IAEA-TECDOC-1144

Probabilistic safety assessments of nuclear power plants for low power and shutdown modes

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

March 2000

The originating Section of this publication in the IAEA was:

Safety Assessment Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

PROBABILISTIC SAFETY ASSESSMENTS OF NUCLEAR POWER PLANTS FOR LOW POWER AND SHUTDOWN MODES
IAEA, VIENNA, 2000
IAEA-TECDOC-1144
ISSN 1011-4289

Printed by the IAEA in Austria
March 2000

FOREWORD

Within the past several years the results of nuclear power plant operating experience and performance of probabilistic safety assessments (PSAs) for low power and shutdown operating modes have revealed that the risk from operating modes other than full power may contribute significantly to the overall risk from plant operations. These early results have led to an increased focus on safety during low power and shutdown operating modes and to an increased interest of many plant operators in performing shutdown and low power PSAs.

This publication was developed to provide guidance and insights on the performance of PSA for shutdown and low power operating modes. The preparation of this publication was initiated in 1994. Two technical consultants meetings were conducted in 1994 and one in February 1999 in support of the development of this report.

The IAEA wishes to thank all those who participated in the development of this publication. In particular, the contributions of P. Boneham and W. de Wit to the development and review of the final version are greatly appreciated. The IAEA officers responsible for this publication were R. Gubler and R. Sherry of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Historically, most probabilistic safety assessments (PSAs) for nuclear power plants (NPPs) have focused on full power operation of the plant. Detailed consideration of low power and shutdown periods in PSAs was initiated during the 1980s. The first detailed PSAs for shutdown mode operation were performed for the 900 and 1300 MW plants in France. Recent PSAs for NPPs considering low power and shutdown operational periods have shown that these periods can substantially contribute to the risk of plant operations. They indicate that shutdown and low-power operations can contribute to core damage frequency (CDF) at a level comparable to full power operations. One important reason for this result is that, traditionally, less attention has been given to the design and operational features of nuclear power plants for these operational states. The variability in plant configurations, simultaneous unavailability of systems, blocking of automatic actuation of safety systems and limitations in operational procedures are the main risk significant characteristics for low power and shutdown operational states.

Although similar to a PSA for full power operation in many respects, a PSA for low power and shutdown modes, called shutdown PSA (SPSA) in this report, may address important additional concerns relating to safety. These include simultaneous system unavailability during different phases of an outage, the importance of operator actions to restore functions, and the wide range of activities taking place during shutdown.

An SPSA can provide useful insights and feedback as regards: (a) outage planning; (b) plant operations and procedures during an outage; (c) shutdown technical specifications; (d) outage management practices; (e) personnel training; (f) emergency planning and emergency operating procedures and (g) hardware modifications. Regarding such applications, risk from all operating states should be considered in an integrated manner. Hence, the shutdown PSA should be considered in the context of the full scope PSA. For example, moving maintenance activities from shutdown operating states to full power operations and changing the duration of allowed outage times in technical specifications can affect not only the shutdown PSA, but also the full power PSA. An isolated view based only on changes in shutdown risk for individual applications without consideration of the risk impacts during other operational states might be misleading.

1.2. OBJECTIVES OF THIS PUBLICATION

This publication is intended to provide guidance for the performance and review of SPSAs, including applications of the SPSA information and results to improve outage safety. Emphasis is given to the assessment of critical human interactions. These are especially important during low power and shutdown conditions, first, because they have a potential to cause or to contribute to initiating events, second, because they may affect the availability of equipment which is required after an initiating event, and third, because the success or failure of operators to terminate or mitigate accident sequences is critical.

The present PSA practice for dealing with the variety of different plant states during low power and shutdown operations is a phased approach which consists in defining a limited number of plant operating states (POSs) for which unique plant configurations and conditions can be identified. The process of determining these POSs and the initiating events which may

occur during these POSs, including categorization and condensation which is necessary to make the assessment practical, are key considerations in the performance of SPSA.

The present publication describes procedures for conducting a plant specific SPSA. The document should be used in conjunction with the following IAEA PSA procedures:

- Procedures for conducting probabilistic safety assessments of nuclear power plants (Level 1) [1].
- Procedures for conducting probabilistic safety assessments of nuclear power plants (Level 2) [2].
- Procedures for conducting probabilistic safety assessments of nuclear power plants (Level 3) [3].
- Treatment of external hazards in probabilistic safety assessment for nuclear power plants, [4].
- Treatment of internal fires in probabilistic safety assessment for nuclear power plants [5].

References [6] and [7] also provide useful insights for the performance of SPSA.

For historical reasons, the focus of the above procedures for Level 1 and Level 2 is on PSA for full power operational conditions. A comprehensive definition of PSA levels is given in Ref. [1]. While there are differences for SPSA compared to PSAs for full power conditions, the overall procedure is similar and therefore the present publication follows the tasks and steps in the PSA procedures for full power conditions as far as appropriate and useful. The most significant differences regarding the application of the PSA procedures to SPSA result from the number of different operating states during low power and shutdown modes.

The emphasis of this publication is on the procedural steps for SPSA in order to promote a standardized framework, terminology and format for documentation. This guidance will also facilitate external review of SPSAs. Finally, this publication includes a discussion of the applications of SPSA.

The procedure for conducting a SPSA described herein is not intended to prevent development and use of new methods. On the contrary, development of other approaches to SPSA is encouraged.

1.3. SCOPE

This publication concentrates on Level 1 (core damage frequency assessment) aspects of SPSA. A limited discussion is also included on the Level 2 (containment performance) SPSA. This publication does not consider Level 3 (consequence assessment) SPSA, since the Level 3 part of an SPSA would be similar to a PSA for full power operation. The following sections summarize the scope and limitations of the report.

1.3.1. Ranges of operational conditions considered in SPSA

A nuclear power plant can be in many operational states, with reactor power ranging from full power to complete shutdown. The focus of this publication is on the outage types which include low power and shutdown operational states. Most SPSAs are carried out after the PSA for full power conditions has been completed, using and adapting the information and models

for full power operation. For the SPSA, the interface to an existing PSA for full power operation needs to be carefully considered and defined to avoid gaps or unnecessary overlaps.

1.3.2. Sources of risk

A Level 1 SPSA provides insights into the importance of various aspects of design, operating practices, maintenance, technical specifications, accident procedures and outage management with regard to the prevention of fuel and core damage and with regard to releases of radioactive materials. It provides for the quantification of risk and the relative importance of the different initiating events, safety systems and other factors with respect to the selected risk measures.

In principle, a Level 1 PSA may cover risks originating from damage to the reactor core, fuel handling accidents and other ex-core accidents such as loss of fuel pool cooling. In PSAs for full power conditions, the emphasis has traditionally been on damage to the reactor core. For SPSAs, other scenarios may also be relevant in the overall risk picture. They are therefore highlighted in appropriate sections in this report.

1.3.3. External and internal initiating events

As for a PSA for full power operation, in a SPSA, initiating events can be categorized as internal, internal area and external. Internal initiating events have their origin in the plant process, directly or indirectly, through human interactions or equipment malfunctions. Most SPSAs have been limited to internal initiators, but it is recommended that SPSAs be extended to consider all important initiator types (particularly internal area events such as fires and floods), since nuclear power facilities are suspected to be particularly vulnerable to these events during shutdown. For area events, the identification of the potential sources, effectiveness of barriers, and the probability of mitigative operator response pose special challenges for SPSA model development and quantification. Similarly, analysis of off-site external events differs from PSAs for full power with regard to plant response and human actions.

1.4. STRUCTURE

This publication is divided into sections corresponding to the major procedural steps characterizing an SPSA. In general, they follow the procedure for a PSA for full power conditions. However, due to the complexity caused by the number of plant operating states during which an initiating event could occur a discussion of the required extra screening phase has been included. This discussion also describes the grouping process necessary to arrive at a manageable number of plant operational states/initiating event combinations to analyse. The procedural steps are as follows.

1.4.1. Management and organization (Section 2)

This step includes the actions and activities necessary for the organization and management of the study. It includes the definition of the objectives and scope, project management, selection of methods and procedures, team selection, organization and training, as well as quality assurance and review activities. Although many of these items are in principal similar to a PSA for full power operation, important differences are indicated in Section 2.

1.4.2. Definition of outage types, plant operating states and accident initiators (Section 3)

The purpose of this step is to identify the potential sources of radioactive release, to produce a list of plant operational states (POSs) and initiating events for the SPSA. POSs are used to model the unique plant configuration and operational conditions during low power and shutdown operation. The step includes information gathering and plant familiarization as well as selection of the outage types to be studied. A preliminary grouping is made of the POSs and initiating events are initially identified. Finally, this step also includes quantification of the initiating events and identification of system dependencies.

Although a preliminary grouping and merging is usually done in the identification process for POSs and initiating events, the resulting number of combinations of POSs and initiating events could result in a very large PSA model. To reduce the PSA effort to a manageable size, further screening and condensation will be necessary.

After the initial list of POSs is developed (pre-POS), it is usually possible to condense the complete list of POSs into a smaller set. This is the process of grouping the pre-POSs into groups with similar characteristics. Grouping of POSs may involve conservative simplifications in that less severe and demanding POSs are attributed to similar, but more demanding POS. It may also be possible to show that some POSs will have a small risk impact because they are unlikely to occur or are of very short duration. These POSs will be of low risk importance and can be eliminated from further consideration with no significant impact on the final risk result. However, for certain applications, such as development of models for incorporation into risk monitors where instantaneous (point-in-time) risk predictions are desired, elimination of short duration POSs should be carefully assessed (see Section 3.10.1).

These processes should follow specified procedures, criteria and rules and should be fully documented. Because this step may be more judgmental than others, documentation is especially important.

1.4.3. Accident sequence modelling (Section 4)

As for a PSA for full power operation, accident sequence modelling involves a number of tasks including consideration of the plant response to the initiating events, event sequence modelling, determination of success criteria for required safety functions and analysis of system reliabilities. For the modelling part of this step, a suitable methodology using a combination of tools such as event trees and fault trees should be chosen. The specific methodology may differ from a corresponding power PSA due to the specific conditions during shutdown. Important activities in the modelling tasks are human performance analysis and dependence analysis.

1.4.4. Data assessment (Section 5)

This major procedural step aims at acquiring and generating all information necessary for the quantification of the model, including component reliability data, test and maintenance unavailabilities, and an assessment of common cause failures.

At present, only a few data bases have been developed for low power and shutdown operation, which means that often data from full power operation must be used with due consideration of specific shutdown conditions. There are situations for which specific shutdown

data must be used or estimates otherwise generated for the shutdown analyses because information from power operation is inappropriate.

1.4.5. Internal and external hazards, heavy load drops and accidents involving other sources of radioactive materials (Section 6)

This section describes the SPSA analysis associated with external event initiators including seismic, external flooding and high winds; and internal areas events including internal fires and flooding. Direct damage can occur as a result of heavy load drops onto the reactor vessel, fuel pool or systems required to maintain the critical safety functions. In addition, the release of radioactive materials may occur if damage occurs to other sources of radioactive materials in the plant, e.g. dropping of reactor fuel assemblies or accidents involving radioactive waste storage tanks.

1.4.6. Accident sequence quantification, uncertainty analysis and sensitivity studies (Section 7)

For SPSAs, accident sequence quantification may be performed using the same techniques as for a PSA for full power conditions. It should be noted, however, that in an SPSA, in which long mission times or recovery times are often applicable, use of Markovian techniques instead of standard fault tree/event tree evaluation methods have the potential to yield more realistic results.

The SPSA, like the PSA for full power operation, should be accompanied by an appropriate sensitivity analysis to provide an appreciation of the sensitivity to variations in the SPSA data, models and assumptions. A formal uncertainty analysis is also recommended. Importance and sensitivity analyses are performed using the same techniques as for a PSA for full power operation.

1.4.7. Documentation and presentation of results (Section 8)

The final step of the SPSA is the documentation and presentation of the information and results. The documentation and presentation of results are very dependent upon the objectives and scope of the study and on the planned uses of the study. If the study is designed only to conservatively represent shutdown risk and identify risk-outliers, then a different set of documentation is needed than if the study is designed to be used by plant personnel to assist in planning future outages. In this regard, documentation refers to the configuration and accessibility of the models and data as well as to the written description and discussion of the SPSA results, methodology, assumptions, etc.

1.4.8. Application of results (Section 9)

After the SPSA has been completed, it should be reviewed to determine if the results highlight any needs for safety improvement measures. Possible areas for such measures are outage planning, operating procedures, technical specifications, accident procedures, emergency planning, hardware modifications, training of personnel and management practices.

Annex I provides examples of plant operational states as defined in SPSA studies for BWR and PWR reactors. A number of low power/shutdown risk analyses are listed in Annex II. Annex III provides examples of the initiating events from several different shutdown PSA studies.

2. MANAGEMENT AND ORGANIZATION

For the management and organization of an SPSA, eight main tasks can be identified. Although the task list is similar to that of a PSA for full power conditions, the details of specific tasks are different. The most significant difference regarding the PSA procedure for SPSA stems from the number of operating states during low power and shutdown modes.

2.1. TASK 1: DEFINITION OF THE OBJECTIVES OF THE SPSA

The objectives and envisaged applications of the SPSA determine the scope, methodology and resource requirements of the study. The objectives of the SPSA are therefore an important consideration in determining the methodology to be followed and level of detail in various aspects of the analysis. The general objectives of a Level 1 PSA, which also apply to the SPSA, are described in the Level 1 PSA procedures [1]. Further details on specific objectives and uses of a SPSA are given in the following sections.

2.1.1. Characterization of risk for a specific outage

The SPSA model can be developed for use in estimating the risk of an actual outage that is completed, under way, or being planned. The SPSA models must be capable of representing the actual configurations of the plant that occur in the outage as well as the actual availability status of equipment.

2.1.2. Comparison with safety goals or criteria

Decisions may be based on the use of probabilistic safety goals or criteria, for example the following risk measures may be compared to various safety goals:

- core damage frequency (Level 1);
- radionuclide release magnitudes/frequency, large early release frequency (Level 2);
- off-site consequences (Level 3).

In addition to the above risk measures, decisions may be based on instantaneous (single point-in-time) values of the risk measures in an attempt to control occurrences of very high risk peaks of short time duration. Occurrence of very high risk for short times may be undesirable even if the average risk is acceptable.

2.1.3. Support for applications

The results and models from SPSAs have been used to support the following applications:

- outage planning and maintenance scheduling
- development/modification of operating/accident procedures
- development/modification of technical specifications
- emergency planning
- decisions on hardware modifications
- training of personnel
- management practices.
-

These activities are discussed further in Section 9.

2.2. TASK 2: DEFINITION OF THE SCOPE OF THE SPSA

It is very important to make a clear distinction between those operating conditions included in the PSA for full power condition and those considered in the SPSA. The definition of an SPSA as regards operating conditions, apart from full power, should include all plant configurations different from those covered under a full power PSA. The scope definition should consider:

- power levels;
- RCS configuration (including RCS integrity, temperature, pressure, and coolant level);
- means of core heat removal;
- status of actuation signal interlocks;
- requirements on availability of safety and support systems;
- requirements on containment isolation and safeguard systems;
- location of the fuel.

