objective contains the element of overall adequacy, in that it is deemed desirable to compare the assessed safety related capability of the plant against given standards. These standards might be explicitly or implicitly defined criteria. The third objective aims at providing information that can assist plant operations. For example this may be in the form of improved Technical Specifications, or advice on monitoring operational reliability or accident management.

The required object of the PSA therefore will partly define the scope and extent of the study and as such PSA has itself developed into a hierarchical structure to accommodate the variation in PSA objectives. These are discussed below.

## 2.2 Analysis Levels

The development of PSA over the years has led to what are three traditionally and internationally accepted levels of analysis.

LEVEL 1

This is the initial and foundation level of a PSA. This level provides an assessment of plant design and operation focusing on those accident sequences which could lead to core damage. It is this part of the PSA which can provide major insights into design strengths and weaknesses, as well as ways into preventing core damage, which in most cases would be a precursor to accidents leading to major radioactive releases with potential health and environmental consequences.

LEVEL 2

This level of analysis builds on the analyses already undertaken in the Level 1 study. Level 2 also addresses the phenomena of core damage accidents but does so in terms of the response of the containment. This analysis assesses the response of the containment to the expected physical loads resulting from a particular accident sequence as well, as the transport of radionuclides from the core to the environment. A Level 2 PSA provides insights into the relative importances of sequences leading to core damage in terms of the severity of the radionuclide releases they cause, as well as highlighting weaknesses and improvements in the mitigation and management of severe accidents.

LEVEL 3

In addition to the analysis undertaken for a Level 2 analysis, a full scope Level 3 PSA also analyses the dispersion of radionuclides to the surrounding environment, analysing both potential environmental and health effects. This level of analysis provides insights into the relative importance of accident prevention and mitigation with respect to the adverse effects on the health of both plant workers and the public and the contamination of the land, air, water, and foodstuffs.

For this PSA course we shall be purely concentrating on the Level 1 aspects of PSA and as a way of an introduction a more detailed breakdown of what constitutes a Level 1 PSA will be given.

## 2.3 Breakdown of a Level 1 PSA

A Level 1 PSA can be broken down into various constituent parts, of which the following can be said to be the most important.

- Definition of the scope of the PSA
- Plant familiarisation and information gathering
- Selection of Initiating Events (IEs) to be assessed
- Accident sequence modelling
- System modelling.
- Data acquisition and assessment
- Accident sequence quantification

All of the above parts of a Level 1 PSA have associated with them numerous analytical techniques and methods. They will be discussed at some point during this course but the majority of the emphasis will be placed upon those methods associated with the accident sequence modelling and the system modelling, namely Event Tree and Fault Tree analysis. However, before launching into any detail on these topics an overview of the Level 1 analysis will be presented.

The overall scope of the Level 1 PSA is given in Figure 1, with the various interactions between the constituent parts.

Definition of the Scope of the PSA is of most importance in order that the defined scope meets the overall objective for undertaking the study. Most PSAs for a nuclear power plant consider initially modelling of the plant at normal operating conditions at 100% full power (or

the power at which the plant spends most of its operating life). All PSAs as a minimum cover those events, which occur internally to the plant, which could potentially lead to a severe accident. The option to include other events such as internal and external hazards e.g. fire, flood and seismic events depends upon the objective and use of the PSA and also to a certain extent on any time and cost constraints.

Plant Familiarisation and Information Gathering can be one of the most difficult and time consuming activities with respect to producing a **PSA.** The shear volume of information required to put together a PSA is enormous and dependent upon numerous aspects. For example whether the PSA is being performed by analyst who already have detailed plant design and operational experience of the plant or at what stage in a plant life eg during its design or following numerous years of operation. Such concerns will have a large effect on the extent of this task. Even if tall the information required for a PSA is available it may not be in a form in which it can be used straight away.

The Selection of Initiating Events is one of the most critical parts of the PSA. This is one of the tasks, which ensures completeness of the PSA within its defined scope, as the omission of one or more events of significance can have a profound effect on the overall results. Within the scope of the PSA, initiating events are derived from various sources, including operating histories, and deductive analysis, to form the starting point of the PSA. The overall list of Initiating Events is normally reduced by grouping together Initiating Events, which impose a similar response upon the plant. Each group can then be cover a single analysis, reducing the analytical effort required.

Accident Sequence Modelling is the determination of the possible plant responses to each of the defined initiating event groups. This modelling results in the generation of accident sequences with a given consequence, and is normally undertaken using Event Tree Analysis. As a result of this analysis, to which the system analysis modelling will ultimately provide an input, event sequences expressed in terms of the initiating event and the success or failure of mitigating systems are created, each for which a frequency can be quantified.

System Modelling provides the detailed modelling of the constituent events of the accident sequences defined by the accident sequence modelling. The most usual events that are modelled are the success or failure of a safety system. Fault tree analysis is the most widely used method for developing system models. Before such modelling can occur however, analysts require to have a very good understanding of the system and its operation, which can be enhanced by the use of quantitative techniques such as Failure Mode and Effects Analysis (FMEAs).

Data Acquisition and Assessment is the final task prior to quantification of the PSA model. The collation of data required as input in determining initiating event frequencies for input into the event trees; component failure, repair, test, maintenance and common cause data for input into the fault trees, as well as human error data is required.

For each of these, the identification of data sources and data collection is required, together with the selection and application of estimation techniques.

Accident Sequence Quantification is the culmination of all the previous tasks of the PSA. Quantification using the Boolean algebraic solutions associated with the event tree/fault tree analysis is undertaken, determining the relative importance to the core damage frequency of

the various contributors. Where conservative estimates of input data or modelling assumptions appear as dominant contributors, further refinements to these data and assumptions may be required and the appropriate sequences requantified in order to achieve an overall balanced PSA model. Quantification of the final models, because of their size and complexity is normally undertaken using computer codes, either utilising a separate event tree and fault tree code, or by using a code which directly links the event trees and fault trees.