2 Risk analyses and protection strategies for the operation of nuclear power plants

[W. Kröger, with contributions from J. Mertens, D. Kogelschatz, S. Chakraborty]

2.1 Introduction

Nuclear fission today supplies almost 7 % of the primary energy and 17 % of the electricity consumed worldwide. In many countries, this technology is controversial and its future uncertain. “Facts” are complex, regarded as ambiguous and contradictory, and confronted with deep-rooted opinions. To the public, nuclear power represents a sword of Damocles, but most experts regard the risks as small and justifiable. Why is this so? The answer is twofold. First, the public perceives the hazard, the possible consequences of a potential accident. The analyst thinks in terms of risk, which incorporates the element of probability. Second, the public view is based in part upon the lack of long experience, because the highly complex nuclear technology is relatively young and still evolving. The analytic view is based upon techniques that have been developed for understanding possible failures and improving plant design, construction and operation. Experience of actual nuclear accidents is thankfully rare, but the probabilistic study of the potential failures of redundant safety systems and of possible accident sequences provides a basis for confidence in the low levels of projected future safety risks.

This chapter attempts to provide a technical basis for the discussion of the analytic techniques used to understand and evaluate nuclear safety systems. Although the discussion is technically oriented, it is aimed at the interested lay reader as well as those who are already acquainted with the subject. It focuses on nuclear power plants, their safety systems and operation, and future development strategies. Other steps in the life cycle of nuclear power have been ignored, including mining, fuel enrichment and fabrication, and waste disposal. These steps have their own risks, which are, however, smaller and less catastrophic.

One of the main goals of this chapter is to present an introduction to probabilistic safety analysis (PSA), and to explain the current state of knowledge and applications. An overview of analyses is presented for light water reactors that are in service in Western countries. Specific examples are also presented for light water reactors of Eastern European design (WWER) and comments made regarding inherently safe reactors (e.g. high-temperature gas-cooled reactors) for the purposes of comparison and the clarification of significant new analytic challenges.

The selection of materials has been made according to the present state of knowledge, particularly based upon international working groups and state-of-the-art reports that reflect expert consensus. These naturally reflect the emphases of the established scientific community and organizations.

The presentation has been limited to the scientific and engineering approach to the concept of risk, and specifically to the concept of calculated risk. The focus is upon risk analysis, including methods for comparative evaluation and the problems of risk management. The discrepancies between calculated and perceived risks which play such a large role in the important realm of public debate and decision-making have been excluded here, in accordance with the character of the rest of the present work.

2.2 Technical fundamentals

Nuclear power plants rely upon the splitting of heavy atoms to produce energy. Being struck by a relatively slow neutron causes the fission of uranium or plutonium, producing two fission products (FP) of different weights and two to three fast, energetic neutrons. The most common reaction used for power production is the fission of ^{235}U, which can be written as follows:

$$ {}^{1}_{0}\mathrm{n} + {}^{235}_{92}\mathrm{U} \rightarrow 2\,\mathrm{FP} + 2\ldots3\ {}^{1}_{0}\mathrm{n} + 207\,\mathrm{MeV}. \qquad (2.1) $$

The fast neutrons carry most of the energy produced and must be slowed, or moderated, to continue the chain reaction. The most usual moderator is common, or light, water. Light water reactors may boil water directly in the reactor (a boiling water reactor or BWR) or use pressurized water from the reactor to generate steam in a heat exchanger (a pressurized water reactor or PWR). In absolute terms the energy which is released per fission is extremely small, so that the production of a Watt-second requires about 3.1 billion (10^9) of individual fissions. However the number of atoms available to fission means that the energy density of the nuclear fuel is approximately 1000 times greater than that of a fossil fuel like coal.

A sustained nuclear reaction can be controlled because there is a fraction of neutrons which are delayed in their release during the fission process. If reactor control fails and the reaction goes beyond the critical or self-sustaining level to a "super-critical" level, the rapid excess heat can fragment the fuel and the reactor structure, leading in the most extreme cases to a core disruptive accident.

Severe core damage can also occur if reactor cooling systems fail to remove the normal heat produced. With light water reactors (LWRs) insufficient cooling can be caused by a loss of the coolant due to a leak in the primary circuit or by loss of the primary heat-sink. Even after the reactor is safely shut down, the "afterheat" produced by the decay of the fission products must be safely stored or removed. This afterheat drops from about 6 % of total reactor power directly after shutdown to roughly 1 % after six hours, and if it cannot be removed a core meltdown will occur.

The primary danger to human health and to the environment lies in the inventory of radioactive isotopes present in the plant[1], and the high temperatures and pressures within reactor systems which represent stored energy available to drive the release of the radioactive inventory[2]. Nuclear fuel is originally only weakly radioactive. The primary inventory of radioactivity lies in the fission products created and the chain of isotopes which decay from them, and to a lesser extent in isotopes which are "activated", or created by the absorption of neutrons. The safe containment of this inventory within the plant is therefore the highest priority.

To avoid such a hazardous[3] potential from becoming a real event, nuclear power plants are equipped with highly reliable and redundant active and passive safety systems. These cooling and containment systems must fail before fission products are released to the environment. Such failures are extremely infrequent and the risk is generally very small. While the term "hazard" indicates conceptually possible consequences, the term "risk" incorporates both consequences and probability. If confidence in the quality of safety systems is high, this multiplication can indicate that risk is minimal, although the consequence of a single series of events might be high.

At present there are about 440 nuclear power plants worldwide in operation. The experience gathered amounts to roughly 9000 reactor-years, 6000 of which stem from LWRs of Western design. Direct experience of accidents is – owing to the safety measures taken – very limited and insufficient for reliable risk-assessment. This means that a theoretical approach using models and other methods must be taken to analyze possible accident sequences and the response of the relevant, highly complex safety systems. In this way, available experience based on component failures can be used in a practical way. Probabilistic risk or safety analysis provides such a framework.

[1]) The radioactive inventory of a P_{el} = 1300 MW reactor amounts to 10^{21} Bq.
[2]) The primary coolant pressure for a BWR is about 8 MPa, and about 15 MPa for a PWR.
[3]) Hazard is defined as the property of a substance or the momentary state of a process which has the potential of endangering human life and the environment as well as material goods.

2.3 Protection strategies

2.3.1 Basic philosophy

The commercial use of nuclear power is bound to specific strategies aiming at protecting individuals, the society and the environment effectively against undue release of radioactive material from the plants. From the very beginning the basic safety concept has followed the "principle of precaution" instead of "trial and error". Three basic safety functions have been established:

– controlling the power (reactivity),
– cooling the fuel during operation and after shutdown,
– confining the radioactive material.

To assure these three safety functions, the fundamental **principle of defence in depth** has been established. It is implemented primarily by means of a series of physical barriers which would in principle never be breached, and which must all be violated in turn before harm can occur to people or the environment. The barriers may serve operational as well as safety purposes (see Fig. 2.1).

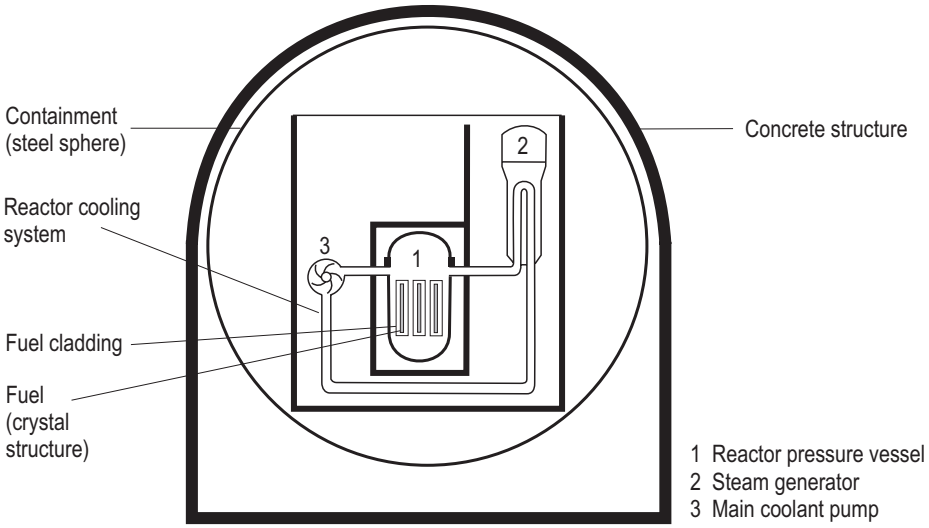


Fig. 2.1. Successive barriers (schematic view for a German pressurized water reactor).

The general strategy is first to prevent accidents and second, if prevention fails, to limit the potential consequences of accidents (mitigation). Defence in depth is generally structured in five levels of protection. The objectives of each level and the essential means of achieving them are shown in Fig. 2.2. If one level should fail, the subsequent level comes into play, and so on. Special attention is paid to hazards that could potentially impair several levels of defence coincidentally, such as fire, flooding or earthquakes.

The first means of **preventing accidents** is to strive for such high quality in design, construction and operation of the plant that deviations from normal operational states become rare. Safety systems are used as a backup to feedback in process control to prevent such deviations from developing into serious accidents. The most important safety systems are those for reactor redundant protection and shutdown, for emergency core cooling and afterheat removal and for confinement of radioactivity. Safety systems make use of redundancy and diversity of design and the physical separation of parallel components, where appropriate, to reduce the likelihood of the loss of a vital function. They are inspected and tested regularly, and operate automatically. They are conservatively designed to cope with design basis accidents and to handle uncertainty by using conservative success criteria and a high degree of redundancy to assure system function even if one train fails on demand and another is under repair.

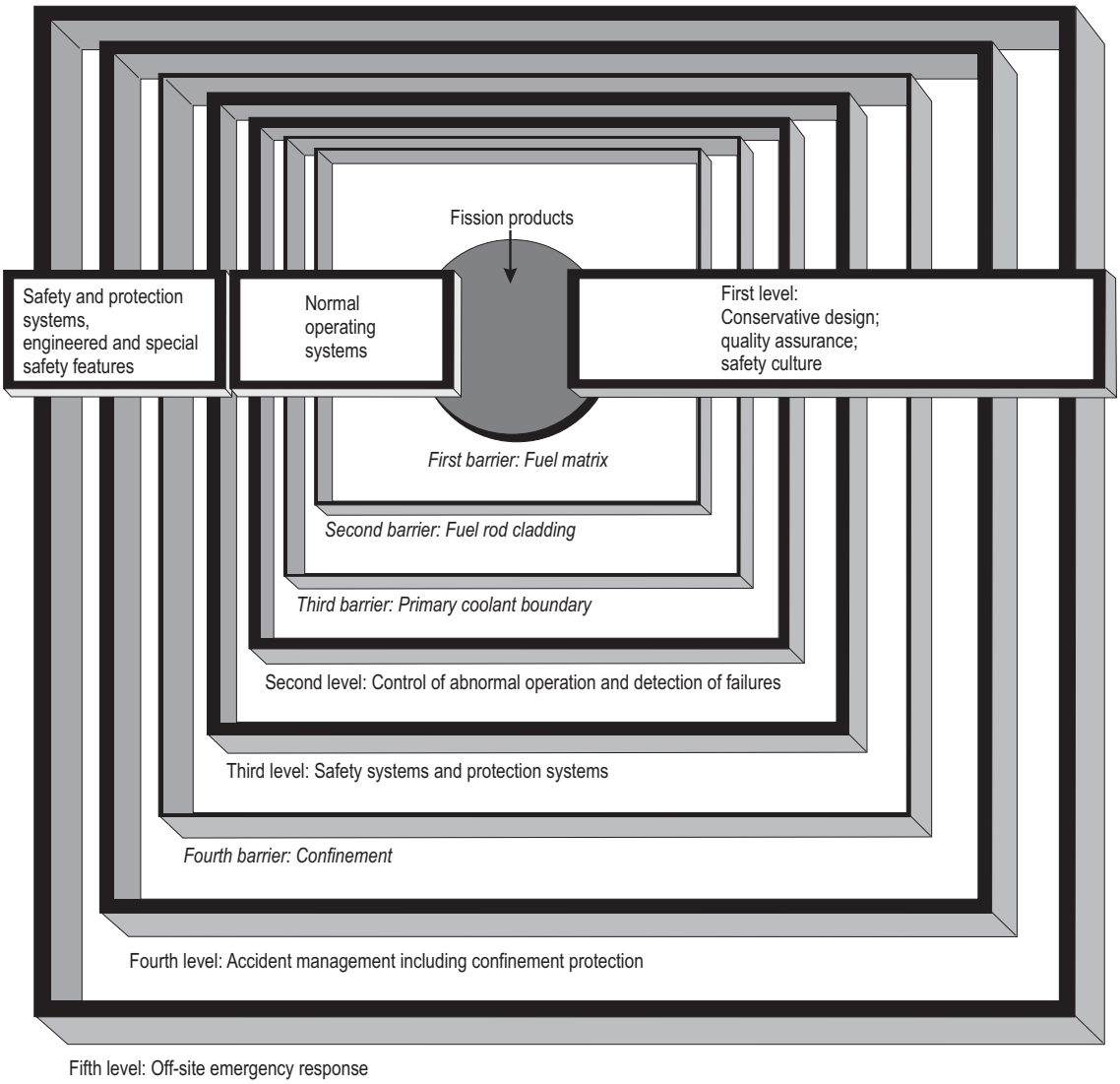


Fig. 2.2. Overview of defence in depth (INSAG-12 [99IAE1]).

Design basis accidents (DBA) are chosen to encompass a representative set of initiating events that could challenge the safety of the plant and place the strongest requirements on the safety equipment. Loss of coolant after guillotine-break of the main coolant line is the most prominent DBA. Analysis is used to show that the response of the plant and its safety systems satisfies predetermined specifications both for the performance of the plant itself and for meeting safety targets. The **deterministic method** uses engineering judgment and accepted analysis to predict the course of events and their consequences. For example nuclear plants are designed in such a way that the simultaneous loss of on-site and off-site electric power (station blackout) will not lead to fuel damage for a specified period of time, although both normal and backup power supplies are designed to ensure high reliability. The reliability of backup electrical power supplies for safety systems is sometimes augmented by means of diverse power supplies, such as direct-drive diesels, direct-drive steam turbines and batteries for instruments and other DC components. Additional electrical power generating sources (e.g. connection to a hydroelectric power station or installation of gas turbine generators) are used in some plants to improve the response to station blackout.

Probabilistic risk, or better, **probabilistic safety analysis** (PSA) is used to evaluate the frequency of any particular event sequence and its consequences (see Sect. 2.4). This evaluation looks at the whole

plant in an integrated manner and may take into account the effects of mitigation measures inside and outside the plant. It is increasingly used to evaluate multiple failure situations, especially to identify the importance of any possible weakness in design or operation or during potential accident sequences that contribute to risk. The probabilistic method can be used to aid in the selection of events requiring deterministic analysis and vice versa. The process employs realistic assumptions and best estimate analyses and tries to quantify uncertainties. It therefore complements the deterministic design basis analysis.

Provisions for **accident mitigation** extend the defence-in-depth concept beyond accident prevention. They are of three kinds, namely, accident management, engineered safety features and off-site countermeasures. Accident management includes pre-planned and ad hoc operational practices which, if the design specifications of the plant are exceeded, would make optimum use of existing plant equipment ways to restore the plant to a safe state. In such circumstances, engineered safety features (barriers) would act to confine any radioactive material released from the core so that discharges to the environment would be minimal. Off-site countermeasures are pre-planned, going beyond the level of protection provided in most human endeavors, to compensate for the remote possibility that safety measures at the plant might fail. In such a case, the effects on the surrounding population or the environment would be mitigated by protective actions, such as sheltering or evacuation of the population, and by prevention of the transfer of radioactive material to humans by food chains and other pathways.

Accident management in operating plants is being extended into the realm of increasingly severe accidents of very low frequency. This requires additional guidelines or procedures, further understanding of the prevailing phenomena, appropriate assignment of responsibilities, and training of the staff.

2.3.2 Commonly shared principles and future requirements

The basic means for ensuring sufficient safety of nuclear power plants have been in common practice, especially in the Western countries. Nevertheless, quite big differences exist in detail. The International Nuclear Safety Advisory Group (INSAG) has recently stated **commonly shared principles** for all types of nuclear power plants and for all countries. This document (INSAG-12 [99IAE1]) contains objectives as well as fundamental and specific principles of how to achieve them. This will set the framework for the future use of nuclear power. It is clear that the safety principles do not guarantee absolute freedom of risk, but when the general nuclear safety objectives are fulfilled the level of risk due to nuclear power plants does not exceed that of competing energy sources.

The INSAG technical safety objectives are

> *"to prevent with high confidence accidents in nuclear plants; to ensure that, for all accidents taken into account in the design of the plant, even those of very low probability, radiological consequences, if any, would be minor; and to ensure that the likelihood of severe accidents with serious radiological consequences is extremely small."*

The frequency of occurrence of severe core damage for existing plants is targeted to be below about 10^{-4} and for future plants to be not more than 10^{-5} per year of plant operation.

Severe accident management and mitigation measures could reduce the probability of large off-site releases requiring short-term off-site response for existing plants by a factor of at least ten. The practical elimination of accident sequences that could lead to large early radioactive releases is another objective for future plants.

Finally the importance of safety culture[4] and pervasive safety thinking as a key element are emphasized.

More stringent **safety requirements for future nuclear reactors** are being developed at an international. **Germany** is the first country to have laid down those requirements in form of a law [98BGB]. According to this law, licences can only be granted on condition that the features and the operation of the

[4]) Personal dedication and accountability of all individuals engaged in any activity which has a bearing on the safety, e.g. full attention to safety matters with the senior management, policies which ensure correct practices, clear lines of responsibilities, authority backed up with adequate resources, sound procedures, training and education, etc. (INSAG-13 [99IAE2]).

power plant exclude any events which would require restrictive measures as prevention against the dangerous effects of ionizing radiation outside the sealed-off area of the plant. This must be demonstrated even for those events which have basically been eliminated as possibilities by pertinent preventive measures.

With respect to LWRs, this means that in case of unlikely accident sequences, such as a core meltdown and its consecutive phenomena, only such an amount of radioactivity may be set free as does not necessitate any emergency measure outside the fence of the plant.

In the **USA** an industry-led effort has resulted in a technical foundation for the design of the Advanced Light Water Reactor (ALWR), either of simpler evolutionary design or with employment of primarily passive means for essential safety functions. The **Requirements Document** [90EPR] presents a clear, complete statement of utilities desires in close co-operation with the US Department of Energy and the Nuclear Regulatory Commission.

The top-tier design requirements include besides more general standards (e.g. 60 years plant design life) and performance criteria (e.g. 24-month refueling interval, less than 1 unplanned scram per year) safety and investment protection goals. The most important stringent requirements for Passive ALWRs are listed in Table 2.1. The key ideas from a safety point of view are to further limit the frequency of core damage and the associated large releases to the environment as well as to strengthen inherent safety features and to be less dependent on off-site emergency planning to protect the public.

A number of major electricity producers has agreed upon common requirements for future LWRs to be built in **Europe** [94EUR]. The main goals are to further improve plant safety and performance as well as to increase acceptance by the public and political authorities.

For severe accidents, discharge activity targets are established so as to limit the societal consequences resulting from health effects and contamination of soil and water. The objectives sought are

- no need for short-term (< 24 hours) off-site countermeasures,
  no need for population evacuation beyond 2…3 km;
- for long-term consequences, need for limited countermeasures such as restriction of consumption of agricultural products only for a limited period (about 1 year) and in a limited area.

Table 2.1. Selection of top-tier ALWR plant design requirements for safety and investment protection [90EPR].