Important features distinguishing an SPSA from a PSA for full power operation are the need to consider (typically) numerous POSs during shutdown, as well as transitions between these states, and the fact that these may change significantly from outage to outage.

2.2.1. Sources of radioactive releases

One important parameter that characterizes the scope of a PSA is the sources of radioactive releases in the plant. The most important (applicable to all types of plants) are:

- the reactor core;
- the spent fuel storage pool;
- the spent fuel handling facilities.

The SPSA can be performed for any combination of these sources, although historically most SPSAs have been confined to the reactor core and spent fuel pool.

2.2.2. Level of detail

The level of detail considered within each area of the PSA should be determined from the start. Depending on available resources, the PSA may be performed in detail from the beginning, or a phased approach may be followed. A two phase approach may involve a qualitative screening analysis followed by a detailed analysis of selected scenarios. In the first phase, a detailed list of plant operational states (pre-POS), initiating events and top events for the event trees may be developed, followed by a screening analysis to select the accident scenarios that contribute significantly to the risk (e.g. in terms of frequency and consequences). This may involve the use of simplified fault trees and event trees, along with conservative assumptions on the accident consequences in each case. The second phase would then involve a detailed analysis of the potentially risk significant accident scenarios. This is the approach that is discussed in the present publication.

2.2.2.1. Treatment of human actions

The depth of treatment of human actions, use of (conservative) screening or best estimate human error probabilities, the extent of inclusion of operator and/or maintenance personnel errors, the extent of inclusion of operator recovery and repair actions and the extent of treatment of errors of commission are particularly important considerations for an SPSA in which the risk is generally dominated by human error.

2.3. TASK 3: PROJECT MANAGEMENT

Compared to a PSA for full power operation, it is even more crucial for the SPSA analysis team to interact with plant operating and maintenance personnel in order to reflect plant design, operational features and practices during low power and shutdown conditions. This kind of interaction and communication with plant staff needs to be organized and reflected in project management. Performing a meaningful SPSA for a plant which is still in the design or construction stage and for which detailed procedures and practices for low power and shutdown operation are not yet available is difficult unless the procedures and practices can be inferred from similar plants already in operation.

2.4. TASKS 4 and 8: SELECTION OF METHODS, ESTABLISHMENT OF PROCEDURES AND QUALITY ASSURANCE

Specific methods need to be selected and specified in procedures for performing the SPSA. Selected aspects and details of methodologies for SPSA are discussed in Sections 3, 4 and 5.

The establishment of a quality assurance (QA) programme is an essential aspect of good management and is fundamental to the achievement of a quality SPSA. A comprehensive review process accompanying the SPSA is essential for its quality. Reference [8] contains a framework for QA which, with appropriate adaptation, can be used to establish QA and review activities for the SPSA. As the methods for SPSA are less developed than those for PSA for full power conditions, it is important to allow for changes and extensions in the procedures in a controlled environment and subject to QA.

2.5. TASK 5: TEAM SELECTION AND ORGANIZATION

Most SPSAs to date have been carried out after the PSA for full power conditions has been completed and the SPSA made use of the information and models of the PSA for full power conditions. It is preferable that the same team or team members who have carried out the PSA for full power operation participate in the SPSA in order to take advantage of this experience. Otherwise, significant time has to be devoted to familiarization with the PSA for full power operation. During recent years increasing weight has been given to the integration of human reliability analysis (HRA) into the overall PSA. The PSA team should therefore be organized in a way that facilitates the required multidisciplinary investigations required for performance of the SPSA. This is especially crucial for an SPSA with its many critical human interactions which need to be considered.

2.6. TASK 6: TRAINING OF THE TEAM

It should be emphasized that additional information and training may be required in the following areas which may not have been addressed to the same level in the full power PSA:

- special SPSA techniques, such as the development of the POSs;
- plant operational features and practices for low power and shutdown operation.

Furthermore, SPSAs carried out for plants of similar design should be reviewed.

2.7. TASK 7: FUNDING AND SCHEDULING

Funding and scheduling for an SPSA can be comparable to a PSA for full power operation. If the PSA for full power operation is available, the effort required for the SPSA can be reduced by taking advantage of the existing logic models and data. However, the determining factors for the effort required for an SPSA are the types of outages to be considered, the level of detail required, the scope of the PSA and the experience of the analysts.

3. DEFINITION OF OUTAGE TYPES, PLANT OPERATIONAL STATES AND ACCIDENT INITIATORS

In contrast to full power operation, plant configurations and conditions significantly change during low power and shutdown operation. In the technical specifications, low power and shutdown operation is usually divided into several operational modes, each having its own operational requirements. Depending on the plant considered, there are different types of outages, such as regular refuelling and maintenance outages and unplanned outages, which follow a disturbance in normal operation. Plant conditions, configurations, timing and transitions between operational modes also depend on the type of outage. The current practice for modelling this changing plant operational environment during low power and shutdown in the SPSA is to define a number of POSs which are used to describe the operational stages during the outages. Task 11, in Section 3.3, describes the selection of outage types and the definition of POSs.

The approach to POS definition used in this publication uses the concept of pre-POS. Pre-POSs generally correspond to different procedural steps or actions which occur during the outage. The list of pre-POSs and their descriptions form the basic information about the outage which is used in developing the SPSA. A POS is a group of pre-POSs which, for the purposes of PSA analysis, may be considered to be equivalent. A typical SPSA may define in the order of 100 pre-POSs which may then be grouped into some 10 to 20 POSs.

In principle, the SPSA needs to address all the initiating events which are feasible in every POS. Clearly, this leads to a considerable number of POS/initiating event combinations which are candidates for a detailed analysis. Thus, some screening and perhaps re-classification may be needed in order to reduce the number of initiating events and POS combinations to a manageable size. The re-classification of POSs and initiating events into a smaller number of representative POSs and corresponding initiating events is called "grouping" in the text which follows. This may be a cyclic iterative process which has to be continuously reviewed as the analysis progresses through the SPSA.

The emphasis given to this screening and grouping process, together with the large number of POS/initiating event combinations to be analysed are the key methodological differences compared to a PSA for full power conditions.

The present section describes the definition of POS, identification of initiating events and quantification of their frequency, and screening of the resultant POS/initiating event combinations to reach a set of "scenarios" which will be analysed in detail. This section covers nine tasks (task 9 to task 17, plus task 24).

3.1. TASK 9: FAMILIARIZATION WITH THE PLANT AND INFORMATION GATHERING

The IAEA Level 1 PSA procedures [1], describe this task as it would be performed for a full power PSA. Much of this material is also applicable to an SPSA. This section describes some key differences.

The SPSA team should become familiar with the design, operation and maintenance of the plant during outages, including technical specifications applicable to shutdown conditions and relevant emergency procedures. Available SPSAs that have been performed for plants of similar design should be studied. A list of completed SPSAs is provided in Annex II. In addition, the team should review the following information sources:

- PSA for full power conditions;
- outage schedules with start-up and shutdown procedures and timetables;
- plant technical specifications and other regulatory requirements relating to shutdown conditions;
- shutdown related event occurrence reports;
- operating and maintenance policies and procedures for shutdown;
- main work order lists;
- work order issuing practices and maintenance work administrative controls;
- emergency procedures for initiating events during shutdown;
- operator logs.

The information listed above is particularly useful to support the definition of pre-POS (and subsequently, POS), as described in Section 3.3. below.

3.2. TASK 10: IDENTIFICATION AND SELECTION OF SITE SOURCES OF POTENTIAL RADIOACTIVE RELEASES

All potential sources for radioactive releases should be considered in the initial screening. For a LWR type reactor the list usually includes the following:

- reactor core;
- spent fuel in the storage pool;
- fuel handling facilities and fuel handling pathways.
- waste facilities (e.g. storage tanks, waste processing facilities, etc.)

3.3. TASK 11: SELECTION OF OUTAGE TYPES AND DEFINITION OF PLANT OPERATING STATES

A clear interface point should be defined between the POS modelled in the full power PSA and those to be modelled in the SPSA. The full power POS PSA and the low power and shutdown POSs PSA then represent a complete PSA for all operational states of the plant.

During low power and shutdown periods a large number of plant configurations exist which would, if handled without grouping, lead to an excessive number of scenarios to be analysed. Typically, nuclear power plants experience various types of outages, from short unplanned outages, which are used for repairs or adjustment, to regular planned refuelling outages, which also include major maintenance activities. In order to develop the plant risk profile over an average operating year, all outage types should be considered.

The current practice for dealing with the variety of plant states during low power and shutdown is to define a limited number of POSs during which the plant status and configuration are sufficiently stable and representative. In order to limit the number of combinations of POSs and initiating events to a manageable size, screening and grouping rounds are usually performed starting from the initially defined pre-POSs.

This section describes the process of defining the shutdown state, selecting the outage types and determining the POSs.

3.3.1. Definition of shutdown state

Defining the interface point between power operation and shutdown (or low power) operation for the purpose of development of the SPSA model is a critical task. The power level (or reactivity coefficient) of the reactor is not the only, nor from the safety perspective the most important, criterion for defining the interface between power and shutdown operation. The status of major safety functions may be more important in defining this interface. Among these, two elements have been traditionally seen as of dominant importance:

- status of automatic actions
- status of support systems.

Typically, below a certain level (this may be defined either by the power level, primary temperature, primary pressure or some combination of these parameters) automatic actuation of the main safety systems may be blocked to prevent inadvertent actuation. For example, at WWERs the large LOCA signal is inactive below 245°C primary temperature. In Westinghouse PWRs, interlocks P-11 and P-12 are generated at RCS pressures and temperatures of approximately 14 MPa and 289°C, respectively, blocking signals related to the automatic actuation of safety injection. Also, at some Westinghouse PWRs, an automatic RPS actuation signal will be blocked below 7% power.

In some cases, as the plant is approaching shutdown conditions, the essential support system configuration may change. For example, the unit power supply may be transferred from one source to another. This may include the transfer from the main transformers to the auxiliary transformers associated with turbine trip. The 15% power interface point chosen in the NUREG/CR-6144 study for Surry [9] corresponds to this sort of configuration change.

In some plants the shutdown sequence would be turbine trip and simultaneous reactor trip, while for other plants a slow reduction of power level follows the trip of the turbine.

3.3.2. Selection of the outage types

There are basically three different types of outages: (1) refuelling outages, (2) planned maintenance outages and (3) unplanned outages. From the SPSA perspective they differ in the following aspects:

- system, train and component availabilities
- sequence, duration and timing
- neutronic and thermal-hydraulic conditions
- primary system and containment configuration.

Outages also include the longer term periods of an unplanned shutdown following a significant accident (the initial portion of the shutdown in this case would be considered in the full power PSA). For specific sites, there might be a planned shutdown prior to an anticipated or imminent external hazard. For many unplanned shutdowns, operation can be resumed after a short delay of a few hours. For these shutdowns it is generally not necessary to go to cold shutdown nor is it necessary to open the reactor vessel head (for vessel type LWRs). For this type of outage only the operational modes which actually occur during the outage need to be taken into account in the SPSA. If the cause of the shutdown is the unavailability of a system, there can be a dependency between the cause of the shutdown and the systems required to respond to the shutdown. To account for dependencies between the cause of an unplanned outage and the mitigating systems requires the same sort of methodological approach as used in modelling initiating events due to failure of plant systems. In contrast to shutdowns, plant startups are similar, regardless of the cause of the shutdown.

Depending on the plant considered, it may be necessary to define different types of planned outages for the SPSA. For example, in a refuelling outage for some PWRs, all the reactor coolant loops may be isolated, which may not be the case for a maintenance outage in which maintenance on only one reactor coolant loop is carried out. Another example common to BWRs and PWRs is an outage of long duration for inspection of the reactor vessel internals in which all the fuel is transferred to the fuel storage pool.

For reactor types with on-line refuelling, such as PHWRs and RBMKs, different types of outages have to be considered compared with LWRs. The planned outages are related to the in-service inspection programme and surveillance requirements.

3.3.3. Selection of POSs

POSs may be defined specifically for each plant outage type. However, similar POSs would be found in different outage types, though possibly with different durations. This may allow for development of models for specific POSs and then development of a model for different outage types as a combination of POS models.

The definition of POSs can be performed in two steps:

- definition of pre-POS
- grouping of pre-POSs into POSs for further sequence analysis.

3.3.3.1. Definition of pre-POSs

A pre-POS is defined as a plant configuration where all parameters of interest could be considered stable for the duration of the POS. Such a condition is a prerequisite for the development of accident sequences. Within a POS, the PSA model may consider a stable plant situation where changes (unavailability due to maintenance, failures etc.) are modelled probabilistically.

A pre-POS is characterized by some or all of the following:

- reactor criticality (and/or shutdown margin)
- decay heat level
- reactor coolant system temperature and pressure
- primary system water level
- open or closed RCS
- status of RCS loops
- location of the fuel
- availability of safety and support systems
- system alignments
- status of the containment.

Typically, the pre-POSs should be uniquely defined by consideration of all of these characteristics, even if this initially leads to definition of a large number of pre-POS. As a general guidance, the change in boundary conditions defined by a significant change in one or more of the above criteria results in the definition of a new pre-POS.

For a SPSA, the pre-POSs should be defined on the basis of actual operational experience. Depending on the selection of the outage type performed in the previous step, one or more outages should be analysed in detail to determine the actual status of all parameters of interest at all times during the outage. The sources to be used for this purpose include:

- shutdown and startup procedures
- outage plan for a specific outage(s)
- general plant practice for outages
- technical specifications for outages
- configuration control guidelines
- other documents providing information on outages (logbooks i.e. for boron concentration)
- maintenance records (for duration of maintenance on specific components)
- interviews with operators and shift supervisors
- interviews with outage planners.

From those sources, all the information relevant for characterizing the POSs should be extracted and documented. After this has been completed, pre-POSs can be defined in terms of their specific characteristics, time duration and chronological order during an outage.

The decomposition into pre-POSs will likely be much more detailed than the plant operating modes defined in the technical specifications. In addition, the availability of non-safety classified systems which do not have a declared safety function in a certain operating mode can be of significance. For example, for a PWR, primary system heat removal using the steam

generators may be possible during certain POSs to perform the residual heat removal function. For a BWR, the fire water system can be used for pool cooling under certain conditions when the RHR is not available.

For plants with sufficient operational experience, the estimation of the duration of each POS can be based on plant experience for the different outage types. For newer plants, estimates may have to be based on expert opinion, and experience from similar plants.

Once the pre-POSs are defined, they can be further characterized by other parameters. For example, the decay heat level can be conservatively defined as the level associated with the earliest entry into the pre-POS. Over long time intervals this might be unrealistic, in which case the POS should be subdivided into a number of time intervals to better represent the varying decay heat level. The timing of the POS is also important, especially for the accident sequence quantification (Section 7). Unavailabilities due to maintenance are also important parameters to consider for the POSs.