Core damage frequency (CDF)	Demonstrate by PSA that CDF is less than 10^{-5} per reactor-year.
Loss of coolant accident (LOCA) protection	No fuel damage for up to a 6-inch break.
Station blackout coping time for core cooling	8 hours minimum (indefinite for Passive ALWR).
Operator action	For Passive ALWR, no core protection regulatory limits exceeded for at least 72 hours, assuming no operator action for licensing design basis (LDB) events including loss of all AC power.
Severe accident frequency and consequence	Demonstrate by PSA that the whole body dose is less than 250 mSv at site boundary for accidents with cumulative frequency greater than 10^{-6} per reactor-year.
Containment margin	Design containment to maintain its integrity and low leakage during a severe accident.
Hydrogen generation	LDB hydrogen concentration less than 13 % in containment for 75 % active clad oxidation.
Emergency planning	For Passive ALWR, provide technical basis for simplification of off-site emergency plan.

Both short-term and longer-term release targets are given in Table 2.2. Iodine, xenon and caesium are selected as representative nuclides. The designer shall demonstrate through PSA studies that the cumulated frequency of a core damage is less than 10^{-5} and of a release exceeding the discharge activity targets is less than 10^{-6}, both per reactor-year.

The requirements also include a standardized siting envelope (e.g. design basis earthquake: 0.25 g), operational targets (e.g. plant design life 40 years without refurbishment; 60 years for unreplaceable components; specified outage duration, less than 1 unplanned automatic scram per 7000 hours) and key economic objectives.

Table 2.2. Discharge activity targets for severe accidents [94EUR].

	Limits for discharge to the atmosphere [10^{12} Bq]	
	short term (< 24 h)	long term
^{133}Xe	100000	1000000
^{131}I	300	2000
^{137}Cs	no value	100

2.3.3 Future role of probabilistic safety analysis (PSA)

The first comprehensive application of PSA-methodology in order to understand the risk of nuclear power plants was the Reactor Safety Study (WASH-1400). It was published in 1975, under the sponsorship of the US Nuclear Regulatory Commission [75RSS]. Afterwards the use of PSAs was mainly concentrated on the evaluation of severe accident vulnerabilities. The methodology became widespread, primarily due to the Three Mile Island accident in 1979. Today, PSAs of different scope and quality are available for most nuclear power plants in the world, at least for each construction series in Western countries.

PSA applications cover several areas. As a future trend PSAs can be used by operators for monitoring the risks of day-to-day operation of nuclear power plants, already a common practice in several countries. PSAs are also routinely used by operators and regulators alike for design and operational optimization. Another important area of application can be identified in system backfit studies and in the resolution of safety issues. In particular, PSAs can be an invaluable aid for determination of whether potential changes considered for resolution of certain generic safety issues reduce risk sufficiently to justify their cost, and to support proposals for additional regulatory backfit requirements to enhance safety.

Other common applications, especially in the regulatory context, include evaluation of proposed changes to plant technical specifications, changes to the Allowed Outage Time and maintenance operations, evaluation of proposed severe accident management measures and emergency plans, efficient and effective inspections.

In recent times PSA also has played a key role for the certification and licensing of new reactor designs. PSAs will also help in prioritizing safety research.

The move to risk-informed regulation opens many new areas where traditional engineering analyses are supplemented and supported by PSA studies and operational experience. It sets apart risk-informed regulation from the existing approach based on deterministic requirements, involving defence-in-depth and sufficient conservatism to account for the uncertainties associated with the design, operation and phenomenological processes.

The large scale use of quantitative risk analysis that has been pioneered in the air and space, offshore and nuclear industries is slowly becoming widespread in other lines of business, including the chemical industry, transportation, the financial, the food and pharmaceutical sectors, computer networks and other critical infrastructures [00Kir].

The evaluation of operational events to learn lessons from plant experience data can be carried out by PSA techniques, such as the Accident Sequence Precursor methodology [98Bel]. By this methodology the likelihood that a given event initiated at a particular plant would progress to a severe accident can be estimated.

2.4 Methodology of PSA

2.4.1 Structure and scope

A PSA for a nuclear power plant deals in its first step with the identification of initiating events and event sequences leading to core damage. An analysis of this scope is called a Level-1 PSA (Fig. 2.3). If the analysis is extended to include the assessment of active containment systems it is denoted Level-1+ PSA [90DRS].

A Level-2 PSA addresses also the physical effects and the containment response for all core damage sequences and the transport of radioactive material from the core to the environment. Typical results are release categories comprising the amount of radionuclides released to the environment, release frequencies and conditions.

A full-scope or Level-3 PSA also analyzes the atmospheric dispersion of the released radionuclides, potential doses and health, environmental and social/financial effects as well as pertinent frequencies.

Figure 2.4 [93Caz1] gives an overview of the methodology and the single steps as carried out in a state-of-the-art PSA. The starting point is the definition of a set of initiating events. In the next step accident sequences are generated and quantified using event trees and fault trees (see Sect. 2.4.3.2). These sequences add to the total core damage frequency. The sequences are binned into plant damage states (PDS) which are defined by characteristics important to containment response and radionuclide transport. The results of additional accident progression event trees are binned into release categories, characterized by source terms and associated frequencies. Consequences and risk values are calculated for a representative set of release categories.

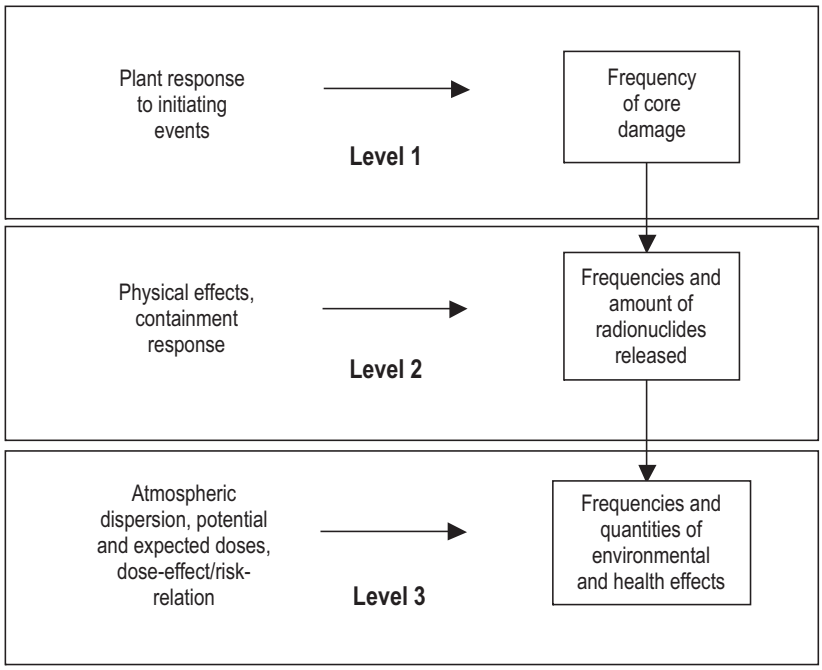


Fig. 2.3. Structure and "levels" of a PSA for nuclear power plants.

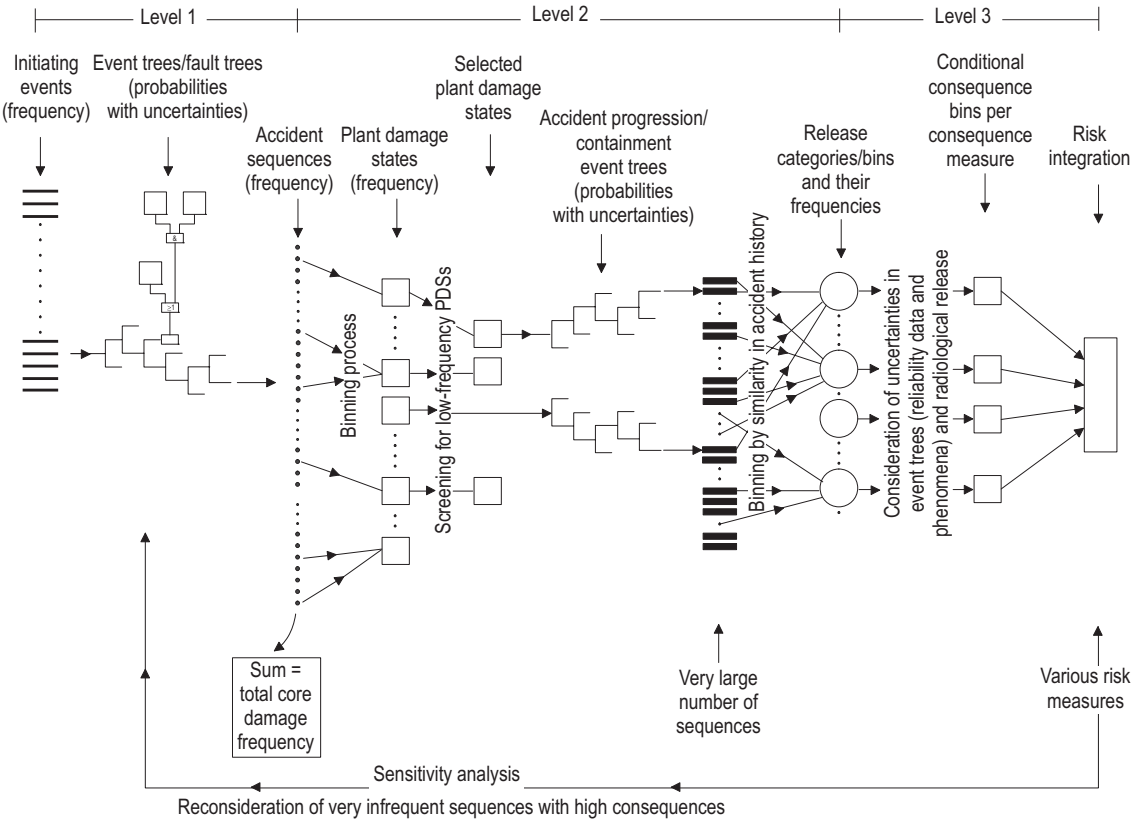


Fig. 2.4. Overview of PSA methodology [93Caz1].

2.4.2 Basic mathematical techniques

The quantification of important PSA methods (e.g. fault-tree analysis, event-tree analysis, probabilistic fracture mechanics) uses probabilities of statistical events (e.g. failure probabilities of basic events in fault trees). Only if there are a sufficiently large series of repeated trials in which the event can occur, the frequency concept is appropriate. Then, the probability is axiomatically defined by the axioms of Kolmogorov [33Kol] (definition of probability) and σ algebra (definition of sets). Statistics are then done, first in order to estimate unknown constant parameters of a population (e.g. failure rate, mean values) with confidence interval, and second to check statistical hypotheses about the population [92Sac]. This is the well-known inductive reasoning for statistical inferences.

Unfortunately, a lot of events cannot be interpreted as a series of trials in practice or the sample size is limited, e.g. many reliability assessments of components are based on sample sizes less than ten failures within the time of observation. For this purpose, the "traditional" inductive reasoning is inappropriate. Propositions or subjective probabilities (hypotheses) are used instead which needs a different notation of probability.

The Bayesian method of statistical inference is distinctly different. An increased data base is used, linking sample data, represented by a sampling model, and an additional prior model containing relevant past experiences based on different data sources, hypotheses, etc. Out of the generalized data pool, the parameters of interest (e.g. failure rates) are random variables instead of constants. This is a deductive reasoning of statistical inferences [82Mar].

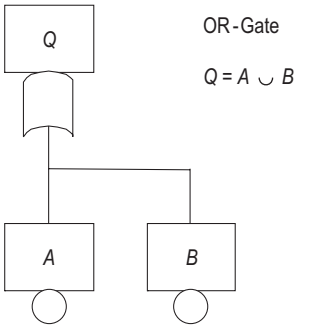
In most current PSAs, a Bayesian framework has been adopted. The merits of this approach are [95Hir]

- the capability for yielding a formal and explicitly structured account of subjective elements;
- the explicit use of relevant past experience, which in combination with sample data may lead to better statistical inferences than those provided by sampling theory;
- the need for a smaller amount of sample data due to the use of relevant past experiences.

The advantages of using the Bayesian approach are particularly evident in cases where sample data are scarce. When the reliability of a specific component at a specific plant is being analyzed, existing data can be used for components which have identical or similar design and which are operating under identical or similar conditions at other plants. The Bayesian approach provides a strict framework for adopting such data and transparency in application of subjective judgment. A disadvantage of the Bayesian approach in PSAs is often blurry data sources and dependence on prior model data.

The formal mathematical basis for reliability analysis as part of a PSA is provided by the so-called Boolean algebra and by a system of axioms formulated by Kolmogorov [33Kol]. Figure 2.5 summarizes some basic properties of probability calculation which are important in the context of quantification of logical models used in PSA.

Boolean algebra

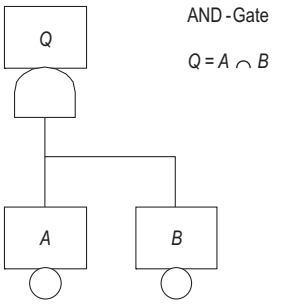


Probability

$$P(Q) = P(A) + P(B) - P(A \cap B)$$
$$= P(A) + P(B) - P(A) \cdot P(B \mid A)$$

Some conclusions:

1) A and B mutually exclusive
$$P(A \cap B) = 0$$
$$P(Q) = P(A) + P(B)$$
2) A and B independent
$$P(B \mid A) = P(B)$$
$$P(Q) = P(A) + P(B) - P(A) \cdot P(B)$$
3) A and B totally dependent
$$P(B \mid A) = 1$$
$$P(Q) = P(A) + P(B) - P(A) = P(B)$$



Probability

$$P(Q) = P(A \cap B)$$
$$= P(A) \cdot P(B \mid A) = P(B) \cdot P(A \mid B)$$

Some conclusions:

1) A and B independent
$$P(B \mid A) = P(B) \text{ and } P(A \mid B) = P(A)$$
$$P(Q) = P(A) \cdot P(B)$$
2) A and B dependent
$$P(Q) > P(A) \cdot P(B)$$
3) Total dependence
$$P(B \mid A) = 1$$
$$P(Q) = P(A)$$

Fig. 2.5. Some basic properties of probabilities for combinations of basis events (A, B).

2.4.3 Fundamentals of Level-1 PSA

2.4.3.1 Selection of initiating events

An initiating event (IE) causes a disturbance in the plant and potentially leads to core damage states. There are several approaches to the identification and selection of internal and external IEs which should be combined [92IAE]:

Engineering evaluation: Systems and major components are systematically reviewed to check whether any of the failure modes could lead directly or in combination with other failures to core damage. Attention should be given to events that may cause simultaneous failures of plant systems (external: e.g. earthquakes, aircraft crashes; internal: e.g. fire).

Deductive analysis: Core damage is made the top event in a diagram similar to a fault tree. This top event is successively broken down into all possible categories of events that could cause it to occur.

Operational experience: Operational history of the plant under consideration and of similar plants is reviewed for IE candidates.

For LWRs, there are two major categories of internal initiating events: loss-of-coolant accident (LOCA) initiators and transient initiators. LOCAs are all events that directly cause loss of integrity of the primary coolant pressure boundary. Transients are characterized by a disturbed balance between heat production and heat removal. They cause a need for reactor shutdown and subsequent removal of decay heat; loss of off-site power is a special kind of transient. About 100 IEs are taken into account in a high-quality PSA. Attacks by war, sabotage (by operators or others) and terrorism are generally not considered. Lists of initiating events and examples of grouping can be found in [92IAE].

2.4.3.2 Event sequence and system modeling

The response of the plant to each group of initiating events is usually modeled by the use of **event trees.** They provide sequences that, depending on successes or failures of relevant systems or occurrence or non-occurrence of events respectively, lead either to a safe or to a core damage state. System failures are identified and quantified by system models like **fault trees** which deduce logical combinations of simpler events like component failures. The combined event tree/fault tree method is mostly used. This static approach is sufficient for most applications and can be complemented by dynamic methods.

The event-tree approach (see Fig. 2.9) simulates the plant response to an initiating event and is based on supporting analyses (e.g. thermohydraulic analysis) which define the minimum successful response required from the safety systems. To be conservative, criteria from the licensing procedure can be used but are in conflict with the fundamental approach of PSA, which is to be realistic. More realistic assumptions can be taken from best-estimate calculations. For instance, in the conservative approach the criteria are not met, if in a redundant system, designed as of 4×50 % capacity, only one train is available. Based on best-estimate calculations, one train can be sufficient to fulfill the safety function. Success criteria must be carefully and clearly defined for every system that is modelled in each accident sequence, because the criteria for the same system can differ for different accident sequences or demand situations.

The fault-tree method is a deductive, analytical technique, which specifies an undesired state of a system (“top event”) and uses graphs to model the various parallel and sequential combinations of failures that will result from the undesired state (Fig. 2.6). Examples are events that are associated with component hardware failures, human errors and maintenance or test unavailabilities.

Important items regarding the development of fault trees are

- the definition of system boundaries and interfaces between primary and support systems;
- the use of computerized methods to ensure consistency and quality;
- a careful selection of a component coding system which provides extensive information about failure modes, the system to which the component belongs and its location, as well as susceptibility to environmental effects;
- the representation of human errors and common cause failures (see Sects. 2.4.3.4 and 2.4.3.5).

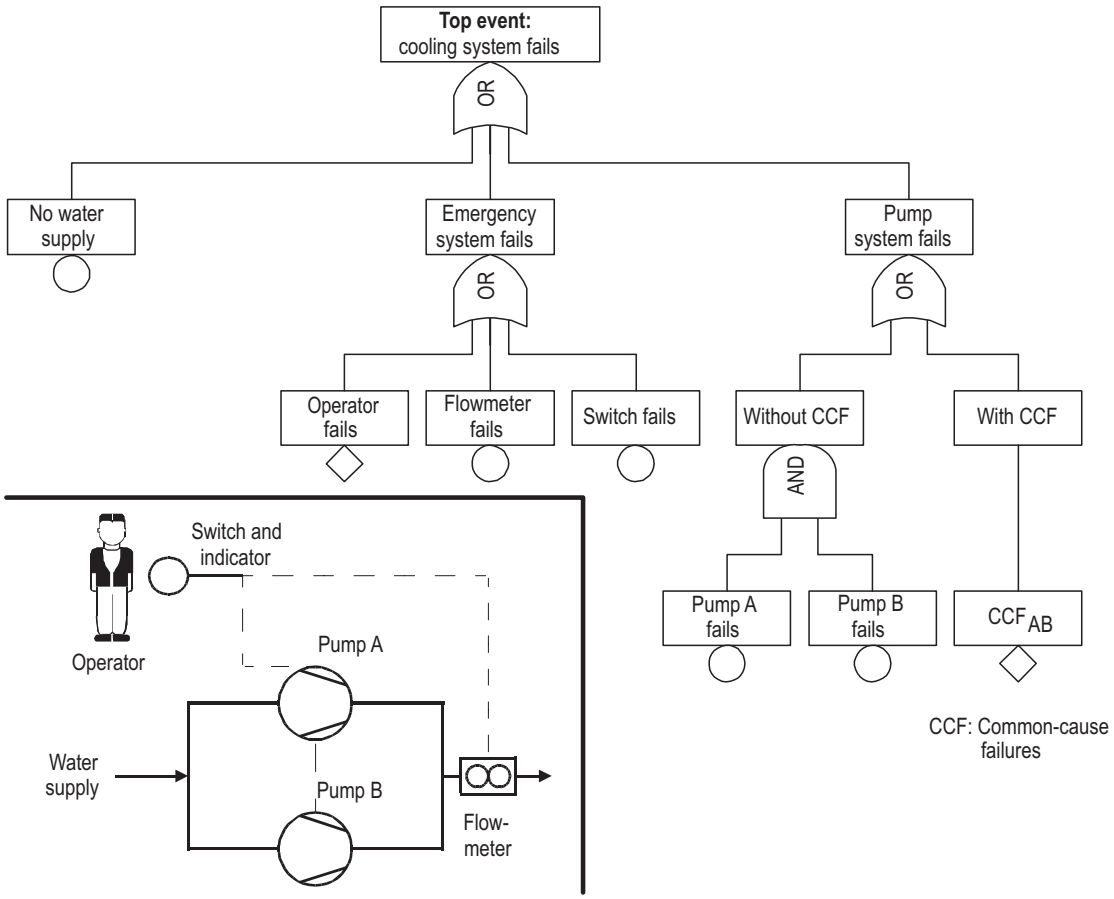


Fig. 2.6. Flow chart and its fault-tree representation (simplified example).

Failure-Mode and Effects Analysis (FMEA) is a table-based technique that focuses on single event failures. It is often used as a screening method to identify relevant component failure modes and to analyze their potential consequences, thus providing background information for more detailed analyses.

A **state space diagram** is a logic model depicting the various states of a system and the paths along which the system can transfer from one state to another. The diagram can be represented by a set of simultaneous differential equations describing how the probability of the states changes with time. State-space analysis can be a very useful tool for modeling scenarios in which system states change cyclically with time. It may be used for availability estimations, particularly for systems subjected to periodic testing and maintenance as well as a failure and repair cycle [92IAE].

The assumption of a **Markov** process, in which the probability of changing states depends only on the initial and final states allows major simplification of the differential equations. Solutions must generally be found by iterative, numerical methods. For analyzing the reliability of real systems, Markov methods remain a very laborious tool. In PSAs for nuclear power plants, Markov models have only been used for complementing fault tree analysis in some specific contexts [91Hau].

2.4.3.3 Data for assessment of frequencies

Data assessment and parameter estimation to calculate frequencies are concerned with the analysis of three major categories of data:

- initiating event data,
- component failure, repair, test, maintenance and common-cause failure data (see Sect. 2.4.3.4) and
- human error data.

In the case of **initiating events** the data required are the number of occurrences of specific events and the total periods over which these events have been observed. Sources of such data are licensee event reports and plant log books. If plant-specific data are not sufficiently available, frequencies may be taken from generic lists or databases.

To reduce the number of event trees needed to pay regard to all initiating events, the events must be grouped. All initiating events in a given group would require the same set of system actions. In this context it is very important that the rationale for such a grouping is clearly stated, because it must be based on the expected plant response and cannot be generalized. As an alternative way, logic models like fault trees are sometimes used for quantifying initiating events.

The objective **component reliability** assessment is modeling component failure, as well as repair, including unavailability due to component testing and maintenance. In general, reliability models estimate the probability that a component will not perform its intended function. The models depend on the mode of operation of the system (operating, standby, maintenance) to which the components belong; the following parameters are of interest:

- failure rate (operating/standby, per hour), λ_0, $\lambda_{s;}$
- averaged unavailability (per demand);
- test interval and duration, T, τ;
- mean time to repair, T_R.

Table 2.3 summarizes component unavailability expressions for online systems and standby systems.

2.4.3.4 Treatment of dependences

The failure-concurrent events A and B are said to be dependent if their frequency cannot be expressed as the product of their unconditional frequencies. Dependence between events A and B leads to: $P\{A \text{ and } B\} > P\{A\} \cdot P\{B\}$.

The consequences of such dependences may be severe if they affect redundant components or systems occurring simultaneously or within a short time interval. A well-known example of dependent failures are those of two or more similar or identical redundant components due to a single shared cause, e.g. two pumps driven by a common circuit or generator. They are referred to as **common-cause failures** (CCF). A more detailed categorization includes [95Hir]:

- common cause initiators (errors of design, construction or maintenance; internal or external events);
- functional dependencies (following from the plant design);
- shared equipment dependencies (same components, subsystems or auxiliary equipment);
- physical interactions (due to environmental stresses as heat, humidity, missiles, etc.);
- dependencies caused by human actions.

Dependences should be explicitly represented in the logic models, e.g. in the event trees and fault trees. Several types of failures must be distinguished in this context:

- failures which can only be detected in case of a real demand;
- failures which can be detected either after test or real demand;
- self-announcing failures.

The last two types of common-cause failures are detected during the normal operation of the plant, and therefore in principle data can be taken from operating experience. Failures which occur or can be detected only in case of a potential accident must usually be predicted using analytical methods. The potential occurrence of such common-cause failures may remain undetected if operational requirements or usual functional tests are not representative for accident conditions.

The quantification of common-cause failures is difficult, because observations are normally scarce. Only a small fraction of component failures are dependent failures, and common causes which have been detected are usually eliminated with the result of a very small probability for similar failures.

Table 2.3. Component unavailability expressions for online and standby systems [92IAE].

Component type/ unavailability mode	Time-averaged unavailability expression	Parameter definitions		Data requirements for parameter estimation
Non-repairable component	$1-e^{\lambda_0 T_M}$	λ_0	Operating failure rate	Number of observed failures Total time to failure
		T_M	Mission time (obtained from success requirement)	
Online repairable component	$\frac{\lambda_0 T_R}{1+\lambda_0 T_R}$	T_R	Mean time to repair	Observed individual times for repair
Tested standby components				
Hardware failure	$1-\frac{1-e^{-\lambda_s T}}{\lambda_s T}$	λ_s	Standby failure rate	Number of observed failures Total component standby time
		T	Component test period	
Test outage	$\frac{\tau}{T} q_0$	τ	Average test duration	Observed test durations (if applicable) obtained from system analysis
		q_0	Override unavailability	
Repair outage	$\lambda_s T_R$	T_R	Mean time to repair	Observed individual times for repair and maintenance, respectively, including detection and waiting time
Scheduled maintenance	$f_m T_m$	f_m	Scheduled maintenance frequency (includes interface maintenance)	
		T_m	Mean time of scheduled maintenance action	
Untested standby component	$1-\frac{1-e^{-\lambda_s T_p}}{\lambda_s T_p}$	T_p	Fault exposure time	Inferred from replacement times of component due to other failures or if not replaced then assume $T_p = 40$ years
Monitored standby component	$\frac{\lambda_s T_{W,R}}{1+\lambda_s T_{W,R}}$	$T_{W,R}$	Mean waiting time plus repair time	Observed waiting and repair time

If operating experience is not sufficient to quantify common cause failures directly, parametric models can be used. By introduction of suitable factors the multiple failure probabilities can be related to the total component failure probability. In the specialized Marshall-Olkin model (or binomial failure rate model) it is assumed that the system's units are identical, or at least similar so that the total failure rates depend only on the number of units failed. Common-cause events are assumed to hit the system at random times; each unit has the same probability p of failure. Given such a shock, the number of failed units is binomially distributed with parameters m (degree of redundancy) and p. The model provides not only a common-cause failure rate estimated from operating experience, but also a parameter describing the degree of coupling between redundant components (Fig. 2.7).

A comprehensive set of methods for performing quantitative dependent failure analysis are presented in [88NRC]. For results of comparative analyses of methods and data and significant insights see [87CEC], [99NEA].

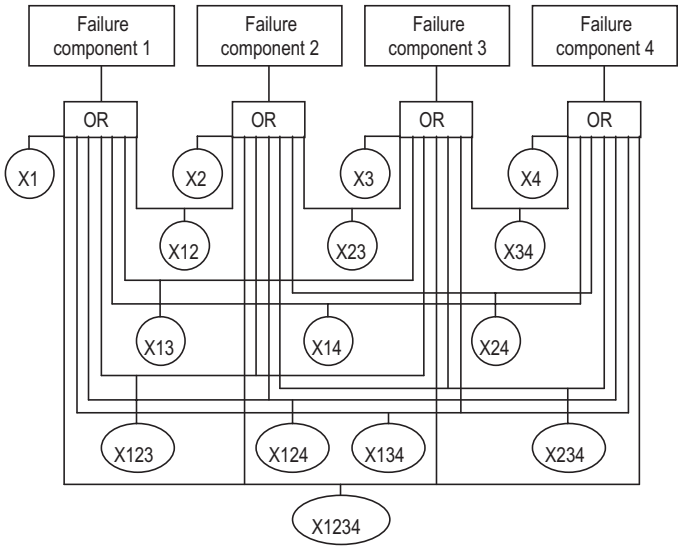


Fig. 2.7. Subtree of a 4-fold redundancy group showing all common-cause failure combinations for the Marshall-Olkin model (for illustration).

2.4.3.5 Human actions and reliability

Human actions can affect the operation and safety of nuclear power plants in various ways. It is therefore important to integrate them adequately into the PSA by **Human Reliability Analysis** (HRA) of which the main objectives are

- the systematic identification of all relevant human interactions and the incorporation into the safety analysis in a traceable manner, and
- the quantification of the success and failure probabilities.

Human interactions can affect both the cause and the course as well as the frequency of an event sequence. They can take place before, during or after the initiation of an event sequence and can either mitigate or exacerbate an accident. Consequently, the human reliability analysis, as it is practice in PSA, addresses in general three categories of actions [92IAE]:

(1) Category-A actions that cause equipment or systems to be unavailable in case of demand. Errors connected with these actions are modelled in a system level fault tree as one or more basic events.
(2) Category-B actions that either by themselves or in combination with equipment failures lead directly to initiating events/faults. They are integrated into the PSA by including them as initiating events and system unavailabilities caused into event/fault trees, respectively.
(3) Category-C post-initiator actions can be separated into three different types regarding their incorporation into PSA:

(a) Type 1: Procedural safety actions, which involve success or failure in procedures or rules to be followed in response to an accident situation. They are incorporated explicitly into fault/event trees.
(b) Type 2: Aggravating actions, also referred to as **errors of commission**, which are very difficult to identify and model. A first sub-type of such actions can occur if the operator's mental image of the plant differs from the actual state, leading the operator to perform the right action for the wrong event. Another sub-type action occurs when the operator correctly diagnoses the event, but chooses a non-optimal strategy for dealing with it. Only a few PSAs have attempted to include this type of post-initiator actions, and only to a limited degree. Very few data are available for their prediction.
(c) Type 3: Recovery/repair actions (accident management) are generally only taken into account if they are dominating risk contributors and if they are well defined, documented and rehearsed. They may include the recovery of previously unavailable equipment or the use of non-standard procedures to ameliorate accident conditions. Such actions are incorporated explicitly into fault trees/event trees.

The process of incorporating human reliability analysis into PSA can be separated into five basic tasks after definition of its scope and approval [92IAE]:

(1) screening (identification of relevant human interactions);
(2) qualitative analysis (detailed description of the most important human interactions and of key influences –"performance shaping factors");
(3) representation (modeling of human actions in logic structures);
(4) quantification (application of data and methods to assign probabilities);
(5) documentation (providing necessary information in a traceable, understandable and reproducible form).

Many methods for the **quantification** of human error probabilities have been developed over the years. Overviews and reviews can be found for example in [89IAE2], [98NEA]. Three main classes of methods can be distinguished:

(1) Methods using decomposition of operator tasks to a level of actions for which basic data are available and can be adjusted according to the special conditions of the respective task (e.g. THERP [83Swa], ASEP [87Swa], Heart [88Wil]).
(2) Time-dependent methods based on the assumption that human error is mainly a function of the time available to perform a task (e.g. HCR [84Han], PHRA [90EPS]).
(3) Methods making direct use of expert judgment techniques (e.g. INTENT [92Ger], APJ [83Sea], SLIM [86Emb]).

Most of these quantification methods attempt to account for the effect of performance shaping factors (PSFs) on human performance [84SHA]. The adequate treatment of such influences is a key problem of HRA, because some of the factors affect a whole task or a whole procedure, whereas others affect certain types of errors, and still other PSFs have an overriding influence on all types of error in all conditions. Combinations of PSFs are taken in current methodological developments to describe the situational context which is used to identify errors of commission [96ATH, 00ATH].

A frequently used decomposition technique is Theory of Human Error Prediction (THERP) which is particularly useful for the quantification of tasks in routine and abnormal operation that are performed by following a written or memorized procedure. The THERP Handbook [83Swa] provides tables that list different kinds of errors for typical actions required in the context of nuclear power operation. Time reliability curves (Fig. 2.8) are included in some models to assess the probability that a correct diagnosis is not done within the time available.

Combinations of several HRA methods can be found in current PSAs. The willingness of the operators to perform well is assumed in all models.

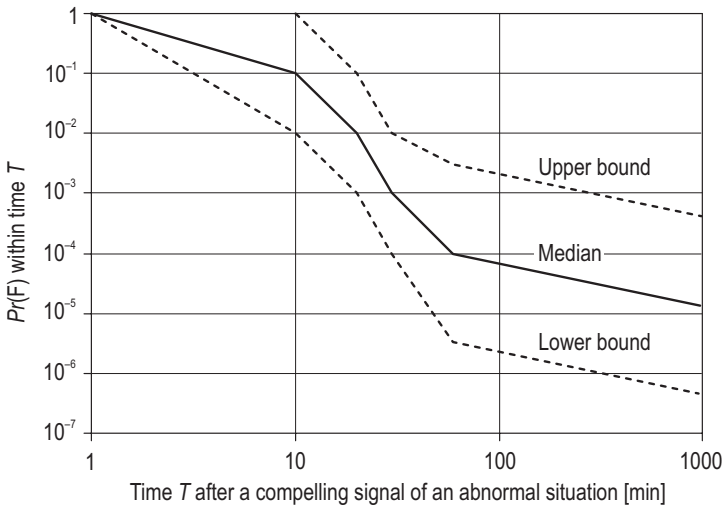


Fig. 2.8. Nominal model of estimated human error probabilities *Pr*(F) and uncertainty bounds (depending on knowledge and training) for right diagnosis within time *T* by control room personnel.

2.4.4 Level-2 PSA

In addition to a Level-1 PSA, focusing on event sequences that can lead to core damage, a Level-2 analysis addresses the phenomena involved in the course of a core damage accident. It also includes the containment function, that is the response of active (closure) systems and of the structure to expected loads, and the transport of radioactive substances from the core to the environment. The interface between the two PSA levels [95IAE1] is provided by grouping Level-1 event sequences with similar effects on containment response and on fission product behavior into plant damage states (PDS, see Fig. 2.4). Examples of important attributes are:

- type of initiating event (loss of coolant, transient or external events);
- status of reactor coolant system at core damage (high/low pressure);
- status of emergency core-coolant system, resulting in early or late core damage or melt-down;
- containment status (isolated/unisolated, failed (mode, time), bypassed (type, size)).

For each of these plant damage states, containment event trees are constructed (Fig. 2.9). These trees provide a structured approach for systematic evaluation of containment capability in coping with severe accidents. They are able to present the identified event chains in sequential order and allow probabilistic quantification. Phenomena of complex physical and chemical processes which are to be considered in this context can be grouped into two categories [95IAE1]:

(1) Phenomena associated with the thermal hydraulics of the accident progression and the associated containment response. These phenomena range from hydrogen generation and core material relocation during the in-vessel phase to ex-vessel steam explosions, interactions between core material and containment structures as well as containment failure modes.
(2) Phenomena associated with the chemical processes affecting the radionuclides during the accident and the potential transport of radioactive material from the fuel through the containment to the environment. Phenomena relevant in this context are inventories of radionuclides, chemistry of isotopes, in particular iodine, aerosol behavior and deposition as well as relocation effects.

The determination of conditional probabilities for the quantification of containment event trees are based on calculations and analyses of varying complexity, using deterministic and parametric computer codes, engineering judgment (for phenomenological questions) and systems analysis codes to assess the availability of active systems.

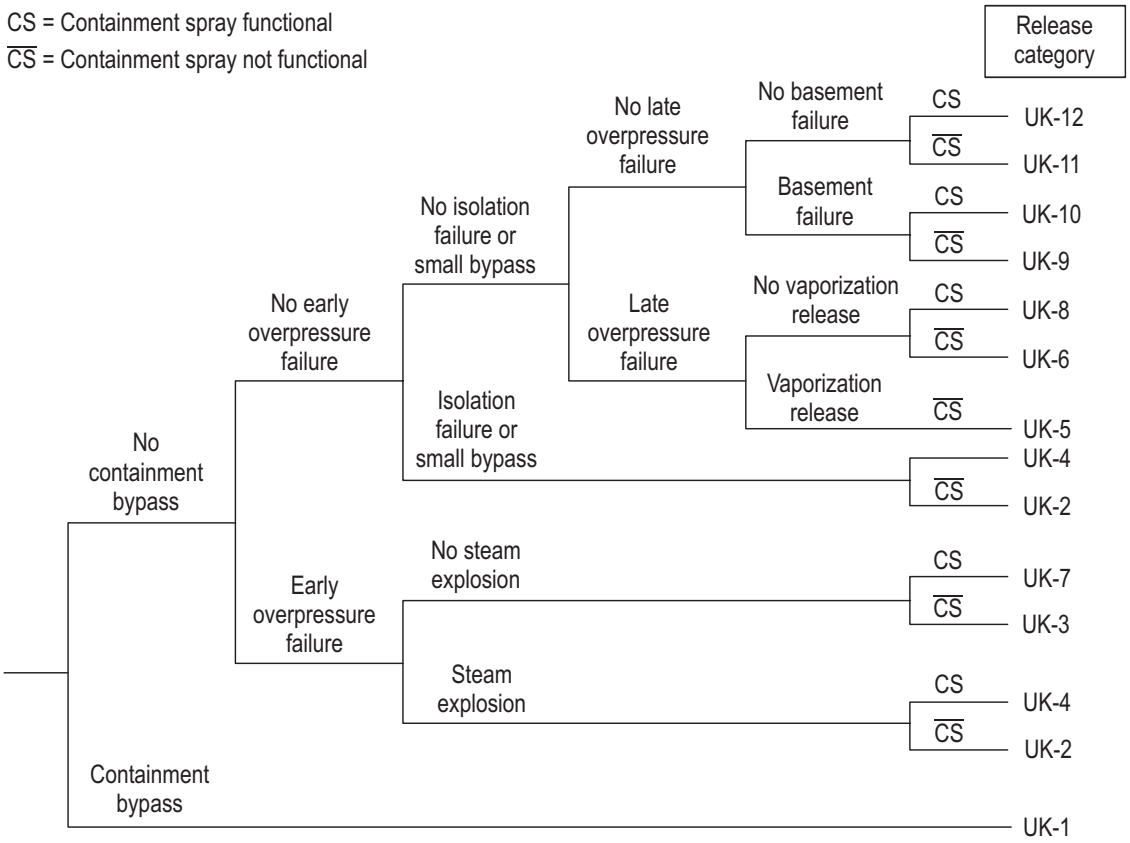


Fig. 2.9. Simplified event tree for source term characterization [82Git].

The containment matrix (Table 2.4, [95IAE1]) provides the conditional probability $C(m,n)$ that a release bin n will occur, given a plant damage state (PDS) m. Tabulation of the containment event trees in form of a containment matrix is very useful in showing the main failure modes and/or release categories for each PDS. Generally, for each of the selected release categories, one representative plant damage state is selected for which a source term is estimated. The selection of the PDS is governed by its frequency and consequence dominance within the release category.

Source terms are defined to describe the quantity of fission products released from the plant[5] as a function of time, including information on the location and the associated energy releases. In [82Git] for example (see Table 2.5) category UK-1 is used for accident sequences in which a bypass pathway exists from the primary circuit to the environment; UK-2 is used for early over-pressure failure of the containment with a source term reflecting a steam explosion; UK-5 describes a late over-pressure failure of the containment and the loss of core debris cooling resulting in vaporization releases.

For the calculation of source terms, attention must be given to different possible releases from the fuel, to different behavior of fission products within the primary circuit and to different fission product deposition and resuspension within the containment. Fission products are grouped according to their chemical and physical characteristics.

[5]) Usually given as fraction of the original core inventory; see Sect. 2.8.1 for values typical for a 1250 MW (el) PWR.

Table 2.4. Containment matrix elements, where $C(m, n)$ denotes the conditional probability of release bin n, given PDS m.

Plant damage state (PDS)	Release bin						PDS frequency
	1	2	·	n	·	·	N	
1	$C(1, 1)$	$C(1, 2)$	·	$C(1, n)$	·	·	$C(1, N)$	$F(1)$
2	$C(2, 1)$	$C(2, 2)$	·	$C(2, n)$	·	·	$C(2, N)$	$F(2)$
·	·	·	·		·	·	·	·
m	$C(m, 1)$	$C(m, 2)$	·	$C(m, n)$	·	·	$C(m, N)$	$F(m)$
·	·	·	·		·	·	·	·
M	$C(M, 1)$	$C(M, 2)$	·	$C(M, n)$	·	·	$C(M, N)$	$F(M)$
Bin frequency =>	$R(1)$	$R(2)$	·	$R(n)$	·	·	$R(N)$	

Table 2.5. Selected release categories and source term values [82Git]. Note: 1 Btu/h = 0.29 W; 2.4 (–9) means 2.4×10^{-9} per reactor-year.