It is advisable to list all original pre-POSs in a table which gives an overview of all the POS characteristics considered. This table can be used as a basis to justify the grouping.

3.3.3.2. Grouping of pre-POSs

In order to have a manageable number of states to analyse, pre-POSs are grouped into POSs, based on qualitative analysis. As the analysis progresses it may be necessary to reconsider the grouping. The grouping process should be clearly documented and justified.

The general guidance for grouping is that all pre-POSs which will be combined into one group shall have a similar plant response to initiators. More specifically, the pre-POSs may be grouped into POSs on the basis of:

- similarity of plant parameters
- similarity of available systems and components in a pre-POS (e.g. plant configuration for RHR)
- similarity of initiating events in the pre-POS.

The process of grouping is an iterative process. Initial grouping should be performed after the pre-POSs are defined. This initial grouping may be performed on the basis of success criteria used in the full power PSA, where appropriate, or of simplified calculations and engineering judgement. The refinement of the grouping will be performed, through interaction with event sequence modelling (Task 18) when thermal-hydraulic (Task 16) and function/system relationship and dependencies (Task 15) results become available.

Task 11 will produce a list of POSs with their basic characteristics and duration and a report documenting the grouping process, including the assumptions introduced during the analysis. The report should contain a table where the original pre-POSs are listed together with the POSs into which they have been grouped. In addition, all the information on success criteria, initiating events and other bases for the grouping should be fully documented in the report.

In most cases, plant conditions such as: pressure, temperature, system availabilities, decay heat level, etc., change within a POS with time. Proper representation of the risk must account in some way for this time dependency. However, in practice it may not always be possible to define realistically a unique plant condition for each POS. In some cases it may be worthwhile to subdivide the POSs into a number of time windows and to determine an appropriate decay heat level for each time window. In other cases, it may be sufficient to make conservative assumptions such as assuming that the decay heat level at the entry into a POS is constant for the whole duration of the POS.

Another way of accounting for the changes within a POS is to determine the fraction of time during which the plant is in a particular configuration given that it is in a particular POS. If the analyst decides to model changing plant configurations within a POS using the fraction of time the plant is in that configuration to quantify the frequency, care is then needed in the interpretation of the results. Using time fractions in this manner may tend to reduce the resolution of the SPSA model, making the analysis less useful for predicting the change in risk with time. The analysis may also be less useful as an aid to planning outages. Assumptions regarding use of time fractions should be explicitly stated and the limitations this places on the application of the SPSA clearly identified.

As an example, the steam generators of a PWR may be isolated from the reactor coolant system by use of loop isolation valves or nozzle dams. Such configurations may or may not be used in the initial definition of POSs. In this example, isolation of the SGs is assumed to "fail" the SGs, and this must be accounted for in the quantification of the system models for this POS. Because of the short duration of this configuration, however, the analyst may decide not to introduce an additional POS to represent it. In such a case, the fraction of time that the SGs are isolated in a POS must be estimated. If time fractions of this type are used in the model, care must be taken to ensure that they are either independent of each other or, if they are not, the correlation between the time fractions introduced into the model should be assessed.

Examples of POSs from a number of LWR SPSA studies are given in Annex I.

3.4. TASK 12: DEFINITION OF CORE DAMAGE STATES OR OTHER CONSEQUENCES

Typically, a wider variety of scenarios with different consequences is considered in a SPSA compared to a PSA for full power operation. Scenarios which have been considered in SPSAs are:

- core damage (fuel in-core or ex-core in the spent fuel pool)
- partial core damage
- physical (mostly mechanical) fuel damage (e.g. from heavy load drops or fuel handling accidents)
- boiling (i.e. risk of a higher radiation level on refuelling floor)
- ex-core criticality events and related damage
- radioactive releases without core or fuel damage, e.g. tritium release for reactors moderated with heavy water.

3.5. TASK 13: IDENTIFICATION, SELECTION AND GROUPING OF INITIATING EVENTS

3.5.1. Identification of initiating events

An initiating event is an event which leads to termination of normal plant operation, requiring protective action to prevent or limit undesired consequences. For an SPSA, a systematic process to identify a complete set of initiating events for all of the POSs should be carried out. The general principles of initiating event identification described in the IAEA Level 1 PSA procedures [1] are also useful for an SPSA. This section emphasizes SPSA specific aspects of initiating event identification.

For shutdown conditions a number of initiating events are unique and different from the PSA for full power operation, for example, heavy load drops. The major categories of initiating events which are of interest for an SPSA are events which threaten critical safety functions:

a) Events which threaten normal heat removal

- intrinsic failures affecting the operational heat removal path
- failures in support systems affecting the operational heat removal path.

b) Events causing a loss of primary circuit inventory

- pipe break LOCAs
- other failures affecting the primary circuit boundary
- LOCAs (draindown events) caused by maintenance errors.

c) Events threatening primary circuit integrity

- inadvertent actuation of high pressure safety injection during cold states.

d) Events affecting reactivity control

- decrease of primary circuit boron concentration
- ingression of unborated condensate (slugs) into primary circuit (core)
- control rod ejection/withdrawal.

This publication recommends the use of systematic identification techniques, together with the above generic list, as a first step in the identification of the initiating events which are of interest for the SPSA study. The following identification techniques are of interest:

- systematic analytical methods, such as master logic diagrams, failure modes and effects analysis, and fault trees
- systematic examination of plant procedures for changing RCS configurations, equipment testing and maintenance procedures. Identification of potential human errors during the execution of such normal plant procedures is one of the key objectives of this process.

Systematic analytical identification techniques as listed above have been used in a number of studies. A systematic investigation of maintenance tasks or operating procedures also

immediately identifies improvements that can reduce initiating event frequencies. These methods can produce highly plant specific initiators but require an elevated effort, both from the SPSA team and from knowledgeable plant staff.

Human activity related initiating events have been seen to be important in many contemporary SPSAs. For example, in the case of a PWR, draining the vessel to mid-loop conditions is a very sensitive operation. If the operator does not carefully monitor reactor vessel water level or misinterprets the procedure, excessive draining can occur, leading to RHR pump cavitation. Likewise, valves may be mis-positioned during maintenance so that a drain path is established from the vessel, through the RHR lines to the sump. These types of events may be grouped with other events (such as "loss of DHR" (Decay Heat Removal) or "large LOCA"), or they could be considered as distinct initiating events to be evaluated with separate event trees. For a BWR, examples of conditions sensitive to human error are the filling of the reactor vessel and the maintenance of main circulation pumps or control rod drives located underneath the reactor vessel.

It is useful to verify or complement the list via talk-throughs and walk-throughs including interviews with plant and design staff.

To ensure completeness of the SPSA initiating event list, it is recommended that initiating events be reviewed from the following sources of information:

- initiating events from the PSA for full power conditions
- other SPSAs
- plant operating history
- experience at similar plants
- generic data from low power and shutdown operation
- other SPSA related material. There are a number of descriptive compilations of events that have occurred during outages. Some of the publicly available sources are listed below:
  a) generic studies (e.g. inadvertent boron dilution events)
  b) licensee event reports (LERs)
  c) event reports from international organizations and plant owner groups.

Usually, each individual plant has developed its own outage practices. Thus, for operating plants, Plant specific initiator data collection is obviously a valuable source of information. The official event reporting schemes can also be used as a first reference. However, it is not always clear whether during the shutdown period all initiating events (or safety related system unavailabilities) have been reported through the official reporting schemes. Consequently, the plant operating history review has to be completed by the collection of other shutdown related experience.

Some initiating events may be physically or functionally precluded by the nature of the definition of the plant operating state. For example, when a PWR is using RHR for heat removal, the "loss of feedwater" initiator, which is applicable during power operation, is not an appropriate initiating event.

3.5.2. Initiating event grouping

A number of initiating event groups are defined for the initiating events identified in the preceding task. An initiating event group should include initiating events which can be analysed using the same event tree and fault tree model; in other words the same accident sequences are applicable for all initiating events in the group. The basic principles for grouping of initiating events are described in [1].

In general terms, the following criteria form the basis for grouping initiating events:

- all initiating events in the group have a similar effect on safety and support system availability and operation
- all initiating events in the group have similar success criteria for safety and support systems
- all initiating events in the group place similar requirements on the operator
- the expected response of the operators is similar for all initiating events in the group
- the assignment of plant damage states to sequence end-points is the same for all initiating events in the group.

In some cases, initiating event groups may include events which do not completely satisfy the above conditions. In such cases, the group characteristics should be defined based on the most restrictive events within the group.

Some examples of initiating event groups which have been defined in previous SPSAs are:

- Loss of RHR. This covers intrinsic failures in the RHR system which do not affect other systems.
- Loss of support systems. Usually, a separate group is defined for each support system since these may have a different effect on frontline system reliability. However, in some cases, conservative groupings of these events may be useful to reduce the magnitude of the analysis.
- Pipe break LOCAs. Since success criteria may change during the outage as decay heat and initial temperature and pressure are reduced, it may be possible to justify some simplification of the grouping. As an example, at some stage after shutdown the system requirements for large and medium LOCA may be similar, meaning that a single group could be defined for these initiators.
- Maintenance induced LOCAs. Events occurring during testing and maintenance activities being carried on during the outage. These events may result in a loss of primary coolant from the RCS either to the containment or into interfacing systems. It may be worthwhile to separate these maintenance-induced LOCAs from pipe-break LOCAs for the purposes of modelling because of the different recovery possibilities (i.e., isolation of the leakage path).
- Loss of external AC power. These events may be caused by the loss of the connection to the external grid or due to plant internal faults. Faults such as short circuits caused by human error may be important contributors to the loss of AC power frequency.
- Events challenging the primary circuit integrity. For example, cold overpressurization and secondary side events leading to thermal transients.
- Reactivity events. For example, boron dilutions, return-to-criticality events, and local criticality events, e.g. refuelling errors or errors in fuel handling.

- Area events. Internal fire and internal flood initiators are discussed in Sections 6.1 and 6.2 below, respectively.
- External hazards. High winds, earthquakes, events leading to losses of service water intakes, aircraft crashes would usually be assigned initiating event groups in a similar way as in the full power PSA. These are discussed in Section 6.3.
- Heavy load drop accidents and other events which could lead to radioactive material releases are discussed in Section 6.4.

Once the initiating event groups have been established, it is useful to construct a table which summarizes the applicability of the initiating events to the POSs defined for the study. The applicability of the initiating events is based on the applicability of the events which comprise the group. An example applicability table is shown below:

Initiating event	POS 1	POS 2	POS 3	POS 4	POS 5	POS 6	POS 7	POS 8
Loss of RHR		X	X	X		X	X	
Medium LOCA	X	X	X				X	X
Cold overpressurization			X				X	

3.6. TASK 14: DETERMINATION OF SAFETY FUNCTIONS

As a part of the process of identifying initiating events, and for the process of grouping the initiating events and plant operational states, it is necessary to define the safety functions required to prevent damage to the protective barriers (fuel cladding for example) and mitigate the consequential radioactive release.

For a LWR, the critical safety functions are typically the following:

- core cooling
- coolant inventory control
- reactivity control
- heat sink availability
- coolant system integrity
- fuel pool cooling.

An initiating event is an event which challenges one or more of the above safety functions, either directly or indirectly, and which as a result requires protective action, automatic or manual, to prevent damage to the protective barriers.

To prevent or minimize releases of radioactive material from the containment the following safety functions may be added to the above list:

- containment isolation
- containment integrity
- containment heat removal
- containment fission product removal.

For cases where the containment is open, the capability to close it within the time requirements imposed by accident scenarios may be a critical safety function.

3.7. TASK 15: ASSESSMENT OF FUNCTION/SYSTEM RELATIONSHIP, DETERMINATION OF SYSTEM/PLANT STATE DEPENDENCIES

One of the characteristics for defining POSs is front line system availability. As a basis for the accident sequence modelling task, it can be very useful to develop a table showing front line system availability for each POS. As for a full power PSA, it is necessary to identify the dependence of all front line safety systems included in the SPSA on the various support systems.

The dependency matrix that was produced for the power PSA can be used as an initial basis. This must be supplemented by adding typical shutdown front line systems, like RHR cooling. This matrix must be checked to assure that it is applicable for all defined POSs. If not, then separate dependency matrices must be produced.

The tables described above can be used for checking system availabilities, for grouping initiating events and plant operation states and for supporting the event tree modelling.

Special support system line-ups that are established during certain POSs to satisfy the single failure criterion while doing maintenance on these systems should be included in these dependency matrices. Other dependencies might be generated between maintenance tasks and it is recommended that the analysis team attempt to identify all such dependencies.

3.8. TASK 16: ASSESSMENT OF PLANT SYSTEM REQUIREMENTS

Although the decay heat levels during shutdown operations are generally much lower than immediately following shutdown from full power, the characteristics of the possible plant configurations may be much less forgiving. Due to disabling of automatic actuation of safety systems, the availability of safety equipment may be reduced and the dependence on operator action increased. Furthermore, the integrity of the primary cooling system and of the containment may be compromised.

The performance of a front line system depends in general on the initiating event, POS characteristics and decay heat level. Functional performance criteria are needed to define the success criteria for the various systems, which may differ from the success criteria for a full power PSA.

The basic approach utilized in shutdown or low power PSAs performed to date is to employ the fault tree models constructed for the full power PSA. With appropriate revisions, these models are generally suitable for shutdown conditions as well. Although the conditional availabilities of components or systems may be different, the logic and response of the system remains basically the same.

It is recommended that thermal-hydraulic calculations be performed to determine realistic success criteria to assure that core cooling assumptions are correct. These calculations may range from simple hand calculations to detailed analyses with integrated thermal-hydraulic models. The level of detail of the thermal-hydraulic analyses will be determined by the requirements of the systems analyses and the primary system configuration. For transitional operating modes (during shutdown and startup) and under hot shutdown conditions the primary system

configuration and conditions are similar to those for transients initiated from full power and models designed for full power accident thermal-hydraulic analyses will be applicable (e.g. RELAP, TRAC, MAAP, MELCOR). For POS involving an open primary system (i.e. reactor vessel head removed) simple hand calculations may be sufficient. For other POS a comparison of the primary system characteristics and the model capabilities will be needed to assess the applicability of a particular code.

For LWRs the thermal-hydraulic success criteria analyses should take into account the following factors:

- primary circuit pressure boundary status
- vessel head removed or de-tensioned head
- safety valve removed/primary system vent open
- loops isolated/ nozzle dams installed
- steam generator secondary side water level
- primary circuit parameters (temperature, pressure, presence of non-condensable gas, shutdown margin)
- water level in primary system
- decay heat level
- containment isolation status.

3.9. TASKS 17 and 24: INITIATING EVENT FREQUENCY QUANTIFICATION

As for full power, quantification of initiating event frequencies follows standard PSA practices [1]. It is important, however, that the quantification of initiating event frequencies for shutdown and low power conditions account for plant specific items such as equipment configuration, availability, technical specifications, and outage management, including refuelling operations. Initiating event frequencies also need to be POS specific, as discussed below.

In a shutdown PSA, initiating event frequencies are usually calculated on a "per calendar year" basis. In other words, the initiating event frequency assigned to a particular POS takes into account both the expected hourly rate of occurrence of the initiator while in a particular POS and the duration of the POS.

When initiating event frequencies are calculated on a "per calendar year" basis, the core damage frequencies calculated for different POS are additive: the total core damage frequency is the sum of the core damage frequencies of the relevant POS.

Three different conceptual models can be applied for the IE frequency calculation in an SPSA, in order to generate "per calendar year" frequencies:

(1) $f_{annual} = f_{hourly} \times t_{POS}$

(2) $f_{annual} = f\_precursor_{hourly} \times P(IE \mid precursor) \times t_{POS}$

(3) $f_{annual} = n\_precursor_{POS} \times f\_POS_{yearly} \times P(IE \mid precursor)$

where:

f_{annual} = "per calendar year" frequency of occurrence of initiator in POS (/year)

f_{hourly} = hourly rate of occurrence of initiator in a particular POS (/hour)

t_{POS} = duration of POS (hours in POS/year)

$f\_precursor_{hourly}$ = rate of occurrence of a precursor event per hour in the POS (/hour)

$P(IE \mid precursor)$ = probability of an initiating event given occurrence of the precursor

$n\_precursor_{POS}$ = expected number of occurrences of a precursor in POS (/entry in POS)

f_POS_{yearly} = expected number of entries into POS (/year).

Model (1) is suitable for initiating events which may occur randomly at any time in a POS. In this case, the initiating event frequency is proportional to the time spent in the POS. This model is useful when initiating event frequencies are estimated directly from operational experience.

In model (2), the initiating event frequency is also dependent on the POS duration. This model is suitable when data is available on the occurrence of precursors, but not on the occurrence of the initiating event itself. A typical situation where this model might be used is for an initiating event which might arise from human error in some manipulation or manoeuvre which is performed with a certain frequency in a particular POS. In this case the conditional probability, *P(IE/precursor),* is the probability of the human error which would lead to the initiating event.

Model (3) is relevant for situations in which the initiating event frequency is not dependent on the duration of the POS. In this case, initiating events arise due to errors or failures following an event which occurs a fixed number of times in the POS. For example, to model the frequency of an overdraining initiating event, $n\_precursor_{POS}$ would be the number of times a draining operation is performed in a particular POS (e.g. once) and *P(IE/precursor)* would be the probability of an overdraining per draining operation. It is important for the analyst to appreciate that situations of this type lead to initiating event frequencies which are not proportional to POS durations and model these accordingly. Recognition of this type of situation is important because the risk from some initiating events can be reduced by shortening the duration of critical POS, whereas the risk from others (e.g. overdraining) cannot.

There are basically three approaches to quantifying initiating event frequencies in a given POS. They are:

- direct estimation from operational experience (the plant being analysed, other plants of similar design, or generic reactor type)
- estimation from power PSA frequencies with supplementary analysis
- use of a logical model including all the foreseen inputs leading to the initiating event

These three approaches are discussed in more detail below.

3.9.1. Quantification based on direct estimation from operational experience

Estimation based on operational experience is performed in a similar manner to direct estimation for a full power PSA. However, there are some pitfalls and drawbacks which the analyst should bear in mind:

(1) The specific POS where an operational event actually took place is seldom easily extractable from the event reports. Hence, for the purpose of estimating initiating event

frequencies, such events are usually distributed between POS in which they are physically/functionally possible.

(2) Direct estimation is most appropriate if there is a reasonable amount of relevant experience. If the number of reported initiating events is 0, initiating event frequency estimation may be performed using a procedure such as that described in [1]. In this case, however, it is important to verify (through interviews with plant staff) that the plant history does not contain any relevant unreported events. In the case of zero observed events, it may be worthwhile considering the use of the modelling approach described below.

(3) Quantification by direct estimation from operational experience does not, normally, provide a thorough understanding of all the mechanisms which could lead to an initiator. The identification of initiating events by using systematic modelling techniques may reveal additional mechanisms.

3.9.2. Estimation based on full power PSA frequencies with supplemental analysis

This approach to frequency estimation is considered to be useful in the following cases:

- data in the full power PSA was taken from generic sources or was based on models
- plant specific data was used in the estimation of full power initiating event frequencies, but there are difficulties in obtaining or processing data for shutdown POS for these initiators (i.e. due to less restrictive reporting requirements, insufficient operational experience in shutdown).

An analyst may feel tempted to scale the full power PSA IE frequencies to match the shutdown conditions solely by using the relative duration of a POS when compared to the power operation annual duration. However, the hourly rate of occurrence of an initiating event is sometimes highly POS dependent and so it may not be possible to deduce frequencies by scaling the full power PSA IE frequencies by the relative duration of the POS. The analyst should be careful to properly justify the assumption of a constant hourly rate for frequencies which are calculated in this way. Common situations in which the assumption of a constant hourly rate of occurrence of an initiator may break down are:

- differences in physical conditions, which may affect, for example, pipe break LOCAs due to lower pressures and temperatures inside a pipe
- changing operational and maintenance activities between the POSs, which may affect, for example, the frequency of LOCAs due to maintenance errors, or increase the probability of support system failures
- changing operational mode or alignment of a system
- initiating events which are associated with a specific event, such as a test. For example, in a PWR, overdraining of the primary circuit can occur due to human errors when reducing the level prior to periods of operation at mid-loop. Another less obvious example would be the possibility of loss of a particular support system due to an error during a test which is performed in a particular POS
- an additional consideration in an SPSA is whether there are events which have been screened out from the power PSA initiating event list because they are only relevant to the shutdown operating mode.

3.9.3. Estimation using systematic modelling techniques

Modelling techniques, such as fault tree decomposition, are generally of most use for infrequent initiating events whose frequency cannot be obtained from operational experience. If modelling techniques are used for events for which the frequency can be estimated from operational experience, the results obtained from the model should be cross-checked with those that would be obtained from operational experience. Differences may be seen for valid reasons; for example, some operational experience events may be less likely to re-occur because of changed operational practices or the statistical base of operational experience may simply be insufficient for reliable parameter estimation. Nevertheless, if significant unexplained differences are seen between reliable experience based estimations and modelled frequencies, experience based estimations are likely to be preferred.

The modelling approach usually involves the explicit or implicit use of fault tree techniques. As an example, a maintenance-induced LOCA may occur because of the erroneous opening of any of several different pathways. These different pathways may have been identified within the initiating event identification task. For each of the different pathways identified, a quantification would be performed based on the frequency of manipulation of the pathway and the conditional probability of errors in these manipulations leading to a LOCA event. Note that this particular example of frequency quantification corresponds to model (2) presented earlier: the frequency of manipulation of the potential LOCA pathway would be expressed as an hourly rate and would be subsequently multiplied by the POS duration to give an initiating event frequency "per calendar year".

Human action quantification in relation to initiating event frequency estimations is typically based on data from approaches such as THERP [10]. For the types of manipulative errors usually involved in initiating events, the human reliability data from such sources is generally considered to be reasonable.

3.10. SCREENING OF POS/INITIATING EVENT COMBINATIONS

The number of POS/initiating event combinations identified by the above guidelines may be considerable. While it is important for the list to be as complete as possible, it may render the final analysis unmanageable in view of the large number of event sequences to be considered. An analysis may be therefore be performed to:

- group the initiating events to reduce the number of different cases to be studied to a more practical level. This process is called grouping of POSs and initiating events;
- identify initiating events/POSs which will have a negligible contribution to the risk of the plant and can be screened out.

One approach for this investigation involves preliminary event tree development and event sequence evaluation which is then used to perform a preliminary prioritization of event sequences. These analyses can provide guidance for the thermal-hydraulic analyses needed for further work. The screening assessment itself can be based on conservative assumptions regarding success criteria. The preliminary event trees can later be used as a starting point for event sequence modelling (Task 18).

After the screening has been performed it is useful to update the table of initiating event/POS applicability to indicate the combinations which have been screened out. An illustrative example is shown below:

Initiating event	POS 1	POS 2	POS 3	POS 4	POS 5	POS 6	POS 7	POS 8
Loss of RHR		X	X	X		X	S	
Medium LOCA	X	X	S				S	S
Cold overpressurization			X				X	

S = Eliminated in screening analysis.
X = Applicable to POS and not eliminated.

3.10.1. Stage 1 screening: initiating events

In most PSAs for full power conditions, initiating events are screened out when their probability per year is lower than a certain threshold value.

The extent to which screening on frequency can be performed may depend on the intended applications of the SPSA. In general, the requirements of an SPSA which is intended for applications such as maintenance scheduling or risk monitoring are rather more strict than the requirements for an SPSA which is intended to provide an overall picture of risk from operation of the plant. The aim of a risk monitor is to provide a continuous picture of the risk from the plant. Thus, high "instantaneous" or "hourly" risk levels are of interest for this sort of application even if their duration, and hence annual risk contribution, is low. A similar situation arises with maintenance scheduling applications, in which it is necessary to compare the risk increment due to a fixed period of unavailability of a system or component, for example, the unavailability of a diesel generator in different plant operational states. Screening of initiating events for short POS where the hourly risk level is not negligible can result in a model that makes this type of application difficult to perform or leads to misleading results.

The definition of screening criteria must consider the intended application of the PSA model. For example:

- If the PSA model is intended only to give an indication of annual risk and the contributors to risk, it is suggested that screening be performed for the lowest frequency initiating events up to a *total* frequency (i.e. sum of the frequency of all screened initiators) not greater than a selected value, for example a value of 5×10^{-7}/year (approximately 5% of a typical shutdown PSA CDF value). A total, summed, frequency criterion is useful because otherwise risk significant initiating events could be screened out simply by reducing their individual frequency by sub-division into a large number of POSs.
- Time to core damage following the initiator may also be considered as a screening criterion. Screening may be considered for initiating events which, with no operator or automatic interventions, would lead to core damage in a time frame greater than 24 hours. However, exceeding 24 hours by itself should not be considered a sufficient basis for screening. Account should also be taken of factors such as high radiation levels (which could rule out or significantly delay recovery), problems in detection of the initiating event (which may delay operator action), and availability of essential equipment and diverse/redundant means to deal with the event (which may be

compromised in shutdown, compared to power operation due to, for example, extensive maintenance activities). The actual time frame above which screening may be performed should be justified, taking into account these points.

- If the PSA model is intended for use in risk monitoring or maintenance scheduling, screening should be performed based on the hourly initiating event frequency, rather than the calendar year frequency. For example, a screening criterion of 10^{-12}/hour (equivalent to approximately 10^{-8}, if the POS duration were 1 year) could be adopted.

3.10.2. Stage 2 screening: preliminary accident sequence quantification

Once it is has been determined which initiating events need to be modelled, preliminary event trees can be developed. For every combination of an initiating event and a POS a separate event tree is required. However, many event trees are likely to be similar, and so at this stage it is useful to define groups of POS/initiating event combinations which can be analysed using the same event tree models. In many cases, it may be necessary to customize the underlying fault tree models using house events (see system modelling description, Section 4.2) to accurately represent the different POS characteristics. However, at this stage of screening, it may be possible to reduce the need for this customization by adopting some conservative simplifying assumptions. Below are several examples of screening assumptions:

(a) For the purpose of screening, event trees may be constructed which only take credit for a sub-set of the functions available for response to the initiator. A screening event tree for loss of a support system in a POS where RHR is used for heat removal (in a PWR) might initially only claim restoration of the RHR function (for example, by aligning the stand-by train). The fault tree model for restoration of RHR might use conservative assumptions about sequence timing and maintenance so that it can be applied to different POSs for the purposes of screening. If the failure to restore RHR sequence frequency was less than the screening criterion for some POSs, this initiating event can be eliminated from further consideration for those POSs. If a detailed analysis was found to be necessary for this initiator, it would take account of additional mitigation strategies such as, for example, use of safety injection.

(b) Screening loss of support system initiators during a POS with heat removal using auxiliary feedwater. A screening event tree for these events might only claim feed and bleed as a viable strategy. It should be relatively simple to modify the relevant fault trees for feed and bleed from the full power PSA for this purpose.

The following table is provided to illustrate how different POS/initiating event combinations might use the same event tree model. It is anticipated that, following completion of this screening step, this grouping may be further developed when the final accident sequence models are constructed.

Initiating event	POS 1	POS 2	POS 3	POS 4	POS 5	POS 6	POS 7	POS 8
Loss of RHR		RHR ET1		RHR ET2		RHR ET1	S	
Medium LOCA	ML ET1		S				S	S
Large LOCA	LL ET1	ML ET1						
Cold overpressurization			CO ET1				CO ET1	

ML ET1 = Event tree 1 for medium LOCA.
LL ET1 = Event tree 1 for large LOCA.
RHR ET1, 2 = Event tree 1, 2 for loss of RHR.
CO ET1 = Event tree 1 for cold overpressure.

The following information can be used for the preliminary event tree development:

- safety analysis report and design basis analyses
- PSA for full power operation
- low power and shutdown operating and maintenance procedures
- interviews with plant personnel.

At this stage, conservative assumptions regarding the plant response are generally adopted. For most NPPs redundancy and diversity in safety features is limited during low power and shutdown periods. It is therefore recommended to consider special uses or realignments of systems or components that could mitigate the sequence. In a PWR, for example, the chemical and volume control system (CVCS) can be used under certain conditions when the RHR systems fails.

Following quantification of the preliminary event tree models, screening criteria would be applied to the initiating events which had been analysed. For example, initiating events contributing 95% of the calculated CDF can be selected for detailed analysis.

In addition to performing a screening function, this preliminary evaluation provides the basis for further modelling decisions, by providing insights in the following areas:

- the analyses required for refining success criteria and to increase the understanding of the plant response
- the need to include more headings in the event trees, e.g. further human actions
- systems models that need to be developed in greater detail
- the identification of the most important human interactions.

4. ACCIDENT SEQUENCE MODELLING

Accident sequence modelling would be performed for the initiating events which survived the screening analysis described in the previous section. As for a PSA for full power conditions, accident sequence modelling typically involves the following steps:

- event sequence analysis and modelling
- determination of success criteria for the various systems (using transient thermal-hydraulic analysis where necessary)
- system modelling
- human performance analysis
- dependence analysis
- use of the transient/severe accident analysis results to redefine the event sequences and system models
- classification and grouping of accident sequences into plant damage states.

In the SPSA Level 2 analysis, further event tree modelling of containment isolation and other containment safeguard systems may be required. This is particularly important for shutdown analyses as the availability of these systems is not necessarily assured in all stages of an outage. The Level 2 analysis (if required) proceeds as for a PSA for full power conditions, see Ref. [2]. The plant damage states of the Level 1 analysis serve as the entry points for the Level 2 analysis which in turn lead to the definition of release categories which are the end-points of the Level 2 analysis.

If the analysis is restricted to Level 1, it may still be useful to define plant damage states (Section 4.6) for grouping the accident sequences. Greater importance would then be associated with accident sequences involving failures of containment isolation and containment safeguard systems. It is recommended that an SPSA should always include, as a minimum, information on the status of containment integrity for each POS.