Release category, description and frequency	Release characteristics					Release fractions of core inventory			
	Release starts [h]	Duration [h]	Warning time [h]	Energy [MBtu/h]	Height [m]	Xe-Kr	I	Cs-Rb	Ba-Sr
UK-1 Containment bypass 2.4 (–9)	1	3	0	0.3	10	9(–1)	7(–1)	5(–1)	6(–2)
UK-2 Early containment failure Steam explosion 4.0 (–10)	1	0.5	0	20	10	9(–1)	7(–1)	4(–1)	5(–2)
UK-5 Late containment failure Vaporization release 8.0 (–9)	8	0.5	4	20	10	1(0)	6(–2)	3(–1)	4(–2)
UK-6 Late containment failure No vaporization release 4.2 (–9)	12	0.5	8	20	10	9(–1)	9(–3)	2(–1)	2(–2)

2.4.5 Level-3 PSA

Level-3 PSA completes the results gained in Level-1 and -2 analyses by expressing the extent and likelihood of adverse effects, e.g. health impacts, contamination of land and foodstuffs and financial losses. Moreover, a Level-3 PSA not only provides insights into the relative importance of accident prevention and mitigation measures for public risk but also assesses the effectiveness of off-site accident management. It integrates seamlessly with Level 2 by assessing the dispersion of the released radioactive substances to air, water and soil, followed by the determination of human doses and the derivation of subsequent effects including the effects of countermeasures.

The assessment of releases to the atmosphere has historically been the principal concern, because releases to the aquatic and terrestrial environment add a comparatively small contribution to the overall risk of nuclear power plants. The quantity and isotopic composition of released radionuclides, together with the release conditions, are described by the source term. Not all of the radioactive nuclides do contribute equally to the consequences. Therefore in practice the radioactivity released from the core is described by a set of representative isotopes which each serve as surrogate for a group of substances with similar properties. The appendix (Sect. 2.9) provides an overview of the most important codes and their major features as well as the source terms used. Further references on atmospheric dispersion and deposition can be found in [96IAE].

All subsequent factors like meteorological conditions, the surroundings of the plant as well as emergency response actions must be considered and where appropriate are reflected by weighting them according to their conditional probabilities of occurrence (see Fig. 2.10). The computer programs used for the calculations are referred to as probabilistic consequence analysis (PCA) codes which were subject of a joint NEA/IAEA comparison exercise [94NEA].

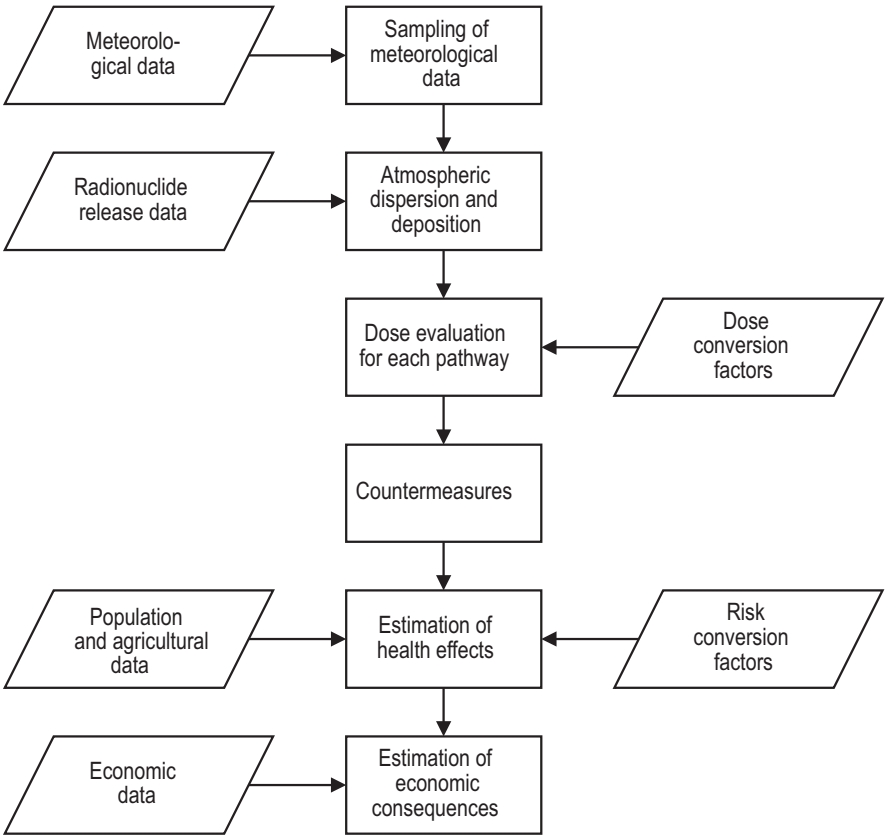


Fig. 2.10. Basic elements of probabilistic consequence assessment [96IAE].

People can accumulate radiation doses after an accidental release of radioactive substances by five principal pathways (see Fig. 2.11):

(1) external irradiation from the passing plume or cloud, referred to as "cloud-shine";
(2) external irradiation from material deposited on the ground, referred to as "ground-shine";
(3) external irradiation from material deposited on skin and clothing;
(4) internal irradiation from material inhaled from the passing plume or following resuspension of the ground deposit;
(5) internal irradiation after ingestion of foodstuffs contaminated by deposited radioactive material.

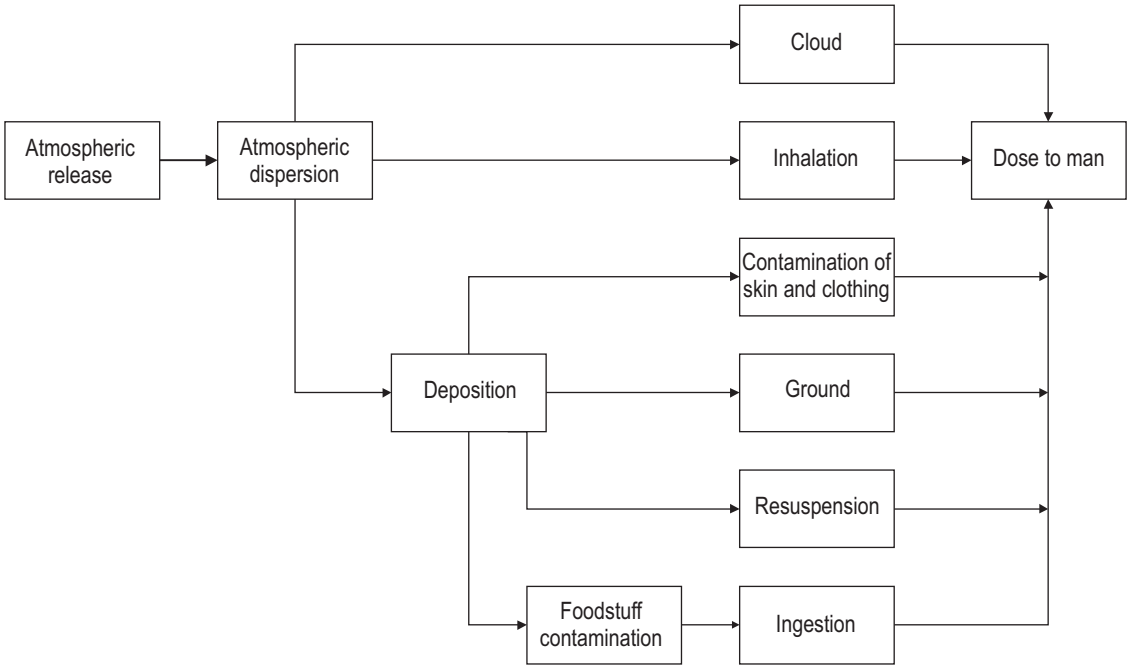


Fig. 2.11. Principle exposure pathways to man following an atmospheric release [96IAE].

It is necessary that PCA codes be adapted to cultural habits in their modeling of uptake of radioactivity into the body. Even within societies ingestion pathways may depend on age, local realities and other influences. In many of these situations conservative assumptions should be applied to assure that the ingestion models do not underestimate the actual dose.

The health effects caused by radiation differ in nature: acute effects are deterministic and result directly from exposure while latent effects are stochastic and appear with delay. Deterministic health effects include burns of the skin, radiation sickness and grey cataracts. Typical stochastic effects are latent effects like leukemia, tumor initiation or genetic damages. In principal, cancer cases induced by radiation cannot be distinguished from cancer forms with a high spontaneous incidence rate in the population.

Both classes of health effects are taken into account through dose-effect/risk relationships. Since acute effects are caused by relatively high doses – first effects are observed above a threshold value of 0.2…0.5 Sv and the lethal dose for 50 % percent of a population (LD_{50}) lies between 4…5 Sv – they occur if at all only in the vicinity of the plant. Therefore the surroundings of the plant (to a radius of about 20 km) are modeled by use of actual local weather and population data. Beyond the area where acute effects are to be expected, data of more generic nature such as average population densities can be sufficient for the determination of stochastic effects. If there is no deterministic end distance assumed for these effects (e.g. 800 km) the effects are calculated down to populations receiving very low doses (< 100 mSv).

The dose-effect-conversion model applied today is referred to as the Linear-No-Threshold Model and is still under debate. This model assumes for latent effects a linear relationship between dose and effect of 5 % per Sv [90ICR]. As the question on dose-effect conversion factors for relatively low doses still waits for scientific clarification, it has been declared that this relationship is valid down to very low doses. These assumptions have a strong effect on the number of latent fatalities accounted for in the consequence estimation.

PCA codes have the potential to evaluate the effectiveness of accident management and emergency response actions, like sheltering, thyroid blocking, evacuation and relocation, and foodbans. Many of these actions have been proven to have positive effects on the course of events in the case of accidental releases. The doses triggering them are calculated in a deterministic manner to assure conservative results and the countermeasures come into action once specific intervention levels are reached.

The focus of consequence assessment is naturally on human health effects which are expressed by both early and late fatalities. This is done for both collective and individual risks. Modern, more sophisticated codes provide the possibility of calculating a variety of additional adverse consequences like:

- amount of crops to be banned,
- number of livestock affected,
- number of people to be relocated (temporarily and permanently),
- area of land and infrastructure interdicted or condemned,
- costs of countermeasures and cleaning options.

The results are typically presented in the form of so-called Frequency/Consequence (F/C) Diagrams with double logarithmic axes (see Fig. 2.12). This kind of representation of results has, unlike the expected value or expected disutility of the consequences, the advantage that no additional rule how to combine the two components of risk (frequency and consequence) needs to be introduced. The number of units of the investigated damage indicator is placed on the abscissa while the ordinate shows the corresponding frequencies. Instead of a pure frequency distribution the complementary cumulative distribution function (CCDF) over the possible range of damages is normally given. This enhances the interpretation of the diagram because for a given degree of damage the sum of all sequences leading to at least this amount of damage follows immediately from the associated frequency value on the ordinate. One problem with the representation of the results is the appropriate cut-off criterion for the frequency axis. In order to assure that all scenarios leading to a significant contribution to the consequences are taken into account even those with very small likelihood should be represented. This conflicts with the validation of very small values of frequency. The actual cut-offs encountered in F/C Diagrams therefore are the product of consensual agreement which among other factors takes into account the shape of the curve (obvious drop of curve).

In general not only the curve for the mean frequency values but also the curves denoting the 5th percentile, 50th percentile (median) and 95th percentile of the distribution over that mean are given. For a given extent of damage these values can be seen by vertical interpretation of the uncertainty bands (horizontal interpretation of the bands is not correct). Thus the variation along a curve is indicative of the variation in risk due to different types of accidents (source terms) and due to weather conditions at the time of the accident while the variation from the 5th to the 95th percentile indicates the uncertainty estimates due to uncertainty in the basic parameters in the analysis of plant damage state frequency, accident progression and source term. Until now there is no analogous treatment of uncertainties in the consequence analysis. Variability in the weather is fully accounted for, but the uncertainty in other parameters, e.g. the dry deposition speed or the evacuation rate, is not considered.

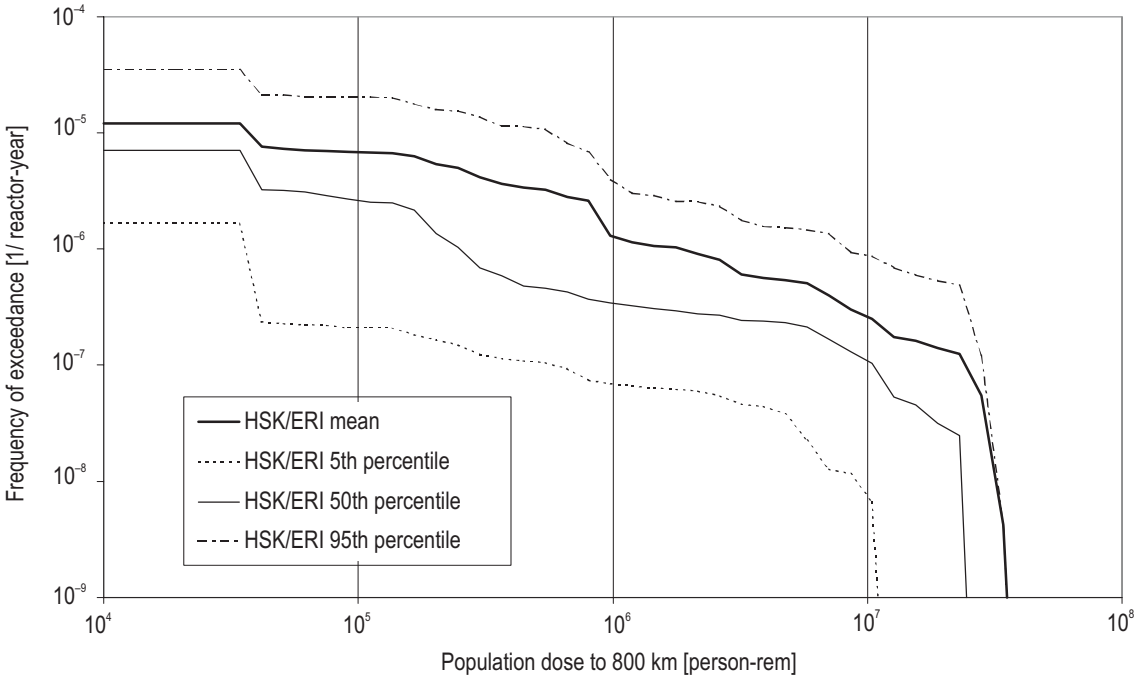


Fig. 2.12. Frequency of exceedence (CCDF) of population dose to 800 km for the Swiss NPP of Mühleberg [93Caz2].

2.4.6 PSA codes

Many computer codes and code systems for **system and reliability analyses** have been developed over the years (see [99Ful]). Recently, combined systems of personal computer codes (suites) have been provided. For example, SAPHIR [94Rus] includes programs for database handling, construction and quantification of fault trees and event trees including minimal cut set generation, cut set management, and graphical editing. Examples of other appropriate codes are RiskSpectrum [98Rel] and PSAPACK [95IAE2]. A compilation of computer codes for Level-1 PSA is provided in [89IAE1].

The codes which model the **phenomenology of severe accidents** (Level 2) are divided into three types according to their capability and intended use [95IAE1]. Deterministic codes attempt to model the phenomena in as much detail as possible and are used typically in severe-accident research. So-called PSA codes use correlations, are designed to run faster and permit to do calculations for many sequences. Simple parametric codes interpolate between fixed points for which calculations with a more complicated code have been performed to determine the values of parameters. An example for a widely used code system is MELCOR [91Sum] developed by SNL for the US NRC. MELCOR is an integrated, relatively fast running code which uses parametric models only in areas with great uncertainties and without consensus concerning an acceptable mechanistic approach. A broad spectrum of severe-accident phenomena in both PWRs and BWRs is treated in a unified framework. Other code systems and a list of some key mechanistic codes can be found in [95IAE1].

There are a number of codes (packages of programs and databases) in existence worldwide that contain all the necessary elements of a **consequence** model and perform the probabilistic manipulations needed for the calculation of CCDFs. Examples of the current generation of probabilistic consequence analysis (PCA) tools include ARANO, CONDOR, COSYMA, LENA, MACCS and OSCAAR (see Sect. 2.4.5 and Sect. 2.9.1).

2.4.7 Treatment of uncertainties

The quantification of the uncertainties of results is an integral part of PSA and comprises three tasks [91Hau]:

(1) Determination of uncertainties in the physical and probabilistic models, including
   – uncertainties of the values of parameters (data), most readily quantifiable at present;
   – modeling uncertainties due to simplified assumptions of models, coped with by sensitivity analysis;
   – uncertainties regarding the completeness of the analysis. (Although a tremendous set of initiators and event sequences are usually analyzed there is no guarantee or mathematical proof that all have been identified and properly assessed.)
(2) Propagation of the (data) uncertainties through the steps of the analyses to the final result, calculating confidence regimes or fractiles by use of analytical or mostly (Monte Carlo) simulation techniques.
(3) Presentation and interpretation of the uncertainties by giving mean/median values and uncertainty bounds (see Fig. 2.12).

Methods for quantifying uncertainties are best developed for the investigation of internal event sequences (Level 1). Results are stated as confidence intervals derived from distribution functions. The uncertainties of the analysis of hazardous plant conditions, of resulting containment loads and of containment failure modes are even larger, and new kinds of uncertainties are added by calculating the transport of radionuclides in the environment and their effects. Such uncertainties are sometimes estimated by expert judgment. Sensitivity studies are usually performed to assess their (relative) importance; it is also possible to quantify a part of these uncertainties through formal uncertainty analyses [99Ful].

2.4.8 Expert judgment

As described before, a PSA is based on reliability models of the safety systems and on physical models describing various phenomena. Owing to existing uncertainties, expert judgment (EJ) is inevitably encountered [99Coj] in this subject. Firstly, most of the models are based on engineering assumptions to some extent. Moreover, the selection of input parameters requires judgment due to inadequate empirical or statistical data, and even the choice between several models is done on the basis of judgments.

To deal with EJ and to understand its impact on results, it is important that expert judgments are made explicitly. Discussing the application of EJ used in NUREG-1150 [90NRC], it was recognized that the disciplined use of expert opinion elicitation was an important advance over informal methods of using expert opinion [99Coj].

Various techniques to structure and carry out EJ have been proposed [87Mos], [91Coo]. Behavioral approaches can be taken to derive a single consensus probability distribution from multiple expert assessments. Alternatively the aggregation of judgments can be done on mathematical basis; indeed numerical judgments can be aggregated on an equal weight basis [89Hor], using Bayesian updating techniques [84Mos], or on a performance-based weighted basis [91Coo].

2.4.9 Team expertise and quality assurance issues

The **expertise** needed to conduct a PSA must include detailed knowledge of the plant on one hand and of PSA techniques on the other hand. Walking through the plant is necessary in order to get reliable information about the design, site and operation conditions. Even if team members have some expertise, it is strongly recommended by the IAEA [92IAE] that some training precedes a study in order to achieve a common understanding of the objectives, procedures and methods of the PSA. The main issues should include comparative reviews of PSAs of similar plants.

The required team composition [92IAE] consists of system analysts (8…10), PSA methodologists/quantification specialists (3…4), human reliability analysts (1…2), data analysts (1…2) and external

hazard analysts (2). Some of the these personnel may not be required for the complete duration of the study or may be involved in more than one task.

Quality assurance (QA) procedures are implemented to obtain a PSA which is credible and which meets the objectives and fills the initial scope. QA procedures apply to the technical work, ensuring consistency between goals, scope, methods and assumptions, as well as accuracy in the application of methods and in calculations.

An important issue related to QA activities is that of interactive, independent peer review. A review report should consist of the following parts to address the concerns of external users:

- background information such as a brief description of the plant considered, organizations involved in the PSA, purpose, objective and scope of the PSA and objectives of the review;
- conclusions of the accurate implementation of the methodologies used;
- final conclusions on the adequacy of the study, results and their associated uncertainties as well as results of sensitivity analysis, and recommendations, if any.