Six tasks (18 to 23) can be distinguished for this procedural step. These are discussed in the sections below.

4.1. TASK 18: EVENT SEQUENCE MODELLING

Event trees are widely used to model the response of the plant and plant operators to initiating events. Other methods, such as Markovian methods and graphs may also be used [1]. It is considered as a good practice to draw detailed event sequence diagrams (ESDs) including human interactions before modelling event sequences. Event sequence modelling should be done by a multidisciplinary team including specialists for human reliability analysis (HRA) from the beginning.

The plant conditions for low power operation and certain shutdown states may be similar to full power operation in terms of system availability and plant response. In this case, the plant response to initiating events is similar, and the event trees developed for full power operation can be modified for low power and specific shutdown states.

The modifications typically involve removal of selected event headings, such as those related to reactor trip if the reactor is already shut down, relaxation of success criteria by modifying the functional requirements (for example, the number of pumps required) and

reviewing the accident sequences for consistency with the specific POS characteristics such as, which systems/trains are available, what signals are generated, what are the available indications to the operator, etc. Event tree headings may also be added to account for operator interactions which are not relevant for the full power PSA.

For shutdown conditions in which the RHR system is in operation, plant and operator response to accidents may not have been analysed in a very detailed manner (or at all) in the full power PSA. Procedures written specifically for shutdown conditions may also be limited. Development of the plant response and identification of methods to prevent or mitigate the accidents are therefore important tasks for the SPSA analysts. A substantial effort from the human reliability analysts is required when the procedures are limited.

Section 3.10 describes a phase of screening, grouping and prioritization of initiating events and POSs in order to obtain a manageable PSA model. The procedure most often used to perform these tasks involves preliminary accident sequence modelling. Therefore, in practice, performing a SPSA is an iterative process.

If the SPSA includes containment response and source term analysis, it is recommended that the Level 1 event trees include headings to assess the performance of containment safeguards systems, and each sequence should be assigned to an appropriate plant damage state (PDS), as set out in the Level 2 PSA procedures [2].

4.2. TASK 19: SYSTEM MODELLING

As for a PSA for full power conditions, the objective of this task is to model in detail the system failures which contribute to the event tree sequences. Fault tree analysis is the most widely used method for system modelling. The basic approach utilized in SPSAs performed to date is to utilize and adapt the fault tree models constructed for the full power condition as far as possible and useful. However, revisions to the existing models may be necessary, or new models may need to be developed, in particular in the following cases:

- existing system models are not suitable for describing the system behavior in different POSs
- a particular system, which was in stand-by during full power operation, is operating during shutdown
- actuation of a system is manual during shutdown in contrast to full power operation where it was automatic
- required mission time may be significantly different
- success criteria changes in different POSs
- number of trains initially available is different in each POS
- time windows and conditions are significantly different, which could make success of recovery actions less probable
- system was not modelled as it was not needed for the full power condition
- system was not modelled as it is only needed for the Level 2 analysis.

Particular systems may require specific modelling for low power and shutdown conditions. For example, fuel pool cooling systems might not be included in the full power analysis, but

could be important during shutdown conditions. Certain modes of RHR system operation may also be used only during outages and should therefore be considered. The system models have to reflect the operating policy and specific system alignments. Success criteria, e.g. k out of n trains of a particular system required, may be less stringent for shutdown or low power conditions because of the lower decay heat level. Detailed thermal-hydraulic calculations should be performed to determine these criteria.

The automatic start features of a system may be bypassed during shutdown or low power conditions in order to prevent an inadvertent start. For example, safety injection systems may be blocked with regard to automatic start mode to prevent actuation during shutdown. Thus, the control logic in the fault trees for these systems must be changed to reflect the fact that the systems have to be manually initiated if required. Models for the related human interactions should also be developed.

Manual recovery actions credited in the full power analysis may not be possible during the outage due to ongoing activities as part of the outage. For example, cross-connecting low pressure systems may be an appropriate action during full power operation. However, during an outage, the cross connection may be locked closed, or a system train may be entirely disabled. Therefore, if actions of this type are included in the fault trees for full power operation, they should be modified for the low power and shutdown evaluation.

In summary, each fault tree from the full power PSA adapted to the SPSA should be reviewed for each POS to determine whether there are any features of that POS which might impact on the logic of the fault tree structure.

The changing availability of the different systems during the outage complicates the system-modelling task. Some systems or portions of system may not be available during certain POSs. Also the probability of failure of a basic event may change. Most PSA software packages are based on a fast cut set algorithm which generates and stores minimal cut set (MCS) equations. An MCS analysis can be carried out on several levels: any fault tree gate, any individual event tree sequence, or any consequence (every event tree sequence can be assigned one or more consequences, e.g. a plant damage state). An analysis case can specify a "Boundary Condition Set" which includes a list of value specifications/changes to apply to the model. The "Boundary Condition Set" can include house event True/False settings, setting of probabilities for basic events and gates, setting of True/False states for basic events and gates and setting of values for parameters. This is very useful for running analyses of the same base model with different variations depending on the POSs. Of course it is also possible to perform this without house events, but then for every "Boundary Condition Set" different individual fault tree models are added to the complete SPSA model, which complicates the modelling and review effort if some changes have to be made because of the number of different fault tree models to be looked at.

4.3. TASKS 20 and 26: HUMAN PERFORMANCE ANALYSIS

The analysis of human interactions during shutdown is complex. Therefore, it is very important that the HRA is performed in a structured and logical manner and that the HRA specialists are integrated in the accident sequence development and modelling process from the beginning. As with other analysis tasks, the HRA process should be thoroughly documented in a traceable way. Regardless of the particular HRA models chosen, the HRA

should aim to generate failure probabilities which are both consistent with one another and consistent with the analysis carried out in other portions of the PSA.

As stated before, required manual system activation, co-ordination and recovery activities are important in SPSA and their role might differ significantly from the one in the PSA for full power conditions. There are many other aspects of shutdown operation, which, in addition, affect the outage safety from the human reliability point of view. Among them is the use of external maintenance staff from outside organizations, frequent overtime work and increased requirements for control room work.

During refuelling or major maintenance outages the amount of maintenance staff at site belonging to external organizations is considerably higher than during normal power operation. This means increased requirements for training. Work supervision can be difficult due to the large number of work activities taking place. This puts pressure on the plant personnel who are responsible for the oversight of these activities.

A widely used practice is to include screening cycles in the HRA process. In this screening, emphasis is first given to the completeness of the identification of human interactions (HIs) and the use of preliminary conservative screening values. Model evaluations are carried out to find out for which of the HIs a more detailed assessment is required and useful. In this way the significant effort to perform a detailed assessment can be limited to the most important HIs.

For an SPSA it is of primary importance to interact with plant operating and maintenance personnel in order to reflect plant design and operational features during low power and shutdown conditions. If this is not possible, e.g. for a plant in the design or construction stage, the analyst should attempt to gain practical experience based knowledge from similar, operating plants.

Three types of human interactions are treated by the HRA task:

- Category A: pre-initiator human interactions that may affect system unavailability
- Category B: human interactions that may cause an initiating event
- Category C: post-initiator human interactions which are performed during the sequences caused by an initiating event.

These three categories of human interactions are discussed in more detail below.

4.3.1. Category A — pre-initiator HIs

These interactions consist of actions associated with testing, maintenance, repair and calibration which may degrade system availability. They may cause the failure of a component or component group or leave equipment in an inoperable condition, e.g. due to misaligned valves. If undetected, the component or component groups are unavailable when required after an initiating event. Particularly important are interactions that have a potential to result in concurrent unavailability of multiple trains or channels of safety systems. Typically these sources of unavailability are included in the system models at the component, train or system level. Although the numerical value of some of these errors may be different from those used in the full power PSA, the basic approach to their quantification is similar.

4.3.2. Category B — Human interactions that may cause an initiating event

These interactions contribute to the frequency of initiating events, as discussed in Section 3.9. The HRA analyst's role is to support the calculation of these frequencies in cases where the human error must be quantified explicitly, rather than being implicitly included in the frequency estimation which has been generated from operational experience.

4.3.3. Category C — Post-initiator HIs

Following an initiator the operator may be called upon to perform actions in order to ensure a successful plant response. These type C human interactions are particularly important during shutdown because of the reduced level of plant automation. They have tended to be dominant contributors to core damage frequency in most SPSA studies performed to date. Thus, a realistic assessment of their failure probability is likely to be important if a realistic CDF estimate is to be made.

There are a number of difficulties in performing a shutdown PSA HRA for type C actions. Existing methods have generally been developed for full power conditions in which the operators are called upon to perform actions which are usually laid down in procedures and frequently well trained, in time frames which are typically less than 60 minutes. Even in the cases where procedural guidance is present for the actions required of an operator following initiating events during shutdown, it is usually less detailed than for the full power situation. Operators usually have less training in response to accidents during shutdown. On the other hand, the time windows for operator response are generally very much longer than for accidents initiated from full power.

The aim of the analysis of type C actions is to take into account these different factors in a systematic manner. Given the scarcity of data relevant to shutdown conditions, most SPSAs have used some adaptation of full power PSA methodologies. Expert opinion often plays an important part in the generation of failure probability values. The present publication does not describe a specific methodology for SPSA HRA, but rather, it describes the areas which should be addressed when selecting a methodology for SPSA HRA or adapting a full power PSA methodology.

The methodology selected should account for the increased difficulties the operators may face because of lack of procedural guidance and training. It should also account for the positive effect of the increased time available for many actions in shutdown. However, it should be noted that care should be taken not to uncritically accept values generated by the use of time reliability correlations designed for power operation, since the time windows in shutdown operation may be well outside the applicable range of these correlations. These correlations may generate very low failure rates when the time available to perform the action is substantial. The methodology should aim to provide error probabilities which are reasonable compared to those used in the full power PSA.

The increased possibility of errors in the diagnosis of initiating events is often raised as a concern in relation to SPSA. An operator could misdiagnose an event and undertake a series of mitigation actions which are appropriate for the diagnosed event but inappropriate for the real event. The analysis of this type of action is not mature and there is no generally agreed quantification method. Nevertheless, some attempt to address these errors would increase the quality of the HRA performed in an SPSA.

References [11] and [12] provide a useful overview of contemporary HRA methods and some discussion of shutdown applications. Reference [11] also provides a discussion of modelling errors of commission.

As in a full power PSA, it is important to consider dependencies between HIs in the same sequence. It has become common practice to assign a high degree of dependence to consecutive HIs, unless there are good reasons to assume low or no dependence. Typically, low or no dependence for consecutive HIs is only credible if the actions are completely separated in time, location and characteristics and are carried out by different staff.

4.4. TASK 21: QUALITATIVE DEPENDENCE ANALYSIS

The objective of this task is to identify dependencies which may influence the logic and quantification of the accident sequence and system models. The main types of dependencies in this regard are functional dependencies on supply and support systems, hardware sharing between systems or process coupling, physical dependence including dependencies caused directly or indirectly by initiating events, human interaction dependencies and common cause failures (CCFs).

The methodology for this task is, in principle, similar to the PSA for full power operation. As a point of departure, the different support system and system interdependencies with regard to full power operation should be reviewed and checked regarding their applicability for the individual POSs. The analysis team should be aware that testing and maintenance activities may create new sources of dependencies. This also includes the timing of particular activities.

Revisions to the dependency models may be necessary, especially if the success criteria change for low power and shutdown operation. Conditions for support and supply systems can change, e.g. requirements for ventilation systems and power supply systems. Systems alignment and components outages should be reviewed as well.

The CCF assessment in SPSA POSs may not be straightforward. The analyst should be aware of the CCF mechanisms and the potential impact of maintenance and other shutdown specific activities on their potential for occurrence.

4.5. TASK 22: IMPACT OF PHYSICAL PROCESSES ON DEVELOPMENT OF LOGIC MODELS

According to [1] this task considers physical processes and phenomena which arise from initiating or consequential events and which lead to alterations in the environments that affect the performance of the required systems.

An example of how physical processes may impact on the development of the logic models in an SPSA would be the effect of primary circuit conditions on the RHR system in a PWR. Procedures may require the operator to isolate the RHR system following symptoms of LOCA, to protect it against damage due to the formation of voids in the primary circuit liquid. Thus, the question may arise in some sequences, where saturated conditions are reached and the RHR is not isolated, as to whether or not its failure or degradation has occurred and whether the probability of subsequent successful functioning should be modified.

4.6. TASK 23: CLASSIFICATION OF ACCIDENT SEQUENCES INTO PLANT DAMAGE STATES

The purpose of grouping the accident sequences into plant damage states is to reduce the number of distinct outcomes of the Level 1 event analysis to a manageable number for further analysis (Level 2 or 3) and for concise presentation of the study results. The expected accident progression (beyond core damage) including challenges to containment integrity and radionuclide transport for all accident sequences that are grouped into a particular plant damage state should be qualitatively similar.

For an SPSA the process of selecting the PDSs is similar to that for a full power PSA. Reference [2] presents guidance on the definition of PDS and the assignment of Level 1 sequences to PDS for full power conditions. However, an SPSA analysis may require additional PDSs compared to a full power PSA. For example, additional PDSs may be required for conditions unique to certain shutdown POSs such as those with the reactor vessel head removed or with the containment equipment hatch open. The following additional Level 1 sequence characteristics have been used in past SPSAs in order to define the PDS:

- POS decay heat level (time since shutdown from full power operations).
- Lack of containment isolation — for POSs where the containment is open, considerations must be given to conditions that determine the time to restore containment isolation and the effectiveness (leak-tightness) of the containment.
- Primary system pressure boundary integrity — vessel head removed, nozzle dams installed, safety valves removed, primary system vent open.
- Primary circuit water inventory — may significantly influence containment conditions including containment pressurization, containment leakage rates and radionuclide transport behaviour in containment.
- If scenarios involving the fuel storage pools and fuel handling accidents are included in the SPSA, it will likely be necessary to define additional PDSs to represent the consequences of these events. In most cases the buildings where the fuel storage pools are located represent some barrier against uncontrolled releases. The conditions that determine the effectiveness of these barriers must be considered in defining the PDSs.

5. DATA ASSESSMENT

As for the PSA for full power operation, this major procedural step is aimed at acquiring and generating all information necessary for the quantification of the model constructed during the previous steps.

The present section discusses development of the following data for the SPSA model:

— component reliability data
— maintenance unavailabilities
— assessment of common cause failures
— other data needs.

Data assessment related to initiating event frequencies and human errors is discussed in Sections 3.9 and 4.3.

5.1. TASK 25a: ASSESSMENT OF COMPONENT RELIABILITY AND MAINTENANCE UNAVAILABILITY

Data for the quantification of shutdown specific component reliability parameters is less widely available than for full power conditions. Thus, a widely used approach has been to adapt data from full power operation and to provide various justifications as regards their applicability. Indeed it is to be noted that the data used in a full power PSA may already include reliability data collected during shutdown operation.