Specific guidance on peer review is given in [90IAE]. Since 1988, the IAEA provides the International PSA Review Team (IPSART) which brings international PSA experience into the review process.

2.4.10 Data collection

The methodology used in PSAs is complex, and assumptions need to be made to assess the plant behavior. Reliability data, which are an important element of PSAs, must be of high quality, and plant specific data are especially needed. Therefore operational experience is needed for checking the assumptions and for providing the data used in the analyses.

For these purposes it is important to collect information on abnormal events with safety significance occurring at plants during operation, surveillance and maintenance activities, including deviations from the normal performance of systems, or personnel errors which all may be regarded as precursors of serious accidents [89IAE2]. Important examples of data collection activities are the following.

To improve the international exchange of operational experience, the IAEA has established an **Incident Reporting System** (IRS, [98IAE]). The system is jointly managed by the IAEA and the NEA/OECD. All 31 of the member states with operating nuclear power plants participate in the IRS, and almost 2800 event reports are now in the database. The annual number of reports in recent years has varied from nearly 100 to more than 140. The system provides a pre-processed set of data increasing the awareness of actual and potential safety problems [99IAE3].

The mission of the World Association of Nuclear Operators (WANO) includes an **Operating Experience Information Exchange** program to collect, screen, analyze and distribute event data relevant to safe operation. Since 1991 WANO's member utilities have reported data on plant performance, reliability and operational safety to a common database. To make data readily available, WANO's member utilities and regional WANO centers are linked by a computerized data system.

The **International CCF Data Exchange** (ICDE) project was initiated in 1994 and is operated under the umbrella of OECD/NEA. The objectives are [99NEA]

- to collect and analyse CCF events in the long term so as to better understand such events;
- to generate qualitative insights into the root causes of CCF events which can then be used to derive approaches or mechanisms for their prevention or for mitigating their consequences;
- to establish efficient feedback of experience gained on CCF phenomena, including the development of defences against their occurrences, such as indicators for risk-based inspections.

The project covers key components of the main safety systems, like centrifugal pumps, diesel generators, and different kinds of valves.

2.5 PSA applications and results

2.5.1 Status of PSA activities

The estimation of risks caused by the operation of nuclear power plants was pioneered by the Reactor Safety Study [75RSS]. The aim was to provide a basis for a comparison with other man-made and natural risks.

Recently, probabilistic analyses of different scope have also been used directly in licensing and supervisory activities. For example, the US NRC demanded an update of the safety reports of all US NPPs within the context of the Individual Plant Examination [97NRC]. In Germany, Periodic Safety Reviews (PSRs) are carried out every ten years for all NPPs in operation, based on a voluntary self-commitment of the utilities. Similar practices can be found in other countries.

At present, PSAs are applied by utilities to an increasing degree for the optimization of plant operation with regard to cost and safety factors. Probabilistic assessments of real events ("Precursor Analyses") are carried out to calculate the remaining safety margins, to assess their safety significance and to verify the methods and results of PSAs. The so-called Living PSA provides a current model which can be used to evaluate the merit of potential modifications (plant design, operational aspects, maintenance or tests) and to monitor risk substitutes.

To assess whether the public risk of a nuclear power plant is acceptable, ultimate safety goals are required. Such goals can be set as technical safety objectives, e.g. for the core damage frequency (CDF), for which a Level-1 PSA is sufficient to demonstrate compliance, while a Level-2 PSA is needed for a source term criterion, e.g. the Large Early Release Frequency (LERF). A Level-3 PSA must be carried out, if goals on individual or public risk need to be met.

Table 2.6 summarizes PSA activities and applications in selected countries. The most important conclusions drawn for Europe are:

- A PSA for operating nuclear power plants is required by the regulatory body in most of the countries. Detailed reviews are carried out in all countries.
- PSA studies are generally required as part of a periodic safety review for operating reactors. For new power plants they are required in the course of a pre-operational licensing process or design certification.
- In general Level 1 PSA studies are carried out. Level-3 PSA studies have been performed in some countries (GER (Biblis B, 1979), NL (Borssele, Doodeward, 1994), UK (Sizewell B, 1982)). Modeling of external events in addition to plant internal initiators and of plant states besides the full power generation state has been performed in some studies.
- PSA procedures guidelines have been produced in Germany [97BfS] and the Netherlands. In other countries PSA procedures are discussed with the regulator bodies at an early stage of studies.
- There are no rigid criteria for plant damage frequencies in any country, although guidelines for an upper limit to the core melt frequency are used in the Netherlands and will be used in the UK for future plants. In Germany there are guidelines for an upper limit to the frequency of core damage accident sequences. Targets for off-site dose or risk, or the frequency of significant radioactive release, are set by regulators in the Netherlands and in the UK.
- PSA results are used to different extent to improve deterministically derived technical specifications and emergency procedures, to support cost-benefit analyses and to compare the risk from different reactors.

In summary, PSA methodology is highly recognized and widely used as a tool for comprehensive plant analysis and estimation of risk attributes. As the effort and uncertainties involved increase from level to level, PSA applications are usually restricted to the first level. Therefore, numerous results of Level-1 PSA are available which allow cross comparisons and some general conclusions. They should be dealt with caution as the basic results are subject to many differences in methods/models, data, etc. as well as in the degree of sophistication.

In general, core damage frequencies (CDF) are taken as key indicator for plant design quality and risk. CDFs vary – with a few exceptions – from 10^{-4} to 10^{-6} per reactor-year. Considerable design improvements of analyzed plants have already resulted during the analyses or afterwards based on adverse findings.

Table 2.6. Scope, practice and status of PSAs for light water reactors [94EUR]. CCI denotes common-cause initiators; Level 1+ means that active containment systems are included, Level 2– is without quantification of source terms.

Country	Scope		Use of Living PSA	Number of NPPs (with PSA)	Level, type of PSA	Guide-lines
	Events	Plant states				
Belgium	internal	all	considered	7 (2)	Level 1+ plant specific	NUREG 2300 etc.
Finland	in- and external	all	yes	4 (2)	Level 1, 2 plant specific	NUREG 2300 etc.
France	internal	all	–	54 (54)	Level 1 plant-type specific	–
Germany	in- and external	other than full power in future	under development	20 (11)	Level 1+, Level 2– (plant specific, DRS B) Level 3 (generic, DRS A)	PSA Leitfaden
Netherlands	in- and external	all	implemented for use	2 (2)	Level 1, 2–, 3 plant specific	based on NUREG 2300
Spain	internal, some external and CCI	all power generation	–	9 (7)	Level 1, 2 plant specific	–
Sweden	in- and external	power generation, shutdown transients	under development	12 (12)	Level 1 plant specific	informal guide
UK	in- and external	all	under development	1 (1)	Level 1, 2, 3 (Sizewell B)	NII principles
Switzerland	in- and external	all	under development	5 (5)	Level 1, 2 plant specific	–
USA	in- and external	all power generation	yes	104 (104)	Level 1, 2 plant specific	NUREG 2300

2.5.2 Results and insights from Level-1 PSA

The information presented below is based on an evaluation of Level-1 results for 8 PWRs and 6 BWRs in different countries [95Wer]. The objective was to compare the results in principle and to identify generic problems, common features and differences in data and methods/models. Referring to the latter, the following can be stated:

- initiating event frequencies depend on (combined) national operating experience and/or on statistical and theoretical approaches, resulting in relatively large differences, esp. for Loss of Coolant Accidents (LOCA);
- realistic success criteria are used for the analysis of the sequences dominating core damage;
- common-cause failures are modeled in all studies, but in different ways and not for the same kinds of components in all cases (pumps, valves and diesel generators in all studies);

– human errors are mostly evaluated using THERP (sometimes SLIM, HCR or ASEP); errors of commission are not considered (with a few exceptions in the French studies);
– recovery actions are included in all studies, but in diverse context and to different extent;
– core damage states are normally taken as undesired events (except in recent German studies, which define hazard states, resulting from the unavailability of engineered safety systems) without taking into account accident management measures.

The core damage frequencies (CDF, mean values) and the associated uncertainty ranges are shown in Fig. 2.13 for PWRs of different design, power size and age, operating in different countries.

The relative contributions of the most important groups of initiating events to the CDF (see Table 2.13) differ from Loss of Off-Site Power (LOSP, max. 69 % Surry) to transients (max. 27 % Beznau) and Loss of Coolant inside Containment (LOCA, 84.5 % Biblis) and indicate a strong dependence on the actual design. In all studies, the significance of measures for prevention of core damage is high. Mostly these measures are applied to failure states associated with degraded heat removal to the secondary side (transients). Therefore, LOCAs often remain as dominant causes for core damage. Owing to design reasons, in some plants the emergency power supply systems (Surry) or the reactor protection system (REP 1300) have the highest risk-reduction importance.

In general, the results of selected PSAs indicate that

– the CDFs for newer plants are about one order of magnitude lower than for older plants (compare REP 800 to 1300), but not without contradictions (compare Westinghouse designs) and great dependence on implemented plant improvements (see Beznau CDF: 2.3×10^{-4} for plant status 1986, 4.4×10^{-6} after major backfits, status 1994);
– the reduction of core melt frequencies in the newer plants is accompanied by a substantial increase of the relative contribution of common-cause failures and a reduction in the relative contribution of human errors (omission of requested action);
– the importance of LOCA events following breaks of different size for the CDFs makes the frequencies of small leaks one of the most important parameter, but current operating experience available today suggests that the LOCA frequencies used in most studies are too high.

The CDFs (mean values) and the associated uncertainty ranges are shown in Fig. 2.14 for different BWRs. Table 2.14 outlines the relative contribution of the most important groups of initiating events to the CDF. For the US plants, the largest contributions to CDF result from LOSP (reflecting the comparably low number of diesels).

Some general observations [95Wer] are:

– The core damage frequencies differ little between older and newer plants, especially if the old plants have been substantially backfitted (Mühleberg has been equipped with a completely independent emergency cooling system); advantages of the newer plants are more redundancies, improved spatial separation of redundant trains and enhanced automation of systems. These features are largely compensated in the older plants by a high degree of intermeshing of systems and by a greater flexibility in using systems for coolant injection and heat removal.
– Owing to the long times and many alternatives available, measures are highly effective to prevent core damage in accident situations that involve the loss of heat removal from the wetwell.

The following insights can be derived comparing studies for Western PWRs and BWRs [95Wer]:

– In general, the core melt frequencies for the BWRs are lower than for the PWRs;
– AM measures are very effective to prevent core damage for both types of plants;
– the highest contribution of common cause failures and the lowest contribution of human errors are observed for the most highly automated plants;
– in the case of LOCA events following small breaks in PWRs, the combined effects of the uncertainties of the initiating event frequencies and of the common-cause failure data strongly influence the numerical results.

The first conclusion is consistent with results from the Individual Plant Examination (IPE) program [97NRC]. In this program 75 analyses (PSAs estimating CDFs and containment performance) are reviewed by the NRC. The average CDFs reported for BWRs are smaller than for PWRs (Fig. 2.15) because of the reduced LOCA vulnerability (more injection systems and better possibilities for depressurization). The variation of CDFs leads to higher values for BWRs than for PWRs in some cases. This is caused by plant design differences, by variability in modeling and by the differences in data used in the quantifying models.

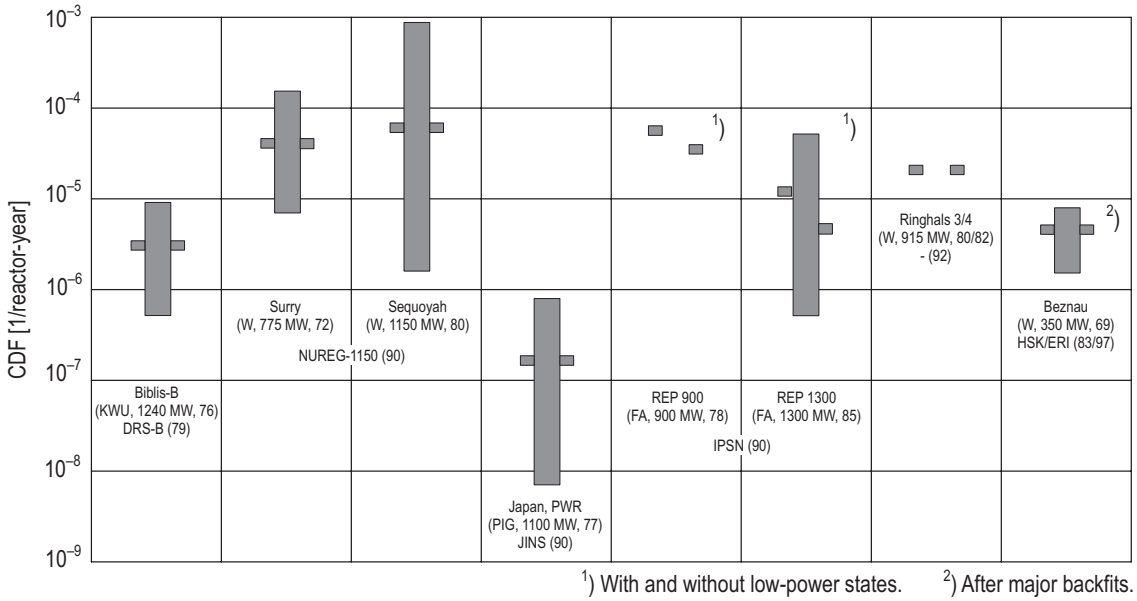


Fig. 2.13. Core damage frequencies (mean and 5 %…95 % confidence interval), PWRs (internal events).

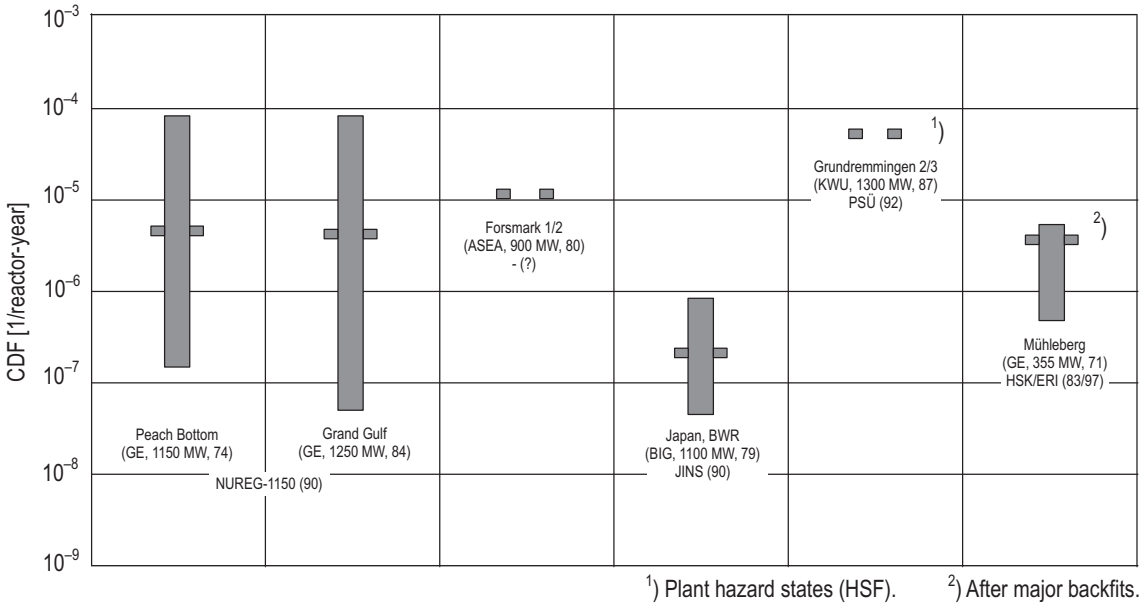


Fig. 2.14. Core damage frequencies (mean and 5 %…95 % subjective confidence interval), BWRs (interval events).

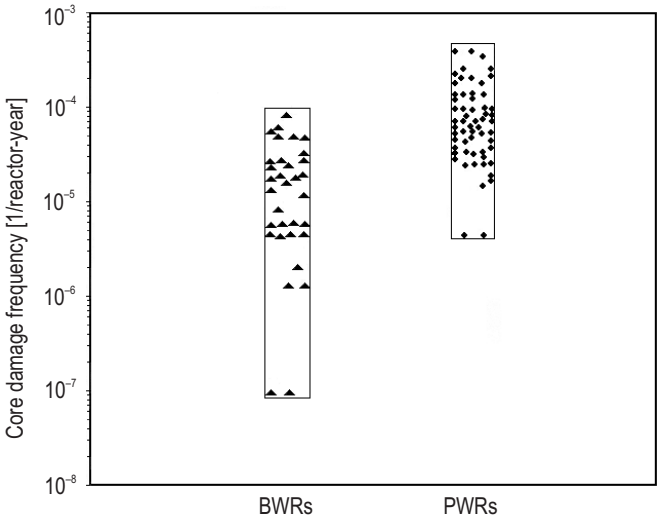


Fig. 2.15. Core damage frequencies from the Individual Plan Examination Program for US BWRs and PWRs.

Besides light water reactors of Western design, 21 nuclear power plants with **PWRs of "Soviet design"** are currently in operation. The WWER (Water-Water Energetic Reactor) follows three basic models: WWER 440/230, 440/213, and 1000 with distinctly different safety features ("generations") but similarities in the design of the operational systems. Meanwhile, modifications have taken place at all three reactor models.

On the basis of the information available, the following compilation of CDFs can be given (Table 2.7). The mean values vary over a wide range. It must to be noted that there is large variability in quality, completeness, and comprehensiveness of the PSAs performed which limits the comparability of the bottom-line results significantly, even for the same reactor design. Several crucial factors need to be mentioned:

- the scope of the study (plant power states, number of initiating events);
- failure data (generic and/or plant-specific) for components;
- approach to human error failure probabilities;
- details of the PSA methods and models (incl. success criteria), technical adequacy of the analyses;
- QA and extent of external review;
- modeling of the plant status (implementation of safety upgrades).

From the review of results and the quality of the PSAs one can conclude that in general the CDFs for Western reactors are lower than those for Soviet-designed reactors because of major differences in design and operation, including the status of improvements of plant safety.

2.5.3 Results and insights from Level-2 PSA

Level-2 results of PSAs for 11 PWRs and 10 BWRs in seven different Western countries have been compared by a NEA/CSNI task group [97NEA]. Fig. 2.16 illustrates for both PWRs and BWRs the calculated frequencies of core damage (CDF), of large release containment failure (LRCF), and of exceeding 10 % release of caesium core inventory, each separated for IPE methodology [97NRC] and other studies. Table 2.15 presents for PWRs the conditional probabilities of containment failure modes (given core damage), the dominant phenomena, and their relative contribution to the conditional probabilities. The table additionally shows frequencies of caesium releases. Corresponding information for BWRs can be found in Table 2.16.

The main insights derived from these 21 studies are [97NEA]:

- The sums of the conditional probabilities of the LRCF modes (given core damage) differ little in the examined studies and are about 0.1.
- For PWRs the largest releases generally result from containment bypass sequences, most notably with unisolated steam generator after preceding tube rupture; failure of containment to be isolated is practically insignificant.
- Releases resulting from LOCA at the high-pressure system/low-pressure system interface have been made extremely unlikely at the plants, owing to improved redundancy/diversity of the high-pressure/low-pressure system isolation and improved maintenance strategies.
- In BWRs with Mark I containment (wetwell surrounding the drywell), there is a potential for early containment failure due to melt-through of the drywell liner. In most studies, the treatment of this issue was connected with large uncertainties; recent research results suggest that the probability of this sequence could be significantly reduced if sufficient quantities of water were available on the drywell floor (e.g. Mühleberg special design).
- The combination of possibilities to flood the containment and of overpressure protection by filtered containment venting leads to low conditional probabilities of early containment failure.

Information about the contribution of external initiating events to the total results of PSAs can be found in Fig. 2.21 and 2.22.

Table 2.7. Core damage frequencies (per reactor-year) for WWERs of different basic design (internal events, for references please refer to Table 2.17).

WWER 440 ($P_{el} \approx 400$ MW)/230			
NPP	Country	Built	CDF [per reactor-year]
Bohunice V1	SK	1978	2.3×10^{-5}
Kola 1, 2	RUS	1973	3.3×10^{-3}
Kozloduy 3, 4	BUL	1980	7.0×10^{-5}
Novovoronezh 3	RUS	1971	2.0×10^{-3}
WWER 440/213			
NPP	Country	Built	CDF [per reactor-year]
Bohunice V2	SK	1980	1×10^{-4}
Dukovany 1	CZ	1985	7×10^{-5}
Loviisa	FIN	1977	1.5×10^{-4}
Paks 1.3	HUN	1982	4.7×10^{-4}
Paks 2	HUN	1984	5.2×10^{-5}
Rovno 1	UKR	1980	9.0×10^{-5}
Mochovce	SK	1998	7×10^{-7}
WWER 1000 ($P_{el} \approx 950$ MW)			
NPP	Country	Built	CDF [per reactor-year]
Balakovo	RUS	1985	5.3×10^{-5}
Kozloduy 5, 6	BUL	1987	3.7×10^{-4}
Novovoronezh	RUS	1980	8.8×10^{-4}
Temelin 1, 2	CZ	2000	8.9×10^{-5}
Zoporozje 5	UKR	1989	1.5×10^{-5}

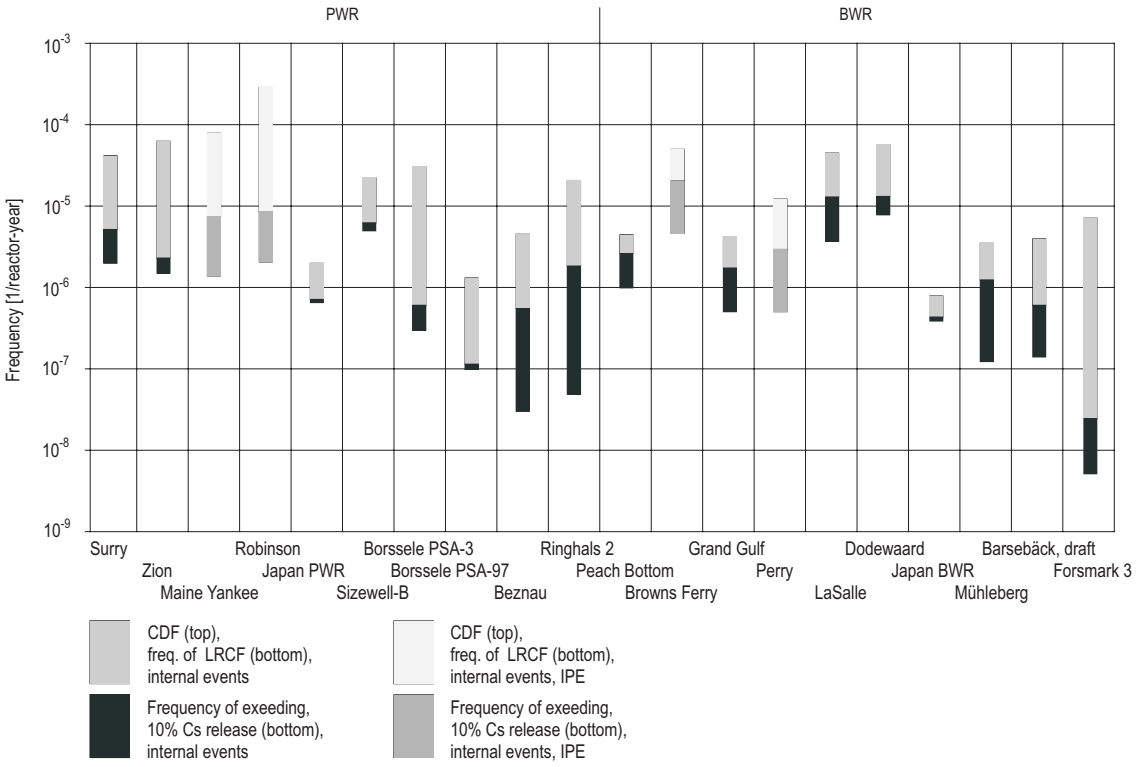


Fig. 2.16. Frequencies of core damage, of large release containment failure and of exceedance of 10 % Cs release, Western PWRs and BWRs (internal events).

2.5.4 Results from Level-1 and -2 PSA from a country perspective

As shown before, the results of PSAs can only be compared with caution, and differences are due to several reasons as the methodology and rules of application have not been fully standardized, even in Western countries. Therefore it is interesting to look at the results of PSAs from the perspective of one country, i.e. Switzerland, or one licensing authority, giving guidance and providing review. As to be seen from Table 4-2, the core damage and large release frequencies finally differ only by a factor of less than 2 and 4, respectively, although the plants differ very much in their original design and in age. The results of PSAs have also been used to harmonize safety levels and to justify plant improvements.

Table 2.8. Frequencies of core damage and large release containment failure, respectively, for Swiss nuclear power plants. SAM denotes Severe Accident Management; large release is defined as greater than 10 % of iodine and/or caesium from the core inventory (for references see Table 2.18).

NPP	Reactor type	Net output [MW]	Operation since	CDF [per reactor-year]	Large release frequency [per reactor-year]
Beznau	PWR	357	3/1972	7.9×10^{-6}	8×10^{-7} (without SAM)
Mühleberg	BWR	355	11/1972	8.2×10^{-6}	3×10^{-7}
Gösgen	PWR	970	11/1979	2.1×10^{-6}	2×10^{-7} (without SAM)
Leibstadt	BWR	1080	12/1984	4.0×10^{-6}	2×10^{-7}

2.5.5 Results from Level-3 PSA

Detailed results are available only from a few full-scope PSAs. Sizewell B (UK) is taken as reference here, as it has proved to be reliable in the public inquiry. In the Sizewell B PSA [82Git] the spectrum of fission product releases was discretized into 12 release categories (see Fig. 2.9 and Table 2.5). RSS methods [75RSS] were used to calculate the release fractions ("first estimate") without benefit of retention of fission products in the reactor coolant system. Such uncertainties and others were addressed by additional, more realistic calculations to examine the sensitivity of the results to data and modeling assumptions, which led to a reduction of the original figures ("second estimate") calculated as probability distributions of release fractions. For instance, in the case of UK-1 (Table 2.5) the probability that the release (except Xe, Kr and I_{org}) will be one half of the first estimate values is judged to be about 60 %, and a release of one tenth or less is calculated to be 15 %. The other release categories are connected with better retention conditions, and the values are close to 5 % and 50 %, respectiverly.

Regarding Level-3-specific issues, the dispersion of the released fission products was treated by the Gaussian model with site-specific parameters, and evacuation and other countermeasures were taken into account as well as the linear dose-risk-relationship and the site-specific population.

The risk of early death to an individual (Fig. 2.17) is estimated at less than 10^{-9} per reactor-year, even for a person living close to the reactor site. As latent effects following an accidental release of radioactive substances have to be considered, the figure includes the individual risk of fatal cancer which is also very low.

The societal risk is expressed as the estimated frequency with which specific numbers of people might be harmed. Figure 2.18a shows the conditional probability distributions (for a given release) of early deaths (UK-1) using first and second estimate release fractions. Figure 2.18b presents the conditional probability distributions (for a given release) of fatal cancers (UK-1) using first and second estimate release fractions. The use of second estimate release fractions results in a decrease in the results. The reductions for fatal cancer are smaller than for early death, because of the assumption that there is no threshold dose for fatal cancer. As may be seen the number of latent fatalities amounts to several ten thousand, nevertheless the risk remains quite small owing to extremely small frequencies. The study demonstrated compliance with the essential design safety criteria of the CEGB [82Kel].

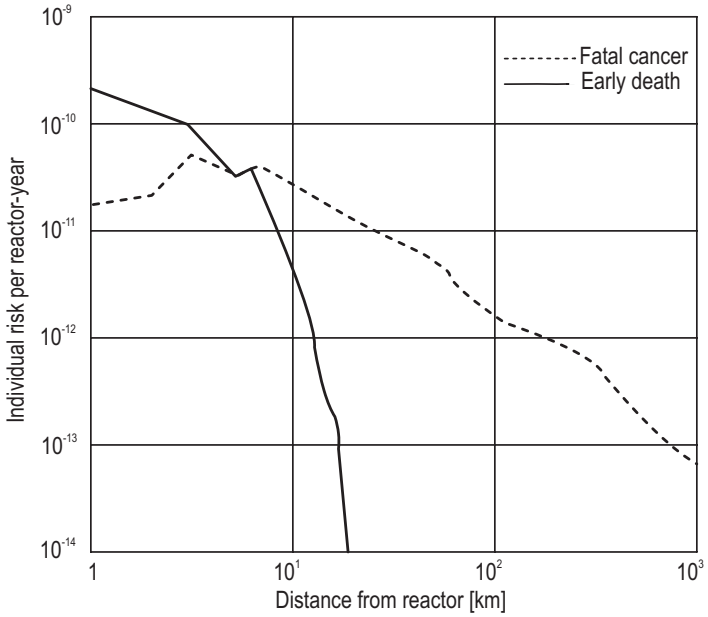


Fig. 2.17. Individual mortality risks from potential degraded core accidents in Sizewell B [82Git].

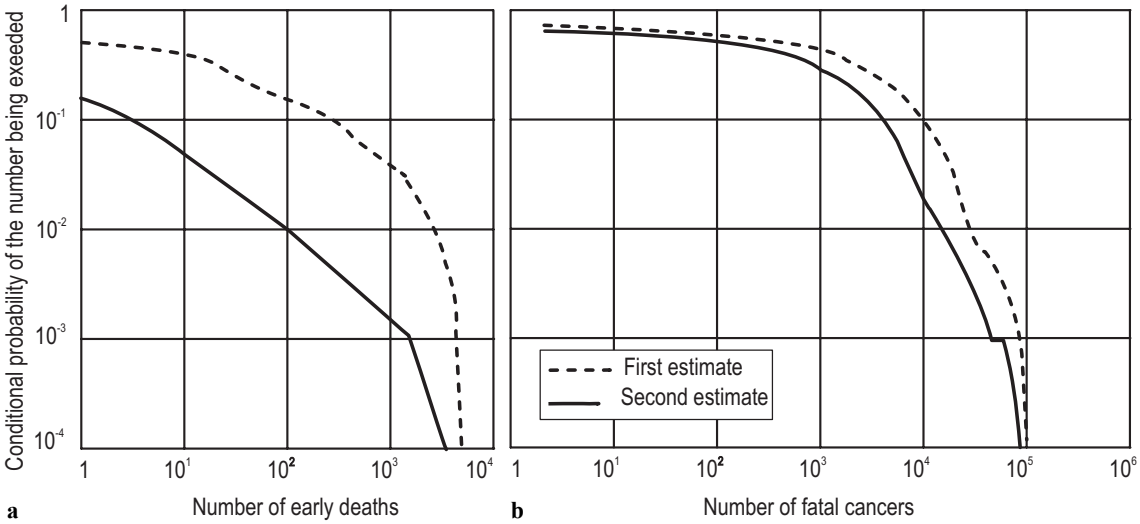


Fig. 2.18. Conditional probability distributions of **(a)** early deaths, and **(b)** fatal cancers using first and second estimate release fractions (UK-1).

Citing some other Level-3 PSAs (NUREG-1150 [90NRC], DRSA [79DRS], Mühleberg [93Caz2]), it can be concluded more generally that

- depending on the severity of the accident sequence, the weather conditions, the efficiency of off-site countermeasures and the population density in the proximity (< 20 km), a few up to a few thousand early fatalities may be expected in case of a severe nuclear accident, though their probability of occurrence is extremely small (< 10^{-7} per reactor-year);
- late effects need to be included which may lead to numbers of victims which may be even higher by more than one order of magnitude depending strongly on the long-distance average conditions and the dose-risk-relationship applied (with or without threshold value). Owing to extremely small probabilities the resulting overall collective risk is in the range of 10^{-3} to 10^{-1} fatalities per reactor-year;
- today's Level-3 PSAs must take additional impacts into account, e.g. contaminated area and temporary land losses, as well as the number of persons affected by emergency measures (Fig. 2.19).

2.6 Approaches and results of risk comparisons of different electricity-producing systems

Comprehensive PSAs carried out for nuclear power plants provide broader information suitable for sound decision making. For instance PSA results form the basis for the comparison of different reactor types or different designs. In order to allow the comparison of completely different energy options or risk sources, the metric including expected damages needs to be normalized. Within the electricity sector this is done by expressing damages per amount of electricity produced (in GWa). With this normalization, comparisons can be put into perspective, not only within the nuclear sector, but also for other competing technologies of electricity production. Furthermore, the benefits of operating such systems can be evaluated.

Risk mostly equates with accidental risk caused by plant operation or in more recent approaches ("from cradle to grave") over the entire supply chain. One should keep in mind that fatality rates in the case of fossil energy carriers are especially small when compared to the corresponding rates associated with the health impacts of normal operation and fuel supply.

While doing this an intrinsic problem hard to overcome is the different nature of the data. While the data derived from predictive PSA studies do reflect the best knowledge about anticipated accidents, the data of most other technologies stem from statistical records or accident databases, respectively. Besides

nuclear, only hydro power systems have a (increasing) tradition of probabilistic assessment of possible accidents. This is due to the fact that the potential adverse affects involved with the use of these technologies can be of an extent that renders "trial-and-error approaches" inadequate.

Both ways of data generation are confronted with the same challenge, the completeness of the data and know-how. Within PSAs one question is whether all relevant initiating events (external and internal) and the subsequent scenarios leading to plant damage states have been included in the analysis and whether the chemical and physical phenomena all the way to potential release of radioactive substances are sufficiently enough understood and modeled. With growing experience in the use of probabilistic methodology, these uncertainties have been reduced to an extent which seems to justify the cautious use of the results of those studies for the purpose of comparison. On the other side, statistical records can fail to cover all energy-related accidents (see Table 2.9). Usually frequency ranges do not go down to the same level of unlikeliness and may not cope with "worst cases" one might identify by use of the theoretical methods like PSA. Moreover statistical data are often compiled from sources of information of different quality. To achieve statistical significance the data samples need to contain a minimum number of events. Data collected over the period of several years or from different geographical areas are often combined. This means that different safety standards as well as general improvements in technology and safety over the years may not be given proper attention. Combining data obtained from different regions can also lead to non-applicable results.

Table 2.9. Experience-based, aggregated severe-accident risk indicators for full energy chains [98Hir]. "Severe accidents" are defined as follows: ≥ 5 fatalities, ≥ 10 injured, ≥ 200 evacuees, ban on consumption of food, ≥ 10 000 t of polluting release of hydrocarbons, ≥ 25 km^2 cleanup of land/water, ≥ 5 MUS$ economic loss.

Energy chain	Number of severe accidents worldwide 1969…1996	Number of immediate fatalities per GW a		
		Worldwide	OECD	Non-OECD
Coal	187	3.4×10^{-1}	1.4×10^{-1}	5.1×10^{-1}
Oil	334	4.2×10^{-1}	3.9×10^{-1}	4.6×10^{-1}
Natural gas	86	8.5×0^{-2}	6.6×10^{-2}	1.1×10^{-1}
Nuclear	1	8.4×10^{-3}	0	5.3×10^{-2}
Hydro	9	8.8×10^{-1}	4.0×10^{-3}	2.2

Owing to the fact that objective state-of-the-art comparisons may only be made using normalized aggregated risks over the entire supply chain, the following results are based on the "cradle to grave" approach.

Figure 2.19 shows a comparison of aggregated, normalized severe accidents that occurred worldwide in the period 1969…1996, distinguishing between OECD (industrialized) and non-OECD countries (less industrialized). The column for the OECD countries in the nuclear section refers to the evacuees due to the accident at TMI/Harrisburg where nobody was hurt, and the columns for the non-OECD countries refer to the accident at Chernobyl.

The fatality numbers presented in Fig. 2.19 for the nuclear sector include both immediate and estimated latent fatalities. This is questionable because on one hand immediate fatalities are caused by deterministic health effects due to high doses of irradiation, while latent effects (cancer) are stochastic in nature and appear after a considerable delay. On the other hand the possibility that latent fatalities can be preceded by a history of chronic illness that clearly reduces the quality of life for those affected is not included.

The curves (Fig. 2.20) for fossil and hydro chains, respectively, are based on historical accidents worldwide in the period 1969…1996 and show immediate fatalities only. For the nuclear chain the immediate fatalities experienced are represented by one point (Chernobyl) and delayed fatalities by a range of values for the same accident. The results for nuclear power originate from a plant-specific PSA [93Caz2] and reflect estimated latent fatalities. This estimation of latent fatalities is based on the use of a linear dose-response-function without threshold.

The variety of possible damages from energy-related accidents also includes environmental effects and infrastructure losses. Within the nuclear PSAs the potential adverse effects can be expressed by a number of damage indicators. One possibility for the aggregation of diverse indicators consists of their monetization and subsequent summation. The methodology for this needs further development.

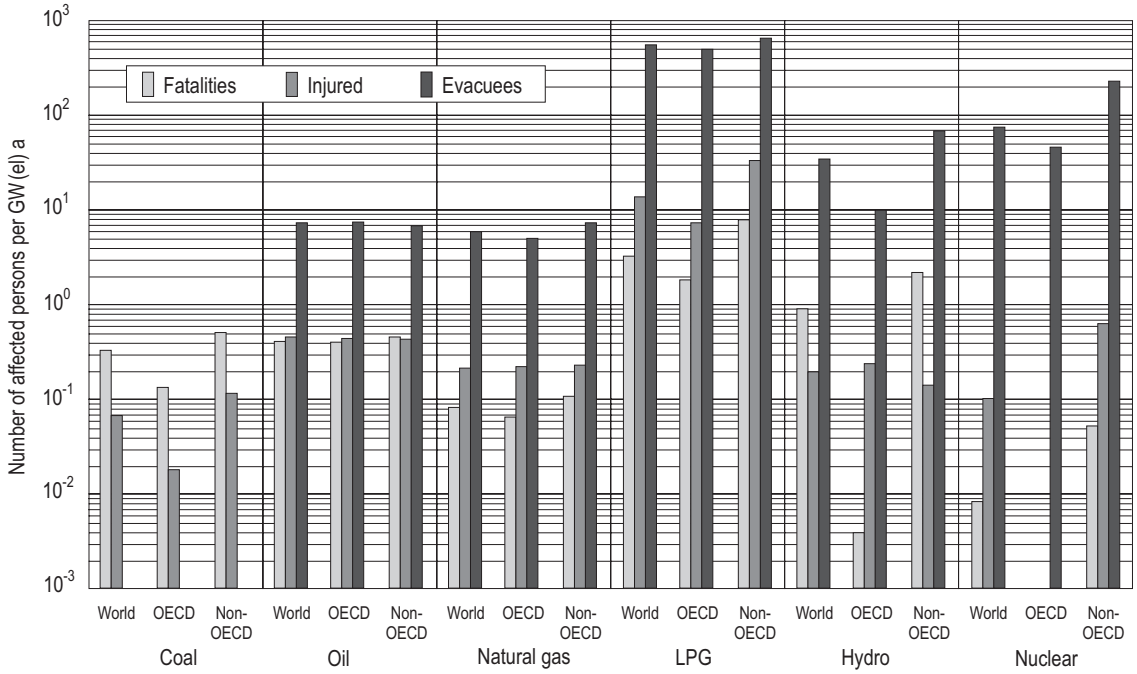


Fig. 2.19. Comparison of aggregated, normalized, energy-related damage rates for severe accidents worldwide, 1969…1996 (affected persons per unit of energy were estimated based on the partial reallocation of damages to OECD countries taking into account imports of fossil energy carriers from non-OECD countries) [98Hir].