The parameters influencing component unavailability and reliability in standard reliability models are maintenance, test intervals, human actions and the component operating policy (standby, on-line operating). A thorough discussion on reliability models and related parameters for components is given in [1]. In the present publication, only the special aspects for low power states and shutdown conditions are discussed. Regarding reliability parameters there are differences between full power operation and low power and shutdown conditions.

5.1.1. Test unavailability

There are normally a number of tests performed in an outage. A major part of the testing serves to assure the function of the components which were previously in maintenance, i.e. these are functional tests before equipment is put back into operation. Consequently, the model of Reference [1] for test outages is applicable:

$$U = t/T$$

where:

U is the unavailability
t is the average test duration
T is the test interval or, more appropriate for shutdown, the duration of the POS if the component is tested during the POS.

A similar expression can also be used for the maintenance unavailability. Where applicable, an override factor for test or maintenance q_o (q_o is the failure probability to override test or maintenance) can be included:

$$U = [t/T]\, q_o$$

In some cases, the plant technical specifications allow testing of a train or a component although it should be operable in the given POS. This may be based on a test arrangement that does not prevent the function on an overriding signal in the case of a demand or because of the short duration of the test (t). An example is the tightness testing of isolation valves, which is sometimes allowed although the train should be in standby.

5.1.2. Test interval T

Component unavailabilities which are influenced by the test interval may vary between the POSs. For example, a specific outage may be entered when one is at the end of a test interval, meaning that the unavailability could be $?_s$ T (where $?_s$ is the stand-by failure rate) and not $?_s$ T/2 (used for the average unavailability in the usual reliability models applied for full power PSAs).

5.1.3. Mean repair time

This parameter is used in repairable component reliability models.

Mean repair times may be dependent on the POS. This may be due to the accessibility of systems and equipment, availability of repair staff, availability of spare parts, and, in some event sequences, the level of radiation in the target component surroundings. During plant shutdown and startup conditions, the repair times do not normally significantly differ from the full power PSA averages. However, in the outages, the restoration possibilities are almost unlimited if the time allowed for the repair is sufficiently long. There are however, a few exceptions to this general observation.

Consideration of repair can significantly increase safety system availability in SPSA POSs. Neglecting it may, in many cases, lead to an overestimation of risk. Repair may be worth considering in fault or event tree models used to generate the initiating event frequencies if plant experience shows that there are good possibilities for recovery.

5.1.4. Component operating policy

The SPSA analysis team should be aware that many components that are in standby during power operation may be running during an outage. If the shutdown operating policy is to cycle the use of redundant components or trains then an appropriate reliability model should be selected.

5.1.5. Mission time

Mission times are used in models which calculate the probability that operating equipment used to maintain or attain a stable state following an initiator fails to continue to operate. They can have a significant impact on calculated system failure probabilities.

A general mission time of 24 hours has been used extensively in PSAs for full power operations. The background assumptions are that:

- After 24 hours accident progression is slow and there is a high probability that in case of failures, repair is successful or means for replacing the equipment function can be improvised, hence failures of operating equipment after 24 hours are likely to be less important than those before.
- After 24 hours there is a high probability that a sufficient number of systems and staff will be available to maintain stable conditions.

In cases where a system has to operate only for a limited time, shorter mission times can often be justified, e.g. for the high pressure safety injection (HPSI).

5.1.6. Maintenance unavailability

Maintenance of a particular system, or train of a system, may be a characteristic directly associated with some POS. The analysis would assume total unavailability of the relevant trains or safety systems in these POS. In that case, the maintenance unavailability is modelled as a reduced number of available trains and not in the component unavailability model. When calculating maintenance unavailability parameters for use in the fault tree models, it is important that the data analysts understand what maintenance has been modelled in that way,

so that experience data can be interpreted appropriately. Generation of the reliability parameters for use in the model can use the formula for scheduled maintenance from Ref. [1].

5.2. TASK 25b: ASSESSMENT OF COMMON CAUSE FAILURE PROBABILITIES

See Ref. [13] for guidance on common cause failure (CCF). There are certain difficulties in forecasting CCF parameters for an SPSA. This is because no databases exist for component data specifically for shutdown operations. Another factor is that usually a great deal of maintenance takes places in an outage potentially affecting the CCF mechanisms. A common technique is to use the same CCF parameters as for full power operation.

5.3. TASK 25c: OTHER DATA NEEDS

As in a full power PSA, an SPSA model will require data on items such as the probability that external power is not recovered in a particular time frame following a loss of off-site power initiator. An example of an SPSA specific data item which has been used in some studies is the probability of sump clogging.

The quantification of these other data items follows standard procedures and no special techniques are likely to be required specifically for SPSA.

6. INTERNAL AND EXTERNAL HAZARDS, HEAVY LOAD DROPS AND ACCIDENTS INVOLVING OTHER SOURCES OF RADIOACTIVE MATERIALS

6.1. INTERNAL FIRE

For the performance of an internal fire analysis the guidance provided in Ref. [5] should be used. The performance of the internal fire analysis for the shutdown states of a plant requires emphasizing several additional items.

In most instances the shutdown internal fire analysis can be based upon the full power PSA internal fire analysis. At the start of the analysis a table should be constructed which delineates all systems required to maintain the critical safety functions for each POS. The required systems will differ among POSs and from those required in the full power PSA. This task will require the analyst to perform data gathering for additional areas and systems.

Because of the numerous activities under way during an outage, the configuration of the plant changes not only in terms of the available systems, plant parameters, etc., but also with regard to area interfaces. During outages adjacent areas may be open and/or fire barriers may be removed for some time. This will result in additional fire propagation routes compared with the full power PSA. These additional propagation routes should be assessed during walkdowns of the plant during an outage. Because it would not be possible to do a walkdown during every POS of an outage, interviews with the outage management and analysis of the outage schedule and activities to be performed must be used to supplement the walkdown information.

Fire ignition frequencies during plant shutdown differ from those during power operation, due to differences in the extent and types of maintenance and repair activities. The maintenance activities often result in the addition of transient combustibles to areas. Cutting and welding activities contribute to elevated fire ignition frequencies. The USNRC has completed

an extensive study of core damage risk from shutdown states. The PWR analysis is published as NUREG/CR-6144 [9]. In support of this study, Brookhaven National Laboratories developed a complete set of initiating event frequencies for PWRs during shutdown conditions. The frequencies are derived from LERs and other USNRC reports of fires, and represent the frequency of a large fire, which has not been suppressed and which has propagated to the point of component damage. Hence, the conditional probabilities of failure of fire suppression are included in the reported fire initiating event frequencies.

To calculate the fire ignition frequencies, both generic information and plant experience (if available) should be used. Bayesian update techniques can be used to combine generic fire frequency data with plant specific data.

6.2. INTERNAL FLOODING

For the performance of an internal flooding analysis the guidance as provided in [1] should be used. The following discussion highlights those aspects of an internal flooding analysis that are unique to shutdown operations.

The shutdown internal flooding analysis is generally based upon the full power PSA internal flooding analysis. For the shutdown operations flooding analysis a critical safety functions table (showing all systems required to perform the safety function) for each POS should be constructed (similar to the table described for the internal fire analysis in Section 6.1).

Consideration should be given to whether flood protection features are routinely defeated during shutdown (e.g. normally closed doors left open, drains blocked, etc.) since these factors influence the extent of flood propagation. As a result of ongoing maintenance activities, quantities of equipment, insulation and other materials may be located near drains, resulting in a higher potential for blockages than for full power. During an outage, flooding sources can also be different. For example, systems pressurized during power can be depressurized, affecting the potential for leakage and the leakage rates. Flooding sources are different as well because water is used for different purposes and located in different regions (e.g. the refuelling cavity). During shutdown operations there may be an increased potential for flood sources from maintenance activities, temporary systems and hoses, and more widespread propagation due to flood protection features being removed or defeated.

During shutdown POSs there is increased maintenance activity, as well as the potential for use of temporary systems or hoses. The maintenance practice at the plant should be reviewed to identify any opportunities for maintenance induced flooding events. Items to be considered are:

- Are temporary fluid systems installed during shutdown?
- Are precautions taken to prevent:
  - unintended opening of an isolation valve?
  - unintended start of a pump of an isolated train?
  - unintended draining of a system after isolation?

A screening analysis should be performed for each identified maintenance induced flooding event. If a maintenance induced flooding event cannot be screened out, a detailed analysis has to be performed.

6.3. EXTERNAL HAZARDS

The external hazards analysis (earthquakes, floods, high winds, etc.) should be performed using Ref. [4] as a guidance. The following items should be considered during the performance of the external hazards analysis for the shutdown PSA.

As for the internal fire and flooding analysis discussed above, a table showing all systems required to perform the required critical safety function for each POS should be constructed. Guidance for the performance of the seismic PSA analysis is contained in Refs [4] and [14]. This guidance also largely applies to the PSA for shutdown operation.

Structures and components which are only present in certain areas during some POSs, should be identified. For example, some plants have their vessel head parked close to the vessel or spent fuel pool and if it is not fixed in place with seismically qualified restraints, could be set in motion and impact upon critical safety equipment. Additional structures are often erected for maintenance activities which could jeopardize essential equipment if not suitably located or restrained. Identification of these configurations generally requires additional walkdowns of the plant during shutdown.

For many plants the containment (equipment hatch) is open during many stages of shutdown operations. Under these conditions external hazards can add additional risk. Seismic events may preclude the rapid closure of an open equipment hatch. High winds may produce missiles that damage critical equipment within an open containment. Failures of building structures outside the containment may result in a direct pathway to the environment for radionuclide release.

6.4. HEAVY LOAD DROPS

Probabilistic safety assessments normally focus on the failure to cool the core inside the reactor vessel or when stored in the spent fuel pool. But other more direct damage can occur, e.g. by heavy load drops onto the vessel, fuel pool or systems required to perform the critical safety functions.

Potential heavy load (e.g. confinement dome, RPV head, spent fuel cask, concrete shielding blocks) drops should be analysed in areas having the potential to damage systems required to perform the critical safety functions or having the potential to directly result in mechanical damage to fuel assemblies. If the load transport pathway is not above fuel nor above regions containing critical equipment, screening out of particular heavy load drop initiators may be possible. However, screening out of all heavy load drop accident initiators is generally not possible because of the significant damage that can occur. Consequently, probabilistic analyses must be performed. The analysis should consider locations in addition to the reactor refuelling floor where heavy loads are handled. For example, some plants (e.g. WWER-440) have open areas in the turbine hall where decay heat removal systems are located which are vulnerable to heavy load drops.

6.5. ACCIDENTS INVOLVING OTHER SOURCES OF RADIOACTIVE MATERIALS

As for full power PSAs, potential accident sequences involving other in-plant sources of radioactive materials should be considered. Potential sources of radioactive material release include: the spent fuel pool, radioactive waste tanks, processing facilities for radioactive

waste, on-site waste storage facilities including (dry) storage of fuel assemblies, etc. For these sources of radioactive materials, potential events or sequences of events, which could potentially lead to significant radioactive releases should be identified. For these events, a preliminary probabilistic analysis should be performed to quantify the frequency of a radioactive release and the potential magnitude of the radioactive material release estimated. A screening analysis should be performed to screen out events which have a low probability of occurrence (e.g. screening value lower than 10^{-6}/year) or which lead to only small radioactive releases (e.g. screening value lower than the yearly allowed radioactive plant release). After this screening step only the significant events need be analysed in detail.

Drain-down and loss of cooling events should be analysed for the fuel assemblies in the spent fuel pool. Identification of initiating events should be performed, including a review of the operating procedures which could lead to drain down and loss of cooling initiating events. Accident sequences should be developed and quantified which takes into account potential recovery actions taken by the operator.

7. ACCIDENT SEQUENCE QUANTIFICATION, UNCERTAINTY ANALYSIS AND SENSITIVITY STUDIES

7.1. TASKS 27, 28 and 29: ACCIDENT SEQUENCE QUANTIFICATION

In Ref. [1] this step involves Task 27, determination of accident sequence Boolean equations, Task 28, initial quantification of the accident sequences and Task 29, final quantification of the accident sequences.

For SPSA, accident sequence quantification may be performed using the same techniques as for a PSA for full power conditions [1]. It should be noted, however, that in an SPSA, in which long mission times or recovery times are often applicable, use of Markovian techniques instead of standard fault tree/event tree evaluation methods have the potential to yield more realistic results.

Some SPSA models have explicitly included the relative durations of POSs as basic events in the model in order to ease the representation in future applications of modified POS durations. This is a useful technique; however, if it is adopted care should be taken to ensure that initiating event frequencies which are not proportional to POS durations are properly represented (see Section 3.9).

When reviewing the results of the quantification, as in the case of a full power PSA, a careful review of the cut sets obtained should be carried out. In an SPSA, the system models may have been re-used and modified (perhaps using house events) to represent the conditions of the different POSs. Given this situation, it is useful to cross-check the cut sets obtained for similar sequences or systems in different POSs, to ensure that any differences in these reflect different POS or sequence characteristics and do not stem from modelling errors.

7.2. TASK 30: UNCERTAINTY ANALYSIS

For the uncertainty analysis, the same techniques are used as for a PSA for full power conditions, see Ref. [1].

7.3. TASK 31: IMPORTANCE AND SENSITIVITY ANALYSIS

Importance and sensitivity analyses are performed using the same techniques as for a PSA for full power operation.

Sensitivity studies can play a much more significant role in SPSA than in a full power PSA. For example, the specific conditions that were selected to characterize a POS represent a wider range of conditions that can actually occur during the POS. There can be different combinations of systems which are unavailable; some more conservative combinations and some less conservative. The POS can have a longer or shorter duration. Times available for human action can vary considerably depending on the time of the POS relative to plant shutdown. Success criteria can also vary depending on decay heat levels.

It is useful to investigate these variations for cases where the modelled POS assumptions (which are likely conservative) result in a dominant contribution to risk.

8. DOCUMENTATION AND PRESENTATION OF RESULTS

The structure of the SPSA report is similar to that described in the Level 1 and Level 2 procedures for a full power PSA [1, 2]. Chapters for describing those aspects which are particular for SPSA should be added, such as a chapter describing in detail the process of the determination of outage types, plant POSs and initiating events.

The results obtained in each major step of the study, discussed in the preceding sections, are to be integrated and displayed, together with the important engineering insights gained from the analysis. Assessments of the overall results and findings and a discussion of the uncertainty analysis, importance analysis and sensitivity analysis should be presented. Finally, more general conclusions and recommendations should be presented and discussed. The following subjects should be discussed in the documentation:

(a) Core damage frequency — important contributions integrated over all POSs

- Contribution of the dominant sequences
- Contribution of the POSs
- Contribution of initiating event groups
- Results of core damage frequency uncertainty analysis
- Results of core damage frequency importance and sensitivity analyses.

(b) Presentation of results per POS

- Contribution of dominant sequences
- Contribution of initiating event groups.

(c) Presentation of Level 2 interface

- Plant damage state characteristics and frequencies.

(d) Qualitative insights and conclusion

- Interpretation of results and engineering insights
- Conclusions, recommendations.

The presentation of the engineering insights and the recommendations must be readable and understandable for non-PSA specialists.

It is useful to use the SPSA results to construct a risk profile for a typical outage schedule, especially for a refuelling outage. Similarly, a frequently experienced repair outage such as for a steam generator may be presented. In this way the plant personnel can visualize the changes in risk as the outage progresses; they can see the relative order of magnitude of risk in different POSs and they can associate the risk with activities in the outage.

The following detailed information from the study should be included in the report (these detailed results will generally be reported in the appendices to the report):

- listing of cut sets for every event tree sequence
- dominant cut sets contributing to total core damage frequency
- dominant cut sets contributing to core damage frequency per POS.

These lists are easier to read when the basic events descriptions are used instead of the basic event codings. More in depth insights can be gained when the cut set listings per sequence are sorted per event tree heading (function). This way you can see what cut set or combination of cut sets fails a certain function in a sequence.

The following presentations can also be useful:

- contribution to core damage frequency of human factors, dependent failures and independent failures
- impact on core damage frequency of the various event tree headings.

The plant model and data should be sufficiently documented and configured in databases and computer files to enable the results to be reproduced and the models readily useable for applications.

9. APPLICATION OF RESULTS

A list of possible objectives of an SPSA has been provided in Section 2. The SPSA results and models can be used to support the following applications:

- outage planning and maintenance scheduling
- development/modification of operating/accident procedures
- development/modification of technical specifications
- emergency planning
- decisions on hardware modifications
- training of personnel
- management practices.

9.1. OUTAGE PLANNING AND MAINTENANCE SCHEDULING

Typically, during an outage, many activities are taking place in overlapping time intervals, with different levels of availability of safety and support systems during these intervals. An SPSA is the most complete way of integrating this information, for revealing risk significant configurations and practices and for risk insights into other aspects of outage planning and conduct. Unavailabilities of trains of safety and support systems, work performed on the primary and secondary circuit, containment isolation and combinations thereof are among the items that may be analysed effectively using an SPSA to provide feedback to outage management.

To facilitate this task, the risk measures may be plotted against time to compare the risk values and time durations for each POS. The risk quantification should reflect as realistically as practical the conditions prevailing during each POS, particularly as regards component or system availabilities and system configuration characteristics of each POS.

The SPSA methodology should be able to rank component and train importances so as to facilitate decision-making regarding component availability during the outage. In this regard, the "risk achievement worth" importance measure is a useful indicator.

Ideally, the SPSA is used during the preparation of an outage plan in an iterative way. Information from the draft plan is introduced into the SPSA model and quantified. After interpretation of the results, sensitivity studies of alternative outage plans can be performed indicating those plan modifications which will result in a reduction in risk.

In practice, the original outage plan cannot generally be followed completely since schedule changes are often required and performance of emerging (unplanned) activities become necessary. The SPSA can be used to make plant configuration decisions on a continuing basis during an outage.

There might be significant financial or operational benefits to changing outage practices that, on first sight, appear to reduce safety. Such activities might include (1) moving some tests and preventive maintenance from shutdown to full power operations, and (2) performing certain tests simultaneously or sequentially. The SPSA can be used to show the safety significance of such changes to provide guidance for management decisions.

The results of the SPSA can also be used to identify those activities where it may be advisable to develop contingency plans to facilitate recovery beyond those that currently exist.

9.2. OPERATING AND ACCIDENT PROCEDURES

By highlighting important accident initiators or sequences in which human actions play an important role, the SPSA may be used to make recommendations on additions or changes to operating and accident procedures. If this is an objective of the SPSA, special attention needs to be given to reflecting these procedures in the analysis in a realistic manner. The SPSA may indicate that certain recovery actions that have not been set down in procedures significantly reduce the risk. These actions may be recommended for inclusion in the plant accident procedures.

For a PWR, examples of additional procedural actions include: measurement of the water level in the primary circuit by independent means during mid-loop draining, methods for providing additional sources of make-up water, limitations on operations that may impact the primary circuit integrity during mid-loop conditions, and procedural steps to prevent fast or slow boron dilution accidents during shutdown conditions.

9.3. TECHNICAL SPECIFICATIONS

By identifying safety and support system unavailabilities, and combinations thereof, which have a significant risk impact, the SPSA may provide feedback for the development of additional technical specifications for shutdown and low power conditions. For an SPSA, in which there may be overlapping unavailabilities of equipment, it is important to ensure that the analysis reflects such correlations whenever they are present, either by using an outage specific PSA or by modelling such correlations to cover all outages conservatively. The assumption of random unavailability (often used in a full power PSA) may prove to be overly optimistic.

9.4. EMERGENCY PLANNING

As regards emergency planning, it may be advisable to consider including accident scenarios from the SPSA in emergency exercises if these are found to be significantly different from full power accidents.

9.5. DECISIONS ON HARDWARE MODIFICATIONS

The SPSA may show that the shutdown risk can be significantly reduced by certain hardware modifications. For example, in the case of a PWR, it may be decided to introduce automatic protection against the fast boron dilution accident if it is found that the only barrier of protection is human interaction.

9.6. TRAINING OF PERSONNEL

Operations personnel can be provided with additional training in the performance of certain operations or recovery actions found to be important to risk in the SPSA.

9.7. MANAGEMENT PRACTICES

As there are typically many activities taking place simultaneously during an outage, the SPSA can be used to highlight certain risk exposures, for example, those caused by errors in the issuing of work orders. The SPSA may indicate that specific management practices be improved to reduce the possibility of such errors.

Annex I

EXAMPLES OF PLANT OPERATIONAL STATES FOR SPSA

TABLE I-1. PLANT OPERATIONAL STATES FOR SURRY UNIT 1 (PWR) LOW POWER AND SHUTDOWN OUTAGE ACTIVITIES, REFUELLING OUTAGE

POS	Description
1.	Low power operation and RX shutdown
2.	Cooldown with SG (from 547°F to 345°F)
3.	Cooldown with RHR (from 345°F to 200°F)
4.	Cooldown with RHR (from 200°F to 140°F)
5.	Drain RCS to midloop
6.	Midloop operation
7.	Fill for refuelling
8.	Refuelling
9.	Drain RCS to midloop after refuelling
10.	Midloop operation after refuelling
11.	Refill RCS completely
12.	RCS heat-up solid and draw bubble
13.	RCS heat-up with RCPs (from 200°F to 350°F)
14.	RCS heat-up with SGs (from 350°F to 547°F)
15.	RX startup and low power shutdown

TABLE I-2. PLANT OPERATIONAL STATES FOR GRAND GULF UNIT 1 (BWR) LOW POWER AND SHUTDOWN OUTAGE ACTIVITIES

POS	Description
1D.	Low power operation and RX shutdown
2D.	Cooldown from operating pressure to 500 psig
3D.	Cooldown from 500 psig to initiation of RHR/SDC
4D.	Cooldown with RHR/SDC to approximately 200°F
5D.	Cold shutdown
6D.	Refuelling with water level raised to steam lines
7.	Refuelling with water level raised to upper pool connected
6U.	Refuelling with water level lowered to steam lines
5U.	Cold shutdown after refuelling or extended outage
4U.	Heat-up from approximately 200°F to point where RHR/SDDC no longer available
3U.	Heat-up to approximately 500 psig
2U.	Heat-up to operating pressure
1U.	Low power operations after refuelling or extended outage

TABLE I-3. EXAMPLE PLANT OPERATIONAL STATES FOR WWER 440/213 LOW POWER AND SHUTDOWN OUTAGE ACTIVITIES, REFUELLING AND MAINTENANCE OUTAGE

POS	Decay heat rate, % of initial power	Cooling	Reactor/Level
Power 1 *(added to full power)*	6.50 –	Steam Generators (steam-water) All RCPs	Closed Level nominal
1	6.50–0.789	Steam Generators (steam-water) All RCPs	Closed Level 8 m.
2	0.750–0.651	6 Steam Generators (water-water) 5 RCPs	Closed Level 8 m.
3	0.651–0.393	2 SG; 1 reserve (water-water) natural circulation	Closed Level 8 m.
4	0.393–0.229	2 SG; 1 reserve (water-water) natural circulation	Closed/Partially open Level 0.5 m under the vessel flange
5S	0.229–0.184	1 SG; 1 reserve (water-water) natural circulation	Open Refuelling level
5L	0.229–0.1115	1 SG; 1 reserve (water-water) natural circulation	Open Refuelling level Core in spent fuel pool
6	0.184–0.1557	2 Steam Generators (water-water) natural circulation	Open Level 0.5 m under the vessel flange
7	0.1557–0.1421	Heating by means of 4 or 5 RCPs	Closed Level 8 m.
8	0.1421–0.1406	4 RCPs running	Closed Level 8 m.
9	0.1406–0.1350	2 Steam Generators (water-water) 0 -> 2 RCPs	Closed Level 8 m.
10	0.1350–0.1342	5 RCPs	Closed Level 8 m. to nominal
11	0.1342–0.1334	All RCPs	Closed Level nominal
12	0.1334–6.50	All RCPs	Closed Level nominal
Power 2 *(added to full power)*	6.50	Steam Generators (steam-water phase) All RCPs	Closed Level nominal

TABLE I-4A. EXAMPLE PLANT OPERATIONAL STATES DEFINED FOR A PWR

POS	Pre-POS	State	Characteristics
Power	0	Steady	Reactor at power; T_o: normal; p_o: normal; L_p: normal Spent Fuel Pool Cooling System: supplies power
	1	Transition	Reactor at low power (100 MWe); T_o: normal; p_o: normal; L_p: normal Spent Fuel Pool Cooling System: supplies power P_s: controlled by turbine bypass valve
Hot early	2	Transition	House loads to startup transformers; Shutdown of pre- and overheaters Change of turbine frequency control
	3	Transition	Reactor at low power; Spent Fuel Pool Cooling System: tripped
	4	Steady	Reactor to hot standby; T_c 290°C; p_c 154 bar; Boron >= CR Heat removal through turbine bypass
	5	Transition	T_c 290°C to 120°C; p_c 154 bar to 29.4 bar; Boron >= CK Heat removal through turbine bypass
Cold shutdown early	6	Transition	T_c 120°C to 100°C; p_c 29.4 bar Heat removal through Residual Heat Removal System MSIVs closed, turbine tripped
	7	Transition	T_c 100°C to 50°C; p_c 29.4 bar Heat removal through Residual Heat Removal System RS not available
	8	Transition	T_c <= 50°C; p_c 29.4 to 4.9 bar (Volume Control System spray) Heat removal through Residual Heat Removal System RS not available
	9	Transition	T_c <= 50°C; p_c 4.9 to 0 bar (Volume Control System spray) Heat removal through Residual Heat Removal System RS not available
	10	Steady	Reactor Coolant System closed; T_c <= 50°C; p_c 0 bar; Boron 2200 ppm Heat transfer through Residual Heat Removal System
Midloop early	11	Transition	Reactor Coolant System draining to midloop

TABLE I-4A. (cont.)

	12	Steady	Reactor Coolant System vents open; Midloop operation RPV head closed
	13	Steady	Reactor Coolant System vents open; Midloop operation RPV head open
	14	Transition	Fill of reactor bassin with TJH; To level spent fuel pool, Open gate between both pools Heat transfer through Residual Heat Removal System and Spent Fuel Pool Cooling System
Core unload	15	Steady	Internals removed from RV; Open gate between both pools Heat transfer through Residual Heat Removal System and Spent Fuel Pool Cooling System
Core unload (contd.)	16	Steady	Transport of fuel assemblies to spent fuel pool; Open gate between both pools Heat transfer through Residual Heat Removal System and Spent Fuel Pool Cooling System
Core empty	17	Steady	Core completely removed from RPV and stored in spent fuel pool; Open gate between both pools; Heat transfer through Spent Fuel Pool Cooling System Reactor Coolant System may be drained
Core load	18	Steady	Transport of fuel assemblies to RPV; Open gate between both pools Heat transfer through Residual Heat Removal System and Spent Fuel Pool Cooling System
Midloop late	19	Transition	Drain of Reactor Coolant System below flange of RPV with TJH
	20	Steady	Midloop operation; RPV head open (bolts not tightened) Heat transfer through Residual Heat Removal System
	21	Steady	Midloop operation; RPV head closed Heat transfer through Residual Heat Removal System
	22	Transition	Refill of Reactor Coolant System by Volume Control System T_c <= 50°C; p_c 0 bar; Boron 2200 ppm Heat transfer through Residual Heat Removal System

TABLE I-4A. (cont.)

Cold shutdown late	23	Transition	T_c<= 50°C to 230°C; p_c 0 to 28.4 bar
	24	Transition	T_c <= 50°C to 150°C; p_c 28.4 bar
Hot late	25	Transition	T_c <= 150°C to 270°C; p_c 28.4 to 154 bar; Boron 2200 ppm
	26	Transition	Power to 21% of normal power; T_c <= 270°C to 303°C; p_c 154 bar Boron lowered by Volume Control System/Emergency Boration System House loads on startup transformers
	27	Transition	Reactor at low power (100 MWe); T_o: normal; p_o: normal; L_p: normal Spent Fuel Pool Cooling System: runnning House loads on startup transformers
Power	28	Transition	Reactor at low power (100 MWe); T_o: normal; p_o: normal; L_p: normal Spent Fuel Pool Cooling System: generator synchronised House loads on startup transformers

T_o: Operating temperature; P_o: Operating pressure; Lp: Operating level; T_c: Reactor coolant system temperature;

P_c: Reactor coolant system pressure

TABLE I-4B. POS DEFINED FOR THE FUEL POOL OF A PWR

POS	Pre-POS	State	Characteristics
Fuel pool early	2	Steady	Gate between both pools closed except for fuel transfer operations heat transfer through Spent Fuel Pool Cooling System decay heat level high (all fuel in pool); T_f <= 50°C
Fuel pool late	2	Steady	Gate between both pools closed Heat transfer Through Residual Heat Removal System and Spent Fuel Pool Cooling System; T_f <= 50°C

ANNEX II

SHUTDOWN AND LOW POWER PSAs

Shutdown PSAs have been reported to have been, or are being performed, for the following plants. (Documentation of the SPSAs for these plants may be incomplete or not publicly available).

Asco PWR	(Spain)
Barsebeck BWR	(Sweden)
Beznau PWR	(Switzerland)
Bohunice V2 WWER-213 PWR	(Slovakia)
Borssele PWR	(Netherlands)
Dodewaard BWR	(Netherlands)
Doel PWR	(Belgium)
Forsmark BWR	(Sweden)
French 900 MW Series PWR	(France)
French 1300 MW Series PWR	(France)
Goesgen PWR	(Switzerland)
Grand Gulf BWR-6	(USA)
Gundremmingen BWR	(Germany)
Loviisa WWER-PWR	(Finland)
Muehleberg BWR	(Switzerland)
Olkiluoto BWR	(Finland)
Paks WWER-213 PWR	(Hungary)
Seabrooke PWR PSA	(USA)
Sizewell B PWR	(United Kingdom)
Surry PWR	(USA)
Tihange 2 PWR	(Belgium)
Vandellos 2 PWR	(Spain)

ANNEX III

EXAMPLES OF INITIATING EVENTS LISTS

INITIATING EVENTS USED IN THE FRENCH (PWR) STUDIES:

- LOCA
- Steam generator tube rupture (SGTR)
- Steam line break (SLB)–feedwater line break (FWB)
- Loss of heat sink [component cooling water system (CCWS)]
- Loss of SG feedwater
- Loss of electrical supply
- Loss of RHRS
- Dilutions.