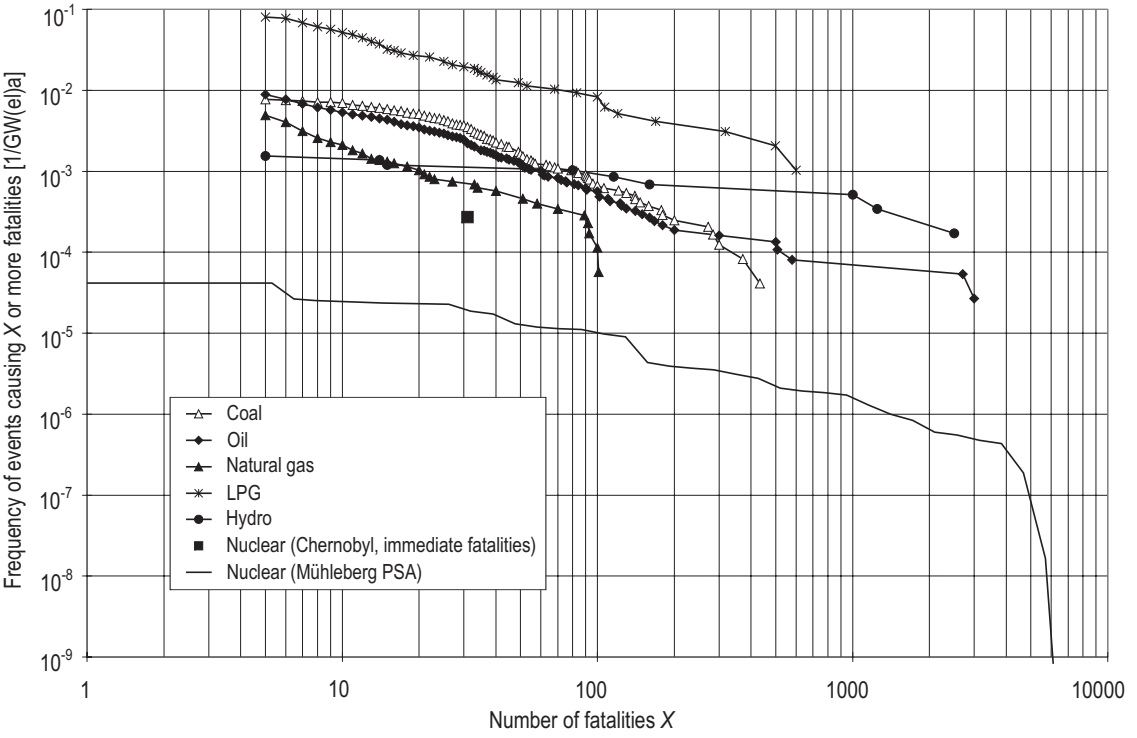


Fig. 2.20. Frequency-consequence diagram for full energy chains worldwide [98Hir].

2.7 Outlook

The method of PSA has attained a high level of maturity and has developed into a reliable instrument for the modeling of plant behavior and event sequences in the field of nuclear technology. It allows the identification and changes of weaknesses in the design of a plant and makes possible a full evaluation of the balance of the safety concept applied.[6]

In most countries, the application of PSAs concentrates on the so-called Level 1, which refers to the frequency of undesired core damage states as the main result or as a risk substitute. The novel focus of analyses for existing reactors lies on the non-full power states and on the completion of the spectrum of (external) initiating events. The tendency towards a "risk-informed regulation" [00NRC] and more cost effective safety measures has resulted in new impulses. The consequent application of this methodology for reactors of Russian design has greatly enlarged the field of application and will continue to do so in future.

PSA methodology has been standardized to a large extent, and guidelines have been or will be fixed.[7] The greatest methodological deficits still lie in the field of adequate assessment of human behavior. Further possibilities for development can be identified in the study and taking into account errors of commission. The increase in the quality of data by use of operating experience and the reduction of uncertainties such as dependencies which have been overlooked or which have been underestimated present further areas for development.

In view of the differences between analyses, a warning against generalizations and uncritical comparisons has been and must still be expressed [90SIA]. This is increasingly true for Level-2 and in particular for Level-3 PSAs, which are carried out far less frequently and where experience is therefore still sparse. This may change and should be changed in the future, especially if

- the tendency towards quantitative safety objectives or goals and risk-informed concepts gains ground (new designs must today be measured against frequency targets for core damage (CDF) and the large early release frequency (LERF); in some countries quantitative health objectives have already been defined, e.g. by US NRC); and if
- risk as one of many indicators of sustainable development becomes part of future decision-making processes in the energy domain.

In this context impulses towards a considerable need for development becomes apparent. The analyses must not only increase in quality, they must also become more transparent and comprehensible. The inclusion of potential failures in digital instrumentation and control as well as potential plant aging effects are major methodological challenges in PSA.

The potential of PSA for system analysis and optimization can have a growing influence in the development of novel reactor concepts. The PSA methodology described in the preceding text is strongly oriented towards the design, safety concepts and accident topology of LWRs. One typical example may be seen in the treatment of loss-of-coolant accidents and the respective classification of causative leaks, as well as in the complex modeling of the technical systems needed to control such events. In plant designs which differ widely from that of LWRs, improved or even new methods as well as a different disposition of PSA may become imperative:

- Small, modular, gas-cooled high-temperature reactors (HTR) are, for example, constructed with a view to inherent safety features so that the after-heat can be passed on to the core structure (graphite) and to external heat-sinks without ensuing any safety problem [97IAE]. This however requires tailored definitions which include respective success criteria, especially in those cases where the plant-safety is measured against results of Level 1 PSAs for LWRs. In addition the design features of such a plant lead to the fact that accidents progress relatively slowly which gives more time for countermeasures to be taken. Convincing methods of assessment for the process of diagnosis and decision-finding by the operators are thus essential.

[6]) See also ILK Recommendation on the Use of Probabilistic Safety Assessments in Nuclear Licensing and Supervision Processes, May 2001, ILK-04.

[7]) A full set of PSA standards will be available for the US in 2008.

– To enable accidents with large release of fission products, the natural dissipation of afterheat must be considerably impaired. Plausible scenarios require the failure of all passive safety systems. Special challenges for probabilistic methods can be foreseen in this field.

The basic PSA methodology is already being applied today in many fields outside that of nuclear technology (e.g. in the chemical processing industries, for the transport of dangerous goods and for complex building structures. On close examination there appear widely differing concepts and degrees in the treatment of details [96Lee]. The regulatory regimes also vary to a high degree. Problems result from completely different initial plant conditions (e.g. non-stationary conditions with chemical batch-processes), which demand adapted and often completely divergent approaches to the solution of problems. In addition, "the non-uniformity in methods, data and application significantly hampers the widespread use of risk assessment for decision-making purposes" [00Kir]. Or, to put it differently: In addition further development in certain individual sectors, a harmonization of methods and data technologies which exceeds the boundaries of a single technology is required.

2.8 Appendix

2.8.1 Appendix for 2.4

Table 2.10. Major features of the PCA codes participating in the OECD/NEA-CEC code comparison exercise [94NEA].

Country		Finland	UK	Germany	Sweden	USA	Japan
PCA code		ARANO	CONDOR	COSYMA	LENA	MACCS	OSCAR
Atmospheric dispersion	Gaussian plume	+	+	+	+	+	–
	Trajectory	–	–	+	–	–	+
	Time variant	–	+	+	+	+	+
Deposition	Dry	+	+	+	+	+	+
	Wet	+	+	+	+	+	+
Meteorological sampling	Stratified	–	+	+	+	+	+
	Other	+	+	+	–	+	+
Exposure pathways	Cloud-shine	+	+	+	+	+	+
	Ground-shine	+	+	+	+	+	+
	Skin	–	+	+	–	+	–
	Inhalation	+	+	+	+	+	+
	Resuspension	–	+	+	–	+	+
	Ingestion	+	+	+	+	+	+
Counter-measures	Sheltering	+	+	+	+	+	+
	Thyroid blocking	+	+	+	–	–	–
	Evacuation	+	+	+	+	+	+
	Relocation	+	+	+	+	+	+
	Foodbans	+	+	+	+	+	+
Health effects	Early	+	+	+	–	+	+
	Late	+	+	+	+	+	+
Economic consequences		+	+	+	–	+	–

Table 2.11. Inventory appropriate for a PWR with $P_{el} = 1250$ MW [94NEA]. Based on [90NRC], taken from probabilistic accident-assessment codes.

No	Nuclide	Inventory [Bq]	No	Nuclide	Inventory [Bq]	No	Nuclide	Inventory [Bq]
1	Co-58	3.08×10^{16}	19	Ru-105	3.51×10^{18}	37	Cs-134	3.85×10^{17}
2	Co-60	1.14×10^{16}	20	Rh-105	3.18×10^{18}	38	Cs-136	1.33×10^{17}
3	Kr-85	2.17×10^{16}	21	Ru-106	1.30×10^{18}	39	Cs-137	2.29×10^{17}
4	Kr-85m	9.25×10^{17}	22	Sb-127	2.93×10^{17}	40	Ba-140	6.14×10^{18}
5	Kr-87	1.70×10^{18}	23	Sb-129	9.95×10^{17}	41	La-140	6.32×10^{18}
6	Kr-88	2.34×10^{18}	24	Te-127	2.85×10^{17}	42	Ce-141	5.92×10^{18}
7	Rb-86	7.96×10^{15}	25	Te-127m	4.37×10^{16}	43	Ce-143	5.44×10^{18}
8	Sr-89	3.37×10^{18}	26	Te-129	9.40×10^{17}	44	Ce-144	3.59×10^{18}
9	Sr-90	1.75×10^{17}	27	Te-129m	1.67×10^{17}	45	Pr-143	5.40×10^{18}
10	Sr-91	4.37×10^{18}	28	Te-131m	3.47×10^{17}	46	Nd-147	2.36×10^{18}
11	Y-90	1.82×10^{17}	29	Te-132	4.85×10^{18}	47	Np-239	7.32×10^{19}
12	Y-91	4.51×10^{18}	30	I-131	3.39×10^{18}	48	Pu-238	3.17×10^{15}
13	Zr-95	5.88×10^{18}	31	I-132	4.96×10^{18}	49	Pu-239	1.11×10^{15}
14	Nb-95	5.81×10^{18}	32	I-133	6.81×10^{18}	50	Pu-240	1.06×10^{15}
15	Zr-97	5.88×10^{18}	33	I-134	7.84×10^{18}	51	Pu-241	3.21×10^{17}
16	Mo-99	6.44×10^{18}	34	I-135	6.40×10^{18}	52	Am-241	2.06×10^{14}
17	Te-99m	5.55×10^{18}	35	Xe-133	6.85×10^{18}	53	Cm-242	6.62×10^{16}
18	Ru-103	5.25×10^{18}	36	Xe-135	1.67×10^{18}	54	Cm-244	2.75×10^{15}

Table 2.12. Examples of different source terms [94NEA]. Please refer to the original literature.

Source term		QT1		QT2	QT3	QT4			QT5
Time before release [h]		2.0	3.0	2.0	2.0	2.0	3.0	5.0	2.0
Duration of release [h]		1.0	5.0	1.0	1.0	1.0	1.0	1.0	24.0
Rate of release [MW]		2.0	0.2	0	0	0	0	0	0
Release height [m]		10	10	10	10	10	10	10	10
Warning time [h]		1.0	–	1.0	1.0	1.0	–	–	1.0
Release fraction	Xe-Kr	1.0	–	1.0	0.1	1.0	–	–	1.0
	I_{org}	0.001	–	0.001	0.00001	0.00033	0.00033	0.00033	0.001
	I	0.1	–	0.1	0.001	0.033	0.033	0.033	0.1
	Cs-Rb	0.1	–	0.1	0.001	0.033	0.033	0.033	0.1
	Te-Sb	0.05	0.05	0.1	0.001	0.033	0.033	0.033	0.1
	Ba-Sr, Ru	0	0.01	0.01	0.0001	0.0033	0.0033	0.0033	0.01
	La	0	0.001	0.001	0.00001	0.00033	0.00033	0.00033	0.001

2.8.2 Appendix for 2.5

Table 2.13. PWR: Relative contributions (in %) of important initiating event classes (internal events) to the core damage frequency.

Plant	Loss of off-site power	ATWS [c])	Transients	Loss of coolant inside containment	Containment bypass (SGTR [d]), V-Sequence [e]))	Total CDF
Surry	69	3.3	4.2	15	8.5	4.0×10^{-5}
Sequoyah	24 .7	3.7	4.2	63	4 .4	5.7×10^{-5}
REP 900 [a])	< 1	8.6	22	29	4.8	3.4×10^{-5}
[b])	< 1	–	11.5	17	< 1	1.7×10^{-5}
REP 1300 [a])	< 1	11	13	14	4.3	4.7×10^{-6}
[b])	< 1	–	7	49	–	6.1×10^{-6}
Biblis B	1.1	1.7	7	84.5	5	2.9×10^{-6}
Japanese PWR	4	< 1	7	82	5	1.6×10^{-7}
Ringhals 3/4	6 .6	–	17.5	62	12	2.0×10^{-5}
Beznau	7.2	5.8	27	33	27	4.4×10^{-6}

[a]) Power generation.
[b]) Shutdown and low power states.
[c]) Anticipated Transient Without Scram.
[d]) Steam Generator Tube Rupture.
[e]) Interfacing systems LOCA.

Table 2.14. BWR: Relative contributions (in %) of important initiating event classes (internal events) to the core damage frequency.

Plant	Loss of off-site power	ATWS [b])	Transients	Loss of coolant	Under high pressure	Total CDF
Peach Bottom	49	4	5	5	65	4.5×10^{-6}
Grand Gulf	97.5	2.5	–	–	97	4.0×10^{-6}
Forsmark 1/2	2.6	4.4	84	13	80	1.1×10^{-5}
Grundremmingen [a])	6.4	2.0	89.8	1.6	46	5.0×10^{-5}
Japan, $P_{el} = 1100$ MW	28	14.7 [c])	68.7	3.3	–	2.0×10^{-6}
Mühleberg	16	26	49	12	39	3.5×10^{-6}

[a]) Only hazard states.
[b]) Anticipated Transient Without Scram.
[c]) Included in transients.

Table 2.15. PWR: Conditional probabilities of containment failure modes, given core damage state, and dominant phenomena and their relative contributions; exceedance frequencies of significant (1 %) and large (10 %) Cs releases, dominant phenomena for large release. Abbreviations used: n.a.: not analyzed; BMT: Basemat Melt-Through; DCH: Direct Containment Heating; ECF: Early Containment Failure; ISF: Isolation Failure; RPV: Reactor Pressure Vessel; V-Seq: Interfacing Systems LOCA.

Plant	Total CDF	Containment failure mode						Exceedance frequency [1/a]	
		Early containment failure	Late containment failure	Containment bypass	Isolation failure	Successful containment venting	Containment intact	for 1 % Cs release	for 10 % Cs release
Surry	4.0×10^{-5}, 3 % at high pressure	0.007, DCH > 90 %	0.06, BMT	0.12, SGTR ≈ 60 %	–		0.81, RPV intact 57 %	6×10^{-6}	2×10^{-6}, SGTR > 90 %
Zion	6.5×10^{-5}, 2 % at high pressure	0.005, DCH > 90 %	0.24, BMT	0.02, SGTR ≈ 90 %	–		0.73	5.5×10^{-6}	1×10^{-6}, SGTR ≈ 30 %, DCH ≈ 70 %
Maine Yankee	7.4×10^{-5}, 16 % at high pressure	0.08, H_2 burn ≈ 70 %, DCH ≈ 30 %	0.47, overpressure	0.02, SGTR ≈ 70 %	–		0.43, RPV intact 30 %	4.4×10^{-6}	1.4×10^{-6}, SGTR ≈ 20 %, H_2 burn ≈ 80 %
Robinson	2.4×10^{-4}, 22 % at high pressure	0.016, DCH > 90 %	0.07, overpressure	0.02, SGTR ≈ 70 %	0.13		0.77	2×10^{-5}	2×10^{-6}, SGTR ≈ 50 %, DCH ≈ 50 %
Beznau	4.4×10^{-6}, < 10 % at high pressure	0.016, DCH > 80 %	0.19, incl. vent failure due to H_2 burn: ≈ 22 %, lower after modification of vent line	0.11, SGTR > 90 %		0.54	0.15	1.2×10^{-7}	3×10^{-8}, SGTR ≈ 45 %, DCH ≈ 55 %

(continued)

Table 2.15 continued.

Plant	Total CDF	Containment failure mode						Exceedance frequency [1/a]	
		Early containment failure	Late containment failure	Containment bypass	Isolation failure	Successful containment venting	Containment intact	for 1 % Cs release	for 10 % Cs release
Biblis B	2.9×10^{-6} 9 % at high pressure	n.a.	n.a.	< 0.04, V-Seq. < 80 % (conservative estimate), SGTR ≈ 20 %				$< 10^{-8}$, PB/F with scrubbing in SG; $> 10^{-8}$ otherwise (only SGTR)	$<< 10^{-8,}$ with scrubbing in SG; $> 10^{-8}$ otherwise (only SGTR)
Sizewell B (conservative)	2.2×10^{-5}	< 0.01	0.19, overpressure	0.09, SGTR ≈ 92 %	< 0.01	–	0.71	8×10^{-6}	5×10^{-6} late overpressurization 80 %
Ringhals 2	2.0×10^{-5}, 12 % at high pressure	> 0.01	0.11, BMT > 95 %	0.08, SGTR > 90 %	< 0.01	0.3	0.5	2×10^{-7} ECF ≈ 50 % ISF ≈ 50 %	5×10^{-8}, ECF > 90 %
Borssele PSA-3	3.6×10^{-5}	< 0.01	0.07	0.01, V-Seq. 50 % SGTR 15 %	< 0.01	0.65	0.26	8×10^{-7}	3×10^{-7}, V-Seq. 70 %
Borssele PSA-97	1.7×10^{-6}	0.01	0.05	0.05, SGTR 60 %, V-Seq. 40 %	< 0.01	0.72	0.21	1.5×10^{-7}	10^{-7}, V-Seq. 70 %, ISF 15 %
Japanese PWR P_d=1100MW	1.9×10^{-6} 18 % at high pressure	0.01, DCH 50 %, H_2 burn 40 %	0.08	0.34, SGTR 80 %	< 0.01	–	0.56	7.4×10^{-7}	6.9×10^{-7}

Table 2.16. BWR: Conditional probabilities of containment failure modes, given core damage state, and dominant phenomena and their relative contributions; exceedance frequencies of significant (1 %) and large (10 %) Cs releases, dominant phenomena for large release. Abbreviations used: n.av.: not available; CC: Core-Concrete-Interaction; DCH: Direct Containment Heating; ECF: Early Containment Failure; ISF: Isolation Failure; RPV: Reactor Pressure Vessel; V-Seq: Interfacing Systems LOCA.

Plant	Total CDF	Containment failure mode						Exceedance frequency [1/a]	
		Early containment failure	Containment bypass	Early containment drywell failure without suppression pool bypass	Late containment failure	Containment venting	Containment intact	for 1 % Cs release	for 10 % Cs release
Peach Bottom	4.3×10^{-6}	0.56, liner failure ≈ 60 %, DCH ≈ 5 %			0.05, overpressure > 90 %	0.11	0.27, RPV intact ≈ 40 %	2×10^{-6}	1.3×10^{-6}, liner failure
Browns Ferry	4.8×10^{-5}	0.46, liner failure ≈ 60 %, overpressure ≈ 8 %			0.26		0.28, RPV intact ≈ 90 %	1.2×10^{-5}	5×10^{-6}, liner failure
Grand Gulf	4.1×10^{-6}	0.21, H_2 burn ≈ 75 %		0.22, overpressure 90 %	0.28	0.04	0.23, RPV intact ≈ 75 %	1.5×10^{-6}	5×10^{-7}, hydrogen burn
Perry	1.2×10^{-5}	0.16, H_2 burn > 90 %		0.07, overpressure > 90 %	0.07	0.31	0.39, RPV intact 70 %	4×10^{-6}	5×10^{-7}, hydrogen burn
Mühleberg	3.5×10^{-6}	0.26, overpressure			0.07, overpressure	0.66		3.3×10^{-7}	1.2×10^{-7} early overpressure failure

(continued)

Table 2.16 continued.