INITIATING EVENTS USED IN THE SURRY SPSA:

I. Loss of RHR
II. Transients
III. LOCAs
IV. Loss of off-site power
V. Low temperature overpressurization
VI. Reactivity accidents
VII. Heavy load drop accidents, refuelling accident
VIII. Support system failures.

INITIATING EVENTS USED IN THE BWR GRAND GULF SPSA

T1	Loss of off-site power (LOOP) transient
T2	Transient with loss of power conversion system
T3A	Transient with PCS initially available
T3C	Transient caused by inadvertent open relief valve
A	Large LOCA
S1	Intermediate LOCA
S2	Small LOCA
S3	Small–small LOCA
V	Interfacing system LOCA
R	Vessel rupture
H1	Diversion to suppression pool via RHR
H2	Diversion to condenser via RWCU
J1	LOCA in connected system (RCIC)
J2	LOCA in connected system (RHR)
K	Test/maintenance-induced LOCA
E1B	Isolation of SDC loop B only
E1C	Isolation of RWCU as DHR
E1D	Isolation of ADHRS only
E1T	Isolation of SDC common suction line
E1V	Isolation of common suction line for ADHRS
E2B	Loss of SDC loop B only
E2C	Loss of RWCU as DHR
E2D	Loss of ADHRS only
E2T	Loss of SDC common suction line
E2V	Loss of common suction line for ADHRS
T4A	Rod withdrawal error
T4B	Refuelling accident (rod or fuel misposition)
T4C	Instability event
T5C	Loss of all SSW
T5B	Loss of all TBCW
T5C	Loss of all PSW (includes radial well)
T5D	Loss of all CCW
TAB	Loss of 1E 4160 V AC bus B
TDB	Loss of 1E 125 V DC bus B
TIA	Loss of instrument air
TORV	Inadvertent open relief valve at shutdown
TIOP	Inadvertent overpressurization (makeup greater than letdown)
TIHP	Inadvertent overpressurization via spurious HPCS actuation
TIOF	Inadvertent overfill via LPCS or LPCI
TLM	Loss of makeup

ABBREVIATIONS

BWR	boiling water reactor
CCF	common cause failure
CCW	component cooling water
CDF	core damage frequency
DHR	decay heat removal
ESD	event sequence diagram
HI	human interaction
HPCS	high pressure core spray
HPSI	high pressure safety injection
HRA	human reliability analysis
LER	licensee event reports
LOCA	loss of coolant accident
LPCI	low pressure coolant injection
LPCS	low pressure core spray
LWR	light water reactor
MCS	minimal cut set
PDS	plant damage state
PHWR	pressurized heavy water reactor
POS	plant operational state
PSA	probabilistic safety assessment
PSW	plant service water
PWR	pressurized water reactor
QA	quality assurance
RCP	reactor coolant pump
RCS	reactor cooling system
RCIC	reactor core isolation cooling
RHR	residual heat removal
RHRS	residual heat removal system
RPV	reactor pressure vessel
RWCU	reactor water cleanup
SDC	shutdown cooling
SG	steam generator
SPSA	shutdown probabilistic safety assessment
SSW	stand-by service water
TBCW	turbine building cooling water

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety Series No. 50-P-4, IAEA, Vienna (1992).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2): Accident Progression, Containment Analysis and Estimation of Accident Source Terms, Safety Series No. 50-P-8, IAEA, Vienna (1995).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), Safety Series No. 50-P-12, IAEA, Vienna (1996).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of External Hazards in Probabilistic Safety Assessments for Nuclear Power Plants, Safety Series No. 50-P-7, IAEA, Vienna (1995).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Treatment of Internal Fires in Probabilistic Safety Assessment for Nuclear Power Plants, Safety Reports Series No. 10, IAEA, Vienna (1998).

[6] OECD NUCLEAR ENERGY AGENCY, A Compendium of Practices on Safety Improvements in Low-Power and Shutdown Operating Modes, NEA/CSNI/R(1997)17, OECD/NEA, Paris (1998).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, PSA for the Shutdown Mode for Nuclear Power Plants (Proc. Tech. Com. Mtg. Stockholm, 1992), IAEA-TECDOC-751, Vienna (1994).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, A Framework for a Quality Assurance Programme for PSA, IAEA-TECDOC-1101 (1999).

[9] NUCLEAR REGULATORY COMMISSION, Evaluation of Potential Severe Accidents During Low Power and Shutdown Operation at Surry, Unit 1, Rep. NUREG/CR-6144, BNL-NUREG-52399, Washington, DC (1995).

[10] NUCLEAR REGULATORY COMMISSION, Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications, Swain, A.D. Guttman, H.E., SAND 80-200, RX, AN, Rep. NUREG/CR-1278, OECD/NEA, Paris (1983).

[11] OECD NUCLEAR ENERGY AGENCY, Critical Operator Actions — Human Reliability Modelling and Data Issues, NEA/CSNI/R(98)1, OECD/NEA, Paris (1998).

[12] NUCLEAR REGULATORY COMMISSION, An Analysis of Operational Experience During Low Power and Shutdown and a Plan for Addressing HRA Issues, Rep. NUREG/CR-6093, Washington, DC (1994).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Procedures for Conducting Common Cause Failure Analysis in Probabilistic Safety Assessment, IAEA-TECDOC-648, Vienna (1992).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessment for Seismic Events, IAEA-TECDOC-724, Vienna (1993).

CONTRIBUTORS TO DRAFTING AND REVIEW

Aldorf, A.	Nuclear Research Institute Rež plc, 250 68 Rež, Czech Republic
Andersson, B.	Forsmarks Krafigrupp AB, Vattenfall, S-742 03 Östhammar, Sweden
Andersson, K.	Karinta Konsult, Box 6048, 18306 Taeby, Sweden
Bennemo, L.	Vattenfall, S-16287 Stockholm, Sweden
Boneham, P.	Enconet Consulting, Auhofstrasse 58, A-1130 Vienna, Austria
Bouwman, E.C.J.	KEMA/PLG, International Team for Risk Assessment and Decision Analysis, Utrechtseweg 310, NL-6812 AR Arnhem, Netherlands
Brook, A.K.	PWR Project Group, Nuclear Electric plc, Booths Hall, Chelford Road, Knutsford, Cheshire WA16 8QG, United Kingdom
Burgazzi, L.	ENEA-ERG-FISS, Via Martiri di Monte Sole, 4, I-40129 Bologna, Italy
Caruso, M.	US Nuclear Regulatory Commission, Washington, D.C. 20555-0001, United States of America
Dagan, W.	ERIN Engineering and Research, Inc., 180 Gordon Drive, Suite 111, Exton, Pennsylvania 19341, United States of America
Delsoir, H.	BELGATOM, Avenue Ariane 7, B-1200 Brussels, Belgium
De Wit, H.W.	NRG Arnhem, P.O. Box 9035, NL-6800 ET Arnhem, Netherlands
Dusek, J.	State Office for Nuclear Safety, Slezská 9, 120 29 Prague, Czech Republic
Edvinsson, H.B.	Vattenfall Ringhals, S-43022 Väröbacka, Sweden
Faig, J.	Asociación Nuclear ASCO, Dirección Técnica, Tres Torres, 7-Barna, E-08017 Barcelona, Spain
Fiol, M.J.	UITESA, Juan Bravo 49 D., E-28006 Madrid, Spain
Gaertner, J.	ERIN Engineering & Research, Inc., 180 Gordon Drive, Suite 111, Lionville, Pennsylvania 19353, United States of America

Giudicelli, J.-M.	TECHNICATOME, B.P. 54000, F-13791 Aix-en-Provence-Cedex 03, France
Görtz, R.	Bundesamt für Strahlenschutz, Postfach 10 01 49, D-38201 Salzgitter, Germany
Grint, G.C.	Nuclear Installations Inspectorate, St. Peters House, Stanley Precinct, Bootle, Merseyside L20 3LZ, United Kingdom
Gubler, R.	Safety Assessment Section, Division of Nuclear Safety, International Atomic Energy Agency, Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria
Hallman, A.	Vattenfall AB, S-162 87 Vällingby, Sweden
Hewitt, J.R.	Science Applications International Corp., 1720 East Wilshire Avenue, Santa Ana, CA 92705, United States of America
Hill, T.F.	Council for Nuclear Safety, P.O. Box 7106, Hennopsmeer 0046, South Africa
Hoeld, A.	Gesellschaft für Reaktorsicherheit (GRS) mbH, Forschungsgelände, D-85748 Garching bei München, Germany
Hoffmann, H.	ABB Reaktor GmbH, Germany
Hooft van Huysduynen, A.M.	NUCON Nuclear Technology BV, Radarweg 60, NL-1043 NT Amsterdam, Netherlands
Julius, J.A.	NUS Corporation, 1303 S. Central Ave. #202, Kent, WA 98032, United States of America
Kaštelan, M.	NEK, Nuklearna Elektrarna Krško, Vrbina 12, 68270 Krško, Slovenia
Kim, T.W.	Korea Atomic Energy Research Institute, Integrated Nuclear Safety Assessment, P.O. Box 105, Yusong, Taejon 305-600, Republic of Korea
Kumano, T.	Institute of Nuclear Safety (INS), Nuclear Power Engineering Corporation (NUPEC), Fujita Kankou Toranomon, Bldg. 7F, 3-17-1 Toranomon, Minato-ku, Tokyo 105, Japan
Maenhout, G.A.G.	AVN, Avenue du Roi, 157, B-1060 Brussels, Belgium

Meyer, A.W.	Siemens AG, Unternehmensbereich KWU, Dept. NDS4, Berliner Str. 295, D-63067 Offenbach, Germany
Mihara, T.	Power Reactor and Nuclear Fuel Development Corporation, 4002 Narita-cho, O-arai-machi, Higashi-ibaraki-gun, Ibaraki-ken 311-13, Japan
Mueller-Ecker, D.	Gesellschaft für Reaktorsicherheit (GRS) mbH, Schwertnergasse 1, D-50667 Cologne, Germany
Neubauer, I.	VEIKI, Budapest V., Zrinyi u. 1, P.O. Box 233, H-1368 Budapest, Hungary
Patrik, M.	Nuclear Research Institute Rež plc, 250 68 Rež, Czech Republic
Pyy, P.T.	VTT Automation, Otakaari 7B, SF-02150 Espoo, Finland
Rao, S.B.	PLG, Inc., 4590 MacArthur Boulevard, Suite 400, Newport Beach, CA 92660-2027, United States of America
Reinhart, F.M.	U.S. Nuclear Regulatory Commission, Washington, D.C. 20555-0001, United States of America
Samoylov, O.B.	OKB Mechanical Engineering, 603603 Nizhny Novgorod 74, Burnakovsky proezd, 15, Russian Federation
Saraf, R.K.	BARC/DAE, Bhabha Atomic Research Centre, Trombay, BARC, Mumbai 400085, India
Schaefer, H.	Gesellschaft für Reaktorsicherheit (GRS) mbH, Forschungsgelande, D-85748 Garching bei München, Germany
Schoonakker, H.A.	EPZ, Wilhelminahofweg 3, NL-4454 PM Borssele, Netherlands
Schubert, B.K.	HEW, Überseering 12, D-22297 Hamburg, Germany
Schüller, J.C.H.	KEMA/PLG, International Team for Risk Assessment and Decision Analysis, Utrechtseweg 310, NL-6812 AR Arnhem, Netherlands
Serbanescu, D.	National Commission for Nuclear Activities Control, Bd. Libertatii No.12, P.O. Box 5, Bucharest 5, Romania
Shahid, M.S.	Design and Engineering Department, Chashma Nuclear Power Plant, P.O. Box No.1133, Islamabad, Pakistan

Sherry, R.	Safety Assessment Section, Division of Nuclear Safety, International Atomic Energy Agency, Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria
Shvyryaev, Y.	Atomenergoproekt, 107815 GSP-6, Moscow B-S, Bakuninskaya 7, Str. 1, Russian Federation
Simon, M.	Gesellschaft für Reaktorsicherheit (GRS)mbH, Schwertnergasse 1, D-50667 Cologne, Germany
Tomic, B.	Safety Assessment Section, Division of Nuclear Safety, International Atomic Energy Agency, Wagramerstrasse 5, P.O. Box 100, A-1400 Vienna, Austria
van der Borst, M.	EPZ, Wilhelminahofweg 3, NL-4454 PM Borssele, Netherlands
van Otterloo, R.W.	KEMA/PLG, International Team for Risk Assessment and Decision Analysis, Utrechtseweg 310, NL-6812 AR Arnhem, Netherlands
Versteeg, M. F.	Ministry of Social Affairs and Employment (KFD), P.O. Box 90804, NL-2509 LV The Hague, Netherlands
Viorel, S.	RENEL, Romanian Electricity Authority, Magheru 33, Sect. 1, Bucharest, Romania
Webster, P.A.	Atomic Energy Control Board, P.O. Box 1046, Station B, 280 Slater Street, Ottawa, Ontario K1P 5S9, Canada
Willers, A.	Atomic Energy Control Board, P.O. Box 1046, Station B, 280 Slater Street, Ottawa, Ontario K1P 5S9, Canada
Wilson, D.G.	RELCON AB, Box 1288, S-1 72 25 Sundbyberg, Sweden
Zander, R.M.	Kernkraftwerke Gundremmingen Betriebsges, P.O. Box 300, D-89355 Gundremmingen, Germany

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities.

The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides.**

- **Safety Fundamentals** (silver lettering) present basic objectives, concepts and principles of safety and protection in the development and application of atomic energy for peaceful purposes.
- **Safety Requirements** (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.
- **Safety Guides** (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA for application in relation to its own operations and to operations assisted by the IAEA.

OTHER SAFETY RELATED PUBLICATIONS

Under the terms of Articles III and VIII.C of its Statute, the IAEA makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its members for this purpose.

Reports on safety and protection in nuclear activities are issued in other series, in particular the **IAEA Safety Reports Series**, as informational publications. Safety Reports may describe good practices and give practical examples and detailed methods that can be used to meet safety requirements. They do not establish requirements or make recommendations.

Other IAEA series that include safety related sales publications are the **Technical Reports Series,** the **Radiological Assessment Reports Series** and the **INSAG Series**. The IAEA also issues reports on radiological accidents and other special sales publications. Unpriced safety related publications are issued in the **TECDOC Series**, the **Provisional Safety Standards Series**, the **Training Course Series,** the **IAEA Services Series** and the **Computer Manual Series**, and as **Practical Radiation Safety and Protection Manuals**.