Plant	Total CDF	Containment failure mode						Exceedance frequency [1/a]	
		Early containment failure	Containment bypass	Early containment drywell failure without suppression pool bypass	Late containment failure	Containment venting	Containment intact	for 1 % Cs release	for 10 % Cs release
LaSalle	4.4×10^{-5}	0.33, overpressure, CCI			0.1	0.46	0.11	1.4×10^{-5}	3.6×10^{-6}, overpressure, CCI
Barsebäck 1/2 (draft)	3.9×10^{-6}	0.1 CCI, 40 % reactor overpressure, impact of vessel head failure 40 %	0.05, isol. fail. of main steam line with reactor at high press. > 90 %		< 0.01	0.84		5.4×10^{-7}	1.4×10^{-7}, steam line isolation failure, CCI, impact of vessel head failure
Forsmark 3	7.2×10^{-6}	2×10^{-3}	5×10^{-4}		8×10^{-5}	0.5	0.48	2.7×10^{-8}	5×10^{-9}, containment bypass
Dodewaard	5.5×10^{-5}	0.25, overpressure 95 %, ex-vessel steam explosion 2.5 %			0.36, CCI or liner attack 90 %, thermal drywell failure 3 %		0.38	n.av.	n.av.
Japanese BWR $P_{el} = 1100$ MW	7.6×10^{-7}	0.51, overpressure failure before core melt 70 %	0.03, V-Seq.		0.29, overpressure > 40 %		0.16	6.5×10^{-7}	4.2×10^{-7}

Table 2.17. References for Eastern country PSA studies.

WWER 440 (P_{el} ≈ 400 MW)/230	
NPP	Reference
Bohunice V1	REKOV1/000/BS/9730/RELK/ZK, April 2000
Kola 1, 2	Choutov, V., Pytkin, Y.: Kola NPP, 2000
Kozloduy 3, 4	
Novovoronezh 3	
WWER 440/213	
NPP	Reference
Bohunice V2	Report RELKO 1R0195, September 1995
Dukovany 1	Assessment of the Living PSA 2000 Results, Report NRI Rez, December 2000 (in Czech)
Loviisa	
Paks 1, 3	
Paks 2	
Rovno 1	
Mochovce	Report VUJE and RELKO EMO PSA/POST''/8, October 1999
WWER 1000 (P_{el} ≈ 950 MW)	
NPP	Reference
Balakovo	
Kozloduy 5, 6	
Novovoronezh	
Temelin 1, 2	PSA for Temelin NPP Unit 1, Interim Summary Report, April 1996 (prepared by Temelin Project Team)
Zoporozje 5	Performed by Moscow AtomEnergoProject (AEP)

Table 2.18. References for Swiss PSA studies.

PWR	
NPP	Reference
Beznau	Beznau Unit – Fullpower Probabilistic Risk Assessment (BERA), NOK, KKB 511 D 127, December 1999
Gösgen	Gösgen Probabilistic Safety Assessment, PLG-0870, February 1994
BWR	
NPP	Reference
Mühleberg	MUSA – Mühleberg Safety Assessment, BKW, PLG-0751, update 1, February 1993
Leibstadt	KKW Leibstadt AG, Living Probabilistic Safety Assessment, EWE-2889, RMA-033, December 1997

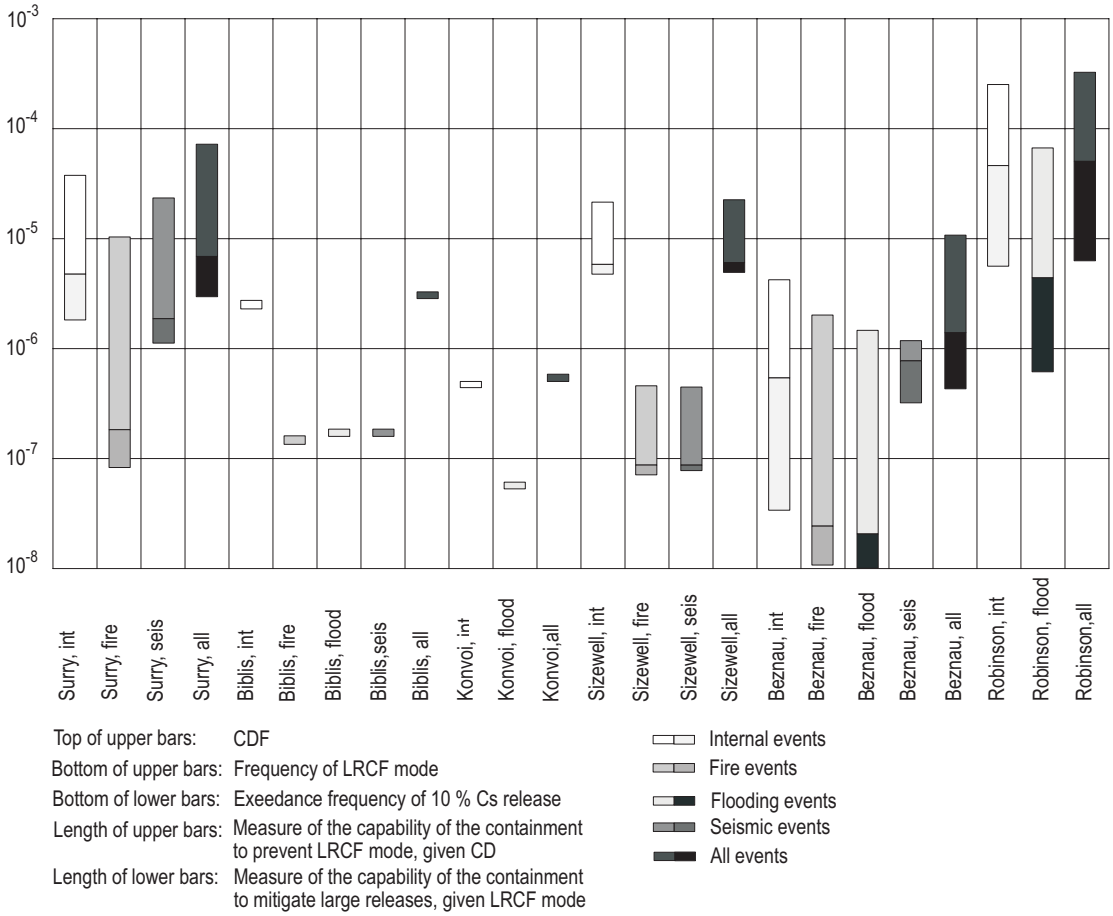


Fig. 2.21. Frequencies of core damage, large release containment failure (LRCF) mode and exceedance of 10 % Cs release for internal, fire, flooding, seismic and all events at PWR plants (for Biblis and Konvoi, Level-2 results are not available).

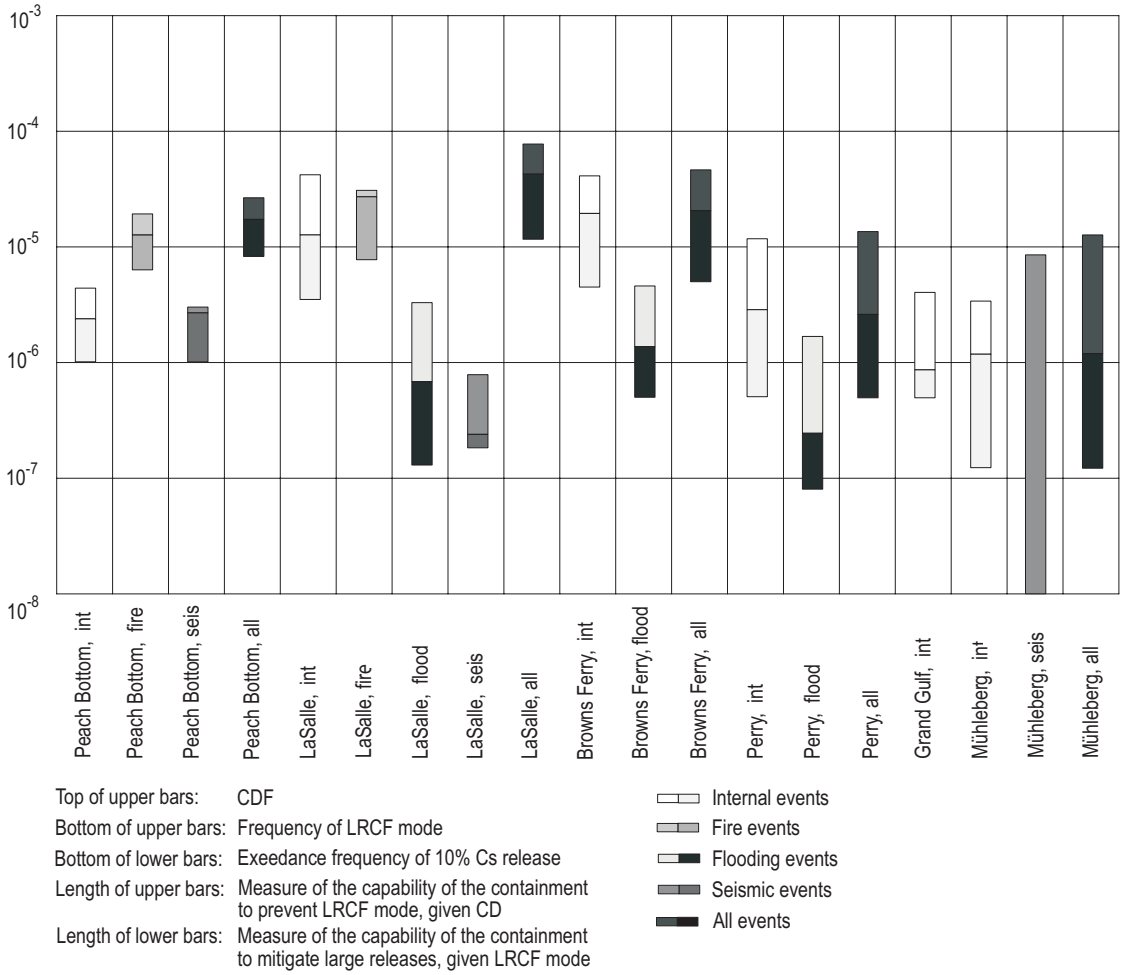


Fig. 2.22. Frequencies of core damage, large release containment failure (LRCF) mode and exceedance of 10 % Cs release for internal, fire, flooding, seismic and all events at BWR plants.

2.9 References for 2

33Kol Kolmogorov, A.N.: Grundbegriffe der Wahrscheinlichkeitsrechnung, in: Ergebnisse der Mathematik, Vol. 2, No. 3, Springer-Verlag, Berlin (1933).

75RSS Reactor Safety Study – an assessment of accident risks in US commercial nuclear power plants., WASH-1400 (NUREG-75/014) (1975).

79DRS Deutsche Risikostudie Kernkraftwerke – Phase A GRS, Verlag TÜV Rheinland, Köln (1979).

82Git Gittus, J.: CEGB Proof of Evidence on Degraded Core Analysis Sizewell B Power Station Public Enquiry, CEGB P 16, London (1982).

82Kel Kelly, G.N. et al.: Degraded core accidents for the Sizewell PWR: A sensitivity analysis of the radiological consequences, NRPB-R 142 (1982).

82Mar Martz, H.F., Waller, R.A.: Bayesian Reliability Analysis, John Wiley & Sons, New York (1982).

83Sea Seavers, D.A. et al.: Procedures for Using Expert Judgement to Estimate Human Error Probabilities in Nuclear Power Plants Operation,. NUREG/CR-2743 (1983).

83Swa Swain, A.D., Guttmann, H.E.: Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report, NUREG/CR-1278, Washington, DC (1983).
84Han Hannaman G.W. et al.: Human Reliability Model for PRA Analysis, NUS-4531, EPRI Project RP2170-3, San Diego (1984).
84Mos Mosleh, A., Apostolakis, G.: Models for the Use of Expert Opinion, Low Probability High Consequence Analysis, Ed. by R.A. Walla and V.T. Cove, Plenum Press, NY (1984).
84SHA Systematic Human Action Reliability Procedure (SHARP), EPRI-NP-3583 (1984).
86Emb Embrey, D.E. et al.: SLIM-MAUD: An Approach to Assessing Human Error Probabilities Using Structured Expert Judgement, NUREG/CR-3518 (1983).
87CEC Commission of the European Communities Ispra Research Centre, Common Cause Failures Reliability Benchmark Exercise, EUR-11054-EN, Ispra (1987).
87Mos Mosleh, V. et al.: Methods for the Elicitation and Use of Expert Opinion in Risk Assessment. NUREG/CR-4692, PLG-0533 (1987).
87Swa Swain, A.D.: Accident Sequence Evaluation Program Human Reliability Analysis Procedure, NUREG/CR-4772, Washington, DC (1987).
88NRC Nuclear Regulatory Commission, Procedures for treating Common Cause Failures in Safety and Reliability Studies, Vol. 1, NUREG/CR-4780, Washington, DC (1988).
88Wil Williams J.C.: A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance. Proceedings of the IEEE 4th Conference on Human Factors in Power Plants, Monterey, Institute of Electronic and Electrical Engineers, New York (1988).
89Hor Hora, S.C., Iman, R.L.: Expert Opinion in Risk Analysis: The NUREG-1150 Methodology, Nuclear Science and Engineering, Vol. 102 (1989).
89IAE1 Computer Codes for Level 1 Probabilistic Safety Assessment, TECDOC-553, IAEA, Vienna (1989).
89IAE2 Models and Data Requirement for Human Reliability Analysis, TECDOC-499, IAEA, Vienna (1989).
90DRS Deutsche Risikostudie Kernkraftwerke – Phase B, GRS, Köln (1990).
90EPR Advanced Light Water Reactor Utility Requirements Document, Vol. 1, EPRI, Palo Alto (1990).
90EPS Probabilistic Safety Assessment of Reactor Unit 3 in the Paluel Nuclear Power Centre (1300 MW), Overall Report, Electricité de France (1990).
90IAE Procedures for Conducting Independent Peer Reviews of Probabilistic Safety Assessment, Guidelines for the International Peer Review Service (IPERS) Programme, TECDOC-543, IAEA, Vienna (1990).
90ICR ICRP, Recommendations for the International Commission on Radiological Protection, Oxford, New York (1990).
90NRC Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants. Final Summary Report. Report NUREG-1150, U.S. NRC, Washington D.C., USA (1990).
90SIA Kröger, W., Chakraborty, S.: Risikobestimmung – Eine Bestandesaufnahme der Methodik für Kernkraftwerke, Schweizer Ingenieur und Architekt **37** (1990).
91Coo Cooke, R.M.: Experts in Uncertainty – Opinion and Subjective Probability in Science, Oxford University Press, New York (1991).
91Hau Hauptmanns, U., Werner, W.: Engineering Risks, Springer-Verlag (1991).
91Sum Summers, R.M. et al.: MELCOR 1.8.0: A Computer Code for Nuclear Reactor Severe Accident Source Term and Risk Assessment Analyses, NUREG/CR-5531, SAND90-0363 (1991).
92Ger Gertmaan, D.I. et al.: INTENT: A Method for Estimating Human Error Probabilities for Decision Based Errors, Reliability Engineering & System Safety **35** (1992).
92IAE IAEA, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1), Safety Series 50-P-4, Vienna, 1992.
92Sac Sachs L.: Angewandte Statistik (7. Auflage), Springer-Verlag, Berlin (1992) 194.

93Caz1 Cazzoli, E. et al.: Approach to Quantification of Uncertainties in Probabilistic Safety Assessment, Proceedings of PSA'93, Clearwater Beach (1993).
93Caz2 Cazzoli, E. et al.: A Regulatory Evaluation of the Mühleberg Probabilistic Safety Assessment, Volume II: Level 2, ERI/HSK 93-304, HSK 11/356 (Limited Distribution) (1993).
94EUR European Utility Requirements for LWR Nuclear Power Plants, Vol. 1, EUR (1994).
94NEA Probabilistic Accident Consequence Assessment Codes Second International Comparison. Overview Report, NEA/OECD, Paris (1994).
94Rus Russell, K.D. et al.: System Analysis Program for Hands-on Integration Reliability Evaluation (SAPHIRE) Version 5, NUREG/CR-6116, Vol. 1-10 (1994).
95Hir Hirschberg, S., Mock, R.: Overview of the Fundamentals and Methodology of Probabilistic Safety Assessment, SVA-Vertiefungskurs "Sicherheit von Kerkraftwerken im Stillstand", Schweizerische Vereinigung für Atomenergie (SVA),Winterthur (1995).
95IAE1 Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 2). Safety Series 50-P-8, IAEA, Vienna (1995).
95IAE2 PSAPACK 42, Computer Manual Series 6, IAEA, Vienna (1995).
95Wer Werner, W.F. et al.: Results and Insights from Level-1 Probabilistic Safety Assessments for NPPs in France, Germany, Japan, Sweden, Switzerland and the United States, Reliability Engineering and System Safety 48 (1995).
96ATH A Technique for Human Error Analysis (ATHEANA). NUREG/CR-6350, BNL-NUREG-52467 (1996).
96IAE Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), Safety Series 50-P-12, IAEA, Vienna (1996).
96Lee Lees, F.P.: Loss in the Process Industries, Sec. Ed., Butterworth-Heinemann (1996).
97BfS Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke (Guidelines). Facharbeitskreis Probabilistische Sicherheitsanalyse, BfS-16/97 (1997).
97IAE Technical Committee Meeting on High Temperature Gas Cooled Reactor Technology Development, Johannesburg (South Africa), Nov 13-15, 1996, TECDOC-988, IAEA, Vienna (1997).
97NEA Results and Insights from Level-2 PSAs Performed in Germany, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States, NEA/CSNI/R(97)18, Paris (1997).
97NRC Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance, US-NRC, NUREG-1560 Vol. 1 and 2, Washington, DC (1997).
98BGB Atomgesetz vom 23.12.1959, in der Fassung der Bekanntmachung vom 15.7.1985, zuletzt geändert am 6.4.1998 (BGBl. I p. 694).
98Bel Belles, R.J. et al.: Precursors to Potential Severe Core Damage Accidents: 1997, Oak Ridge National Laboratory, NUREG/CR-4674, ORNL/NOAC-232, Vol. 26 (November 1998).
98Hir Hirschberg S., Spiekerman G. and Dones R.: Severe Accidents in the Energy Sector, first edition, Project GaBE: Comprehensive Assessment of Energy Systems, PSI Bericht Nr. 98-16, ISSN 1019-0643 (1998).
98IAE IAEA/NEA Incident Reporting System (IRS) Reporting Guidelines, IAEA/NEA-IRS (1998).
98NEA Critical Operator Actions: Human Reliability Modeling and Data Issues, Final Task Report, NEA/CSNI/R(98)1.
98Rel RiskSpectrum, Relcon AB, Sweden (1998).
99Coj Cojazzi, G.: Benchmark Exercise on Expert Judgement Techniques in PSA Level 2, Final Summary Report, JRC Ispra (1999).
99Ful Fullwood, R.: Probabilistic Safety Assessment in the Chemical and Nuclear Industries, Butterworth-Heinemann (1999).
99IAE1 INSAG-12: Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, IAEA, Vienna (1999).
99IAE2 INSAG-13: Management of Operational Safety in Nuclear Power Plants, INSAG Series No. 13, IAEA, Vienna (1999).

99IAE3 Measures to strengthen international co-operation in nuclear, radiation and waste safety, Report on the General Conference, GC(43)INF/8 (1999).
99NEA ICDE Project Report on Collection and Analysis of Common-Cause Failures of Centrifugal Pumps, NEA/CSNI/R(99)2 (1999).
00ATH Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA), NUREG-1624, Rev. 1 (2000).
00Kir Kirchsteiger, C., Cojazzi, G.: Promotion of Technical Harmonisation on Risk-Based Decision Making, Summary Paper, EC/JRC Joint Workshop, Stresa and ISPRA (May 2000).
00NRC Framework for Risk-Informed Regulations, Draft for Public Comment, Rev. 1.0 (February 10, 2000).